PHD IN SECURITY & RISK MANAGEMENT

A Study of Cyber Security Management within South Korean Businesses – An examination of risk and cybercrime involving industrial security

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth.

By

JEYONG JUNG

July 2018

Institute of Criminal Justice Studies

Faculty of Humanities and Social Sciences

ABSTRACT

This study aims to empirically explore and evaluate the current state of cyber security management for small and medium-sized businesses in South Korea. As academic discourse relating to the cyber security management of businesses is relatively new, there is a clear lack of literature relating to this discipline. This study, therefore, looks to address this issue by taking an exploratory approach to the subject. Based on various sources in the UK, this study used the UK's cyber security framework as a conceptual model against which conditions in South Korea were examined.

Drawing on a mixed methods approach, this study employed three research methods: documentary research, quantitative questionnaires, and qualitative interviews. In the quantitative phase, current situations of the businesses in relation to cyber security were assessed and differences by business sectors and sizes were identified. In the qualitative phase, five themes were identified. Findings from the quantitative and qualitative research were triangulated with the existing literature, including the qualitative results describing the empirical field of enquiry, to present a holistic picture of cyber security management of South Korean businesses.

It was revealed that small and medium-sized businesses did not have a structural mechanism to prevent or mitigate risks at the pre-breach stage. Rather, they focused on responses at the post-breach stage. This finding demonstrated that small and medium-sized businesses were not prepared for the risks and threats from a preventative point of view. In addition, management of cyber security in businesses was not an isolated mechanism, but affected by external influences and initiatives. However, small and medium-sized businesses relied more upon private organisations than public organisations, which indicates that there was an insufficient role of public sector organisations in protecting small and medium-sized businesses.

In conclusion, this research has proposed an integrated cyber security risk management model. The framework was based on the argument that cyber security management relates to three elements: risk assessment, organisational behaviours and external factors. It is here that the biggest gains can be made if businesses manage cyber security in a holistic manner and if national leadership is strengthened in the Korean cyber security governance. This empirical research has made a contribution to knowledge in relevant studies by presenting a comprehensive landscape of cyber security management of businesses.

LIST OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY & ABBREVIATIONS

Action Fraud is a centre for the national fraud and cybercrime reporting in the UK. It is a single point of contact for fraud and cybercrime.

ANOVA is an abbreviation of 'Analysis of variance'. It compares three or more sample means.

Big data is loosely defined as large and complex data sets (structured, semi-structured and unstructured) that conventional software tools cannot efficiently process and analyse. Through computational analyses, the data sets may reveal behavioural patterns and social interactions of people.

Biometrics are authentication tools that depend on the uniqueness of human characteristics, automatically checking physical characteristics. Biometrics are often used for identification and access control.

Bonferroni is one of multiple-comparison procedures for carrying out the follow-up tests that compare each pair of means.

Botnets are an army of connected computers which are used to commit coordinated attacks on the command of a control server.

Bring Your Own Device (BYOD) is a policy that allows employees to bring their own personal mobile devices to work so that they can access the corporate network and data for work via these personal gadgets.

Children Exploitation and Online Protection Centre (CEOP) aims to protect children from sexual abuse and violence. It identifies the threats to children and coordinates child protection activity with other partners across the UK and overseas.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Definition from the NIST).

COBIT 5 is a framework from ISACA for the cyber security governance and management of businesses.

Correlation quantifies nature of the linear relationship between two variables.

Cyber and Government Security Directorate (CGSD) is responsible for all aspects of government protective security as a policy and standards organisation.

Cyber-Security Information Sharing Partnership (CiSP) is a UK government-led joint industry initiative, creating a forum to facilitate information sharing and increase awareness of cyber threats.

Department for Business, Innovation and Skills (BIS) is the department for economic growth in the UK. The department is dedicated to raising skills and education and boosting innovation.

End-point devices are hardware devices that can be connected to the Internet. The term includes computers, laptops, smart phones, tablets, etc.

Enterprise Resource Planning (ERP) is business process management software. This software supports an organisation to integrate and manage various business activities, such as procurement, inventories, sales, accounting, manufacturing, and human resources.

European Union Agency for Network and Information Security (ENISA) is an agency of European Union. It was set up in 2004 to secure information technologies and computer networks of member countries.

Firewall is a network security system that controls the incoming and outgoing network traffic based on present security rules.

Government Communications Headquarters (GCHQ) is a British intelligence agency responsible for defending Government systems from cyber threat and providing signals intelligence and information assurance to other government entities.

Her Majesty's Inspectorate of Constabulary (HMIC) is an independent entity that inspects and assesses police forces in England and Wales and their policing activities.

Information and Communications Technology (ICT) is an umbrella term that includes any communication devices and applications. The primary examples are a computer, mobile phone, television, broadband, Wi-Fi, network, and website, etc.

Information Security Management (ISM) is a comprehensive framework to protect an organisation's computing environment, including its people, activities, data, technology, and network (Definition from Raggad, 2010).

International Organization for Standardization (ISO) 27001 is the best-known international standard which recommends a set of policies, procedures, documents and technology for managing cyber security.

International Telecommunication Union (ITU) is an agency within the UN and deals with information and communication technologies (ICTs) internationally.

Internet Data Centre (IDC) is a facility that is established when it is necessary to collect and concentrate servers that are the core of an Internet connection.

Internet of Things (IoT) is the network of interconnected physical objects that are equipped with electronic identifiers. The identifiers have the ability to automatically send collected data over a network.

Internet Service Providers (ISPs) are businesses that provide services to people for accessing the internet and related services.

Internet Watch Foundation (IWF) is an organisation that consists of Internet Service Providers to eradicate obscene imagery online.

Intrusion Detection System (IDS) is a device or a software application that detects malicious activities to maintain network and data security.

Kendall's tau-b is one of measures of association on the strength of a relationship.

Korea Federation of Small and Medium-sized Businesses (K-BIZ) is an interest group whose members include almost all SMEs in South Korea.

Korea International Trade Association is a non-profit organisation that represents international trade community in South Korea.

Korea Internet & Security Agency (KISA) is a Korean public agency which governs cyberspace and ensures cyber security across the nation. This organisation also leads the computer emergency response team (KrCert).

Major Projects Authority (MPA) evaluates major governments' projects, working with HM Treasury and other government departments. It provides independence assurance

on the projects and aims to improve the way other government departments manage and deliver projects.

Mayors Office for Policing (MOPAC) sets policing priorities and budget for the Met.

Metropolitan Police Service (The Met) is a territorial police force for Greater London, excluding the City of London. It also has national responsibilities such as counter-terrorism and protection of senior members of the Government.

National Aeronautics and Space Administration (NASA) is in charge of various space programmes along with aeronautics and aerospace research.

National Audit Office (NAO) is an independent parliamentary body which audits central government departments, agencies and non-departmental public bodies.

National Cyber Crime Unit (NCCU) takes the lead in the UK's response to cybercrime. As a part of the National Crime Agency, this unit supports and coordinates other police forces to fight against the most serious cybercrimes.

National Cyber Security Programme (NCSP) is managed by the Office of Cyber Security and Information Assurance and Cyber and Government Security Directorate, both in the Cabinet Office. This programme has a budget of £860 million and is running from April 2011 to March 2016.

National Fraud Intelligence Bureau (NFIB) is a unit in the city of London Police whose mission is to gather and analyse intelligence in order to combat fraud and financially-motivated cybercrime.

National Institute of Standards and Technology (NIST) aims to support US public and private sector organisations by developing measurement science, standards and

technology. (**NIST 800 Series** is a collection of documents that include computer security policies, procedures, and guidelines of the US federal government.)

National Intelligence Service (NIS) is an intelligence agency of South Korea. Major duties include security investigation, intelligence on North Korea, counter-espionage, industrial security, international crime, and cyber security.

National Police Agency (NPA) is a national police force of South Korea which provides all policing services throughout the country.

National Police Chiefs' Council (NPCC) is a non-profit organisation for chief police officers in England, Wales and Northern Ireland to coordinate policing strategies and practices. It has been replaced by the National Police Chief's Council.

Office of Cyber Security and Information Assurance (OCSIA) is part of the Cabinet Office. This unit coordinates cyber security and information assurance programmes run by the UK government. It manages the National Cyber Security programme and delivers the Cyber Security strategy.

Packet is a unit of data that is carried from an origin and a destination on the Internet.

Pearson's chi-square test ($\chi 2$) is a statistical test that compares observed frequencies with expected frequencies under assumption of independence. It is a formal test of whether two categorical variables are statistically independent.

Police Central e-Crime Unit (PCeU) was part of the Specialist Crime Directorate of the Metropolitan Police Service in London. In 2013 this unit has been merged into the NCCU.

Reconnaissance General Bureau is an arm of Armed Forces in North Korea. This organisation is responsible for collecting overseas intelligence and ordering special military offenses against foreign countries including South Korea.

Serious Fraud Office (SFO) is an independent department that investigates serious fraud and corruption cases.

Significance level refers to the probability of rejecting the null hypothesis, given that the null is true. Also, it is the possibility of committing a type I error, known as alpha (α). Type I error occurs when rejecting the null although the null is true. $\alpha = 0.05$ is conventional significance level.

Small and Medium Business Administration (SMBA) is a South Korean public body which provides Small and Medium-sized Enterprises with supportive policies to promote their businesses.

Small and Medium-sized Enterprises (SMEs) refer to companies with more than 9 and less than 300 employees in this research.

Specialist, Organised and Economic Crime Command (SCECC) leads the investigation of all crimes related to economic gains. Types of crimes include economic crime, corruption, human trafficking, prostitution, etc.

STATA is a widely used statistical software package from 1985.

***t*-test** is used when comparing two different groups on a variable of interest. The test is run by comparing the means of the two groups.

UK-CERT is the UK National Computer Emergency Response Team that responds to cyber security breaches in the UK in alliance with public and private partners and CERTs of other nations.

Virtual Global Taskforce is an international organisation that works with law enforcement agencies to respond to online child abuse.

DECLARATION

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award. (Word count: 77,960 / excl. footnotes and bibliography)

ACKNOWLEDGEMENTS

I would like to thank all of those who have supported me immeasurably during my work on this thesis. First and foremost, my sincere appreciation goes to my supervisors, Dr. Victoria Wang, Chris Lewis, and Barry Loveday who provided discerning advice, valuable suggestions and endless encouragement throughout my work in completing this thesis. Their probing questions and insight always encouraged me to rethink, evaluate and expand my ideas. Every supervisory meeting has provided me with fruitful discussions and encouragement.

This thesis could not have been completed without support of my Korean colleagues as well as international colleagues in the Postgraduate Research Student Centre. It was always great to carry out research with such an inspirational group of researchers. They not only gave me academic advice, but also shared their precious time to be engaged in outside venues.

My family merits special recognition. I wish to thank my beloved wife, Hyunju Lee, for her encouragement and constant support throughout a long period of my research. There is no doubt that her support sustained me. During my research she gave birth to our first son, Yunwoo Jung. I am very happy that he has been well during my absence. Last but not least, I thank my parents and parents-in-law for their wonderful support and great patience. In particular, my parents-in-law sacrificed themselves to take care of Yunwoo. I would like to dedicate this thesis to my family.

DISSEMINATION

Relevant Publication

Aziz B., Malik A., Jung J. (2017). Check Your Blind Spot: A New Cyber-Security Metric for Measuring Incident Response Readiness. In Großmann J., Felderer M., Seehusen F. (Eds.), *Proceedings of the 4th International on Risk Assessment and Risk-driven Testing, Lecture Notes in Computer Science: Vol. 10224* (pp. 19-33). Cham: Springer.

CHAPTER 1: INTRODUCTION

1.1 Introduction

Using Information and communications technology (ICT) has become a pervasive phenomenon in much of both the public and private domains, and accordingly this has introduced cyber security risks and threats against individual and organisational users. As we develop and adopt new types of ICTs, associated problems emerge in spite of human efforts to stop them. The nature of the risks and threats is not static and develops over time, thus requiring continuous responses. Such concerns have led to a growing body of discourses and publications exploring these problems. Efforts to address risks and threats in cyberspace face some inherent challenges. Also, cyber security risks and threats are intertwined with deviant behaviours in the physical world. It is difficult to capture the nature and extent of the relationship between the 'online' and 'offline' worlds.

In terms of managing cyber security risks and threats, a wide range of technical controls at operational level have been accepted as the most applicable and feasible solutions (Singh et al., 2013). Researchers from computer science and computing disciplines focused on developing technical measures to protect information systems. However, there is a growing consensus that cyber security problems cannot be mitigated by technical controls alone (Furnell & Clarke, 2012; Rhee, Ryu, & Kim, 2012; Safa et al., 2015; Safa, Von Solms, & Furnell, 2016). Instead, social science approaches to cyber security risks and threats have become increasingly prominent in understanding the nature of the risks and threats, drawing on non-technical aspects such as humans and managerial support as a solution (Johnston & Warkentin, 2010; Kayworth & Whitten, 2010; Singh, Gupta, & Ojha, 2014; Singh, Picot, Kranz, Gupta, & Ojha, 2013; Werlinger, Hawkey, & Beznosov, 2009; Young & Windsor, 2010).

This research will also take a social science approach in exploring how South Korean small and medium-sized enterprises (SMEs) approach cyber security risks and threats - for more details of the definition of SMEs (see: Section 3.2.3, p. 84). Taking an interdisciplinary approach, this research is expected to disclose interactions between humans and technology in the context of business management from a sociological perspective. This will shed light on the role of organisational behaviours such as leadership, communication, culture, decision-making processes, managerial roles and employees' attitudes in the management of cyber security risks. Moreover, SMEs' cyber security management will be explored within the wider national context in which they operate, including socioeconomic arrangements beyond organisational boundaries.

1.2 Understanding the thesis

1.2.1 Business opportunities and security risks from ICTs

It was estimated that 3.2 billion people around the world and more than 80% of people in developed nations were using the Internet by the end of 2015 (International Telecommunication Union [ITU], 2015a). In particular, mobile-broadband penetration rates were expected to reach 47% in 2015, about four times as high as they were 5 years previously (ITU, 2015b). This growth of Internet and wireless communication has changed the behaviour of end users in terms of how people interact with one another and engage in social activities. The UK and South Korea have highly innovative ICT infrastructures and people in both countries have relatively advanced computer skills and knowledge compared to those in other countries (ITU, 2015b; United Nations, 2014a).

In a seminal book, Castells (2010) defined *network society* as the dominant social structure of the Information Age, relying on decentralised networks. Social networks are driven by electronic communication technologies, such as the Internet or mobile telephones. He acknowledged that the network society would not have existed without

a technological revolution. The way in which people interact with others has changed significantly as people embraced new types of technical devices. For example, a huge portion of social interactions occur via micro-electronic communication devices without meeting personally.

Not only individuals, but also organisations, have had to adapt to a new environment dependent on internet-based communication networks. In order to maximize profits and reduce costs, companies of all sizes have attempted to take advantage of ICTs. As an increasing number of people use social networking services as a venue for communication and information sharing, the massive spread of virtual social interactions creates an opportunity for businesses to open up new markets. Additionally, ICTs help businesses manage themselves in a variety of ways, such as improving performance, sharing business information, and reducing costs. In this sense, ICTs have become increasingly essential in business operations on a daily basis (Soomro, Shah, & Ahmed, 2016). The adoption of ICTs is now one of the crucial prerequisites for increasing competitive edge in business (Harris & Patten, 2014; Hashim, 2015).

The rise of cloud computing[1], Internet of Things[2], and social media platforms has contributed to a very great increase in data sets. Using Big Data[3] analytics, companies carry out data-driven decisions rather than intuition-driven ones. McAfee and Brynjolfsson (2012) argued that management decisions based on data raise business performance, ultimately building a competitive advantage. Whereas Internet of Things and social media services are data sources, cloud computing is an underlying engine that enables users to access, save, and manage data (Hashem et al., 2015).

1 Cloud computing commits data to information systems handled by third parties on remote servers.

2 Internet of Things is the network of interconnected physical objects that are equipped with electronic identifiers.

3 Big Data is loosely defined as large and complex data sets that conventional software tools cannot efficiently process and analyse (Snijders, Matzat, & Reips, 2012).

The technological revolution has changed business communication and management. However, there is a downside to all this. The Internet - as the core part of ICT - has the potential to be a breeding ground for cybercrimes (Wall, 2007). In South Korea, the number of cybercrimes reported to the police increased significantly by about 31% from 116,961 in 2011 to 153,075 in 2016 (National Police Agency [NPA], 2012, 2017a). In a similar vein, in the UK, the number of cybercrime offences and online fraud cases were estimated to be about, respectively, 2 million and 3.6 million in the 12 months (Office for National Statistics, 2017). The rapid growth of ICTs has provided grounds which generated new types of risks and threats. As far as businesses are concerned, an increasing reliance upon those devices has exposed SMEs to various cyber security threats (Moradoff, 2010). This has given rise to cyber security breaches (e.g., hacking, theft of business or customer information, and system disruption) which have caused major economic and social losses to companies, at least temporarily.

1.2.2 Main targets from cyber security threats: Research gap

Three main sectors are under attack by different kinds of cyber security threats. Those are government bodies, businesses, and individuals. According to a survey by the UK government (Cabinet Office, 2011a)[4], the cost of cybercrime to the UK economy was estimated at £27 billion per annum, about 77.8% (£21 billion) of which fell on businesses. Globally, the cost of cybercrime against businesses has increased steadily. The Ponemon Institute (2017) suggested that the global average annualised cost per company was US$ 8.7million between 2013 and 2017, and the average percentage change of the costs over the five years was 62%[5]. These figures demonstrate that businesses are the main target of cybercrime justifying government efforts to protect business sectors. For example, the UK government sought to make London the most secure place in the world to do business.

4 Although this survey has been questioned of its reliability and accuracy of the types of estimates (e.g., Anderson et al., 2013), it was referred to here because this survey measured the costs by types of victims (i.e., the Government, businesses, and citizens, respectively).
5 This analysis pertained to 254 companies with a minimum of over 1,000 employees.

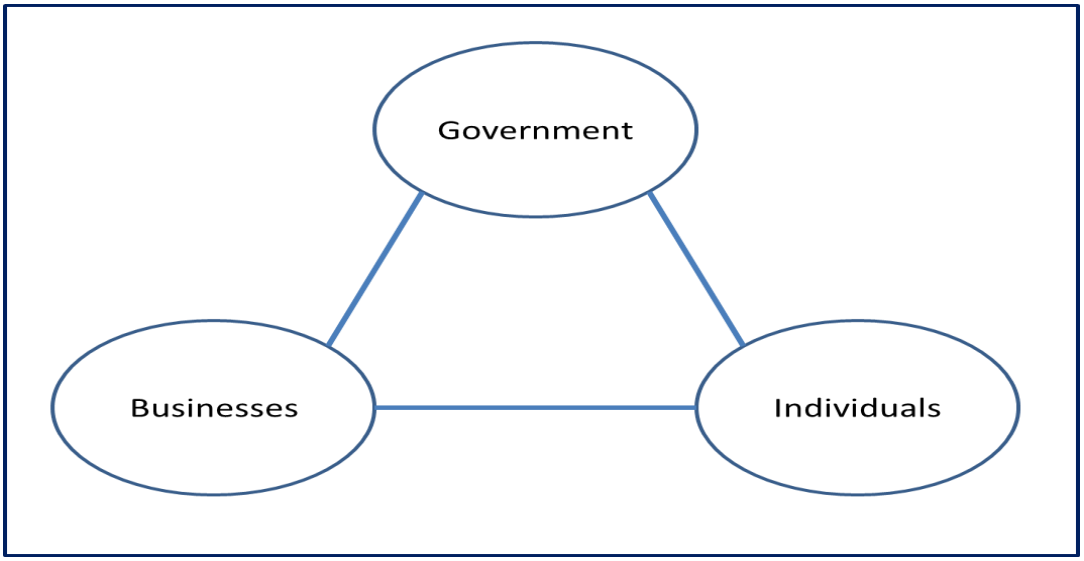


Figure 1.1 Three main targets from cyber security threats

When it comes to cyber security threats, there are two strands of concern in South Korea - for more details (see: Section 3.3.1). The first is cyber terrorism and the second is cyber financial fraud. Cyber terrorism is a great concern for any nation. South Korea has a different cyber terrorism concern derived from its unique historical background. Although South Korea in itself is a target of cyber-attacks from external states and non-state entities, cyber terrorism perpetrated by North Korea has been a major problem for both the government and public (Chung, Lim, & Kwon, 2016; Kwon, 2016). It targets the government, military, and large companies which run critical national infrastructures. Similarly, the UK is always cautious of cyber terror attacks from other nations as well as non-state terrorists (Cabinet Office, 2011b; HM Government, 2016).

Within general cybercrime, cyber financial fraud does serious harm to individuals (Kim, Kang, & Kim, 2015; Yoon, 2013). Fraudsters use hacking skills and social engineering techniques, targeting a disproportionately large number of people via automated machines. In 2013, the total damage of cyber financial fraud was estimated at £39.3 million, with each case causing the loss of £2,520 (NPA, 2014).

Due to these two concerns, the government, large companies, and individual citizens are well recognised as potential targets from cybercriminals in South Korea. Accordingly,

the government has provided protective measures based on this recognition. However, SMEs are left on their own. SMEs amounted to 99.9% of the total number of businesses, and they employed 85.7% of the total workforce in South Korea in 2016 (National Statistical Office, 2017). Despite the significance of SMEs in the national economy – for more details (see: Section 3.2.3), the government and academia have overlooked the exposure of SMEs to high levels of cyber-attacks. As a result, very little attention has been paid to cyber security risks and threats on South Korean SMEs.

This tendency may also be replicated internationally. Holtfreter and Meyers (2015) noted that globally small businesses were not recognised as potential cybercrime victims, and contrasted this with the greater attention paid to individuals, large companies and governments. The lack of attention to SMEs indicates that SMEs' cyber security management is an uncharted territory, requiring and meriting further investigation. This thesis therefore, seeks to address that gap with a clear focus on SMEs.

Currently many of those cyber security risks and threats have been discussed under the big umbrella term, *cybercrime*. For example, cybercrime tends to be seen as generic across the social spectrum. However, Graham (2017) contends that cybercrime is about protecting families and individuals based on an understanding of the socio-psychological aspects of criminals and victims, while cyber security focuses on protecting government and corporate networks by mitigating security vulnerabilities. As reflected in research subjects and questions, the focus in this research is on security and risk. Since crime is a potential source of risk (Levi, Morgan, & Burrows, 2003), cybercrime will also be discussed in conjunction with cyber security risks and threats. Hence, this study will focus on cyber security management of risk, threats, and cybercrime from preventative, preparatory, and protective points of view.

Given this uncharted territory, the research is intended to be exploratory, seeking to examine internal arrangements within businesses as well as their surrounding contexts as to cyber security. Researchers explore when there is little knowledge about the

research subject they are interested in and when it is worth investigating (Stebbins, 2001). In social science exploration is defined as “a broad-ranging, purposive, systematic, prearranged undertaking designed to maximize the discovery of generalizations leading to description and understanding of an area of social or psychological life” (Vogt, 1999, as cited in Stebbins, 2001, p. 3). Such an exploration is expected to help to build a comprehensive picture of the landscape surrounding SMEs which has not been drawn before. Therefore, this exploratory research is driven by empirical data rather than testing pre-identified hypotheses.

1.2.3 Research aim and objectives

The aim of this study is to empirically explore and evaluate the current state of cyber security management of SMEs in South Korea. In order to undertake the assessment, it is necessary to have some ancillary objectives.

The first objective is to identify cyber security risks and threats against SMEs. When it comes to SMEs’ cyber security, there is an obvious lack of risk and threat assessment. Considering the scale and importance of SMEs in the national economy, it needs to be understood which types of risks and threats SMEs face. The risks and threats are perceived differently depending on organisational characteristics and behaviours. Therefore, the extent and scope of the risks and threats can be better understood if the nature of those organisational characteristics and behaviour are made clear. This will be a basic diagnostic tool in assessing the overall cyber security context surrounding SMEs.

The second objective is to examine whether SMEs are prepared to address the risks and threats they face. SMEs’ preparedness will be measured by the extent of organisation of cyber security management. This examination will include not only various aspects of cyber security management itself, such as its practices, structure and decision-making processes, but also external factors which influence the management of cyber security. The inclusion of external factors will expand the scope of this research by shedding light

on relationships between SMEs and external organisations. Furthermore, structural loopholes in SMEs' cyber security management are expected to emerge through this examination.

The third objective is to suggest policy recommendations to strengthen the cyber security management of SMEs. The process of identifying and selecting appropriate recommendations will be guided by the empirical data within considerations of the research context. The research undertaken to meet the first and second objectives is expected to reveal a full picture of SMEs' cyber security management. This then will inform proper recommendations, which means they will emanate from empirical data. This process will allow the recommendations to be immediately applicable in the South Korean context.

The fourth objective is to propose an effective framework for protecting SMEs from cyber security risks and threats. This data-driven research is expected to disclose unknown dimensions and factors that are associated with cyber security management in SMEs. Not only organisational factors but also influences from external organisations will be incorporated in the framework in order to present a comprehensive account of SMEs' cyber security management.

1.2.4. Research questions

Research questions serve as the driver for carrying out a successful research project (Robson & McCartan, 2016). They help a researcher not only to advance a research project in a structurally organised way but also to achieve research goals, objectives, and purposes at the same time. Research questions are critically important because they govern research design as well as specific data analytic procedures (Onwuegbuzie & Leech, 2006). There are some criteria for good research questions, such as clarity, coherence, significance and purposiveness (Robson & McCartan, 2016). Above all, research questions should be formed as a coherent set to ensure the formality of the

research project. Five research questions developed to meet the objectives of this study are suggested:

(1) The extent to which South Korean SMEs are exposed to cyber security risks?
(2) How serious are cyber security breaches for South Korean SMEs?
(3) The extent to which South Korean SMEs are prepared to prevent or mitigate cyber security risks and breaches?
(4) What are the characteristics of external influences and initiatives in South Korea?
(5) What is the nature of relationships in South Korea between SMEs and other public or private sector organisations?

These five questions are the fundamental guidance for an exploration of the research problem: '*how is cyber security managed in South Korean SMEs?'.*

1.3 Explaining the approach

This study uses a mixed methods approach as the research design - for more details (see: Section 4.3.2). The mixed methods approach draws on both quantitative and qualitative research strategies, generating various benefits such as triangulation and comprehensiveness (Johnson, Onwuegbuzie, & Turner, 2007; O'Cathain, Murphy, & Nicholl, 2007; Robson & McCartan, 2016). This approach will both increase the validity of findings and the academic rigour of this research.

In this mixed methods approach, three research methods are used in sequence: (1) documentary research (qualitative), (2) quantitative questionnaires and (3) qualitative interviews - for more details (see: Section 4.4). In this thesis, documentary research was undertaken by utilising public and private documents and records. These sources are mostly used to supplement Chapter 2, the Literature Review, and to construct Chapter

3, the Empirical Field of Inquiry. It was necessary to have some knowledge of the research context before embarking on data collection because cyber security in SMEs was such an unexplored area. Secondly, quantitative questionnaires were used to assess the cyber security context faced by SMEs. The questionnaires were self-administered and completed online for easier access. Thirdly, semi-structured interviews were carried out in a flexible manner to gain further information about issues and problems relating to cyber security management of SMEs. These three methods and their findings were employed in triangulation to enable a comprehensive and holistic pursuit of the research questions.

Following the documentary research which provided preparatory information on cyber security conditions in South Korea, the quantitative questionnaires and qualitative interviews involved data collection and analysis. The table below is a summary of data collections:

Table 1.1: Data collection methods and analysis of quantitative and qualitative research

	Quantitative research	**Qualitative research**
Data collection method	Online survey questionnaires	Semi-structured interviews
Data collection period	28 Oct 2016–27 Dec 2016	02 Feb 2017–28 Feb 2017
Samples	328 responses	25 interviewees
Respondents	IT managers/owners of SMEs	- 16 IT managers/owners of SMEs - 9 government officials
Response rate	7%	-
Sampling strategy	Convenience sampling	- Generic purposive sampling - Snowball sampling

Analytical approach	Statistical approach	Thematic analysis (Braun and Clarke, 2006)
Analysis method	STATA programme (version 14)	QSR NVivo programme (version 11.3)

The survey questionnaires were collected across the nation which consists of eight provinces[6] and nine self-governing areas[7] (see: Figure 1.2). Of these, four provinces and five self-governing areas[8] were selected for data collection.

6 These are Gyeonggi-do, Gangwon-do, Chungcheong buk-do, Chungcheong nam-do, Jeolla buk-do, Jeolla nam-do, Gyeongsang buk-do and Gyeongsang nam-do.

7 These are one special city (Seoul), six metropolitan cities (Busan, Daegu, Incheon, Gwangju, Daejeon, and Ulsan), one metropolitan autonomous city (Sejong) and one special self-governing province (Jeju-do).

8 These include Gyeonggi-do, Gangwon-do, Gyeongsang buk-do and Gyeongsang nam-do, Seoul, Busan, Daegu, Daejeon and Ulsan.

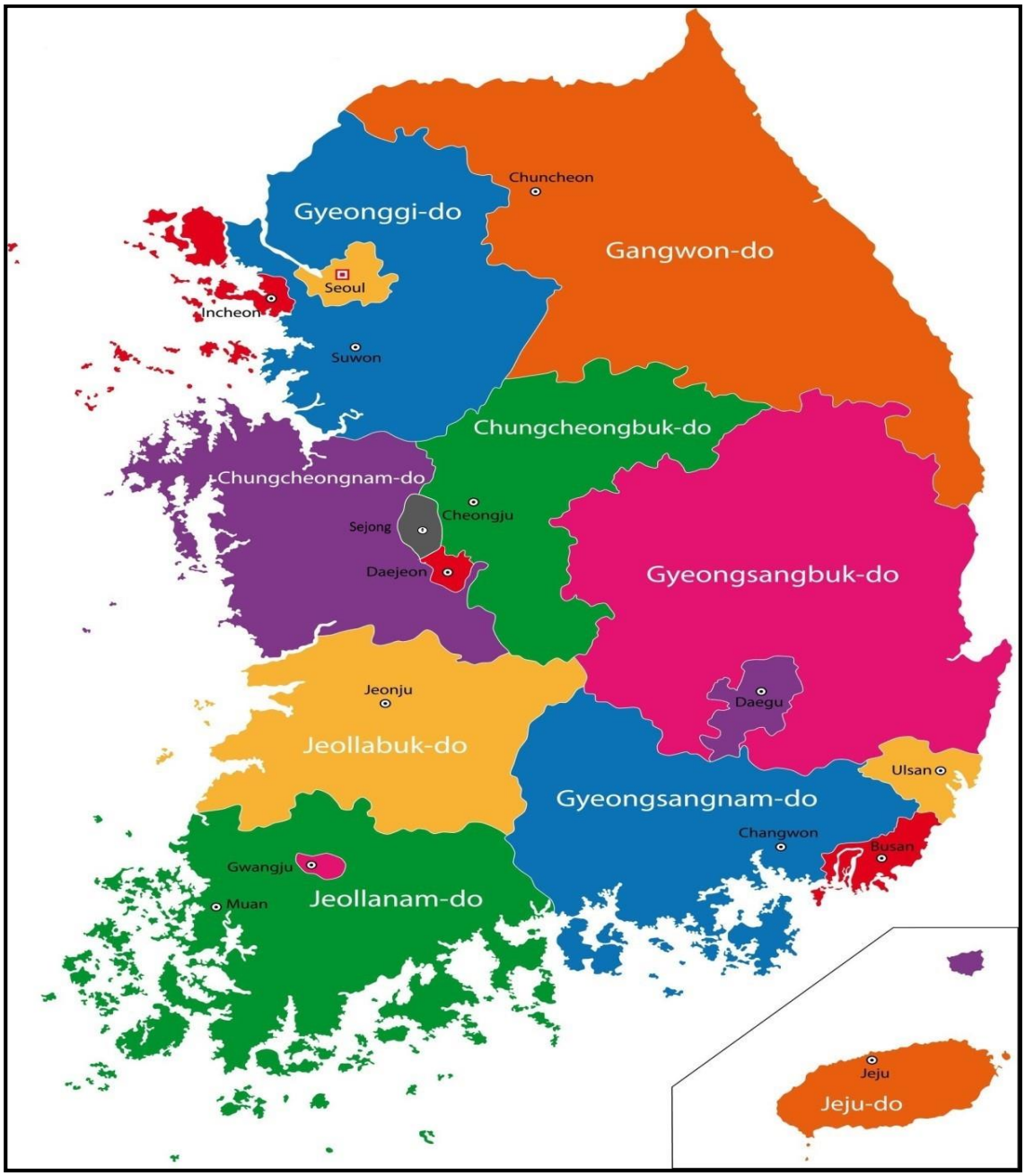


Figure 1.2 Administrative divisions of South Korea (from http://blog.investkorea.org)

In terms of data analysis, quantitative survey data has been analysed by descriptive and inferential statistics via STATA programme (version 14). The findings also include analyses by business size and business sector. Qualitative interview data has been analysed via QSR NVivo programme (version 11.3). Thematic analysis is used to examine patterns or themes within the interview data (Braun & Clarke, 2006). This analysis in turn generates descriptive codes, analytic codes and themes.

1.4. Mapping the thesis

This thesis consists of eight chapters. The first chapter has outlined the scale of the study and the research strategy used to accomplish its goal and objectives. Chapter 2 addresses the theoretical literature on cyber security risks and threats as well as various dimensions of cyber security management. Also, the UK's cyber security governance is explained to identify loopholes and weaknesses in the Korean cyber security governance - for more details (see: Section 3.4.4).

Chapter 3 provides a socioeconomic overview of the empirical field of inquiry, or South Korea, to inform the research context regarding cyber security and cybercrime. This chapter is intended to help the reader to better understand the interpretation and discussion of research findings in later chapters.

Chapter 4 discusses the research methodology and the specific methods employed in this study: documentary research, quantitative questionnaires, and qualitative interviews. The research has been carried out in a rigorous and scientific manner. In order to establish this, the researcher provides justifications for the choice of the methodology and methods; and other procedural choices.

Chapter 5 examines quantitative findings and delivers an assessment of SMEs' current situation by using descriptive statistics, chi-square tests and *t*-tests.

Chapter 6 explores qualitative findings and proposes five main themes emerging from the interview data.

In Chapter 7 discussion focuses on a triangulation of the quantitative and qualitative findings with the existing literature. This triangulation is adopted as a strategy to increase research rigour by shedding light on agreements as well as conflicts between different sources.

The final chapter provides an assessment of whether the research goal and objectives are met, and questions how this study contributes to the field of cyber security management in South Korea. In addition, it includes a consideration of the limitations of this study and, finally, proposes directions for future research.

1.5. Conclusion

Cyber security risks and threats have increased in recent years, causing significant economic and social losses to public and private organisations as well as individuals. Among multiple risks and threats, cyber terrorism from North Korea and cyber financial fraud are considered serious problems in South Korea. Discourses around these problems drove government initiatives and academic research to focus on protecting large businesses, the public and governments. In contrast, there has not been much attention to the impact of cyber threats on SMEs.

Due to the relative lack of concern over SMEs, this thesis takes the form of exploratory research. In order to uncover an unexplored subject, a set of research questions are designed to be answered in a sequential order. Research methods are undertaken in a sequence to effectively map out a holistic picture with regard to the research problem.

The increase in cyber threats against businesses and the associated economic impacts make research on cyber security management of SMEs imperative within the specific South Korean context. Recognising the need for such research, this thesis aims to investigate internal arrangements within SMEs, but also to illustrate the external interactions of SMEs with outside entities. The necessity to conduct an in-depth analysis of the cyber security management process calls for the use of a mixed methods approach. This approach is adopted to provide a scientific basis for research in this study.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

This literature review provides a theoretical framework for cyber security management and a discussion which focuses on the research questions. This chapter starts by examining a definitional difference between information security and cyber security and theories of risk. Based on the theoretical underpinnings, this chapter goes on to outline various types of cyber threats and, more specifically, cyber security risks against SMEs.

As main part of this chapter, cyber security risk management frameworks are presented. Although many frameworks were available at the time of the research, only four representative frameworks are suggested. The next section explores various aspects of cyber security management in businesses. Firstly, how cyber security management can be implemented is illustrated by examining – (i) related measures and practices, (ii) a balanced approach to security controls, (iii) the role of knowledge and (iv) role of managers and their leadership. Secondly, the significance of cyber security culture is discussed. To conceptualise cyber security culture, it is represented as an adaptation of organisational culture. As elements of culture, managerial roles and leadership are considered to take an important role in establishing a constructive cyber security culture.

In the final part of this chapter, the UK's cyber security governance is discussed. The UK's framework is taken as a conceptual model as well as a conceptual lens against which conditions in South Korea are examined. Discussion of the UK's cyber security governance begins by investigating the national cyber security structure and pays special attention to the specific schemes directly related to protecting SMEs. Based on descriptions of participating governmental and non-governmental organisations, the discussion centres around whether, and how, the UK governance reaches out to protect SMEs. As a vital part of the framework, a UK's reporting mechanism is investigated. Critical analyses and evaluations of the UK situation are provided throughout this section.

2.2. What is cyber security?

In this section, definitions of information security and cyber security are discussed. Without a clear definition of key terminologies, further discussions may have limited value as a subject of sustained empirical investigation. The two terms, cyber security and information security are frequently used interchangeably without much distinction (Von Solms & Van Niekerk, 2013; e.g., Öğüt, Raghunathan, & Menon, 2011). However, these are not entirely analogous concepts. It is of importance to look into ideas underlying the two concepts in order to fathom the views formed around them.

Information security is "the protection of information resources against unauthorized access" (Raggad, 2010, p. 18). It means that only authorised people or ICTs should have access to information resources, such as data, hardware, software, and network. This definition is clearly related to a business management aspect because decisions on the authorisation should be dependent upon business objectives. When certain people are considered necessary for attaining a business objective, those people need authorisation to access a certain amount of information resources directly relevant to the business objective. By controlling unauthorised access, information security focuses on reducing business damage in a way that mitigates the probability and impact of security incidents. At this point, a fundamental question arises: what should be protected?

As one of the most important international standards, ISO/IEC 27000 (2016) defines information security as the preservation of confidentiality, integrity and availability of information. Integrity, availability, and confidentiality (Known as 'CIA Triad') are depicted as three aspects of information that should be protected to achieve security goals. It can be explained that only authorised persons should gain access (availability) to the accurately represented information (integrity) without disclosure to unauthorised persons (confidentiality). They are also called characteristics of information security. If one of those characteristics is compromised, it is said to be a security failure. There are

some other researchers (Raggad, 2010; Whitman & Mattord, 2011) who argue that more information characteristics need to be included to address adequately the constantly changing nature of ICTs. Whereas Whitman and Mattord (2011, pp. 11-12) suggested that accuracy and authenticity were two other critical characteristics of information which the value of information comes from, Raggad (2010) contended that authentication and non-repudiation need to be added to the 'CIA Triad', constituting 'the Security Star'. Authentication implies that the identity of human or system is verified before access permission is granted and non-repudiation is a mechanism designed to enforce the fulfilment of accepted obligations. Non-repudiation is based on the logic that the message sender cannot later deny that he or she sent the message. These five elements are interpreted as security goals that lead to the achievement of business goals (Raggad, 2010, pp. 20-22).

Jung (2011) defined cyber security as protecting information and communication networks, and information from cyber-attacks or cyber threats that occur in the cyberspace or network. This definition emphasised protection from attacks and threats. The ITU (2008) defined this from a different angle as follows:

> "Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (p. 2)

This definition highlights elements of cyber security and a range of subjects which need to be protected. One commonality between information security and cyber security is that the two concepts both aim to maintain the security properties of confidentiality, integrity and availability (ITU, 2008; Jung, 2011). However, the ITU's definition contains a broad aspect of safeguarding technical and non-technical elements. The expanding nature of the Internet allows cyber security to have unique traits (see: Table 1).

Table 2.1: Unique traits of cyber security (ITU, 2011, p. 13)

- While information security initially worked on segregated systems, cyber security addresses global threats which engage jurisdictional problems.
- Cyber security competes with an Internet architecture that makes attribution of an attacker very difficult.
- While information security stresses confidentiality, cyber security mainly involves integrity and availability.

Due to these traits cyber security faces various extensive issues, such as jurisdictional uncertainty, global threats and attribution difficulties. There is another difference in terms of asset protection. In cyber security, both human and non-human entities are considered assets which should be protected. Von Solms and Van Niekerk (2013) argue that cyber security protects various assets such as humans and society as well as their information resources, while information security aims to secure information-based assets only. This argument represents that cyber security considers impacts of information technologies on humans and society. Therefore, cyber security is capable of addressing socio-legal issues regarding cyber threats which are not dealt with by information security. This indicates that cyber security is a broader concept than information security, encompassing additional dimensions (Safa et al., 2016).

It was a tradition that organisations implemented security controls from the information security perspective (Reid & Van Niekerk, 2014). However, the boundaries of information are not confined to the border of an organisation any more due to communication networks such as internet and extranets (Chang & Ho, 2006). In particular, Bring Your Own Device (BYOD) and cloud computing services are widely adopted by individuals and organisations. These technological advances surpassed geographical and jurisdictional boundaries and changed traditional working hours. Nowadays, it is usual that an organisation's information is retained and monitored by third parties. However, these technological changes brought with them associated risks. Businesses have to think beyond the organisational context, considering business

partners, customers, and their environments. Business environment and relevant organisations need to be taken into consideration when they engage in protecting assets from the risks in cyberspace. As a consequence, this changing landscape is better captured by the concept, cyber security, rather than information security.

In this thesis, the researcher will use the term, cyber security, rather than information security, because cyber security can cover the broad scope of this research. This research encompasses inside management processes in relation to securing assets from cyber threats as well as external influences and relationships with public and private organisations. Organisational arrangements within a business will be examined first, but it will extend the examination beyond the organisational borders by incorporating outside entities.

2.3. Cyber security risks, threats, and cybercrime

2.3.1. Theories of risk

Nowadays, *risk* is a constantly encountered term. There are virtually no human activities which do not involve any risk (Borodzicz, 2005, pp. 1-2). In the seminar book, *Risk Society*, Beck (1992) posits that complex technologies humans have invented gave rise to unprecedented uncertainty. Understanding of the uncertainty and risks is extremely challenging. It is impossible for humans to predict hazards and future consequences from the uncertainties. Because risk is embedded in every aspect of society, the author diagnosed contemporary society as a risk society. However, there is no widely accepted definition of the term. In academia, scholars in a variety of disciplines approach this topic to understand how risk involves and develops in their own disciplines. Due to a wide range of theoretical positions, interpretations of risk concepts are based on their "epistemological foundation" (Zinn, 2008, p. 4).

Table 2.2: Formal definitions of risk (Vlek, 1995, p. 566)

- Probability of undesired consequence
- Seriousness of (maximum) possible undesired consequence
- Multi-attribute weighted sum of components of possible undesired consequences
- Probability x seriousness of undesired consequence ('expected loss')
- Probability weighted sum of all possible undesired consequences (average 'expected loss')
- Fitted function through graph of points relating probability to extent of undesired consequences
- Semivariance of possible undesired consequences about their average
- Variance of all possible consequences about mean expected consequences
- Weighted sum of expected value & variance of all possible consequences
- Weighted combination of various parameters of the probability distribution of all possible consequences
- Weight of possible undesired consequences ('loss') relative to comparable possible desired consequences ('gain')

In terms of understanding risk, three approaches are mainly identified: (1) realist approach (2) psychological approach, and (3) sociological approach. The first approach conceptualises risk in an objective manner based on the assumption that risks are real events or dangers. In natural sciences, risk is quantitatively measured to find out discrete time points as well as a proper scale of intervention. For example, National Aeronautics and Space Administration (2007, p. 139) defines risk in a measurable manner as having two elements: (1) the probability of failing to achieve a particular outcome and (2) the consequences/impacts of failing to achieve that outcome. It can be denoted as follows:

$$Risk \ = f(probability \ \ or \ \ likelihood \ * consequences \ \ or \ \ impacts)$$

In conceptualising terrorism risk, Willis (2007) asserts that risk is the intersection of three dimensions: threat, vulnerability and consequences (Figure 2.1), defining risk as the consequences of potential attacks on assets with vulnerability. Risk from an attack can be quantified as the unconditional expected value of damages from the attack. The greatest advantage of this approach is high application. As risk is denoted through probabilistic terms, risk can be understood in line with business management activities. Quantitative measures therefore are frequently used to communicate risks to non-security managers. As quantitative measures, metrics are effective in enabling constant risk assessment (Button, 2008) as well as informing business' decision-making (Aleem, Wakefield, & Button, 2013).

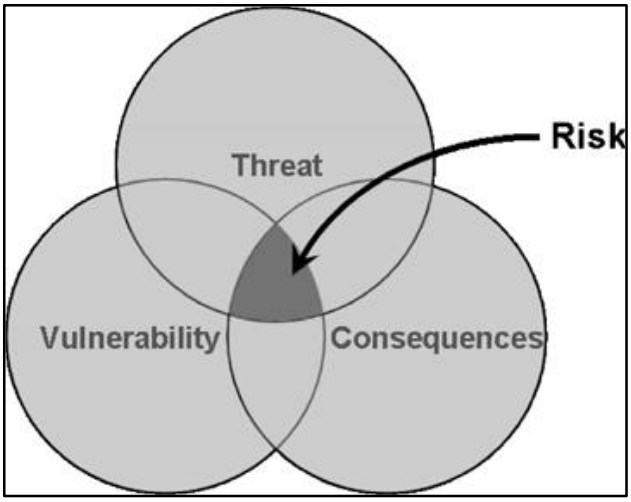


Figure 2.1. A risk definition by Willis (2007, p. 599)

The second approach is psychological one. This approach is concerned with how people perceive risk. Risk perception has been a great concern in social sciences. For example, in criminology and psychology risk perception is a major focus of interest. Two influential risk perception approaches are psychometrics and cognitive/behavioural decision-making (Borodzicz, 2005. p. 14).

The leading contender of risk perception studies, the psychometric model, aims at measuring psychological concepts of individuals in relation to hazards and risk. Psychometric studies attempt to develop measurements for human perception on risk

from sociopolitical, natural, and man-made events. The psychometric model is of importance as it produced a great body of empirical data regarding risk perceptions (Royal Society, 1992).

Risk perception is also closely associated with cognitive decision-making process of individuals (Sitkin & Weingart, 1995). Historically, risk perception research originates from the nuclear debates in 1960s (Sjöberg, 2000). The research from the nuclear field attempted to propose a set of reasonable choices for decision-makers. The decision-making process has been widely studied from a multidisciplinary approach, including mathematics, economy, and psychology. Among them, a psychological approach addresses how cognitive factors influence the risk-related decisions. For example, Kahneman and Tversky (1979) showed that humans rely upon mental shortcuts, heuristics, which significantly influence the decision-making process. Individuals may make some irrational choices for their behaviours (e.g., risk-taking or risk-avoidance), depending upon the way, and the extent to which, they perceive particular risk. Risk perception studies hugely influenced the development of behavioural theories not only in politics, but also in business management.

The third approach postulates that risk is a socially or culturally constructed concept. Cultural theory postulates that risk perception is a reflection of the social context to which a person belongs (Sjöberg, 2000). More specifically, risk perception reflects aggregate values in sociocultural contexts along with individuals' values and beliefs of risk (Royal Society, 1992). It considers risk is an outcome of social processes, which means that risk can be controlled by managing social factors. Although the cultural theory expanded risk perception discourses, it was not widely welcomed due to an abstract nature of the concept, social context (Sjöberg, 2000).

There are more approaches beyond these three. Some take more nuanced positions, while some others incorporate elements of more than two approaches. It is a recent development that those approaches have merged by integrating several theoretical

perspectives (Royal Society, 1992; Taylor-Gooby & Zinn, 2006). In particular, the converging process was found in sociology and psychology. While psychological thinking recognised social and cultural factors on framing risk perception, sociological work put more emphasis on individualist accounts of perceiving risk (Taylor-Gooby & Zinn, 2006). Recently, Grant, Edgar, Sukumar, and Meyer (2014) explored the impact of risk perceptions of key stakeholders in SMEs on decision-makings. In the study, the authors posited that risk estimation is predicated on an amalgamation of personal exposure, social, demographic, cultural and organisational contexts.

As this research takes an interdisciplinary approach, all the three approaches toward risk are relevant. Firstly, the realist approach leads to security management concerns on risk prevention and mitigation, which reflects the research problem. In addition, one of the main underlying frameworks in this research, risk management frameworks suggested below (see: Section 2.4), are from computer science and computing disciplines. These disciplines are based on the realist approach. Secondly, it is important to understand cognitive processes of individuals within a business. SMEs' employees and managers in a company have their own personal accounts on risk recognition and response. Lastly, aggregate risk perception on the organisational level is conditioned by the surrounding contexts. SMEs in general are susceptible to external influences and relations with outside entities. How those contextual factors shape their risk perception on cyber security is to be considered. The compounding approach to risk in this research could add some complexities, but it is necessary to have an in-depth understanding of cyber security situations and practices in SMEs.

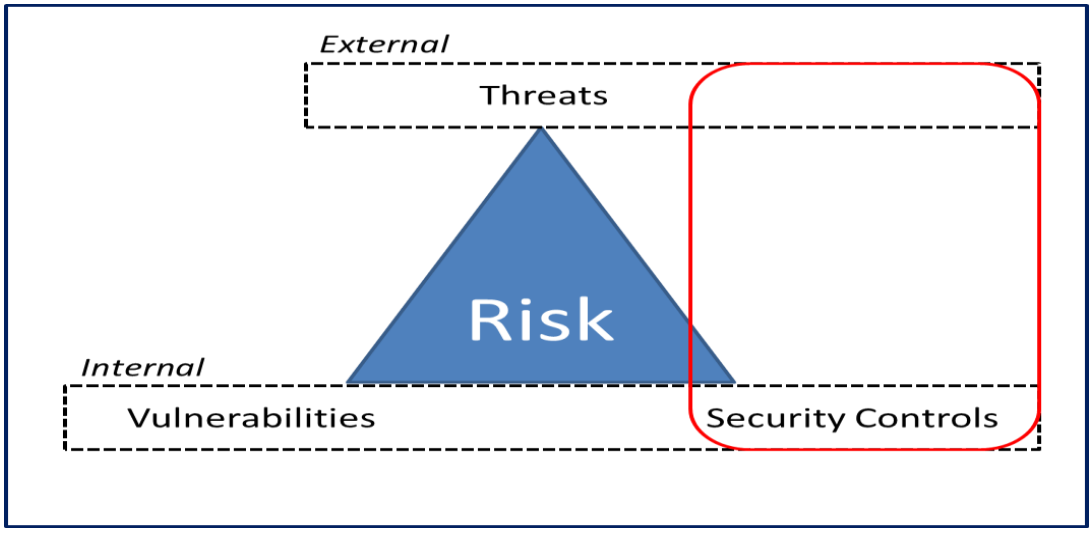


Figure 2.2 Triangle of risk in computer/cyber systems (Raggad, 2010, p. 292)

2.3.2. Cyber security threats and typologies

2.3.2.1. Threat sources and origins

Cyber threat sources include disaffected employees, investigative journalists, cybercriminals, extremist organisations, hacktivists, organised crime groups, and foreign intelligence services (ITU, 2011). Among them, sources that attempt to target SMEs are employees, cybercriminals and organised crime groups. These sources engage in their cybercriminal activities to pursue economic gains or to express their hatred against an employer. Compared to them, other sources (i.e., investigative journalists, extremist organisations, hacktivists, and foreign intelligence services) are motivated to attain political or social causes.

Cyber security threats can be divided into two types depending on origins of threats: (1) internal threats and (2) external threats. Previous research on cyber security did not pay much attention to insider threats compared to external threats (Jang-Jaccard & Nepal, 2014). Internal threats refer to an intentional misuse of information systems by employees who have authorised access rights. This type of threat is based on the assumption that humans are the weakest link in cyber security management (Guo, Yuan,

Archer, & Connelly, 2011; Ifinedo, 2014; Warkentin & Willison, 2009). Employees have malicious intentions for various reasons, such as disgruntlement at an employer, pecuniary motives or antagonism of corporate values. Misuse behaviour includes pure sabotage, stealing business or customer information, and knowingly participating in the outsiders' commission of a cybercrime. It is challenging to defend against insider attacks in that insiders take advantage of their access privileges already acquired for legitimate uses (Jang-Jaccard & Nepal, 2014). These are a form of deviant behaviour in the workplace, which provides a reason why criminology theories can be useful in understanding insider threats (Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Theories, such as general deterrence theory, social bond theory, and social learning theory, have been suggested to explain insider misuse of information systems.

Secondly, external threats are posed by an entity outside the security perimeter. Outside attackers refer to all groups of cyber attackers after excluding insiders. Gehem, Usanov, Frinking and Rademaker (2015) noted that most cyber-attacks derive from outside the organisation. IBM (2014) reported that in 2013 over half (56%) of attacks came from outsiders and less than a fifth (17%) of attacks emanated from insiders. They use various threat tools and techniques[9] to infiltrate targeted computer system. Among them, malware (e.g., worms, spyware, and ransomware) has been found as one of the prevalent cyber threats to individuals, businesses and public sector organisations (Choo, 2011; Jang-Jaccard & Nepal, 2014). In 2016, 357 million unique malware variants were detected for the first time and a large volume of malware was distributed via email (Symantec, 2017). However, clear division between insider and outsider threats gets blurred. Around a fifth (22%) of cyber-attacks is committed through cooperation between outsiders and insiders (IBM, 2014). This malicious cooperation has a potential for exacerbating victimisation situations by expediting an attack process or raising its success rate.

9 Frequently used tools and techniques are malware, spam phishing, (D)Dos, theft and physical damage, espionage, defacement, targeted attack, ransomware, and web app attacks (Gehem et al., 2015).

2.3.2.2. Typologies of cyber threats

Threats in cyberspace can be classified by various formats depending on perpetrators, victims, modus operandi and damage. A researcher with different research orientation tends to use a different typology. There are no unified sets of typologies which are accepted by the majority of cyber security researchers. Nye (2010) suggested four types of cyber threats to national security: cyber terrorism, cyber war, cybercrime and economic espionage. Cyber war is an array of hostile activities in cyberspace against an enemy state by a nation or its agents by using information technologies. Defending against cyber war is related to international law, being different from criminal investigation and prosecution by domestic law. Unlike the other three types, cyber war is out of the purview of this research.

Cyber terrorism was first termed by Barry Collin (1997) in the 1980s. The term has been commonly used by various entities in society, such as academics, policy makers, and media. Mass media is considered the main driver of the popular usage of the term, using this term to capture any sort of large scale cyber-attack cases (Conway, 2008). Mass media tends to overhype stories and events to create media sensation. In this respect, the term, *terrorism*, is preferred by media due to a high level of fear and violence attached to it. These days, cyber terrorism has become an overused term without consideration of the attributes and characteristics it carries. Hoffman (2006, p. 40) suggested five major criteria of terrorism: (1) political aims and motives, (2) violence or threatened violence, (3) planned to entail long-term psychological repercussions beyond the immediate victim or targets, (4) executed by an organisation with a chain of command or conspiratorial cell structure or by (a small collection) of individuals influenced by ideological aims, and (5) committed by a subnational group or non-state entity. If these traditional criteria are applied to cyber terrorism, it can be defined as illegitimate attacks or threats to violence against computers, electronic networks and digital information by a non-state or subnational group for its political or social aims. However, cyber terrorism is a form of abusing information technologies and it can be

understood as a subset of cybercrime. Criminal justice departments deal with cyber terrorist attacks not as a new type of cyber-attacks, but as part of cybercrime (Jang, 2014, p. 34). It is of importance to note that cyber terrorism and cybercrime are not mutually exclusive concepts.

The proliferation of electronically stored information has created more opportunities to steal digitised information. Economic espionage refers to the act of acquiring trade secrets from domestic companies or government entities to benefit a foreign state (Danielson, 2009). It is carried out to satisfy a nation's economic interests, which are considered a crucial dimension of its national security. As opposed to this, industrial espionage is a misappropriation of trade secrets, perpetrated by private entities for economic gain. However, there is some overlap between these two concepts and their usage by researchers is not consistent (Nasheri, 2005, p. 13). In reality, it is not easy to distinguish these two in that attribution of any cyber-attacks is extremely difficult. Both types of espionage escalate tensions between nations and discourage business motivation for technological innovation. Therefore, there are serious reasons that government has to intervene. It is predominantly the US corporations that are targeted most because they invest more resources in Research and Development (R&D) (Tucker, 1997). Due to the damaging effects of espionage, the US set up the Economic Espionage Act of 1996. This Act criminalises two forms of trade secret theft: theft for the benefit of a foreign entity (economic espionage) and theft for pecuniary gain (industrial espionage) (Doyle, 2016).

Cybercrime has been used as a generic term for describing crimes that occur in cyberspace. The term refers to "criminal or harmful activities that involve the acquisition or manipulation of information for gain" (Wall, 2007, p. 10), focusing on activities related to information. Due to its abstraction this definition is able to include a wide array of deviant behaviours in cyberspace, but it lacks cyber or technical concepts. In other words, what differentiates cybercrime from offline crime is not clearly touched upon.

Compared to the Wall's definition, Robinson et al. (2012) defined cybercrime as "a broad range of activities that involve the misuse of data, computer and information systems, and cyberspace for economic, personal or psychological gain" (p. 17). This definition points out the nature of activities in cyberspace in detail, incorporating cyber and technical elements. However, the term, *misuse*, is vague. This term needs to be defined clearly for application to real cases. In addition, this definition includes intentions of a perpetrator, but does not consider criminological perspectives involving criminogenic nature of activities and impact on victims. This can lead to a failure of a distinction between economic espionage and cybercrime. Understanding cybercrime varies greatly depending on the person who wants to define it. Policy makers, researchers or practitioners will have different approaches to comprehend cybercrime.

Table 2.3: Typology of cyber threats

	Actors	**Motivation**	**Law**	**Targets**	**Damage**
Cyber war	States	Hostility against an enemy state	International law	Government	Loss of state functions or military capacity
Cyber terrorism	States/ non-state entities	Political or social aims	Domestic law	Government/ Large businesses	Damage that leads to psychological impacts
Espion-age	States/ private entities	Economic interests	Domestic law	Government/ Businesses	Theft of national secrets /proprietary information
Cyber-crime	Private entities/ individuals	Economic/ personal/ psychological gain	Domestic law	Businesses/ Individuals	Financial/physical /psychological damage

A useful way of understanding cybercrime is categorising it. Due to its complex nature, it is difficult to identify categories of cybercrime by a single approach. The Council of Europe Cybercrime Convention (2001) suggested three categories, which are 'offences against the confidentiality, integrity and availability of computer data and systems' (Title One), 'computer-related offences' (Title Two) and 'content-related offences' (Title Three). The first category considers offence objects (i.e., computer data and systems), while the other two categories focus on the modus operandi of the offence (United Nations Office on Drugs and Crime, 2013). Based on this categorisation, specific acts which belong to each category are presented below (Table 2.4). However, cybercrime categories and acts which constitute cybercrime do not exist in a fixed format. They are changeable over time as newly developed information technologies reshape social interactions and human behaviours.

Table 2.4: Typology of cybercrime (United Nations Office on Drugs and Crime, 2013)

Categories	Acts
Acts against the confidentiality, integrity and availability of computer data or systems	• Illegal access to a computer system • Illegal access, interception or acquisition of computer data • Illegal interference with a computer system or computer data • Production, distribution or possession of computer misuse tools • Breach of privacy or data protection measures

Computer-related acts for personal or financial gain or harm	• Computer-related fraud or forgery • Computer-related identity offences • Computer-related copyright or trademark offences • Sending or controlling sending of Spam • Computer-related acts causing personal harm • Computer-related solicitation or 'grooming' of children
Computer content-related acts	• Computer-related acts involving hate speech • Computer-related production, distribution or possession of child pornography • Computer-related acts in support of terrorism offences

2.3.3. Cyber security risks against SMEs

Mobile devices, such as smartphones, laptops, and tablets are widely used in businesses. According to Osterman Research (2012), the use of personally owned mobile devices at work is a widespread phenomenon in organisations of all sizes. This movement is referred to as BYOD. BYOD allows employees to access corporate network and data for work via personal gadgets. Examples are accessing corporate e-mail accounts, systems, and internal documents. As employees are already familiar with the functionalities of their personal devices, BYOD enhances work efficiency and flexibility of users (Gajar, Ghosh, & Rai, 2013). For companies, allowing employees to use them for business is a good way to save costs and increase productivity (Gupta, Dhiman, & Sangroha, 2013). Small companies which lack enough resources are the main beneficiaries. Therefore, they are more likely to allow employees to use their personal mobile devices at work.

The sheer number of devices used at work represents the extent of connectivity in business environments. The widespread adoption of mobile devices at work gives more challenges to businesses, posing new security threats to the safety of businesses and their customer information (Gajar et al., 2013). As an increasing number of end-point devices are connected to the corporate network, it is a new challenge for a company to control all the operating systems and applications of employees' mobile devices. An IT team needs to ensure that the connected devices are secure in order to protect data assets and network integrity. Small companies are vulnerable to security risks from BYOD due to their unpreparedness (Madzima, Moyo, & Abdullah, 2014), whereas large companies have resources to adopt mobile device management and corresponding policies and procedures.

It is true that the adoption of new ICTs provides small companies with business advantages along with challenges mentioned above (Baek & Sohn, 2011). However, there is little research on the causes of security risks that they face. Questions such as "Are SMEs more vulnerable than large ones?" and "Where does the vulnerability originate from?" need to be addressed. Trim and Lee (2015) cautioned against applying the same assumptions about cyber security to businesses of all sizes, demanding a differential approach to small businesses. Although virtually all organisations house a risk and security function in any form, there is a discrepancy from each other based on organisational context (Borodzicz, 2005, p. 51). It is therefore of great importance to examine the organisational context of SMEs. Some studies (Gupta & Hammond, 2005; Truong, 2010) attempted to identify organisational factors which contribute to the vulnerability of SMEs in relation to cyber security.

Firstly, the size of an organisation is associated with various aspects of cyber security (Organ, 2015). In most cases, the number of employees and the volume of assets increase proportionately. When it comes to cyber security, a large company is more likely to use risk assessment tools (Bauer & Dutton, 2015) or to accept cyber security management (Chang & Ho, 2006; Kwon & Kim, 2017) by tapping into its specialists and

financial resources. On the contrary, small companies do not have sufficient supportive resources (i.e., IT specialists, budgets, software and hardware) to address cyber security threats (Bauer & Dutton, 2015; Harris & Patten, 2014; Kwon & Kim, 2017; Singh et al., 2013; Truong, 2010). This makes small companies unequipped and unprepared. Gupta and Hammond (2005) asserted that there was a significant difference in countermeasures between large companies and small ones. For example, in the case of cloud computing, a large company is capable of managing cloud-related risks with the support of sophisticated risk management and experienced IT teams (Brender & Markov, 2013; Organ, 2015). Some small owners who are aware of these risks are hesitant to adopt cloud computing in spite of its potential benefits due to privacy, security, and data integrity reasons (Truong, 2010).

Secondly, decision-making dynamics in small companies are highly leveraged by the owners (Blackburn, 2012; Herbane, 2010). Large companies have a hierarchical structure with several layers of management to manage resources efficiently (Ghobadian & Gallear, 1997). Their decision-making is undertaken through functional departments (e.g., marketing, finance, accounting, human resource, and IT). Though top-level strategic decisions are conducted by a CEO or board members, most of the functional and operational decisions derive from managers. Therefore, decision-making is carried out via known, formal, and hierarchical channels. However, small companies have a relatively flat organisational structure with an absence of bureaucracy (Levy & Powell, 2005). Their management structure is not formalised and changeable based on organisational and external influences. This structure may bring in more flexibility, but the downside is that this can produce overly reactive and short-term decisions (Grant et al., 2014). In fact, SMEs' decision-making mechanisms are dominated by few decision-makers (Ghobadian & Gallear, 1997). Decision-making mechanisms are centralised and dependent upon the owners (Blackburn, 2012). In this case, knowledge and attitude of the owners and senior managers are greatly important factors to produce effective decisions.

However, SME owners and managers had an insufficient understanding of the security risks and were not aware of possible measures to mitigate the risks (Harris & Patten, 2014). The owners therefore were not capable of undertaking an intensive evaluation of cyber security decisions. This can pose a serious challenge against SMEs in that professional competencies are not available to them. Herbane (2010) stated that when it comes to risks, small owners were more concerned about financial risks or profits, and that risk assessment itself was subjective because of the strong influence of ownership over management. He also asserted that the framing of risks was not research-based or data-driven, but based on the owner's experience and knowledge derived from informal networks. In addition, preoccupation with daily issues made owners demonstrate a lack of concern towards security issues (Bhattacharya, 2011). These justify why business owners need to be educated on cyber security risks. Dojkovski, Lichtenstein, and Warren (2007) argued that external initiatives such as awareness programmes and scenario-based approaches were needed to foster business owner support.

For businesses, cybercrime is a potential source of security risk that could have a disruptive impact. Cybercrime can be a reliable proxy measure of cyber security threats although cybercrime rates cannot represent all potential risks. In the UK, cybercrime has been measured recently due to the growing concern of increasing criminal activities in cyberspace. The Office for National Statistics published the first estimates of the UK level of cybercrime in June 2015. In the following year, the crime survey estimated that the number of cybercrime offences was about 2 million and the number of online fraud cases was about 3.6 million in the 12 months (Office for National Statistics, 2017). The survey also highlighted that traditional or offline crimes were about 6.2 million total offenses[10] and this figure was on the downward trend. All these figures represented that online crimes occurred on the similar magnitude with offline crimes (5.6 million versus 6.2 million cases). The sheer volume of the estimated online fraud and computer misuse figures were staggering. The scale and severity of cyber fraud were significantly larger than expected. Common types of cyber fraud were bank and credit account/card

10 This figure did not include cyber fraud and cybercrime, which were published separately.

fraud, theft of personal information on bank accounts, misuse of credit card details, along with online shopping scams.

Table 2.5: Fraud and cybercrime statistics (Office for National Statistics, 2017)

Crime classification	Total cases (thousand)	Occurrence rate (per 1,000 adults)
Fraud	3,617	79
Bank and credit account fraud	2,452	53
Non-investment fraud	939	20
Advance fee fraud	118	3
Other fraud	108	2
Computer misuse	1,966	43
Computer virus	1,300	28
Unauthorised access to personal information (including hacking)	667	14

According to the Cyber Security Breaches Survey (Department for Digital, Culture, Media and Sport, 2018), nearly 47% of small businesses and 64% of medium businesses in the UK suffered a security breach in the past 12 months. The survey also suggested a large discrepancy in breach cost by business size. The average breach cost estimates were higher among medium and large businesses compared to small businesses. Across all breaches, micro/small businesses' mean cost was estimated to be £894, while medium businesses' mean cost was calculated as £8,180. These UK survey results indicate that SMEs were targeted by cybercriminals and that the damage was serious enough to merit further attention. A security breach could cause problems including minor inconvenience, reputational damage, loss of customer data, fines, and, in the worst case, company closure. Damage from a breach may have more serious consequences on SMEs than large corporations because SMEs generally have no emergency recovery plans and capacity to mitigate the damage.

2.4. Cyber security risk management frameworks

Risk management is referred to as a series of activities of controlling risk within its acceptable level (Raggad, 2010). Cyber security management is not just a selection of security controls. A one dimensional process posits that there is a simple causality or relationship when it comes to decision-making. However, cyber security management involves a series of decision-making processes to select, implement, and maintain the proper controls. Security threats change over time and supportive resources are limited. Therefore, there is no hard and fast rule regarding an evaluation of effective security activities. In this respect, cyber security management is seen as a multi-dimensional decision-making process rather than the one-dimensional process in this study.

There are a wide range of variations of risk management frameworks and how they should be defined. Such frameworks are proposed by government organisations (e.g., National Institute of Standards and Technology [NIST] and National Aeronautics and Space Administration), international organisations (e.g., European Union Agency for Network and Information Security [ENISA]), or international professional associations (e.g., ISACA [11]) as well as prominent scholars (e.g., Raggad). In this section, four representative risk management frameworks are suggested.

Raggad (2010) suggested a risk management life cycle which consists of:

(1) risk planning,
(2) risk analysis,
(3) risk treatment and
(4) risk monitoring.

11 It was recently announced that ISACA uses its acronym only, although it was previously known as the 'Information Systems Audit and Control Association'. (see: http://www.isaca.org /about-isaca/Pages/default.aspx)

Risk planning involves developing a preparatory strategy which covers identifying risk and assets involved and determining a set of available responses. Secondly, risk analysis includes risk identification and risk assessment. Risk can be identified via various methods such as vulnerability or threat analysis, event tree analysis, and attack trees. These methods intend to identify risk, but using different concepts (i.e., vulnerability, threat, or attack). Upon identification, risk is assessed through determining the level of risk and the potential impact of the risk. A technique that is widely used is a risk matrix. It calculates risk criticality of each asset by measuring the likelihood and impact of the risk involved. Risk assessment is useful to prioritise treatment efforts and to measure expected benefits resulting from the treatment against the risk impact. These two sub-stages refine the nature of risk events and consequences of them. Thirdly, risk treatment involves the implementation of security controls. Decisions on what sort of security controls will be taken, how, and when to take them depend on the risk involved because this phase aims to maintain the identified risks to acceptable levels. The last phase is risk monitoring. Risk needs to be continuously monitored as existing risks change and new ones appear. This process evaluates whether risk is properly under control by revisiting the prior phases. The whole phases constitute an iterative process as is described as 'life cycle'. This life cycle is a continuing process that needs to reflect the internal and external dynamics of an organisation as well as the changing nature of security risks.

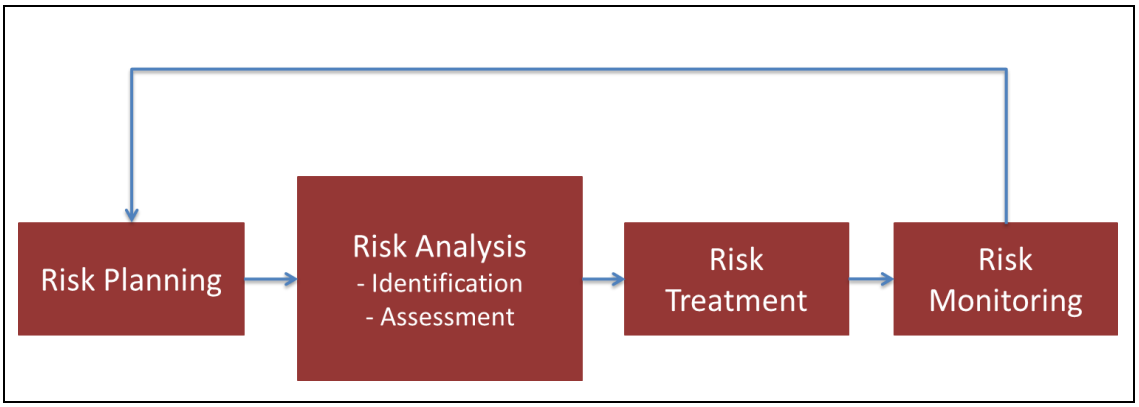


Figure 2.3 Raggad's risk management life cycle (Raggad, 2010)

A COBIT 5[12] framework from ISACA (2013) consists of similar phases to the Raggad's risk management life cycle. It includes:

(1) risk identification,
(2) risk assessment,
(3) risk response and
(4) risk monitoring and reporting.

Techniques and methods from the Raggad's framework can also be used in most of the phases here. However, there are some subtle differences. One is an emphasis on risk reporting. Risk analysis needs to be reported to managers and owners in order to support their decision-making. From practitioners' point of view, internal reporting of risk is a crucial reflection of whether senior management accepts cyber security as a priority.

The third phase, risk response, is the same concept with risk treatment in the Raggad's framework. It refers to acting upon the identified risks, aiming to align the residual risks within acceptable tolerance. There are four strategies: (1) acceptance, (2) transfer, (3) mitigation, and (4) avoidance. Risk appetite is the amount of risk that an organisation is willing to accept without acting upon it. If risk is below risk appetite, the risk will be accepted. Risk can be transferred to or shared with a third party organisation (e.g., purchasing insurance, outsourcing to other organisations, or using cloud computing). Also, risk can be mitigated by deploying security controls (e.g., access control policies, firewall or recovery plans). The most drastic strategy is risk avoidance. Risk can be avoided by shutting down a part of IT system which exposes vulnerabilities or risks in question. Although these strategies are explained in the book by Raggad (2010, p. 305), they are not indicated as strategies for risk treatment.

12 COBIT 5 is a framework for the cyber security governance and management of businesses.

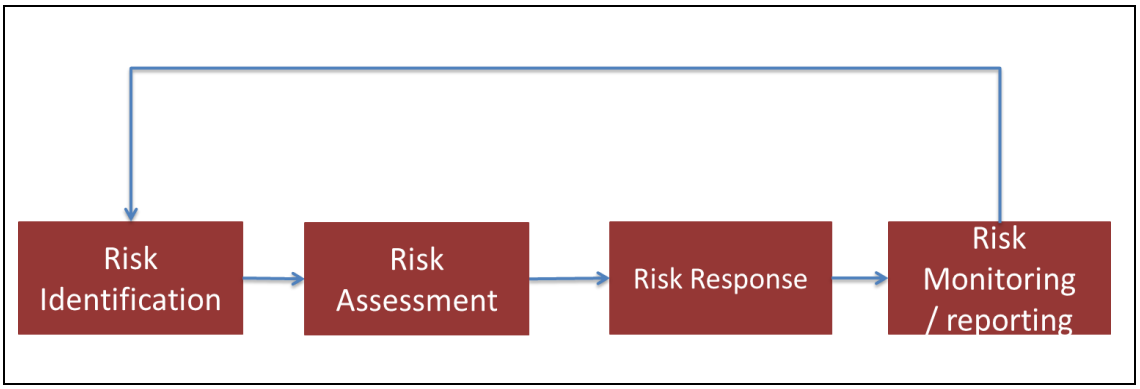


Figure 2.4 ISACA's risk management life cycle (ISACA, 2013)

NIST's framework is also based on a risk approach. It involves the management of organisational risk in relation to information system. It consists of six steps (NIST, 2017, pp. 9-10):

> (1) it starts by categorising information and its system based upon an impact analysis,
> (2) select a set of control baseline and adjust it based on risk assessment and organisational conditions,
> (3) implement the security controls and document how the controls are deployed,
> (4) assess the security controls using appropriate procedures,
> (5) authorise the information system operation based upon a determination of the risk and
> (6) monitor the selected controls in the information system on a regular basis.

This framework is constructed as part of an organisation-wide risk management approach (NIST, 2017), putting emphasis on strong engagement of organisational resources. Risk concerns are dealt with at three levels: (1) organisation level, (2) mission/business process level, and (3) information system level. This approach requires risk management to be combined into organisation management. In contrast to other frameworks which predominantly focus on aspects of risk, this framework extends the scope of risk management. First and foremost, it involves a successful execution of risk

management. Methods and processes of undertaking risk management are developed in line with organisation management aspects, such as cost-effectiveness, business missions, business success, and organisational structure. Secondly, this framework aims to protect not only information assets, but also individuals. Impacts or consequences of risks against individuals are concerned in this framework.

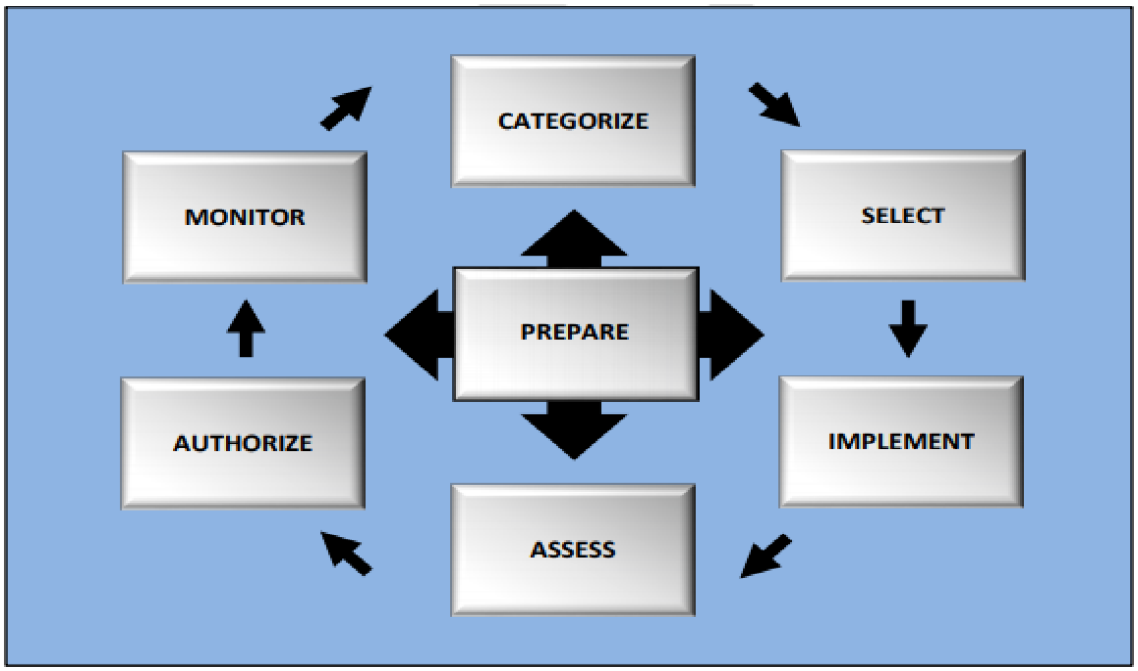


Figure 2.5 NIST's risk management framework (NIST, 2017, p. 10)

A risk management framework by ENISA (2006) is quite similar to the first two frameworks aforementioned in terms of constituting phases. However, it is distinctive in that this framework acknowledges risk assessment as a significant part of risk management. Risk assessment is perpendicular to several risk management phases (see: Figure 2.6). This shows that risk assessment is carried out at discrete time points (e.g., quarterly or yearly) to evaluate current risk (ENISA, 2006). One important common feature of all the frameworks is that they are presented as iterative processes without an end point.

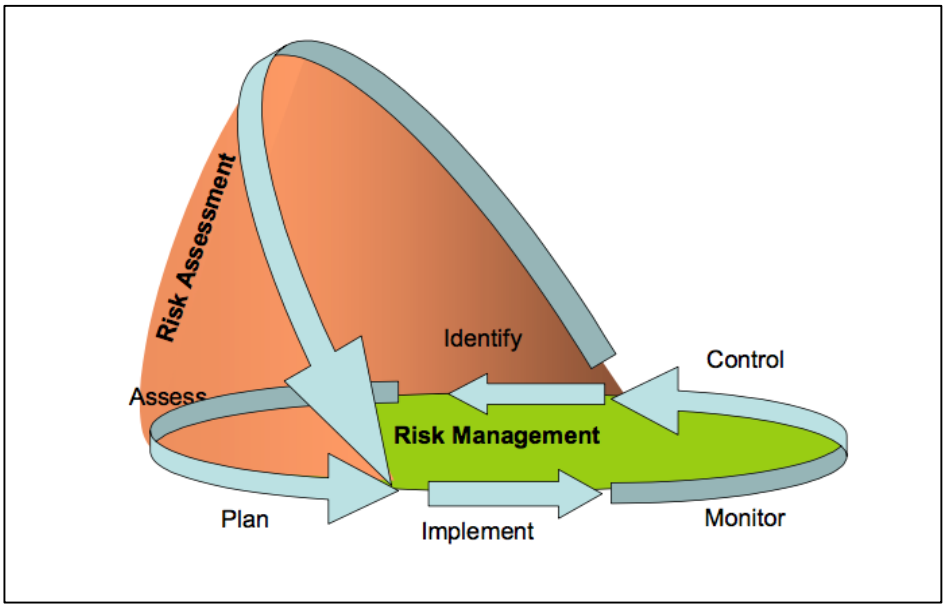


Figure 2.6 ENISA's risk management framework (ENISA, 2006, p. 6)

2.5. Management of cyber security and organisational behaviours

2.5.1. Cyber security management measures

Cyber security risk originates from the deep infiltration of IT systems and devices into business activities. This creates a management environment in which cyber security is no longer confined to an IT department, but requires senior management attention (Lee, 2013). It implies that cyber security should be accepted as one of the management priorities that senior managers are aware of. In this respect, it is highly recommended for cyber security professionals to have competent business and management skills (Rainer Jr, Marshall, Knapp, & Montgomery, 2007). This approach argues that cyber security should be considered in a management context (Chang & Ho, 2006; Singh et al, 2013; Soomro et al., 2016), becoming core part of business management. This argument is in line with Borodzicz and Gibson's (2006) claim that management of risk and security ought to be considered as part of mainstream business management. It is therefore worth looking at how cyber security can be intermingled with business management.

2.5.1.1. Security policy

Security policy outlines what kind of security controls a company adopts and how they should be implemented, providing a direction and support to cyber security activities. Security policy theorists argue that cyber security policy should be established, implemented, and maintained (Hong, Chi, Chao, & Tang, 2003). Creating a policy that reflects both internal and external contexts is just the start of cyber security management. Establishment of policy requires management concern and support toward cyber security. Policy should be formulated first, but implementation of it cannot be overemphasised. It is of importance for employees to realise the significance of abiding by the policy. Once security policy is adopted, execution of the policy is in the hands of employees. One keen interest is how to encourage employees to increase their compliance with cyber security policies.

It is argued that cyber security awareness and training are significant factors to raise policy compliance (Soomro et al., 2016). Siponen, Mahmood, and Pahnila (2014) argued that awareness of employees positively influenced their compliance with security policy, and it is also noted that a training program had a positive impact on employees' compliance behaviour (Albrechtsen & Hovden, 2010; Puhakainen & Siponen, 2010). Siponen et al. (2014) further emphasized the role of senior managers in that they were primary facilitators for raising employee awareness. At the same time, senior managers need to ponder over how to communicate the policy to end users in a company in order to properly implement it. Managerial intervention is an effective measure to make employees perceive vulnerability and severity of cyber security threats**.** Several scholars (Doherty, Anastasakis, & Fulford, 2009; Singh et al., 2013) claimed that an existence of policy had a causal impact on the effectiveness of cyber security.

As new technologies are introduced, a policy needs to be changed accordingly. It is important to review the policy regularly with the changing business environments (Singh et al., 2013). This is because every new technology has its own security weaknesses

along with business benefits. For example, BYOD and cloud computing have gained widespread adoption by SMEs quite recently. Once adopted, they need to be included in the scope of the policy. In addition, companies need to ensure that their subcontractors and consultants are covered by the policy. It is especially true when computer servers of the subcontractors and consultants are foreign-based. Companies need to make sure of two things: (1) the servers are physically safe from natural and man-made disasters; and (2) they are embedded in secure network environments. The same argument can be applied to cloud computing services. How to control new technologies and services provided by third parties is a continuous challenge when it comes to a cyber security management policy.

2.5.1.2. Senior management support and responsibilities

It is of vital importance to ensure that senior managers in the business support an agenda (Aleem et al., 2013), and this is also the case with cyber security management. Cyber security management cannot be effective without support from senior management (Choi, Jeong, & Kim, 2014). In a business, plans and policies are manifestations of various aspects of cyber security management. It is senior management that can launch those plans and policies in a balanced and comprehensive way (Dutta & McCrohan, 2002). It is important for senior management to accept the idea that cyber security is not a technical issue any more but a business one (Kayworth & Whitten, 2010). A prerequisite for gaining this support is the change of viewpoint regarding cyber security, which means that cyber security strategies are required to be aligned with business objectives and needs. If cyber security is not adequately interpreted in business terms, it is hard to elicit support from senior managers who are familiar with business language. In this respect, cyber security risks should be quantified to measure their effects on corporate assets and share price. This is a good way of demonstrating that cyber security contributes to business performances. As evidence of this, a Korean study argued that perceptions of top management on cyber security increased business performances and competitiveness (Choi et al., 2014).

One way to institutionalise senior management support is to make some members responsible for cyber security. Assigning responsibility to a person or group is generally known to elicit more effective results in business management (Mitchell, 1993). It is an official announcement of an organisation which conveys its willingness to address associated situations. Likewise, designating cyber security responsibility to senior management will be recognised as a strong declaration for its focus on cyber security. In the hacking case of Hyundai Capital in South Korea, a lack of senior management support was pointed out as one of the crucial loopholes (Lee, 2013). A UK survey by Department for Digital, Culture, Media and Sport (2017) found that less than a third (29%) of UK businesses had board members with responsibility for cyber security. Also, there was a large gap across business sectors. Board-level responsibility was most common in the finance and insurance sector (54%).

2.5.1.3. Staff training / awareness programme

Internal training and education aim to achieve two objectives: (1) How to prevent and minimise insider threat (i.e., human deficiencies) and (2) How to encourage employees' positive attitude and behaviour (i.e., human efficiencies). This perspective posits that security breaches stem from employees' either intentional or unintentional attitudes (e.g., ignorance, resistance, apathy, and negligence). Thus, to attain behavioural change among employees, their attitude must change first. Considering that insiders can normally have access to the entire network from their end devices, their malicious activities pose a greater threat to cyber security (Warkentin & Willison, 2009) (see: Section 2.3.2.1).

Recent literature considered whether training and education had a causal impact on the increase of attitude and behaviour of employees. Albrechtsen and Hovden (2010) argued that small-scale workshops effectively improved security awareness and behaviour of employees. Continuing in this vein, Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) reported that both training and education positively

influenced employees' attitude and behaviour regarding cyber security policy. Using the Theory of Planned Behaviour, Safa et al. (2015) pointed out that training improved employees' awareness. Sequentially, awareness improvement changed their attitude and, in turn, the attitude affected security care behaviour in a positive manner. International/national standards, such as ISO 27001[13], COBIT 5, and NIST 800 series[14] in a similar vein put emphasis on staff training. However, staff training was not widely used as a cyber security practice among SMEs in the UK. Only a quarter (25%) of small firms had staff attend training over the year, and the provision of training was commensurate with firm size (43% of medium firms and 63% of large firms) (Department for Digital, Culture, Media and Sport, 2017).

2.5.1.4. Risk management tools

As seen in Section 2.4, risk management aims to maintain risk at acceptable level, and measuring risk involves threats, asset values, vulnerabilities and security controls. Risk management theory posits that cyber security threats and vulnerabilities can be estimated and assessed (Hong et al., 2003). Assessment results inform what sort of security requirements and controls need to be adopted. Risk management is an iterative process which requires extensive resources.

Identifying risk is a first step. There are various ways of identifying risk, such as business-as-usual or ad-hoc health checks, internal audit, and threat intelligence (Department for Digital, Culture, Media and Sport, 2017). Among the management process, risk assessment is recognised as a core part of risk management (ENISA, 2006). To assess risk, lots of information is required in advance. Which assets are the threats against? What sort of vulnerabilities does a business have? What are values of assets? What is the current level of risk? Is it acceptable or not? Based on risk assessment results, a company

13 This is the best-known international standard which recommends a set of policies, procedures, documents and technology for managing cyber security.

14 This series is a collection of documents that include computer security policies, procedures, and guidelines of the US federal government.

makes a choice for efficient responses. Risk responses for mitigation include technical (e.g., access control, encryption, and intrusion detection system), managerial (e.g., policies and staff training), and operational controls (e.g., segregation of duties and limitation of permissions). Popular security controls that businesses chose are software updates, malware protection, firewalls, and data backup (Department for Digital, Culture, Media and Sport, 2017). There are a wide range of practices for the establishment of risk management processes. Therefore, it is of significance for businesses to find the most suitable form as they have different business structure and operate in a different sector.

International standards (e.g., ISO 27001 and COBIT 5) provide useful guidelines for preventing a business from security threats. ISO 27001: 2013 is the most widely accepted standard for cyber security management. It is claimed that this standard can be adopted in all types of businesses, irrespective of business size, sector, and nature (Candiwan, 2014). However, adopting an international standard requires devotion from business management because of high costs and the lengthy process involves.

2.5.1.5. Cyber insurance

Insurance is accepted as a means of hedging against potential risks. Businesses traditionally have relied on insurance to protect against economic, sociopolitical and natural risks. As modern businesses operate on a basis of the Internet or electronic networks, they are exposed to another risk, which is called cyber security risk. Cyber security scholars (Böhme & Schwartz, 2010; Bolot & Lelarge, 2009) approach insurance as a tool to address residual risk after business' risk reduction efforts. Internationally, there are a handful of insurance companies (e.g., American International Group, Lloyds, Fidelity, and J.S. Wurzler) which have put cyber security insurance on the market. Providing cyber-related insurance policies invokes different concerns from traditional ones (Gordon, Loeb, & Sohail, 2003). In particular, setting a realistic price for insurance products and high-risk businesses is difficult. Since only known risks are covered by

insurance (Borodzicz, 2005, p. 4), a lack of historical records involving cybercrime is a great problem (Gordon et al., 2003). In addition, technological elements add more complexities. How to consider ever-evolving technologies when creating actuarial tables is not a straightforward process; this may explain why academic research on cyber insurance is so limited (Öğüt et al., 2011).

A business survey by Department for Digital, Culture, Media and Sport (2017) found that around two fifth (38%) of firms said they had insurance which covered a cyber security breach or attack. However, only two among 671 businesses filed a claim on this policy. The low claim rate compared to a higher breach rate (46%) indicates whether firms were not aware of their victimisation or whether they were not well acquainted with the insurance policy. A qualitative study in the survey revealed that it took over a year for a micro business to make a cyber insurance claim and a senior director from the business described the claiming process as stressful.

2.5.2. A balanced approach to security controls

Technical solutions at operational level have been emphasized in dealing with the cyber security challenges (Singh et al., 2013). In the early era of research, researchers from computer science focused on developing and configuring technical security measures to improve operational levels of detection and protection. This trend was reasonable in that technical elements are the core parts when it comes to cyber security. As the literature on technical aspects of cyber security management increased, deploying technical controls for detection and mitigation became the suitable solution. Technical controls, such as network security (e.g., firewall, Intrusion Detection System), data protection (e.g., encryption), and access controls (e.g., biometrics), were proposed as feasible measures to prevent security breaches. Thus far, companies adopted technology-oriented security strategies in designing safe business environment, stressing the principal role of technology (Siponen, 2005). However, despite the

advancement of technical controls, the frequency and severity of cyber security breaches continued to rise.

The complexity of technology is one of the biggest challenges not only for security practitioners but also for senior managers who make decisions on cyber security management (Werlinger et al., 2009). Without proper knowledge of technology, it is very hard to understand the nature of cyber threats. To make matters worse, if senior managers do not have enough understanding of technology, management decisions might be misaligned with the configurations of technical systems.

Against this backdrop, a broader approach was needed. Recent studies (Baek & Sohn, 2011; Furnell & Clarke, 2012; Herath & Rao, 2009; Parsons et al., 2014; Rhee et al., 2012; Safa et al., 2015; Safa et al., 2016) reported that technology alone could not deliver satisfactory solutions to security breaches. Along with technical controls, managerial support and human behaviour were proposed to be taken into consideration, and these are now examined in more detail.

How much a company values management agendas is reflected in resource allocation and organisational structure. If cyber security is deemed as one of management priorities, a reasonable amount of resources needs to be appropriated for it and there needs to be an IT team or professional staff. Employees with IT expertise are needed to handle technical security measures. Their training needs to be refreshed on a regular basis to keep track of ongoing cyber security issues. In the same way, technological systems and gadgets also need to be regularly updated. From the business management point of view, it is not straightforward to decide how much resources need to be provided for efficient cyber security management. Furthermore, SMEs do not have sufficient resources to put into cyber security management. Considering the importance of SMEs in the economy, the lack of available internal resources necessitates other forms of support such as business-wide initiatives, cooperation between companies, and government support.

There are two schools of thought in regard to human factors in an organisation. The first one considers people a significant part of a security problem or the weakest link (Guo et al., 2011; Ifinedo, 2014; Warkentin & Willison, 2009). It is the human behaviour that leaves computer systems vulnerable from malicious viruses and worms. This perspective evolves around how to efficiently control both intended and unintended human behaviours. On the other hand, other studies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Furnell & Clarke, 2012; Spears & Barki, 2010) recognised that people were not a cause of the problem, but one of the most important controls in an organisation. Rhee et al. (2012) argued that it was necessary to include human factors in cyber security management along with technical dimensions. This perspective is based on the assumption that humans actually deploy, configure, and maintain technology systems after an organisation adopts technical controls through managerial decisions. Thus, it is of vital importance to understand employees' attitude and behaviour on cyber security for successful implementation of policies and procedures. However, it is not reasonable to take a dichotomous approach to human factors. In fact, humans make errors, but also correct problems at the same time. It is equally important to understand the advantages and disadvantages of human factors. How to view the role of humans in relation to cyber security management is dependent upon the perspective of a researcher.

Numerous studies have been carried out to comprehend human-computer interactions in relation to cyber security. Improving individual attitude and behaviour was recognised as one of the effective methods of enhancing cyber security (Baek & Sohn, 2011; Crossler et al., 2013; Li, Zhang, & Sarathy, 2010). The primary concern was to identify determining factors that have a positive impact on compliant perceptions and behaviours of end users (Dinev & Hu, 2007; Johnston & Warkentin, 2010; Safa et al., 2015; Safa et al., 2016). Safa et al. (2015) found that security awareness, policy, experience and involvement, attitudes, subjective norms, threat appraisal, and self-efficacy positively influenced users' behaviour. Based on social bond theory and involvement theory, Safa et al. (2016) argued that knowledge sharing, collaboration, intervention, experience, commitment, and personal norms had a significant influence on employees' attitude. In relation to risk

perception, Johnston & Warkentin (2010) found that fear appeals had a positive impact on changing end users' behavioural intentions. This study provided security managers with the practical insight that fear-inducing communications could be customised based on perceptions of end users. Unlike these studies, Baek and Sohn (2011) studied the impact of security awareness and behaviour on security performance in Korean SMEs, and identified a positive influence.

Some studies (Kayworth & Whitten, 2010; Young & Windsor, 2010) approached cyber security through integrating managerial and technical processes. Kayworth and Whitten (2010) argued that a combination of technical competence and socio-organisational factors made it more possible to ensure effective cyber security, while Young and Windsor (2010) found out that integrating cyber security and business planning processes efficiently and effectively protected information assets.

Taking a more holistic approach, some studies (Singh et al., 2013; Singh et al., 2014; Werlinger et al., 2009) suggested that management and human aspects are crucial elements, along with technology, in establishing a cyber security management system. Those studies took a different perspective on technological, managerial, and human factors. First, Singh et al. (2013) viewed them as controls that could be managed by a company. Secondly, Werlinger et al. (2009) and Singh et al. (2014) regarded them as challenges that created difficulty implementing security controls. Despite the different perspectives, a commonality is that those studies took an integrated view of technological, managerial, and human factors in cyber security management.

The balanced approach has become important as people have realised that technical aspects cannot be the sole solution to security breaches. Technical, managerial, and human controls are indispensable elements to form an effective system. However, finding an optimum point in the combination of these controls may vary according to the context in which a company is positioned as well as the goals and strategies of the company. Regardless of circumstantial differences, the adoption and maintenance of

cyber security management, based on the balanced approach, could be the fundamental basis of ensuring survivability of a company. More studies need to be performed concerning the relationships and interplay of these controls.

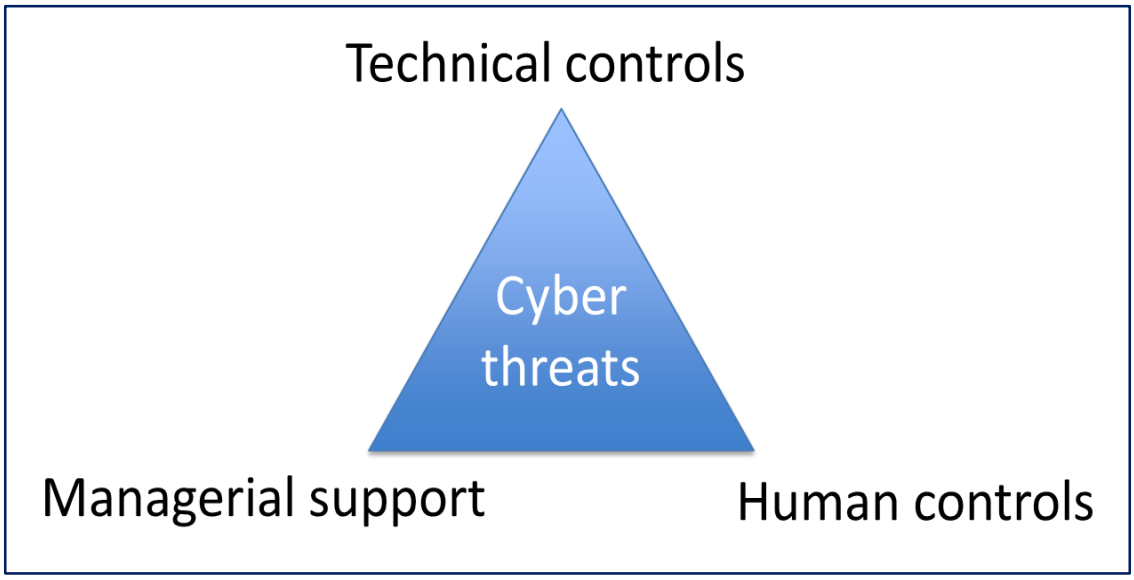


Figure 2.7 Three components of a balanced approach to cyber threats

2.5.3. Knowledge for risk reduction

Knowledge is "the theoretical or practical understanding of a subject, fact, information, value, or skill achieved through education or experience" (Safa et al., 2016, p. 72). It is an invaluable asset that can bring a competitive edge to businesses by supporting cost reduction, asset distribution and decision-making processes. In knowledge management, making the best use of knowledge is to share it (Wang & Noe, 2010). Knowledge sharing needs to be emphasised in cyber security in that any employee without a proper knowledge can be a weakest point from cyber threats. Cyber security knowledge sharing is of significance in raising users' awareness as well as reducing cyber security risks (Safa et al., 2016).

There is a great body of studies which address the relationship between knowledge and risk mitigation (Arachchilage & Love, 2014; Asgharpour, Liu, & Camp, 2007; Ben-Asher

& Gonzalez, 2015; Cranor, 2008; Han & Yoo, 2016; Parsons et al., 2015). Several studies noted that knowledge had a positive impact on various dimensions of cyber threats. Arachchilage and Love (2014) found that the combination of conceptual and procedural knowledge positively influenced phishing threat avoidance behaviour. Evaluating the role of knowledge on threat detection, Ben-Asher and Gonzalez (2015) found that cyber security knowledge increased correct detection of malicious attacks. They argued that threat detection was the dimension that knowledge could be taken advantage of. However, there is another aspect which requires consideration. The causal relationship between knowledge and risk mitigation is facilitated through decision-making processes (Ben-Asher & Gonzalez, 2015). In other words, risk mitigation is a desirable result of the decision-making process which is conditioned by knowledge. For example, more knowledge of security policies is related to behavioural compliance to those policies (Parsons et al., 2014). This is why knowledge is recognised as an indispensable element in making risk-reducing decisions (Cranor, 2008). From a slightly different aspect, it was argued that cyber security knowledge by top management could mitigate risks by changing perceptions and behaviours of employees (Han & Yoo, 2016).

Other studies focused on a disparity between individuals with knowledge (e.g., cyber security experts) and those without knowledge (e.g., business managers and general employees). Cyber security experts in general are aware of the nature of risks and threats and technical elements of their IT environments. Therefore these experts are expected to make better decisions than inexperienced ones (Ben-Asher & Gonzalez, 2015).

Asgharpour et al. (2007) studied psychological aspects of the relationship between computer security knowledge and risk management. The authors suggested that individuals with knowledge had different mental models from non-experts. Furthermore, they went on to argue that the gap between mental models of experts and non-experts caused risk miscommunication, which led to ineffective risk management. A mental model is a cognitive conception on real interactions and events around a person

(Morgan, Fischhoff, Bostrom, & Atman, 2002). Knowledge governs a formation of a mental model, which in turn influences decision-makings. If an input-output analysis is applied, an extent of knowledge as an input will generate different outcomes (e.g., security controls or policies) though the mental model and decision-making process.

The studies above imply that there is a considerable gap between cyber security professionals and laymen on the level of knowledge, decision-making, and approaches to risk management. This knowledge gap has led cyber security professionals and business managers to become concerned with a different set of important issues. Rainer Jr et al. (2007) found that business managers focused on managerial-oriented issues, such as backup and recovery, business continuity planning, and access controls, whereas cyber security professionals attended to technological-oriented issues, such as firewalls, layered defence, and risk mitigation. The authors pointed out the importance of moving toward each other for effective cyber security management.

This raises a pressing question for cyber security management: What sort of cyber security management strategies or practices would be efficient to address this problem? To bridge the gap, cyber security management practices, such as awareness programmes and training, need to be provided to employees. However, these practices in reality are neither widely adopted nor well-structured for the long-term implementation. In the UK, a fifth of businesses (20%) have provided internal or external training on cyber security in the last 12 months and the provision of training centred on senior management (75%) and IT staff (43%) rather than general staff (31%) (Department for Digital, Culture, Media and Sport, 2017). More training for IT staff rather than general staff is not expected to reduce the knowledge gap. An existence of the gap gives a profound implication on cyber security management. The knowledge gap can lead to inefficient risk communication (Asgharpour et al., 2007), and this can be a cause for conflict between professionals and laymen.

2.5.4. Cyber security culture as an adaptation of organisational culture

It is argued that an effective cyber security culture has a significant influence on the management of cyber security (AlHogail & Mirza, 2014b; Mahfuth, Yussof, Baker, & Ali, 2017; Parsons et al., 2015). In a study by Knapp, Marshall, Rainer and Morrow (2004), organisational culture was identified as 7th key issue by 874 certified information security professionals. Cyber security culture is a certain form of organisational culture. Before examining the theoretical foundation of cyber security culture, organisational culture needs to be understood. There is a lack of consensus on the definition of culture as a concept (Pfeffer, 1997). Organisational culture has been attempted for conceptualisation from various aspects. Organisational culture can be seen as a set of criteria that distinguish one organisation from another (Robbins & Judge, 2013, p. 512) and as a mechanism that binds old and new members of the organisation together (Stroh, Northcraft, & Neale, 2002, p. 297). The organisational culture not only influences perceptions, behaviours, and decision-makings of employees (Parsons et al., 2015), but also it is shaped by them along with organisational visions, goals, and strategies.

Schein (2010) describes organisational culture as:

> "a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration, which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." (p. 18)

This definition emphasises patterning, integration, and shared learning experiences. What does culture imply? Culture has several characteristics, such as structural stability, depth, breadth, and integration (Schein, 2010, p. 16). Culture develops through a socialisation process and social learning over time. It is not a static concept, but rather a dynamic phenomenon (Borodzicz, 2005, p. 39). If shared assumptions exist in an organisation, culture can act as a mechanism of social control as new comers will be

taught through social interactions with older members. O'Reilly and Chatman's definition (1996, p. 160) is based on managerial perspectives, viewing culture as a form of organisational control. They define organisation culture as "a system of shared values (that define what is important) and norms that define appropriate attitudes and behaviours for organizational members (how to feel and behave)" (p. 160). They argue that a strong culture is maintained if the norms and values are "widely shared and strongly held throughout the organization" (p. 166).

A better way to understand culture is to decompose it into three levels: artefacts, values, and underlying assumptions (Schein, 2010, p. 24). Level one is artefacts, which are observable manifestations such as structures or processes. Language, technology and products are examples. Level two is espoused values. These are shared values which an organisation wants to uphold and pursue. Artefacts are visible manifestations of these values. Level three is underlying assumptions, which are based on unconscious perceptions and thoughts. Underlying assumptions are closely linked to one's cognitive and interpersonal worldview. These are formulated when a certain strategy or solution proves to be successful (Schein, 2010, p. 28). Upon the success of the strategy, related values behind the strategy are to be taken for granted, which become shared tactic assumptions.

As a subset of organisational culture, cyber security culture mirrors fundamental elements of organisational culture. As such, it is reasonable to theorise cyber security culture in relation to organisational culture. A cyber security culture evolves based on social interactions of employees as well as perception and behaviour that employees show within the context of cyber security. This is why most cyber security culture frameworks are adapted from organisational culture. In this research, a definition from Da Veiga and Eloff (2010) will be adopted for two reasons: (1) this reflects cyber security needs within the context of the organisational culture and (2) this is comprehensive enough to cover the large scope of this research. The following is the definition:

"the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e., incidents) evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets." (p. 198)

2.5.5. Cyber security culture frameworks

A cyber security culture framework has not been studied much by researchers. Among 62 papers from 2003 to 2013 which involved cyber security culture (Alhogail & Mirza, 2014a), only 14 papers presented the frameworks (AlHogail, 2015). The Table 2.6 shows the main thesis of the studies with regard to the frameworks. This reveals that the frameworks touched on different aspects of the culture and shed light on various associations of the culture with other factors.

Table 2.6: Summary of papers which presented a framework in security culture (2003-2013) (adapted from Alhogail & Mirza, 2014b)

Study	Main thesis of the framework presented by the study
Chia, Maynard, & Ruighaver (2003)	An adaptation of an organisational culture framework by Detert, Schroeder, and Mauriel (2000) to a security culture framework
Schlienger & Teufel (2003)	An analysis of information security culture based on the model by Schein (2010)
Zakaria (2006)	Identifying data collection techniques in information security culture research
Koh, Ruighaver, Maynard, & Ahmad (2005)	Analysing how security governance changes the security culture
Chang & Lin (2007)	Quantifying the impacts of organisational culture traits on the effectiveness of implementing information security management

Ruighaver, Maynard, & Chang (2007)	Defining the concept of information security culture using Detert et al. (2000)
Dojkovski et al. (2007)	Developing an information security culture in SMEs in a national setting
Lim, Chang, Maynard, & Ahmad (2009)	Determining to what extent the information security culture is embedded into organisational culture
Alnatheer & Nelson (2009)	Understanding information security culture in the Saudi context
Alfawaz, Nelson, & Mohannak (2010)	Classifying and organising the characteristics of organisational subjects involved in information security practices
Da Veiga & Eloff (2010)	Comprehensive framework to establish information security culture
Van Niekerk & Von Solms (2010)	Developing an information security culture in SMEs by emphasising the important role of business owner support.

Among these studies, three studies (Da Veiga & Eloff, 2010; Dojkovski et al., 2007; Van Niekerk & Von Solms, 2010) will be reviewed. These three are chosen because of comprehensiveness of their frameworks. The remainder of these studies failed to provide a holistic view which incorporated the human, managerial, and technical dimensions (Alhogail & Mirza, 2014b).

Drawing on the three levels model by Schein (2010), Van Niekerk and Von Solms (2010) added an additional level, which was knowledge. The authors argued that cyber security knowledge was the fundamental basis for the three layers to be created. A clear benefit of adding knowledge is that this allowed a deeper understanding of culture and interactions among its underlying layers. The conceptual framework in the study can be quite useful in diagnosing whether the security culture is stable or secure. The authors also emphasised creation and transfer of knowledge to build a constructive security culture. As a good method for this, they suggested awareness campaigns to educate employees to attain a good understanding of cyber security itself as well as environmental settings.

Da Veiga and Eloff (2010) proposed a comprehensive framework based on two propositions: (1) cyber security component categories such as leadership, governance, policies influence cyber security behaviours on individual, group, and organisational tiers and (2) the behaviours cultivate the levels of cyber security culture (i.e., basic assumptions, values, and artefacts). It is important to note that this framework links behaviour on the three tiers to the security culture. This brings a practical implication. Despite its complexity, this framework can provide a clear indication which component category needs to be strengthened to change the behaviour or which cyber security behaviour is influential in cultivating the culture.

However, these two frameworks limited the scope of research within their organisational settings, overlooking the national environment. Dojkovski et al. (2007) explored cyber security culture of Australian SMEs in a national context in which they operated. A major difference of this framework from the two is that this framework factors in external influences and initiatives such as national culture, government initiative, and vendors. Cyber security culture is considered as an output of interactions between external influences and organisational ones. In other words, the security culture is shaped by organisational influences which are conditioned by the national influences and initiatives. The scope of this conceptual framework fits into the scope of this research.

Cyber security culture aims at protecting information assets by influencing employees' perceptions and behaviour (Alhogail & Mirza, 2014b). There has been a predominant consideration that fostering cyber security culture is a requisite for addressing insider threats (Dhillon, 2001; Dojkovski et al., 2007; Magklaras & Furnell, 2004) or a viable countermeasure to threats incurred by human factors (Reid & Van Niekerk, 2014). However, does security culture deal with insider misuse threat only? What about external threats? Employees are willingly or unwillingly engaged in risky behaviours which expose vulnerabilities of information systems to external threats. Some good examples are clicking unknown e-mail attachments, downplaying formidable threats,

and ignoring security policies or protocols. Most hackers and cybercriminals rely on social engineering techniques. Social engineering refers to “the use of social disguises, cultural ploys, and psychological tricks to get employees of a company to assist hackers in their illegal intrusion or use of computer systems and networks” (Erbschloe, 2004, p. 61). A vital communication tool, e-mail, is seriously abused by cybercriminals for breaching computer systems. In 2016, one in 131 emails was found to contain malware (Symantec, 2017). As a primary source of external threats, e-mail attachments need an insider’s engagement (e.g., clicking) for execution. This example shows that insiders’ behaviour can be either a facilitator or inhibitor of external threats. In this respect, security culture can take a role in motivating insiders to be vigilant to external threats. This is not reducing human errors, but strengthening positive human behaviours which can prevent or mitigate threats.

2.5.6. The role of managers and their leadership

A growing body of cyber security studies addressed the role of senior managers. The role of senior management has been examined in relation to various organisational factors. Many studies found that senior management support was a significant factor in fostering cyber security culture within a business. Knapp, Marshall, Rainer, and Ford (2006) found that top management support had a positive causal impact on both cyber security culture and policy enforcement. The authors achieved the credibility of the study by using a mixed method strategy. Firstly, they used open-ended questions to develop a survey instrument, and secondly, tested hypotheses with survey results. In line with this study, Dutta and McCrohan (2002) argued that senior management had a key role in providing the leadership which contributed to nurturing cyber security culture. Hu, Dinev, Hart, and Cooke (2012) extended the scope of research on this topic. Their conceptual model included organisational culture as having mediating effects. Top management participation had a positive impact on cyber security compliance behaviour of employees and the impact was mediated by organisational culture.

Some studies concerned the impact of top management structure on cyber security management. Kwon, Ulmer, and Wang (2012) asserted that the involvement of an IT executive in top management and the amount of his/her compensation were negatively associated with the likelihood of cyber security breaches. In a similar vein, Higgs, Pinsker, Smith, and Young (2016) contended that creation of a board-level technical committee was effective in mitigating cyber security breaches. These studies indicate that better treatment of IT staff and managers within an organisation is expected to have risk mitigation effects.

Leadership is the ability to influence a group in order to attain a set of goals (Robbins & Judge, 2013, p. 368). It can be displayed by any member in a group and is not an exclusive province of a few members at the top (Bass & Riggio, 2006, p. 2). Not all managers are considered leaders. While managers focus on business affairs from management aspects, such as budgeting, staffing, and problem solving, leaders motivate and inspire employees for an organisational change by presenting achievable visions (Stroh et al., 2002, pp. 250-251). Based on formal positions, however, managers are more likely to become leaders due to their managerial roles within an organisation. Cyber security managers are responsible for safeguarding IT systems and employees of an organisation from cyber security threats. To accomplish this goal, cyber security managers need to urge and persuade employees to partake in maintaining cyber security. However, they do not have an authority to order and discipline general employees, but they can reveal leadership in order to inspire and motivate those employees to change their attitude and behaviour (Choi, 2016). The most crucial moment when leadership is needed is crisis situations. Since modern crisis involves complex threats and contexts, effective crisis leadership should not be one-dimensional, but should take multiple features into consideration. For example, Devitt and Borodzicz (2008) proposed interwoven leadership by balancing significant features, such as interpersonal skills, personal attributes, stakeholders' awareness, and task skills in any response.

Using a survey data of Korean SMEs, Yoo (2014) found that the leadership of senior management had a significant influence on the implementation of cyber security controls. However, the operational definition of leadership was problematic because it did not adequately reflect the concept. The author used 'degree of importance that top management thinks about information security' as operational definition of leadership of top management. However, this operational definition does not capture the nature and components of leadership. Instead, it can be better captured by another concept, 'priority' rather than 'leadership'.

Among various leadership styles, transformational leadership has been applied to the context of cyber security in a company. Transformational leadership inspires and motivates followers to attain unexpected outcomes, emphasising intrinsic motivation, positive development, and satisfaction of followers (Bass & Riggio, 2006, p. xi). This leadership is comprised of four components: (1) idealised influence or charisma, (2) inspirational motivation, (3) intellectual stimulation, and (4) individualised consideration (Bass, 1985). In the context of cyber security, a transformational leader suggests a clear vision of cyber security management and shows followers how to achieve related goals (Flores & Ekstedt, 2016). Transformational leadership is found to be effective in various aspects of cyber security management. Flores and Ekstedt (2016) contended that transformational leadership had a positive impact on both security culture and employee's security awareness. Drawing on data from public institutions in Korea, Choi (2016) asserted that transformational leadership by cyber security managers increased the effectiveness of cyber security. It was also revealed that the enforcement and relevance of cyber security policies had mediating effects in the causal relationship between the independent and dependent variables.

2.6. The UK cyber security governance

It should be noted that this research drew on multiple sources within the UK to reflect its cyber security context. This was because the UK's cyber security framework was

taken as a conceptual model as well as a conceptual lens against which conditions in South Korea were examined. The UK's framework was used as a tool which was adapted to fit South Korean context. The relevance of the UK's framework to South Korea is fully expressed in Section 3.4.4. There are three reasons for this. Firstly, as this research was carried out in the UK, and for the UK audience it would be more understandable if the UK context is presented to explain this emerging phenomenon. Secondly, in South Korea, the UK's cyber security governance is praised for its high standard. The UK's governance is often referred to as a benchmark against which cyber security governance of South Korea could be assessed (e.g., Kim, 2017; Kwon & Seok, 2016). Thirdly, the questions in the survey questionnaire were built upon a set of questions that HM Government (Department for Digital, Culture, Media and Sport, 2016, 2017, 2018) used to investigate the cyber security situation in the UK – for more details (see: Section 5.1).

2.6.1. The cyber security structure

Taking a top-down approach, the UK's cyber security structure exhibits a logical consistency from the Cabinet Office to operational law enforcement agencies. The whole structure is derived from the National Security Strategy which selects cyber-attacks as one of the six highest priority (Tier One) risks alongside terrorism, international military conflict, public health, major natural hazards, and instability overseas (HM Government, 2015). The next stage concerns cyberspace. Lying within the National Security Strategy, the National Cyber Security Strategy focuses on securing cyberspace to stimulate growth as well as protecting society (HM Government, 2016). Both of the strategies are administered by the Cabinet Office. When establishing a strategy or expecting a possible cyber-attack, it is a higher entity that renders the decision whether to take a law enforcement or national security approach (Clark, Berson, & Lin, 2014). In the UK, the higher entity is the Cabinet Office. The alignment of the two hierarchical strategies is also found in other countries in Europe. In a comparative study, Guitton (2013) found that the UK, France and Germany adopted the national cyber security strategy which was in line with their national security strategy.

The National Cyber Security Strategy goes down to cybercrime level, which is diverted into two streams. Whereas the National Cyber Crime Strategy / Serious and Organised Crime Strategy deal with general online crimes, the National Fraud Strategy specifically targets online fraud. The latter is an independent strategy which only handles fraud because it does serious harm to the public and business. Fraud is exacerbated by their scale and reach because of the use of networked computers and other ICTs. The UK statistics (Office for National Statistics, 2017) supported this argument by presenting that in 2016 cyber fraud accounted for about two-thirds (64.8%) of the total cybercrime in the UK. Finally, a framework for internet investigations was set up to implement cybercrime strategies at local forces on an operational level (National Police Chiefs' Council, 2015).

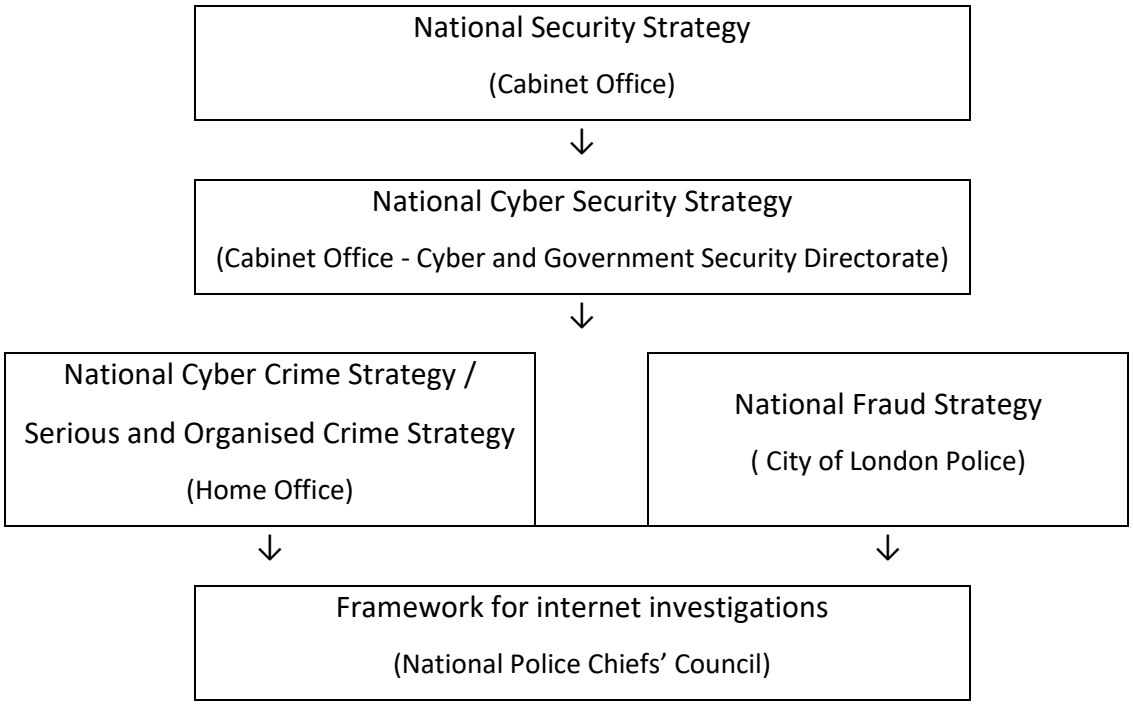


Figure 2.8 The UK's cyber security structure

2.6.2. Related government departments and agencies

Firstly, the Cyber and Government Security Directorate (CGSD)[15] in the Cabinet Office takes the lead in building a national cyber security governance framework. This unit is responsible for all aspects of government protective security, including the delivery of the National Cyber Security Strategy and the management of National Cyber Security Programme (NCSP) (Cabinet Office, 2018). As a policy and standards body, the CGSD prioritises cyber security agendas and provides strategic direction for the related departments and agencies.

Secondly, the National Cyber Security Centre (NCSC) under Government Communications Headquarters (GCHQ) is an organisation which provides advice and support for the public and private sector organisations on cyber security as well as the management of cyber security incidents (House of Commons, 2017). The NCSC was established in October 2016 as a result of amalgamating several government organisations, such as Communications-Electronics Security Group (i.e., the information security arm of GCHQ), the Centre for Cyber Assessment, and Computer Emergency Response Team UK (UK-CERT). As the UK's technical authority on cyber security, the NCSC is aimed at reducing the cyber security risk to the UK by raising cyber resilience (NCSC, 2017).

Thirdly, the Centre for the Protection of National Infrastructure (CPNI) is a government authority made responsible for protecting the national infrastructure[16] from cyber terrorism, national or industrial espionage. This centre offers security advice to stakeholders, such as other government organisations and business enterprises. Because much of the national infrastructure is owned and managed by the private sector, it is vital to create a trusted environment with businesses (Cabinet Office, 2011b).

15 The Office of Cyber Security and Information Assurance was superseded by Cyber and Government Security Directorate (CGSD) from 2016 (National Audit Office, 2016).

16 UK's critical national infrastructure includes communications, emergency services, energy, financial services, food, government, health, transport, water, defence, civil nuclear, space, and chemicals (Centre for the Protection of National Infrastructure, n.d.).

Fourthly, the main goal of the BIS is to boost economic growth. Its main role is to support businesses, consumers and students in developing their innovation and skills in various ways. When it comes to cyber security, the BIS is positioned as a conduit for linking strategic levels of government organisations such as the NCSC and CPNI to SMEs. Compared to the NCSC and CPNI, the BIS keeps a close relationship with SMEs as to cyber security, based on interactions with and better understanding of SMEs. Therefore, the BIS takes the lead in the creation of detailed information on security schemes such as Cyber Essentials and SMEs: What you need to know about cyber security with the help of other government organisations.

Fifthly, police organisations, in principle, maintain order in cyberspace and enforce law. They are supposed to be first responders to cybercrimes, providing frontline services to citizens. However, the effectiveness of the police response to cybercrime has been seriously questioned (Loveday, 2017). As evidence of this, Yar (2013, p. 13) argued that under-reporting and under-recording of cybercrimes are serious issues (see: Section 2.6.5). Most regional police forces in the UK either have their own cybercrime units or unite with neighbouring forces to provide these services (Wall, 2007/11). This shows that the police try to tackle cybercrime on a regional basis. A report from Her Majesty's Inspectorate of Constabulary (HMIC; 2015) questioned the effectiveness of that approach, mentioning that cybercrime was not the exclusive domain of a specialist unit any more. As cybercrime is on the rise, frontline police officers' capability of handling cybercrimes becomes more important. However, it is noted that frontline officers still have insufficient knowledge or skills to deal with cybercrimes (HMIC, 2015).

These main government units can be categorized into three groups: the strategic, functional and operational level. The first, the CGSD, concentrates on determining priorities and coordinating the cyber security programme on the strategic level. Secondly, the NCSC under the GCHQ, and the CPNI are dedicated to achieving their own functional missions. These two agencies have a specialised mission, respectively, securing cyberspace and protecting national infrastructure. Regardless of the

differences in their own duties, their functional goals are aligned with strategic goals. Thirdly, the role of the BIS is more tuned to businesses, acting as an advocate for SMEs. It ponders what SMEs need and how SMEs can be protected from security disruptions.

2.6.3. Initiatives to implement national strategies

In order to implement the national strategies, the UK government took a program-based approach in the long term. The government carried out two very important initiatives: National Cyber Security Programme (NCSP) and Cyber-Security Information Sharing Partnership (CiSP).

2.6.3.1. National Cyber Security Programme

The Office of Cyber Security and Information Assurance in the Cabinet Office oversaw the five-year NCSP from April 2011 to March 2016, which amounted to £860 million investment to upgrade the online business environment (National Audit Office [NAO], 2014). The government-driven programme intended to reach all primary stakeholders. One of the priorities of the project was to have a positive impact on perceptions and behaviours of commercial organisations and private individuals in relation to cyber security by educating and informing end users. A practical version of services such as Cyber Essentials and Ten Steps to Cyber Security guidance was launched as part of the NCSP. These Schemes are explained below.

Table 2.7: Four objectives of the NCSP (NAO, 2014, p. 4)

- Tackling cybercrime and making the UK one of the most secure places in the world to do business
- Making the UK more resilient to cyber-attack and better able to protect interests in cyberspace
- Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies
- Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

The public audit report by NAO (2014) showed what percentage of budget was allocated to private sector engagement and awareness. The program has spent about £19.3 million from 2011 to 2014 (Years 1 to 3) and £21.1 million from 2014 to 2015 (Year 4). Considering that the annual amount for Years 1 to 3 was about £6.4 million on average, the allocated expenditure for private sector during Year 4 was approximately 220% more than the average amount in the previous 3 years. There is no official document that suggests a reason behind this abrupt surge. However, in general, a greater budget allocation for a particular purpose comes from the realisation of the importance of the purpose. It is likely that the huge increase of expenditure for private sector reflects the growing importance of protecting private sector.

Evaluations on the NCSP were carried out separately by Major Projects Authority and NAO. These recognised the progress that the NCSP has achieved. As a body that provides independent assurance on major projects, the Major Projects Authority has rated the Programme as 'green'[17] (Cabinet Office, 2015), the highest rating out of five levels. In line with this, the NAO (2014) found that "The Programme's financial management and

17 According to the description of Delivery Confidence Assessment ratings in the repot (Cabinet Office, 2015), green rating is defined as "successful delivery of the project on time, budget and quality appears highly likely and there are no major outstanding issues that at this stage appear to threaten delivery significantly" (p. 28).

governance mechanisms are strong, and have improved over the Programme's life to date" (p. 5). These recognitions represent the overall performance of the NSCP.

The report from the NAO (2014) showed a more detailed picture on how the programme made progress in different subcategories. The evaluation was based on a survey from respondents across government, industry, and academia. The respondents ranked performance in five areas of the NCSP with a score between 1 and 5. The five areas were: (1) government's understanding of the threat, (2) government's encouragement of business to mitigate cyber risk, (3) government's support to trade and exports, (4) government's efforts in reducing the skills gap, and (5) overall value for money of the programme. The results of the survey showed that the second category or 'government's encouragement of business to mitigate cyber risk' was slightly over 3.0. This rating score was lower than the scores of three other areas, and only higher than that of 'government's support to trade and exports'. This survey result questions the argument that the NCSP and its derivatives were effective in supporting businesses with respect to cyber security. In addition, moving more towards this research topic, the report acknowledged that the NCSP has not provided enough guidance to meet the demands from SMEs, therefore "having a limited impact with SMEs" (NAO, 2014, p. 5).

2.6.3.2. Cyber-Security Information Sharing Partnership

As a crucial strand of the NCSP, the CiSP was launched in March 2013. This is a government-led joint industry initiative, creating a forum to facilitate information sharing and increase awareness of cyber threats. When it was set up, only 80 companies and 750 individuals joined to participate. However, the number has increased significantly since then. As of February 2016, over 1,700 companies and 4,400 individuals registered for this service (UK-CERT, n.d.). The core part of the CiSP is the Fusion Cell which is composed of an analytical team from both industry and government agencies (Cabinet Office et al., 2015). The analysts examine cyber information from various sources and produce up-to-date intelligence that benefits stakeholders. Once becoming

a member of the CiSP, they cooperatively provide and receive the latest feeds of information, contributing to the accumulation of collective knowledge as a result.

The CiSP has changed the scope of its initiatives. In the first place this forum aimed to protect critical national infrastructures in the UK, but secondly it has broadened its mission into supporting SMEs (Ring, 2013). This change was based on the realisation that SMEs were not properly protected even though they were the next target of cybercrimes. In order to meet the needs from SMEs, the CiSP needed to change its operating strategy because SMEs are scattered across the nation. Working with Regional Organised Crime Units, UK-CERT has launched 10 regional nodes of the CiSP (UK-CERT, 2016). As a continuation of the national CiSP platform, the localisation strategy intended to support local businesses in a way that promotes the information sharing of cyber security on the regional basis. It represents how the UK government tries to extend coverage for local businesses.

The primary expectation from the CiSP is information sharing between government organisations and private enterprises. However, the growth in membership does not necessarily indicate that the intended information sharing is actually happening. Based on the interviews of corporate managers, Ring (2013) argued that information sharing occurred in a one-way direction. This argument suggested that government agencies got necessary information from private sector partners, but they were unwilling to share their information with business people. It is the inherent nature of government organisations that they are accustomed to collecting information, but not sharing that information.

Another expectation from the CiSP is information diffusion among private companies. The participation of companies of all sizes has opened the gate for information diffusion from large ones to small ones. Large companies normally have a more structured cyber security management with professional staff and knowledge than smaller companies. The CiSP provides an opportunity for business people to form informal networks

through socialisation. Information diffusion is expected to occur via the networks. However, there is a crucial factor that works as an inhibitor of the information diffusion. Due to an ongoing escalation of cyber threats, having a stable cyber security management system within a company is considered an invaluable business asset. If some participating companies in the CiSP are found to be competitors, information sharing is the last thing that they do voluntarily. This inhibiting factor can be a challenge to sustain information diffusion atmospheres in the CiSP.

2.6.4. Specific schemes on the operational level

There are four large government schemes that directly target SMEs. These are Ten Steps to Cyber Security, Cyber Essentials, Innovation Vouchers, and Project FALCON (Fraud and Linked Crime Online). These schemes are intended to raise awareness of cyber threats and encourage businesses to carry out cyber security management practices.

Firstly, the guidance, Ten Steps to Cyber Security, was published by GCHQ at first in 2012 to provide concrete advice on how to secure a company's personal data, networked services, and intellectual property (Cabinet Office et al., 2015). Since then, GCHQ has continuously updated this guidance to make sure that it kept close relevance to the fast-changing climate of cyber security.

Secondly, the BIS produced Cyber Essentials working with Information Assurance for Small and Medium Enterprises[18] and Information Security Forum[19] (BIS, 2014). Cyber Essentials covers basic hygiene measures of cyber security in corporate IT systems. The BIS had worked with the private sector to come up with a preferred organisational standard in cyber security. As the response to feedback from businesses, the BIS concluded that the next stage after the Ten Steps to Cyber Security guidance was to

18 This is one of five businesses appointed as Accreditation Bodies for certifying against the UK Government's Cyber Essentials Scheme.

19 This is an independent information security organisation with a membership comprising lots of the world's leading companies.

make businesses adopt an organisational standard (BIS, 2013). Clearly, this scheme was the outcome of continuous cooperation between the government and businesses.

The government's flagship scheme consists of two parts, requirements for basic technical protection from cyber-attacks and assurance framework. While the former contains a set of basic technical controls, the latter provides security professionals with guidance to carry out different levels of assessment. The problem is that the scheme addresses only technical aspects, and does not consider managerial and human controls. For example, senior management support and staff education can be principal controls to successfully implement technical controls. Without addressing other types of controls, it is hard to guarantee the effectiveness of Cyber Essentials.

One distinctive feature of this scheme from others is that it has a certification process. The Cyber Essentials certification costs between £200 and £400 at a basic level, which is quite affordable for SMEs. The government clearly encourages SMEs to go through the certification process. Since October 2014, any government suppliers applying for contracts related to handling of personal information and provision of certain ICT products and services are required to adopt Cyber Essentials (Crown Commercial Service, 2014). Although this policy incentivises government suppliers to implement, to a certain extent, security controls suggested in the Cyber Essentials (Bauer & Dutton, 2015), no information is provided as to what kind of incentive structure is offered to SMEs. An appropriate framework regarding incentives should be given to SMEs so that small business owners can seriously consider applying for getting a certificate.

Thirdly, Innovation Vouchers worth up to £5,000 are provided to SMEs by the BIS (Department for Digital, Culture, Media and Sport & Vaizey, 2015). The vouchers can be used to get advice from external experts to improve business strategies ranging from cyber security to intellectual property. Considering that SMEs do not have enough budgetary resources to beef up computer systems (see: Section 2.3.3), it is seen as one of the tailored schemes of the UK government. Another benefit from this scheme is that

it also helps cyber security industry to grow by making SMEs form partnerships with cyber security specialists.

The last one is a regional-based programme in London. The Metropolitan Police Service initiated Project FALCON in January 2014 within the Specialist, Organised and Economic Crime Command for combating fraud and cybercrime through cooperation with other key agencies such as National Fraud Intelligence Bureau (NFIB), National Cyber Crime Unit, and Mayors Office for Policing. Working with the business sector, the Met regularly participates in business forums to encourage cybercrime reporting. The whole purpose is to build public confidence in a policing capability so that they are confident to carry out their business in London. Basically this is aimed at attracting investors and business people from around the world. Despite spatial boundedness of the programme within London, it has a nationwide effect as cybercrime is not confined to local boundaries.

As derivatives of the NCSP, the four schemes mentioned above intend to improve security situations of SMEs in the UK. These governmental measures are not just sporadic initiatives to deal with separate cyber threats, but coordinated efforts to formulate a set of structures that handle constantly changing cyber security risks. From the policy point of view, they can be analysed as the UK government's ongoing process of embedding cyber security values in SMEs.

There are two positive features of these schemes. Firstly, they are aligned with national strategies from the higher level. It implies that goals and values of National Security Strategy and Cyber Security Strategy are incorporated into these operational schemes. Starting to defend critical infrastructures and government organisations, the UK's cyber security structure has broadened its scope into protecting SMEs. On the national scale, the proper alignment of a set of strategies and schemes is the most vital element to gain expected outcomes. Secondly, they are intended to raise awareness of SMEs without mandating security standards through legislation and regulation. If the government attempted to use regulative measures, this must have given SMEs managerial and

financial burdens. Considering that cyber security is a relatively new risk to SMEs, the government's focus on raising awareness corresponds to what SMEs actually need. However, there is a weakness in non-regulatory measures. Whether to implement suggestions from the schemes is left to the discretion of SMEs depending on their business situations. It gives more flexibility to SMEs, but at the same time it decreases the certainty of the implementation of the schemes. In fact, the UK Cyber Security Breaches Surveys (Department for Digital, Culture, Media and Sport, 2017, 2018) found that the government's schemes and standards were not widely known in SMEs. In particular, SMEs had low awareness of Cyber Essentials and Ten Steps to Cyber Security which were directly launched as part of the NCSP. The surveys also indicated that medium firms tended to be more aware of each of these schemes than small firms.

A great challenge worth noting is that quantifying and measuring the effectiveness of these schemes is difficult. This limitation is generally applied to most government policies. Without rigorous evaluation of government policies, no one can confidently say that they have a significant impact on targeted groups. In reality, embarking on empirical research on the schemes on a national scale requires commitment of time and cost. This may be why there have been few empirical investigations into the performance of the NCSP and its schemes.

2.6.5. A reporting mechanism

Cybercrime is divided into three categories. These are crimes in the machine (e.g., obscene or racist material), crimes using the machine (e.g., fraud related), and crimes against the machine (e.g., hacking) (Wall, 2007/11). The first category, crimes in the machine, is reported to Internet Watch Foundation (IWF), an independent organisation created in 1996 by Internet Service Providers (ISPs) to fight against obscene imagery. The IWF assesses the reports and chooses whether to act upon them or pass them on to the UK Police, IWF equivalents, and Child Exploitation and Online Protection Centre. The second category, crimes using the machine, is related to cyber fraud. Action Fraud

is the central reporting system[20] which receives online fraud reports as well as other types of cybercrime reports, and transfers the reports to the NFIB. The NFIB uses a scoring system which decides whether a report should be reviewed or not (NFIB, 2013). If an aggregate value of a report reaches the predetermined critical value, the NFIB will review the report and, if necessary, disseminate it to appropriate local police force for further action[21] (Action Fraud, n.d.). The last category, crimes against the machine, is reported to UK CERT. Cybercrimes of this category, particularly hacking, consist of technical elements and its consequences can be nationwide or international. Therefore, it requires responses from national agencies, such as National Cyber Crime Unit, Serious Fraud Office, and security services.

It is noticeable that the UK reporting mechanism includes private organisations and international partners such as IWF, Interpol, and Virtual Global Taskforce. This mechanism corresponds with the notion of Wall (2007, p. 183) that the role of the public police should be understood within internet governance. Providers of the internet governance include ISPs, governmental non-police agencies, corporate entities, non-government/non-police hybrids, and so on (Wall, 2007, p. 168). Though the reporting mechanism is part of internet governance, the mechanism and internet governance share the important assumption that policing cyberspace cannot be solely secured by the public police. The broad range of partnerships with non-public entities will ensure that policing the internet will be more feasible. The networked nodes will enable them to take preemptive measures (e.g., shutting down child abuse websites) as well as to clamp down on cybercriminals beyond their jurisdictions.

In terms of the scale of participating nodes, the cybercrime reporting mechanism is quite similar to the 'fraud justice network' which encompasses the multiple public and private systems of justice as well as criminal justice system (Button, Tapley, & Lewis, 2013).

20 Even when online victims go to local police stations for cybercrime report, they are referred to Action Fraud.

21 The NFIB sends organised cybercrime or high-profile cases to Regional Organized Crime Units and individual or minor cybercrime cases to local police forces.

Individual victims of fraud could depend on not only public but also private and voluntary sectors at the reporting, reported, and criminal justice stage. Because fraud covers a wide range of illegal and immoral behaviours (Button et al., 2013), it is hard to pin down and categorise all relevant behaviours. Therefore, it seems reasonable to have this complex network to address the very diverse offence. One downside from the complexity of the network is that fraud victims could have difficulty in deciding who to report to. This is different from the cybercrime reporting mechanism. While dozens of report receiving bodies exist in the fraud justice network (Button et al., 2013), each category of cybercrime has a single point of contact for the public (i.e., IWF, Action Fraud, and UK CERT) (Downing, 2011). In the cybercrime reporting mechanism, other public, private, and international organisations have a different role as a participating node, but not as a report receiving entity.

Receiving cybercrime reports by a single channel will give an advantage of developing its expertise in three aspects: (1) information gathering, (2) data analysis, and (3) information diffusion. The single point of contact can provide a clear guidance to victims and this will be a factor that encourages victims to make a report. From the victims' point of view, the ease of contacting is of great benefit. Secondly, the analysis of a massive volume of cybercrime reports in one node has more chances to generate meaningful intelligence that other organisations may be interested in. For example, collected information can be analysed by Big Data technologies, which increase the possibility of identifying large-scale patterns in human activities (Boyd & Crawford, 2012). Thirdly, this can lead to an effective diffusion process. Once the data analyses are undertaken, some results need to be shared with other organisations. Rather than diffusing information from multiple nodes, information diffusion via a single node ensures this happens in a structured manner. Considering that crime-related information may contain sensitive data, the diffusion process should be managed and controlled with great caution.

The reporting mechanism presented by Wall (2007/11) is the broad architecture concerning how cybercrime reports are transferred via participating nodes. However, the mechanism does not indicate whether they work well in practice, and few empirical investigations have been carried out to date. Though the structure of the reporting mechanism seems quite organised in a way that facilitates cybercrime reporting, under-reporting and under-recording are still recognised as serious issues (Yar, 2013, p. 13). Individuals and companies may not know whether they are victimised or may be reluctant to acknowledge their victimisation. Another explanation may be that victims do not expect the police to solve cybercrimes (Wall, 2007, p. 165). The under-reporting and under-recording are contributing factors that give rise to “dark figures" of cybercrime (Yar, 2013, p. 13).

In terms of police responses to cybercrime reports, a challenge emanates from an unfavourable working environment and a lack of adequate skills. The impact of cybercrime spreads over various jurisdictions, which requires the attention of several local forces. However, local forces have their own local priorities set by an elected Commissioner (Wall, 2005/15). In general, the police work in two ways: (1) capacity-building to follow a recent crime trend and (2) cooperation with international and private organisations to increase their readiness. The normative role of the police apart, actual performance of police activities is often questioned. According to Hunton (2010), cybercrime investigation requires the combination of technical and non-technical disciplines and investigative skills. His argument indicates that cybercrime investigators need to have higher levels of qualifications. However, the police lacked responses to cybercrimes (Sommer, 2004) and professional skills (Leukfeldt, Veenstra, & Stol, 2013). In recent years, these problems have been exacerbated by budget cuts of the Conservative led Coalition government (Loveday, 2017). When online victims try to get help from the local police, they are referred to Action Fraud first and have to wait for months until the police investigation ends. This is why police officers who deal with cybercrime should be regularly trained to comprehend the current nature of cyber threats. On a more radical change, recruiting IT skilled citizens by direct entry can be an

effective way to catch up with cybercriminals more quickly (Loveday, 2017). Designing an efficient reporting mechanism is only a first step. To run the mechanism successfully, it is of significance to have the reporting mechanism which is supported by effective police responses.

2.7. Conclusion

In this chapter, a wide range of theoretical considerations were examined under the central theme of cyber security management. Drawing on the nature of the risks and threats, various aspects of cyber security management, such as risk management frameworks and organisational behaviours, were investigated in order to understand the management processes. This investigation is expected to lay the foundation for the effective and efficient implementation of cyber security management. Cyber security is an emerging area and resolving cyber security problems requires an interdisciplinary approach (Trim & Lee, 2015). This means that it is a challenging area in which technical, human, and managerial factors should be taken into account. Integrating these factors requires attention to multiple aspects of organisational behaviours, such as culture, leadership, managerial roles, decision-making, and group attitudes and perceptions. The literature review suggests that an understanding of human-computer interaction, decision-making, cyber security culture, and the role of management is a core part in safeguarding a business from cyber threats.

This chapter also introduced the UK's cyber security framework to identify loopholes and weaknesses of the South Korean cyber security governance. The distinctive aspect of the UK's conceptual framework is its consistent and logical structure which benefits SMEs. There needs to be an acknowledgement that the conceptual lens has not been empirically investigated by academic researchers, but the importance of the investigation should not be underestimated. Therefore, the critical analyses of the UK's cyber security governance in this chapter should be of value not only to this study but also to future studies.

CHAPTER 3: SOUTH KOREA - THE EMPIRICAL FIELD OF INQUIRY

3.1 Introduction

In this chapter, a socioeconomic overview is carried out in order to relate basic information about South Korea. The widespread adoption of ICTs and the importance of SMEs in the economy are discussed to give a better understanding of the South Korean context. Crime trends and comparisons with traditional crimes are analysed to give an overall view of cybercrime. How cyber security strategies and a reporting mechanism are formulated is also explained in order to identify the environment in which SMEs operate. Finally, focusing on the cyber security of SMEs, the extent of the problems and vulnerabilities of government strategies and policies are discussed.

3.2 Understanding the sociocultural context

3.2.1 General background

South Korea encompasses a total of 100,210 square kilometres, making it approximately half the size of the UK. As of the end of 2015, the total population was estimated at 51.5 million with a density of 505.1 people per square kilometre. This means it is the 12th most densely populated country in the world, which implies that the government needs to build high-rise apartment complexes in major cities to alleviate housing shortages. The International Monetary Fund (2015) showed that South Korea had a GDP per capita of US$ 27,513, ranking it 29th internationally.

From a socioeconomic standpoint, South Korea is a society divided between the rich and the poor, and the cities and the countryside. These divisions can be traced back to the 1950s. After World War II, South Korea was left in ruins, with high levels of poverty and hunger. From the 1960s, the government undertook substantial measures to develop

heavy industries such as shipbuilding, coal mining, and car manufacturing. In the 1990s, South Korea was one of 'Four Dragons'[22] in the Asian economy, along with Singapore, Hong Kong, and Taiwan. Strong government intervention has been considered as the primary source of the rapid economic growth in the short span of 30 years.

Rapid industrialisation, spurred on by national initiatives, has accompanied drastic changes in the spatial distribution of human settlements. The urban population, which accounted for only 27.7% of the total population in 1960, tripled to 82.5% in 2015 (United Nations, 2014b). In particular, over 40% of the total population is currently living in Seoul and its satellite communities.[23] The increase in the urban population is primarily due to rural-to-urban migration for job opportunities and education. Even though government-led initiatives effectively brought the country into the modern era as quickly as possible, there remains a big discrepancy between cities and rural areas.

Initiated by a military regime[24] after it took control in a coup in 1961, the economic measures were forced through in a military style rather than a democratic manner. Centralised and hierarchical approaches were taken in most government initiatives. From then on, strong government leadership and a hierarchical approach have been applied to every aspect of South Korean society. Due to this political background, a few top controllers manage most public organisations. This sociopolitical feature is also reflected in the policing system.

South Korea has a centralised national policing system, consisting of 252 police stations (NPA, n.d.). There are local police forces, but none of them are independent. All police officers are directly hired by the NPA. In addition, all police stations adhere to strategies

22 This term that describes the four most rapidly developing economies in Asia before the 1990s.

23 Seoul's satellite communities are within the jurisdiction of 'Kyonggi-Do', which includes several cities. 'Do' is equivalent to a county in England and Wales.

24 The military regime effectively governed the nation for about 18 years, from 1961 to 1979.

and policies from the headquarters. This national system allows for citizens to receive standardised services across the nation.

This also gives officials at headquarters substantial power over all the local forces through the hierarchical command structure. This is an example. A policy that concerns the working conditions of police officers will be initially formulated at headquarters. As the policy passes down to the local forces, it, theoretically, can be changed. However, there is no room for substantial change because the policy was formulated in detail from the outset. Local police officers complain that policies from headquarters are detached from the reality in which they work. This hierarchical system does not allow much discretion to local forces, including both their managers and rank-and-file. In many cases, headquarters directly investigates and manages high-profile cases. Local forces think of interventions from the central authority as unnecessary measures that cannot meet local demands. For this reason, there is a distrust between headquarters and local police forces.

3.2.2 Infiltration of ICTs and dependence on mobile devices

South Korea has experienced rapid technological innovation. Correspondingly, most people in South Korea have proactively accepted technological changes. In fact, technology is deeply embedded in the daily lives of citizens. The technological advance brought about different patterns of human behaviour and social interaction on the individual level and social changes on the macro level.

Organisation for Economic Co-operation and Development (OECD)'s broadband statistics (2017b) show that fixed broadband penetration (i.e., subscriptions per 100 inhabitants) in South Korea was 40.9, ranking it 7th and mobile broadband penetration were 111.1, taking 8th place internationally. Only 11 countries[25] surpassed the 100%

25 These are Japan, Finland, Australia, Denmark, the USA, Estonia, Sweden, Korea, Iceland, Ireland, and New Zealand (in descending order of mobile subscriptions).

penetration threshold, which means that some people have more than two mobile devices. In terms of high-speed access to the Internet, virtually all fixed broadband subscribers in South Korea have internet connections with speeds greater than 10 Mbit/s (ITU, 2014). This implies that South Korea has one of the fastest average internet connection speeds in the world. High levels of connection to the Internet and the fast speed demonstrate that the telecommunication infrastructure is well established in South Korea (Bae, Park, & Kim, 2015).

Government-led initiatives were the driving force in building national networks for internet-friendly environments. From the administrative point of view, the South Korean government has taken the initiative to achieve technological advances. The United Nations' e-government survey (2014a), which is conducted every two years, found that the South Korean government took the global lead in the e-government rankings three times consecutively from 2010. This survey measured three things: (1) the availability of online services, (2) telecommunication infrastructure, and (3) human capacity (United Nations, 2014a). On a similar note, the ITU (2015b) published a report which measured ICT Development Index. This index was measured by three dimensions: ICT access, ICT use, and ICT skills. Each dimension consists of a set of indicators. It could be used to assess and monitor developments in ICT between countries. South Korea topped the list among 167 countries: for the sake of comparison, the UK ranked 4th. The noticeable point from these surveys is that they measured not only infrastructure but also human skills and knowledge of ICT. This suggests that educating people to adapt to an ever-changing environment is an important criterion that needs to be included when measuring ICT development.

It is worthwhile looking at how the proliferation of mobile devices has changed human behaviour in South Korean society. Mobile devices in particular have become crucial tools for online transactions. According to a report from the Bank of Korea (2017), the number of daily internet transactions processed via computers and mobile phones in 2016 was 87.5 million on average; 60.5% of them (52.9 million) were conducted via

mobile devices. The number of daily mobile transactions drastically increased over three years. The figure in 2016 was 148.4% higher than that of 2013 (52.9 million versus 21.3 million). Likewise, the number of registered online users was 122.5 million in 2016; 64.1% of them (74.7 million) were mobile users. The number of mobile users increased 100.8% over the three years (74.7 million versus 37.2 million). A huge embrace of mobile phones in daily lives transformed the landscape of internet banking. The table 3.1 shows that the annual increases in mobile banking overwhelm those in internet banking.

Table 3.1: Use of internet and mobile banking (Bank of Korea, 2014, 2015, 2016, 2017)

Internet banking[26]				
	The number of users	**Annual increase (%)**	**The number of daily transactions**	**Annual increase (%)**
2013	95.5 million	10.5	54.3 million	18.7
2014	103.2 million	8.1	66.5 million	22.4
2015	116.9 million	13.2	78.0 million	17.4
2016	122.5 million	4.9	87.5 million	12.2
Mobile banking				
	The number of users	**Annual increase (%)**	**The number of daily transactions**	**Annual increase (%)**
2013	37.2 million	55.2	21.3 million	66.5
2014	48.2 million	29.6	31.0 million	45.5
2015	64.8 million	34.4	42.2 million	36.3
2016	74.7 million	15	52.9 million	25.3

This trend has changed not only customers' behaviour but also the service practices of the banking sector. Traditionally, customers had to visit local branches to execute

26 Internet banking includes transactions via all sorts of devices; thus, figures relating to internet banking include mobile banking.

transactions. However, in 2015, non-face-to-face transactions (e.g., CD/ATM, telephone banking, internet banking) made up 88.7% of all transactions, and internet banking constituted almost half of all non-face-to-face transactions (Bank of Korea, 2016). The banking industry had to adjust to the changing transactional behaviour of customers. Banks increased investment in providing comprehensive and safe online services while slowly closing down their local branches. About 7.7% local branches[27] have been closed from 2012 to 2016 due to the rapid rise in the number of internet transactions (Financial Supervisory Service, 2017).

This changing landscape in monetary transactions indicates that, on a daily basis, a huge amount of money is transferred online: the use of physical notes and coins is dwindling. From a criminal's point of view, targeting online transactions seems more lucrative than snatching money from others' pockets. It is expected that offline fraudsters and thieves will move to cyberspace either alone or in alliance with accomplices who have computer skills, as cyberspace offers more financial opportunities. An explanation of this phenomenon is presented in later sections.

3.2.3 The significance of SMEs in the economy

According to the Small and Medium-sized Enterprises Basic Law in South Korea, company size is determined by annual turnover and not by the number of employed staff.[28] Enterprises were considered as SMEs if their annual turnover was less than from 150 billion won (£100.9 million)[29] to 40 billion won (£26.9 million), depending on the business sector in which they are operating. However, at the time of this research government agencies were still using the previous criterion, categorising company size by the number of employees. In particular, the most representative agency which publishes national statistics, the National Statistical Office is an example. Also, this study

27 596 branches were reduced from 7,699 in 2012 to 7,103 in 2016 nationally.
28 When the law was reformed in June 2015, the criteria for SMEs have changed.
29 In this research, the Korean Won-to-British Pound ratio was calculated at the exchange rate of March 13, 2018 (1 British Pound = 1,485.33 Korean Won).

excludes micro businesses which employ less than 10. This is because micro businesses tend to have highly personalised and informal management styles (Matlay, 1999), which indicates that they merit a separate study from larger SMEs (e.g., Mir & Feitelson, 2007; Parry, 2012). Therefore, SMEs in this study refer to companies with more than 9 and less than 300 employees. More specifically, small businesses employ 10-49 staff and medium businesses employee 50-299 staff. This criterion effectively excludes micro and large businesses.

It is indisputable that SMEs contribute to output and employment in society. In 2016, companies with less than 300 employees were about 3.94 million which amounted to 99.9% of the total number of businesses, and they employed about 18.2 million people, 85.7% of the total workforce (National Statistical Office, 2017). These figures show that the South Korean economy relies more heavily on SMEs than the economy of any other nation.

Table 3.2: Distribution of companies by company size (National Statistical Office, 2017)

Company size (employees)	The number of companies	Percentage	The total workforce	Percentage
1~4	3,173,203	80.3	5,705,551	26.8
5~99	758,333	19.2	10,211,699	48.0
100~299	14,710	0.4	2,292,599	10.8
Over 300	3,946	0.1	3,049,394	14.3
Total	3,950,192	100.0	21,259,243	100.0

An OECD report (2017a) presented some criteria for measuring the state of entrepreneurship among its member countries. The report, *Entrepreneurship at a Glance 2017*, compared the employment rate by enterprise size in the total economy. It

showed that South Korean large companies with over 300 staff[30] hired 13% of the total business economy, which was far short of the OECD average of 42%. On the other hand, the proportion of employment by SMEs was 87%. This figure is about 29 percentage points higher than the OECD average of 58%, ranking it 2th among the 37 countries. These comparative figures demonstrate that South Korean SMEs have a pivotal role in employment compared to those in other nations. Sometimes, based on these statistics, critics of larger companies argue that public policies need to focus more on protecting SMEs.

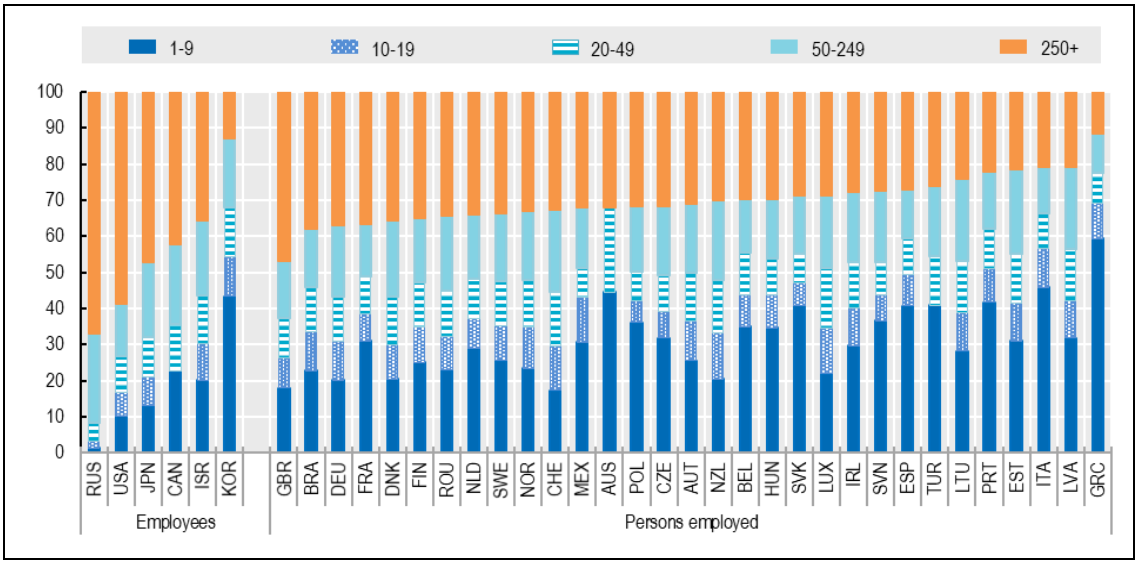


Figure 3.1 Employment by enterprise size (OECD, 2017a)

The Small and Medium Business Administration (SMBA)[31] provides statistics online from its database system. *Industry classification by company size* in 2014 categorised business activity in each sector (see: Table 3.4). Wholesale/retailing, accommodation/restaurant, and other services were found to be the top three industries in which SMEs operate. However, large businesses showed a different pattern.

30 Unlike other countries, the size class "250+" refers to "300+" for South Korea due to the differences in domestic statistical criteria.

31 As of July 26, 2017, the Small and Medium Business Administration was officially renamed Ministry of SMEs and Startups. This study however used the previous name because the name was changed at the later part of this research.

Over 50% of large businesses were in manufacturing, facility management/business support, and the real estate industry in descending order.

Among the classified sectors, wholesale/retailing, accommodation/restaurant, education services and other services can be grouped as labour-oriented industries. These services can be provided if certain elements such as facilities, appliances, and labourers are available: they do not require a high level of technology to function. Around 58.9% of SMEs operated in this category, which implies that over half of SMEs were not in industries that depend on high levels of technology. On the other hand, manufacturing, construction, publication/broadcasting communication/information services, facility management/ business support, and science/technical services can be classified as technology-oriented industries. Technology is an important factor in the provision of these services. Over 58% of large businesses were involved in this category, whereas 30.9% of SMEs were placed there. Technology-oriented industries are the backbone of the export trade.[32] The table 3.3 shows that large businesses accounted for about 81% of exports in 2012.

Table 3.3: Exports by company size (Korean Statistical Information Service, 2013)

	Total amount	**Percentage**
SME	US$102,872 million	18.8%
Large business	US$444,046 million	81.1%
Others	US$951 million	0.2%
Total	US$ 547,870 million	100%

32 The Ministry of Strategy and Finance (2015) announced 13 major export items in 2014, which were semiconductor devices, refined petroleum, cars, general machinery, petrochemical products, ships, steel, flat displays (e.g., LCD, OLED, PDP), wireless communications equipment, car parts, textiles, home appliances, and computers.

Table 3.4: Industry classification by company size (SMBA, 2016)

	Micro business		Small business		Medium business		Large business	
Manufacturing	325,621	10.63%	56,988	15.09%	10,056	9.89%	696	22.29%
Construction	106,420	3.47%	19,046	5.04%	2,328	2.29%	224	7.17%
Wholesale/retailing (sales)	876,093	28.60%	76,073	20.14%	34,204	33.63%	292	9.35%
Logistics	364,231	11.89%	8,347	2.21%	2,803	2.76%	102	3.27%
Accommodation/ restaurant	616,086	20.11%	68,208	18.06%	16,887	16.60%	81	2.59%
Publication/ broadcasting communication / information services	21,587	0.70%	13,508	3.58%	1,411	1.39%	112	3.59%
Facility management /business support	30,268	0.99%	14,038	3.72%	2,882	2.83%	565	18.09%
Real estate	107,054	3.50%	7,339	1.94%	4,283	4.21%	356	11.40%
Financial/insurance	7,381	0.24%	1,347	0.36%	2,667	2.62%	134	4.29%
Science/technical services	59,340	1.94%	26,599	7.04%	1,452	1.43%	216	6.92%
Education services	124,966	4.08%	15,543	4.12%	8,685	8.54%	80	2.56%
Other services[33]	418,213	13.65%	68,034	18.02%	11,531	11.34%	213	6.82%
Etc.[34]	5,741	0.19%	2,570	0.68%	2,520	2.48%	52	1.67%
Total	3,063,001	100%	377,640	100%	101,709	100%	3,123	100%

33 This includes healthcare, fixing, leisure, and social welfare services.

34 This includes sectors which take an extremely small portion such as mining, agriculture, forestry, fishing, electricity, gas, and environmental processing.

3.3 Cyber security issues in South Korea

3.3.1 Primary cyber security concerns

In contrast to the rapid advancement of ICTs, in-depth research on the criminogenic nature of new technologies and their security problems has not yet been carried out. Only a few countries like the US and the UK provide a legal framework and institutional support to deal with cyber security at a national level. This clear lack of national initiatives is partially attributed to the nature of cyber security. While crimes and disasters in the real world accompany physical damage such as casualties and destroyed buildings, cyber security breaches do not necessarily lead to visual consequences. In many cases, people believe that nothing serious has happened if there is no visual damage. Likewise, a government does not normally take measures until real damage has materialised. Without institutional support it is difficult to prepare preventative measures against cyber threats due to a lack of urgency in formulating cyber security laws and policies.

The UN (2014a) and ITU (2015b) reported that South Korea has the most state-of-the-art ICT infrastructures as well as users with high computer skills and knowledge. These facts and figures are nothing more than an indication that South Korea is a technology-friendly place for IT users. On the contrary, a higher level of dependency on ICTs makes users and computing environments more exposed to cyber security risks. As an example, Symantec (2017) reported a number of identities stolen in 2016 by countries. In South Korea 10,394,341 identities were stolen, ranking it 7th in the world.

When it comes to cyber security threats, South Korea in itself is a target of cyber-attacks from external states and non-state entities. In particular, cyber terrorism perpetrated by North Korea is considered the top priority in South Korea (Chung et al., 2016). North Korea recognised cyber-terror attacks as effective provocations to gain the upper hand at a future military campaign (Kang, Kim, Kim, & Yoo, 2016). Military experts argue that

thousands of North Korean hackers under the Reconnaissance General Bureau attempt cyber infiltration against enemy states on a daily basis (T. Kim, 2014). Since 2011, North Korea committed six major cyber-terror acts, primarily targeting government institutions, communication stations, and the financial sector (Table 3.5). Even though those attacks did not take the form of cyberwarfare, they caused massive chaos and damage[35] to South Korean society. Throughout the series of cyber-terror attacks, the South Korean government faced heavy criticism and lost public confidence with defending cyberspace (Jang, 2016).

It is only fairly recently that North Korea has tried to hack into the mobile devices of government officials (Jo, 2016). A smartphone contains a lot of personal information about the owner. This personal information includes contact lists, text messages, emails, records of online activities, documents, and media files. In early 2016, the head of the National Intelligence Service made public in a parliamentary briefing that emails containing malicious software had been sent to about 300 government and military officials; as a result, 40 smartphones had been infected (Kwon, 2016). This malware not only enabled North Korean hackers to gain contact lists and text messages, but also to wiretap phone conversations. North Korea is notorious for acting in an unpredictable manner, but in terms of cyber terrorism there is one thing that is predictable: North Korea constantly changes its cyber terrorism tactics in response to technological developments (Kang et al., 2016). Previously, it attempted to attack public institutions and national infrastructure. Now, it directs its cyber offences towards infiltrating the mobile devices of a few important individuals.

Provocations by North Korea in cyberspace compelled the South Korean government to focus on: (1) cyber terrorism rather than overall cyber security and (2) protection of critical national infrastructure owned by public organisations and large corporations (Choi, 2010; T. Kim, 2014). The political circumstance has created a vacuum in overall

35 However, official figures were not estimated for the damage in aggregate.

aspects of cyber security other than cyber terrorism, leaving behind stakeholders such as individual citizens and SMEs.

Table 3.5: Major cyber-terror activities by North Korea

Time	Type of attacks	Target
12 April 2011	Malicious codes	National Agricultural Bank
28 April 2012	GPS interruption	International airports
9 June 2012	Hacking	Joong-Ang newspaper
20 March 2013	APT attack	Major television stations, banks
25 June 2013 – 1 July 2013	Hacking, DDoS	69 government institutions (Ministry of Defence, National Intelligence Service, the Blue House, etc.)
February 2016 - March 2016	Smartphone hacking	High-ranking government officials, including military officers

Secondly, within general cybercrime, cyber financial fraud has emerged as a crucial social problem (Kim et al., 2015; Yoon, 2013). Cyber financial fraud includes phishing[36], pharming[37], smishing[38] memory hacking[39], etc. In cases of phishing, fraudsters steal personal information of millions of individual citizens, and call or send emails randomly to individuals on their lists. Most types of cyber financial fraud take advantage of malicious codes to lure people into danger. These attacks are random and automated, so any person in South Korea could be a potential victim.

36 Phishing is a compound word of private data and fishing. Fraudsters either call or send emails to random people and deceive them to transfer money to the crime account.
37 Pharming is manipulating the victim's PC via a malicious code to steal financial information. The code stealthily directs the victim to be connected to the false banking site.
38 Smishing is a compound word of text message (SMS) and phishing. If a person clicks on the Internet address in a random text message, malicious code is installed on smartphone. The code steals financial data or takes away some money.
39 Memory hacking is due to a malicious code resident in the victim's PC memory. The code withdraws the victim's money from the normal bank site.

What the law enforcement agencies underestimated was that cyber financial fraud evolved quickly following technical advancement. After realising the severity of these new types of crime, the police started to tally up basic statistics in relation to cyber financial fraud from 2013. The number of cyber financial frauds amounted to 33,763 cases with £17.3 million worth of damage in 2013 (NPA, 2014). In 2014, though the number of reported cases decreased by 53.8% to 15,596 cases, the total amount of damage increased by about 149% to £43.1 million (NPA, 2015). This means that the average amount of damage per case surged by about 439% between 2013 and 2014. Also, the arrest rate in 2014 was just above 42%. This figure is much lower than the average arrest rate for all cybercrimes from 2011 to 2014, which was 69.3%. While criminal proceeds increased, the probability of being caught decreased. From a classical criminological perspective, it can be argued that there were low deterrence effects because the benefits from these crimes outweighed the costs. This demonstrates that cyber financial fraud offers more lucrative opportunities to cybercriminals than other cybercrimes.

Table 3.6: Cyber financial fraud statistics (NPA, 2014, 2015, 2016, 2017a)

	The number of reported cases	**The number of arrests**	**Arrest rate (%)**	**The total damage**	**The average damage per case**
2013	33,763	-	-	25.7 billion Won (£17.3 million)	761,129 Won (£512)
2014	15,596[40]	6,567	42.1	64.1 billion Won (£43.1 million)	4.1 million Won (£2,760)
2015	14,686	7,886	53.7	-	-
2016	6,721	4,034	60.0	-	-

40 The sudden drop of this figure was attributed to a change of the scope of cyber financial fraud from 2014 onwards.

These cyber financial crimes took advantage of loopholes in financial transaction systems (e.g., insufficient authentication layers). Even though the crimes provoked public distrust in financial institutions, the banks at first provided no countermeasures. South Korean banks argued that they did not have legal responsibility because they just provided banking services without any involvement in the online transactions between victims and fraudsters. However, considering that cyber financial fraudsters use online transaction services, the cooperation of the banking industry was a requirement for effectively dealing with these types of cybercrimes. The Prime Minister's Office began a government-led joint industry initiative and came up with a broad framework consisting of several public and private organisations in December 2013 (Financial Supervisory Service, 2013). The involved entities were the Police, financial watchdog agencies, banks, and the Korea Federation of Banks. All the participating organisations agreed that they needed to make an all-out effort to prevent and respond to cyber financial fraud. Firstly, for prevention, the watchdog agencies pressured banks to set up more security layers to detect cyber fraud. Secondly, for a swift response to minimise damage to the victims, the Police and banks created hot lines to freeze the bank accounts of both victims and criminals. This government-led joint industry initiative was based on a regulatory framework which relied on the authority of public watchdogs along with a crime control framework that stressed arrests and prosecutions of criminals.

The concern on cyber terrorism by North Korea justified that the government and large companies should be protected because they run critical national infrastructures. On the other hand, cyber financial fraud targets individual citizens. Unfortunately, these two main concerns did not recognise that SMEs could be potential cybercrime victims. Despite the significance of SMEs in the national economy, the exposure of SMEs to high levels of cyber-attacks was overlooked. This tendency was also found on the international level (Holtfreter & Meyers, 2015).

3.3.2 Cybercrime figures

Based on the White Paper (2014) of the NPA, cybercrime statistics in South Korea combine the figures relating to cyber terrorism incidents and general cybercrimes. The former includes cyber-dependent crimes such as hacking and the spread of viruses and worms, while the latter consists of cyber-enabled crimes. Cyber-enabled crimes are traditional crimes that are strengthened in their scale and capacity by the use of ICTs (McGuire & Dowling, 2013). Fraud and theft are examples. The total number of cybercrimes is composed of about 10% of cyber terrorism incidents and 90% of general cybercrimes (NPA, 2017a). The number of total cybercrimes reported to the police increased significantly by about 30.9% from 116,961 cases in 2011 to 153,075 cases in 2016. This increase rate is much higher than that of traditional crimes which recorded 5.5% increase over the same period of time.

Table 3.7: Comparison between traditional crimes and cybercrimes (NPA, 2012, 2013, 2014, 2015, 2016, 2017a)

	Traditional crimes			Cybercrimes			
	The number of reports	The number of arrests	Arrest rate	The number of reports	The number of arrests	Arrest rate	Prosecution rate
2011	1,752,598	1,382,463	78.8	116,961	91,496	78.2	46.6
2012	1,793,400	1,37,121	76.4	108,223	84,932	78.4	47.6
2013	1,857,276	1,420,658	76.5	155,366	86,105	55.4	34.4
2014	1,778,966	1,392,112	78.3	110,109[41]	71,950	65.3	35.8
2015	1,861,657	1,500,234	80.6	144,679	104,888	72.5	-
2016	1,849,450	1,552,455	83.9	153,075	127,758	83.5	-

To understand the nature of offending, it is worth investigating how cybercrime is associated with traditional crime and whether traditional crimes are being replaced by

41 The sudden drop of this figure was attributed to a change of the scope of cybercrime. From 2014 onwards Cyber Bureau developed and used a new classification scheme for cybercrime statistics.

new types of offending. These can be examined by comparing cybercrime figures with traditional crime figures. However, simply comparing the total number of traditional crimes and cybercrimes would not make sense because some types of cybercrime are purely new and do not have relationships with traditional crimes. For example, cyber-dependent crimes such as unauthorised access and cyber terrorism are purely technology-driven cybercrime with different criminal motivations. Therefore, it would be reasonable to examine comparable types of crimes in order to explore crime transitions from offline to online. As such, the comparison in this part is limited only to crimes for financial gains: traditional theft and fraud are compared with cyber fraud. Conceptually, these two traditional crimes are in parallel with cyber fraud. The difference is whether an act of crime occurs within physical boundaries or in cyberspace.

The Table 3.8 shows that traditional theft and fraud have decreased significantly from 2012 to 2016 (respectively, 30.1% and 10.8%). In contrast, cyber fraud has increased drastically over the same period of time (130.8%). Although there was a small decrease between 2013 and 2014, this was most likely a minor correction of the big increase in the previous year. The basic pattern was that traditional theft and fraud decreased while cyber fraud increased over time.

This pattern seems to support the argument that traditional offline crimes are replaced by cybercrime. Organised crime groups increasingly rely on cyber fraud because this type of cybercrime produces a high rate of return on investment compared to other types of crime (Gehem et al., 2015). For some criminals, cyberspace is a more attractive place than physical space because of anonymity and issues over jurisdiction. Thus, it is a good reason that traditional criminals prefer cyberspace to physical space. However, there are not enough sample years included in the study to make a firm conclusion that the decrease in traditional theft and fraud is associated with the increase in cyber fraud. Therefore, these figures should be interpreted cautiously.

Table 3.8: Annual changes of traditional crimes (theft and fraud) and cyber fraud (NPA, 2013, 2014, 2015, 2016, 2017a)

	Theft	Annual change (%)	Fraud	Annual change (%)	Cyber fraud	Annual change (%)
2012	290,460	-	270,868	-	46,394	-
2013	288,343	-0.73	269,082	-0.66	85,856	+85.1
2014	266,222	-7.67	238,409	-0.11	72,263	-15.8
2015	245,853	-7.65	247,293	+3.73	96,535	+33.6
2016	203,037	-17.42	241,613	-2.30	107,090	+10.9

Although cybercrimes were on the rise, police responses to cybercrimes were rather unstable (see: Table 3.7). The arrest rate has dropped from 78.2% in 2011 to 55.4% in 2013, and increased to 72.5% in 2015 and to 83.5% in 2016. On the other hand, the prosecution rate has continuously decreased from 46.6% to 35.8% between 2011 and 2014. No explanation on the weak police responses was provided in the White Papers, however one possible explanation is the emergence of new types of cybercrimes. As suggested above in this section, new types of financial fraud have been incorporated into the statistics from 2013. 33,763 cases of new financial fraud were reported to the Police in 2013, but information on how many cases were processed was not revealed in the Whiter Paper. Another explanation is the jurisdiction in which cybercrimes were committed. It is difficult to arrest cybercriminals located in a foreign nation because cooperation with the local police of the nation requires a commitment of time and cost.

To uncover the nature of offending, it is also important to compare law enforcement activities in traditional crimes and cybercrimes. The arrest rates for both were very similar in 2011 and 2012, but they showed a discrepancy from 2013 onwards. There was a big drop in the arrest rate for cybercrimes, from 78.4% in 2012 to 55.4% in 2013. In 2013, the arrest rate for cybercrimes was 21.1 percentage points lower than that for traditional crimes, and 13.0 percentage points lower in 2014. The arrest and prosecution rates for cybercrimes have fluctuated between 2011 and 2016, but the arrest rate for

traditional crime has been stable during the same period. This analysis demonstrates the unstable nature of law enforcement activities against cybercrimes. Relatively ineffective police responses to cybercrimes are assumed to be found in other countries: they are not limited to a South Korean context only. In contrast to the constant evolution of cybercrimes, the effectiveness of law enforcement activities against cybercrime is questionable. Law enforcement officers face many difficulties in dealing with cybercrimes.

Firstly, the ability of cybercriminals to adapt to new technological developments outpaces that of the police. Cybercriminals normally have strong technological backgrounds with IT expertise, whereas police officers tend to lack computer knowledge and skills. Recently, the police have invested more in hardware and software for the investigation of cybercrimes. In order to retain more skilled IT personnel, the South Korean Police provided more structured training to officers and sometimes have directly hired skilled professionals into the police force (Kwon, 2014). Although the police are attempting to catch up with cybercriminals, the latter are always far ahead of the law enforcement officers.

Secondly, jurisdiction issues are the main hurdles in front of law enforcement activities. The problem lies in the fact that the police operate locally, whereas cybercrime is a globalised issue (Wall, 2007). Taking action against cybercriminals located outside of one state's jurisdiction requires more time and effort (Yar, 2013, p. 89). In some cases, a local police force may need the cooperation of law enforcement agencies in other nations, but it can take time for the foreign agencies to embark upon the necessary course of action. If a reported crime is an online fraud case which involves a small amount of money, the police may not be willing to devote their resources to it. In voice phishing[42] cases, most fraudsters operate in China, Thailand, Vietnam, and the Philippines, where

42 Voice phishing is a type of cybercrime which uses social engineering techniques over the telephone to gain access to the victim's financial data.

criminal justice systems rarely deal with these crimes (Kim, 2016). Thus, it would be reasonable to assume that a huge portion of the reported cases were not resolved.

Thirdly, the police officers responsible for cybercrime have a heavy caseload but limited resources. This phenomenon is due to the nature of cybercrime. Cybercrimes may only do minor harm to individuals, but the damage is large in aggregate (Wall, 2007). In particular, online fraud and scams disproportionately victimise many individuals with small amounts of damage. This is termed by Wall (2007) as the asymmetry of the offender-victim relationship. A few spammers send bogus emails to millions of people by using botnets. Botnets are an army of connected computers which are used to commit coordinated attacks on the command of a control server. The NPA recorded 85,856 online fraud cases in 2013, which accounted for 55.2% of the total cybercrimes. One in two cybercrime cases reported to the police was related to online fraud. As the most prevalent type of cybercrime, online fraud creates some difficulties for police investigators. Even though many individual victims come to local police stations to report their cases, it is questionable whether the investigators pay the same amount of attention to them as they do to traditional crimes. They will think that undertaking a substantial effort is not worthwhile because the damage is small, thus justifying their investment of time and effort into bigger cases.

There is one type of cybercrime which has caused damage to Korean businesses, which is trade fraud. Trade fraudsters target businesses which engage in foreign exports. They see a window of opportunity from physical distance, time difference, and email communications between trade partners. As the Korean economy relies heavily on export-oriented growth, it is no wonder Korean businesses are targeted by trade fraudsters. Trade fraudsters take advantage of hacking skills to steal information such as invoices from a trade partner as well as social engineering skills to push money transfers. Impersonating its trade partner, fraudsters send the revised invoice to a company employee which contains changed payment details (i.e., bank account numbers). They exploit the fact that most trade partners communicate via emails.

The Korean Police did not provide statistical data on this type of crime in any publications. It may be because cyber trade fraud is still in its early stages. However, the researcher could get these data through an official information request system.[43] Cyber trade fraud has steadily increased between 2013 and 2017 (NPA, 2018, p. 1). The average annual increase rate was about 81.3% during those years. Although information on the total amount of damage was collected only in 2013 and 2014 (Ryu, 2016), these figures provide meaningful information in terms of the scale of the damage.

Table 3.9: Cyber trade fraud statistics[44] (NPA, 2018, p. 1; Ryu, 2016)

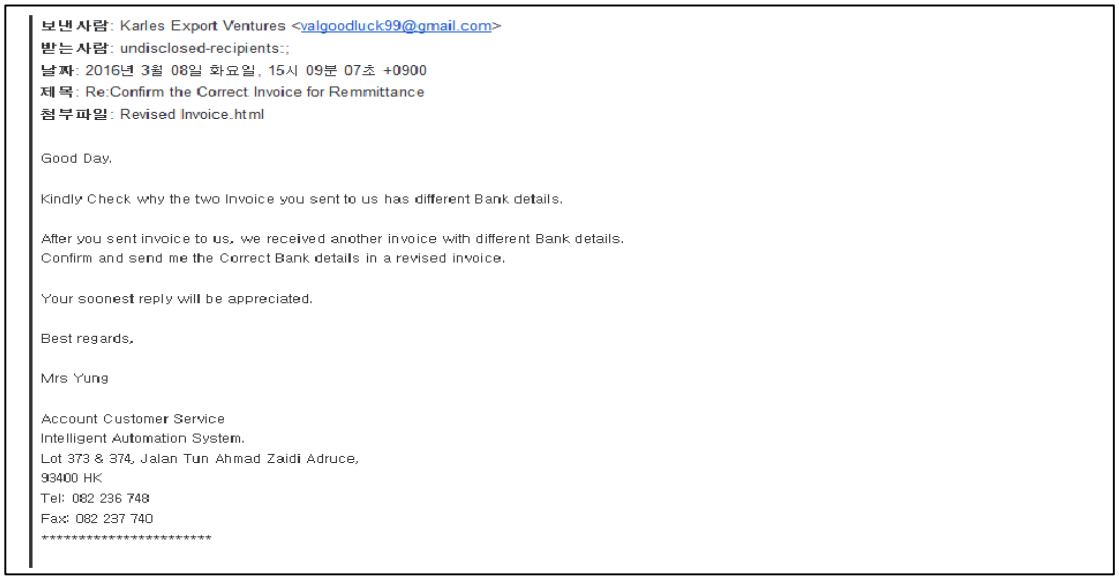
	The number of reported cases	**The total damage**	**The average damage per case**
2013	44	4 billion Won (£2.7 million)	90.9 million Won (£61,204)
2014	88	6.5 billion Won (£4.4 million)	73.9 million Won (£49,728)
2015	150	-	-
2016	155	-	-
2017	187	-	-

Cyber trade fraud emerged as a noticeable type of cybercrime from 2015 onwards. Unlike large companies, which have an abundant experience with exporting and importing, SMEs are generally unaccustomed to international transactions. In this respect, SMEs tend to fall for trade fraud when trade fraudsters target them. The Korea International Trade Association (2015) announced that it would host meetings with SMEs from June 2015 to inform them about fraudsters' *modus operandi* and the appropriate preventative measures to be taken. This effort was intended to alert and educate SMEs, but there was a clear lack of coordinated efforts from government

43 Anyone can request official statistics and data from any public sector organisations via www.open.go.kr.

44 The figures in this table involve cyber trade fraud perpetrated via emails only.

agencies. Whereas public and private organisations gathered together to deal with cyber financial fraud on a national scale, cyber trade fraud did not command enough attention from the concerned public entities. The email below is an example of trade fraud.



보낸사람: Karles Export Ventures <valgoodluck99@gmail.com>
받는사람: undisclosed-recipients:;
날짜: 2016년 3월 08일 화요일, 15시 09분 07초 +0900
제목: Re:Confirm the Correct Invoice for Remmittance
첨부파일: Revised Invoice.html

Good Day.

Kindly Check why the two Invoice you sent to us has different Bank details.

After you sent invoice to us, we received another invoice with different Bank details.
Confirm and send me the Correct Bank details in a revised invoice.

Your soonest reply will be appreciated.

Best regards.

Mrs Yung

Account Customer Service
Intelligent Automation System.
Lot 373 & 374, Jalan Tun Ahmad Zaidi Adruce,
93400 HK
Tel: 082 236 748
Fax: 082 237 740
****

Figure 3.2 An example case of cyber trade fraud

There may be a shift underway in cyberspace from financial fraud to trade fraud. This is called crime displacement. Committing cyber trade fraud does not require special skills other than the general ones needed for cyber financial fraud. Thus, cyber financial fraudsters do not need to put more effort into committing cyber trade fraud. There is no additional entry barrier between cyber financial fraud and cyber trade fraud.

One reason behind the crime displacement is a cost-benefit analysis. Potential criminals are more likely to commit a crime which gives them more benefit for the same amount of effort. The benefit (i.e., the average damage per case) from cyber trade fraud greatly outweighs that from cyber financial fraud (see: Table 3.6 and 3.7). Another reason is deterrence effects. When crime prevention policies have deterrence effects on certain types of crime, motivated offenders will move onto other crimes. In the case of cyber financial fraud, the Prime Minister's Office led the national initiative, formulating a holistic framework from the end of 2013. In fact, the number of reported crimes

consequently decreased between 2013 and 2016 (see: Table 3.6). This decline may be interpreted as the result of effective deterrence against cyber financial frauds. If this interpretation is assumed to be true and the trend continues, crime displacement may happen from cyber financial fraud to cyber trade fraud.

3.4 National cyber security governance

3.4.1 Cyber security agendas and initiatives

In South Korea, the government ministries and agencies[45] involved in cyber security are divided according to the sector (i.e., military, public, and private) they are required to protect: KrCert is the agency that is responsible for engaging with the private sector (National Intelligence Service, 2015).

The National Security Office (NSO) under the Presidential Office takes on the roles of a command station for dealing with national cyber threats, acting as a hub of emergency responses (National Intelligence Service, 2015). The National Cyber Security Centre under the National Intelligence Service (NIS)[46] supports the NSO by leading the involved public and private sector organisations. The centre has an authority to coordinate not only a wide range of policy implementations, but also practical operations, no matter which sector is concerned (J. Kim, 2014). The related agencies do their part according to national directives. However, the structure is oriented to emergency management rather than coordination of activities and prioritisation of agendas. There is no review mechanism on the regular basis within the structure (Yun, 2016). In this respect, many scholars argue that there is no control tower which concerns a cyber security strategy (Jang, 2014, p. 110).

45 The government entities involved are the National Security Council, National Intelligence Service, Ministry of National Defence, National Police Agency, Communications Commission, Personal Information Protection Commission, Ministry of the Interior, the Ministry of Science, ICT and Future Planning, etc.

46 NIS is a Korean intelligence agency equivalent to MI5 or MI6 in the UK.

To comprehend the cyber security governance, three distinct characteristics need to be pointed out. Firstly, from the legal point of view, the government's cyber security activities do not have a fundamental legislative basis (J. Kim, 2014). In fact, those are based on the 'National Information Security Management Regulation', which is an ordinance, not a law or even a presidential decree. An ordinance is a government order that only affects subordinate government agencies. They cannot regulate the rights of citizens. However, the government's cyber security measures have a huge impact on businesses and individual citizens. Many legal scholars argue that these government activities do not have a sound legal basis; as such, they violate constitutional values. Additionally, most civic groups have serious doubts about the overwhelming authority of the intelligence agency (NIS), asserting that the government's countermeasures are likely to infringe on human rights. This weak legal standing has led to the lack of public legitimacy (Park & Kim, 2013).

Secondly, the NIS dominates the whole national agenda with respect to cyber security. This is somewhat understandable, considering that South Korea has to confront North Korea's communist regime. The protection of national infrastructure from North Korea has been deemed the government's top priority. In the event of cyber terrorism, the NIS effectively takes charge of all investigations into cyber security breaches, as stipulated in the 'National Information Security Management Regulation'. It is considered so serious a problem that the NIS is authorised to coordinate every aspect of governmental strategy and to distribute resources. Due to the significant role of the NIS, the cyber security framework mainly involves responding to cyber terrorism on the national level. While most government resources are devoted to protecting critical infrastructure such as telecommunications, electricity, transportation, chemical production, and financial services, which are run by public organisations and large corporations; however, on the other end of the spectrum, SMEs have been largely neglected. This skewed focus is perhaps unjustified since there is not much concrete evidence for the spread of cyber terrorism and the actual threat it presents (Denning, 2000; Yar, 2013).

Thirdly, the South Korean government does not have a proclaimed national cyber security strategy (Jang, 2014, pp. 105-113). However, there is a quasi-strategy, which is called, 'National Cyber Security Comprehensive Measures'. This report was set up in July 2013 and aimed to achieve: (1) raising responsiveness against cyber threats, (2) establishing smart cooperation among involved departments and agencies, (3) providing solid security measures in cyberspace, and (4) preparing for a creative cyber security platform (Ministry of Science, ICT and Future Planning, 2013).

However, the publication of the report was a hasty response to the 3.20 cyber-terror[47] and 6.25 cyber-terror [48] which targeted important public institutions and large corporations. At that time, dealing with cyber terrorism was the focal point of the government. Due to the situational urgency, there was a lack of discussion on what components the report needed to encompass and how it could be associated with other policies on higher and lower levels. This means that the 'National Cyber Security Comprehensive Measures' was not aligned with other strategies. Unlike the UK's cyber security structure, which shared mutual goals and objectives, the Korean equivalent failed to maintain a logical structure at either the strategic level or the operational level. In addition, this report failed to sufficiently take cyber security governance, legal framework, and international cooperation into consideration (Yun, 2016). There was also a problem in relation to report dissemination. The government did not disclose the full text of the report and the report was not passed on to several involved departments and agencies, including the NPA (Jang, 2014, p. 105). Thus, this report was understood as a publication of comprehensive countermeasures, rather than a national strategy.

47 On 20 March 2013, the electronic networks of major television stations and banks were paralysed. A North Korean cyber warfare agency, Bureau 121, was blamed for this attack.

48 On 25 June 2013, 69 major government institutions, including the Blue House, were victims of website change, DDoS, information theft, and code injection. Upon discovering that the hackers used similar hacking methods to those deployed during the 3.20 cyber terror, the South Korean government announced that North Korea was behind this incident.

The absence of a national strategy delivers a serious problem. Korean public and private sector organisations as well as international society do not know what the Korean government's position is in terms of cyber security. The absence of the strategy reflects that the Korean government approaches cyber threats from a narrow perspective. One noticeable thing is that cyber security threats and cybercrime are not viewed as requiring public and private partnerships or an inter-departmental approach. The perception behind this could be that those problems can be solved by only a handful of government agencies or departments.

3.4.2 Reporting mechanisms

There are two strands of reporting mechanisms in South Korea. One involves general cyber security breaches, and the other concerns cybercrimes. Firstly, KrCert, or the Korea Computer Emergency Response Team Coordination Centre, deals with cyber security breaches in SMEs (National Intelligence Service, 2015). The KrCert covers the whole private sector except for the financial services industry, which is protected by an independent public entity, the Financial Security Institute[49]. When a suspicious activity is found in computers or networks, businesses are offered a consultation from the KrCert. The KrCert investigates the case to identify the cause and source of a breach. However, this investigation is rather a technical inspection, and is therefore different from a criminal investigation.

Secondly, the police initiate an investigation if a breach is recognised as having violated the law. Because the Korean Police are one national police force, local police stations and sub-stations provide standardised services to public across the nation. In terms of reporting criminal cases and investigation, a local approach is taken. Once citizens

49 The assumption that underlay the creation of the Financial Security Institute was that the protection of financial assets of customers was of vital importance, especially since the financial services industry was the main target of cybercriminals.

realise that they are victimised, they can go to the nearest police station to report the case. There is no national reporting centre like Action Fraud in the UK.

It is worth mentioning that no studies or government publications suggest that private or international nodes are partners in reporting mechanisms. Unlike the UK's single point of contact, victims in Korea can contact several public agencies: KrCert, the Police or Prosecutor's Office[50]. The absence of a single point of contact has given rise to confusion among the public and inefficiency from the agencies involved. On realising the disadvantages, the NPA dispatched three police officers to 118 call centre in Korea Internet & Security Agency (KISA) from 2015 which handled phone calls from citizens and companies with cyber security problems. If a call handler suspected an incident was related to cybercrime, he or she referred the call to the dispatched police officers to provide a detailed consultation. In 2016, the 118 centre received 365,735 calls and 4,416 calls among them were referred to the police. However, of 4,416 calls, only one incident was booked for official investigation (NPA, 2017b). This can be interpreted in various ways. It may be that victims did not want to engage in actual investigation or that the absolute majority of the referred calls did not even provide enough evidence for the investigation.

SMEs can also approach these points of contacts when they find suspicious online activities. It is questionable how much information SMEs get from government organisations. When an agency receives reports from SMEs in need of help, information starts to flow from the latter into the former. While SMEs try to give all information possible to get support, the agency is usually reluctant to share information that might help SMEs to protect themselves in the future. This indicates that the relationship between SMEs and these government agencies is unilateral rather than bilateral, which results in asymmetric information sharing. The unbalanced relationship comes from the nature of the reporting mechanisms, which is reactive rather than proactive.

50 The Prosecutor's Office has a statutory authority to investigate a criminal case of any kind, but direct investigations into cybercrimes by the prosecutors are rare.

3.4.3 Cyber security initiatives for SMEs

The South Korean economy depends heavily on the export of manufacturing products, and technology-oriented industries account for most of its exports (Ministry of Strategy and Finance, 2015; Observatory of Economic Complexity, n.d.). Because of the economic importance of exports and technology, protecting technology information is one of the government's principal interests. The government has concentrated its resources on securing the proprietary information of businesses directly related to exports (Choi, 2010; Park, Lim, Lee, & Lim, 2013). Following this governmental drive, in academia much of industrial security researchers has studied technology protection of businesses. Between 2010 and 2016, over two thirds (78.7%, 37 out of 47) of studies on industrial security were found to focus on technology protection (Lee, 2017). This tendency is also applied to research on SMEs. Academic studies on SMEs' cyber security focused on technology leakage (e.g., Chang, 2010; Kang, 2015; Y. Kim, 2014; Nam, 2012). The focus on technology protection and leakage is problematic in that this narrow scope of research excludes many areas in the industrial security discipline (Jung, Ryu, & Kim, 2012).

In terms of the government's initiatives, there are two policies that aim to protect exporting companies from cyber security breaches. Firstly, the KISA has created a security standard called the 'Information Security Management System (ISMS)'. This security standard is a modified version of ISO/IEC 27001 for protecting enterprises in South Korea. The ISMS is predicated on the 'Act on the Promotion of Information and Communications Network Utilisation and Information Protection'. This national standard was designed to cover large companies[51]. If a company does not go through the process, it will be ordered to pay a penalty of 30 million won (£20,197). Unless SMEs operate in a sector related to the Internet or online data, the standard is not compulsory (Kim & Kim, 2016). The certification costs over 10 million won (£6,732), but the KISA

51 Clause 47 stipulates that ISPs, Internet Data Centres, enterprises with an annual turnover of over 150 billion won (£100.9 million), and online enterprises with a turnover of more than 10 billion won (£6.7 million) or with more than one million daily users must obtain ISMS certification.

reimburses 30% of the cost for SMEs (KISA, 2016). However, this means that SMEs still have to pay 7 million won (£4,712) for the process, which is a great deal of money for them. In addition, the KISA has not clearly outlined the potential benefits of the certificate for SMEs. The agency is certain that the certificate can increase cyber security levels, but how it can help SMEs to increase their business values is not presented. It is questionable how many SMEs will voluntarily apply for the certificate.

Secondly, the SMBA, a public body, established a security operations centre in Seoul to monitor, assess, and defend the systems of SMEs 24/7 in November 2011 (SMBA, 2011). This centre provides registered businesses with security monitoring, vulnerability check-ups, incident alarms, and monthly feedback. The main objective of this service is to prevent the leakage of confidential technology information, such as proprietary information, intellectual property, and trade secrets. When it embarked on this service, it aimed to extend its reach from 250 enterprises in 2011 to 5,000 enterprises in 2015. Most participation came from medium companies: there was meagre participation from small businesses. This lack of registration was caused by one of the service's requirements whereby a registered company must have network systems such as an Intrusion Prevention System, a firewall, and an Intrusion Detection System (SMBA, n.d.). However, installing these systems is costly and small owners are unaware of the requirement to do so. While the security operations centre was intended to cover SMEs, its requirements have created an entry barrier that has prohibited SMEs from registering. The creation of the security operations centre was based on the assumption that cyber security breaches targeting proprietary information of SMEs were serious. However, it should be questioned whether there is compelling evidence to prove this argument.

3.4.4. Relevance of the UK's cyber security framework to South Korea

The cyber security framework was constructed through a top-down decision-making process both in the UK and South Korea. As cyber security was interlinked with national security, the framework was established with a focus on maintaining national interests.

However, the two governments looked at this issue from a different angle due to the disparate socioeconomic contexts in which they were situated. There were several distinctive points found between the South Korean and UK's cyber security frameworks. Documentary research has found some differences in three dimensions (see: Table 3.10).

Firstly, the most distinctive trait of the UK's framework was the alignment of the hierarchical strategies (see: Section 2.6.1). From National Security Strategy to framework for internet investigations by National Police Chiefs' Council, there was a logical consistency. By dealing with cybercrime as a subset of cyber security, cybercrime could be viewed as a continuum of cyber security and risks. This allowed for policy makers to broaden an understanding of cybercrime in association with cyber security agendas. Thanks to the comprehensive coverage of the strategies, the UK government clearly recognised that SMEs were potential victims which needed to be protected.

In contrast, there was no national cyber security strategy in South Korea. With the absence of the strategy, the government could not have a structured approach to cyber risks and threats. Thanks to the socio-political background, this resulted in focusing heavily on cyber terrorism perpetrated by North Korea. While cyber terrorism was dealt with on the national level, cybercrime was deemed as a local matter and primarily the police were responsible for it. With having no coordination and prioritisation of agendas, protection of Korean SMEs was not on its list of priorities. In this respect, discourses on cybercrime, cyber security, and general risks and security were separated and not discussed in connection with one another. The great loss from this porous structure was that it failed to reach and protect SMEs from cyber risks and cybercrime.

Secondly, the UK government adopted a program-based approach to implement the national strategies. The NCSP ran for five years with £860 million investment (see: Section 2.6.3.1). Based on the clear objectives, this programme supported not only public organisations but also businesses. In addition, there was an emphasis on the public and private cooperation (see: Section 2.6.3.2). In connection with Regional

Organised Crime Units, 10 regional offices of the CiSP attempted to reach local businesses in order to promote the information sharing of cyber security issues. Along with the aligned cyber security structure and strategies, the two underpinning initiatives, the NCSP and CiSP, aimed to support SMEs in a different manner.

On the other hand, the Korean government took an issue-based approach. National approaches to cyber security were oriented towards emergency management rather than risk management. Most attention was given to resolving a breach on the national level without focusing on how to manage risks in normal times. As an example, when cyber financial fraud emerged as a primary social problem in 2013, the Prime Minister's Office took the government-led join industry initiative to address the issue (see: Section 3.3.1). This initiative involved various watchdog agencies and law enforcement agencies for implementation. This indicates that it was based on a regulatory or crime control framework (see: Section 3.3.1). The nexus between the issue-based approach and the regulatory or crime control framework is intuitive in that they were considered to be effective in resolving an abrupt issue within a short period of time. Although the use of regulations and arrests could attain a strong effect in the short term, these were, rather, reactive measures which did not necessarily relate to risk management.

Thirdly, the UK reporting mechanism included private and international organisations based on the assumption that cyberspace could not be secured only by the public police. Forming broad partnerships with non-public nodes was necessary in dealing with cybercrime which is global, asymmetric, and automated. When it comes to a reporting system, it took a national approach based upon a single point of contact (see: Section 2.6.5). As to cyber fraud and cybercrime, the UK government received reports on a national basis via Action Fraud. Depending on the NFIB's scoring criteria, reports which were judged to be worth investigating were passed on to local forces for a criminal investigation.

Compared to this, the Korean government did not include non-public entities as their partners. There was no clear indication that private or international organisations were their working partners. Besides, the Korean reporting system allowed for several points of contact (see: Section 3.4.2). Cybercrime victims could report to any police stations, KrCert, or Prosecutor's Office. Public reports were expected to be readily reviewed by an investigator. In principle, this guaranteed a swift process, which was of great benefit to victims. However, redundant reporting mechanisms could entail management inefficiency for the agencies concerned. Not only that, the localised and redundant mechanisms could make national agencies have difficulty comprehending the cybercrime trend on the national level.

In conclusion, the UK framework was formulated through national leadership which provided a guidance for involved government departments and agencies. Furthermore, the UK framework acknowledged the significant role of private and international organisations, embracing the concept of internet governance. There was a consistency among the cyber security structure, approaches to cyber security, and reporting mechanisms. The greatest gain could be that the UK framework was more likely to reach and protect SMEs. In contrast, it was analysed that there was a clear lack of national leadership in the South Korean framework, ranging from the structure, approaches, and reporting mechanisms. These three dimensions were not interlinked because the framework was unstructured without having national strategies and underpinning initiatives. As a result, two tendencies were identified from the South Korean framework: (1) its orientation to reactive measures and (2) a lack of structured interdepartmental as well as public and private sector coordination. From a risk management point of view, the UK's framework was more tuned into addressing risks and threats while the South Korean framework focused on managing emergencies or breaches. A great difference of this was that the Korean government looked at the past when the UK government looked at the future. It would be interesting to see if the analyses here correspond with findings from the quantitative and qualitative data in the later Chapters.

Table 3.10: Comparisons of cyber security frameworks between the UK and South Korea

	UK	South Korea
The Cyber security structure	• Alignment of the hierarchical strategies • Recognition of the role to protect SMEs	• No national cyber security strategy • A lack of attention to SMEs
Approaches to cyber security	• Program-based approach (e.g., NCSP) • Emphasis on public-private cooperation (e.g., CiSP)	• Issue-based approach • Regulatory / crime control frameworks
Reporting mechanisms	• Inclusion of private actors and international partners • Single point of contact • National approach	• No recognition of non-public partners • Several points of contact • Localised approach

3.5 Conclusion

In this chapter, the empirical field of inquiry, or South Korea, was examined. Starting from providing background information of the sociocultural context, cyber security issues and the national cyber security structure were investigated. The government has failed to provide a holistic cyber security framework that includes a wide range of the cyber security breaches against SMEs. Compared to governments, large companies, individuals, SMEs stand alone, without much support from the government.

One small attention paid to SMEs was centred around preventing the leakage of technology information. The government's initiatives targeted only one third of SMEs (30%) which had high levels of technology. Considering that around 60% of SMEs were in labour-oriented industries (see: Section 3.2.3), the majority of SMEs were excluded

from these cyber security initiatives. Some might argue that there can be general deterrence effects from this policy, but measures for technology protection do not necessarily increase overall cyber security. SMEs are also vulnerable to other types of breaches, such as the theft of personal information, cyber financial fraud, or trade fraud.

CHAPTER 4: RESEARCH METHODOLOGY

4.1. Introduction

This chapter begins by introducing two research paradigms germane to research methodologies, and outlines the research design and the process that advances throughout the research. In social science, research methodology is grounded on ontological and epistemological perspectives and closely interlinked with data collection and analysis techniques. How to collect and analyse data hinges on research methodology which is bounded by epistemological paradigms. Furthermore, interpreting research findings is determined by research methodology. Therefore, the selection of appropriate research methodology cannot be overvalued. For future studies, it is important to describe research methods used in this study in detail in order that this study can be replicated, or at least repeated in a similar way in another country.

First of all, research questions should be clearly stated before research design is established. Research questions guide the research progress as they take the role of a reference point for the research as a whole. The following sections investigate the appropriate research methodology in addressing the research questions. After examining the pros and cons on the compatibility of the two fundamental research methodologies, mixed methods research was chosen as the suitable one for this research. Lastly, data collection methods, data analysis process, and research issues are touched on in the later part of the chapter.

4.2. Summary of the research methodology

This study was based on both positivism and interpretivism for philosophical foundations due to the interdisciplinary nature of this research and the large scope of the research problem. As the research design, a mixed methods approach was taken to raise comprehensiveness as well as to increase the validity of findings. The research was

carried out in three phases: (1) documentary research, (2) quantitative questionnaires, and (3) qualitative interviews. Among various types of mixed methods design, explanatory sequential mixed methods was adopted so that findings from the quantitative data could be explained in more detail with the qualitative data.

Firstly, documentary research was conducted to have some contextualised knowledge relating to the research topic before embarking on data collection. For high reliability and representativeness, the researcher mainly referred to documents and records from international organisations and the governments, such as trend analysis reports, statistics reports, white papers, policy reports, and investigation reports. Moreover, the researcher tried to rely on primary sources to use basic and original data. The government documents for this research were obtained from official channels. This resulted in supplementing Chapter 2, the Literature Review, and constructing Chapter 3, the Empirical Field of Inquiry.

Secondly, quantitative research was carried out via online survey questionnaires. Distribution of the survey questionnaires were facilitated through an online platform of the Korea Federation of Small and Medium-sized Businesses (K-BIZ). As this organisation was aimed at promoting interests of SMEs, this research was found to fit with interests of the organisation. After consultation with the K-BIZ, four provinces and five self-governing areas were chosen in terms of the geographical scope for data collection. Using convenience sampling, emails which included research introduction and the survey link were sent to 5,028 SMEs in those nine administrative areas, and a total of 352 SMEs returned the questionnaires. The response rate was 7% (see: Appendix 6). However, 24 samples were discarded due to poor quality of responses. To sum up, 328 samples were collected from SMEs' IT managers and owners among the total population of around 0.5 million SMEs.

Thirdly, semi-structured interviews were conducted to reflect the points of view from the researcher and respondents. Interviews consisted of two stages: (1) interviews with

IT managers and owners in SMEs and (2) interviews with government officials. Generic purposive sampling was used for the interviews with IT managers and owners in SMEs. These interviewees were selected from the survey respondents in the previous phase. All survey respondents were invited to join an interview through the survey questionnaire guide (see: Appendix 1) and 35 survey respondents accepted the invitation. Finally, the researcher chose 13 IT managers and three owners in SMEs in ways that answered the research questions and that widened variation in organisational characteristics, such as business sector and size. At the next stage, the interviews with government officials were carried out. This stage pertained to three government agencies (i.e., National Police Agency [NPA], Korea Internet & Security Agency [KISA], and Small and Medium Business Administration [SMBA]). Only officials working in the headquarters were appropriate for interviews because cyber security policies were formulated in the headquarters. Snowball sampling was employed because the researcher had difficulty in identifying and accessing appropriate interviewees. Hence, the first contact was found on the website of each organisation and the contact recruited more participants. Three officials from each agency or in total nine officials were selected. The exact number of interviewees at both interview stages was decided during the data collection process, following the criterion of data saturation. Both the quantitative and qualitative phases used non-probability sampling techniques and this approach was appropriate in that this study was oriented to be exploratory.

In terms of data analysis, the quantitative data was analysed via STATA (version 14) which produced descriptive statistics as well as inferential statistics (see: Section 5.3). On the other hand, thematic analysis suggested by Braun and Clarke (2006) was used to identify themes within the qualitative data (see: Sections 6.2, 6.3, 6.4, 6.5 and 6.6). The use of QSR NVivo (version 11.3) provided efficient data management and data transparency (see: Appendix 7). Findings from the quantitative and qualitative research were triangulated with the existing literature to obtain a comprehensive picture of cyber security management in Korean SMEs (see: section 7.2). The triangulation strategy

contributed to gaining additional knowledge and maximising the validity of research findings.

4.3 Research methodology

4.3.1. Philosophical foundations

The choice of research methodology and methods is based on the research problem (Creswell, 2014) and research questions of the study (Johnson & Onwuegbuzie, 2004). In addition, a researcher's perspective on the nature of reality (ontology) and acceptable knowledge (epistemology) in a discipline influences the use of specific methodology and methods. The research approach is related to the interplay of philosophical assumptions, research design, and related methods (Creswell, 2014). Creswell (2014) used the term, *worldview,* to represent ontological and epistemological positions of a researcher. The worldview provides philosophical reasons why the methodology is chosen. Subsequently, the methodology informs the available methods that are used in a study. In other words, the methods selected in a research depend on the methodology which, in turn, is affected by the ontology and epistemology of the researcher.

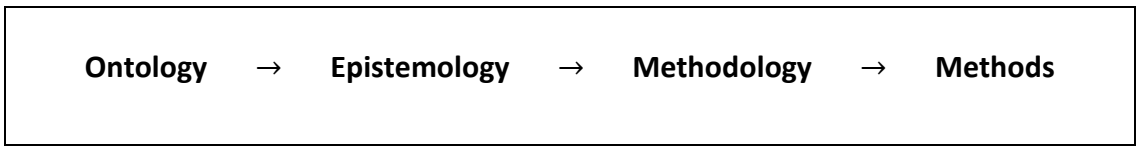


Figure 4.1 Philosophical foundations for research methodology

4.3.1.1. Ontological and epistemological positions

According to Chalmers (2013), a paradigm is "made up of the general theoretical assumptions and laws, and techniques for their application that the members of a particular scientific community adopt" (p. 100). A research paradigm is a philosophical framework that governs research, and also reflects a belief system, worldview, and

theoretical assumptions of researchers (Willis, Jost, & Nilakanta, 2007). Debates on a paradigm revolve around ontological and epistemological positions.

Ontological considerations are concerned with the nature of social entities. There are two ontological positions which are often referred to. The first position, objectivism, implies that social phenomena and meanings exist independently of social actors. Although their existence is not under the influence of social actors, they can work as a restraining force against social actors (Bryman, 2016). For example, organisation and culture as external constructs can constrain social actors through rules and internalised beliefs. The second position is constructionism. This position sustains that social phenomena do not exist separately but are constructed by social actors. Meaning is a social outcome which is constantly revised through human interactions.

Epistemological stances are of great importance in considerations of research strategy (Bryman, 2016). Epistemology concerns the study of how people can know about reality or knowledge. Positivism and interpretivism are the two research paradigms mainly mentioned.

Positivism involves the idea that research methods used in the natural sciences can be applied to the study of social phenomena (Sarantakos, 2013). French philosopher Auguste Comte, who established positivism, advocated sociology, which is called *social physics*, to be validated by the scientific methods (Flyvbjerg, 2001). It is assumed that a reality derived from unchangeable natural laws and mechanisms exist in the form of cause-effect relationship (Guba & Lincoln, 1994). Positivists explain social phenomenon in the same way as natural phenomenon is explained. Objectivity is the most crucial characterisation in this approach and it is required for the researcher to be detached from the research subjects under investigation in order to develop universal causal laws (Weber, 2004). Hypotheses and measurements are incorporated in the research without consideration on contextual factors surrounding research subjects. Based on the

rigorously scientific methods, the findings from particular observations are used to draw broad inferences for population.

Positivism is considered the primary philosophical basis of quantitative research. Quantitative methodology is predicated on the belief that social phenomenon exists objectively. It is assumed that the whole society can be divided into parts or units for research. Emphasis is given to the generalisation of the findings to the whole population. This approach emphasizes that data from social reality are quantified for collection and analyses. Quantitative research follows deductive reasoning. Researchers start off by suggesting a theory to be tested and make hypotheses as presumed answers. After collecting data, they seek to investigate causal relationships among variables via statistical or mathematical techniques based on hypotheses testing. Above all, during this process it is significant for a researcher to take a neutral and objective stance during the research process.

On the other hand, interpretivism is predicated on the view that researching humans is fundamentally different from studying objects in the natural sciences. This position posits that social realm is constructed through interactions among people, indicating that people engage in the interpretation of reality. To study human interactions and behaviours, it is critically important for a researcher to comprehend the subjective perceptions of human subjects in their social and cultural context (Willis et al., 2007). Social constructions such as language, meanings, and instruments are gateways to understand the social world. This approach advocates that the subjectivity of the researcher takes an integral part in the research (Weber, 2004).

Interpretivism constitutes the philosophical underpinnings of qualitative research. Interpretivist approaches and constructionist approaches tend to be spoken of inter-changeably (Robson & McCartan, 2016). Qualitative methodology postulates that social phenomenon is constructed by people in society rather than exists independently. Because the whole society cannot be comprehended by merely aggregating parts of it,

it is critical for a researcher to interpret social phenomena with understanding of the context through multiple perspectives. The reflection of subjective perceptions of a researcher during the research is accepted as a natural process, thus researchers tend to employ case studies, interviews and observation to reflect different aspects of the issue (Robson & McCartan, 2016). Predicating on inductive reasoning, qualitative research closely investigates cases or perceptions and behaviours of people to find hidden concepts or themes. Relationships of concepts are explored in the course of data collection and analysis without predetermined hypotheses.

Table 4.1: Comparisons of philosophical assumptions between the two methodologies

	Quantitative	**Qualitative**
Ontology	Reality exists objectively	Reality is socially constructed by people
Epistemology	Independence between subjects and the researcher	Interdependence between subjects and the researcher
Axiology	Value-free research	Value-oriented research

A long-standing discussion on ontological and epistemological paradigms revolved around the connections between philosophical stances and research methods. Guba and Lincoln (1994) tried to find links between research paradigms and specific methods. For example, positivism is often considered to have a close association with quantitative research, while qualitative research is assumed to be based on an interpretivist or constructivist position. Although these associations are normally expected between ontological/epistemological positions and research approaches, there are no definitive connections (Bryman, 2016). Either qualitative or quantitative research is not wholly or exclusively committed to a specific philosophical stance. Researchers can choose research methods that are appropriate to their research rather than being predisposed by research paradigms.

4.3.1.2. Positivist and interpretive research inquiries

Creswell and Plano Clark (2011) suggested that multiple worldviews can be used in a mixed methods study and that the choice of worldviews is related to the type of mixed methods design. They further explained that researchers can change their worldviews depending on phases in the project. In this study both positivism and interpretivism were taken. The researcher shifted from a positivist worldview in the first phase of the research (quantitative) into an interpretivist worldview in the second phase (qualitative). The nature of the study and research questions worked as a guidance for choosing an appropriate research philosophy. The two stances became philosophical foundations of this research for establishing an appropriate research design that were expected to bring about desired research outcomes.

First of all, the positivist inquiry was chosen to conduct this research scientifically and objectively with empirical data. As was explained in Section 4.3.1.1, positivism is adequate to quantitative research. This study used survey questionnaires as a quantitative tool and quantitative data was statistically analysed through the structured process. Independence between the researcher and subjects and statistical rigour were expected to limit bias as well as to generalise the findings.

Secondly, the interpretivist inquiry was necessary for underscoring the issues being studied in this research. This research intended to be exploratory to build a comprehensive portrait surrounding SMEs' cyber security management. Interviewees from different SMEs were exposed to different business environment and had disparate experiences of security breaches and cybercrimes. Providing this, the interviewees held their own perceptions of the risk, practices, and countermeasures. Also, their interpretations and perceptions were reinterpreted by the researcher to come up with a framework at the final stage of this research.

Table 4.2: Comparisons between quantitative and qualitative methodologies (Halfpenny, 1979, p. 799)

Quantitative	Qualitative
Fixed	Flexible/fluid
Objective	Subjective
Deductive	Inductive
Hypothesis testing	Speculative/illustrative
Value-free	Political
Positivist	Interpretivist
Universalistic	Relativistic
Explanatory	Descriptive/exploratory

4.3.1.3. Debates on mixed methods research

Mixed methods research has emerged as a distinct research approach since 1980s (Creswell, 2014). Although there is no consensus on the definition of mixed methods research, which is often termed as multiple methods, multi-strategy, and triangulation, the general idea is to use more than one method or source of data in the research of social phenomenon. Pragmatism has provided dominant philosophical bases in mixed methods research (Johnson et al., 2007). Pragmatists put more weight on the research question than research methods or worldviews (Tashakkori & Teddlie, 1998). Their perspective indicates that the choice of a research strategy and methods is largely dependent upon the research question in the study. Any valuable research tools can be used if they are deemed to successfully address the research question (Tashakkori & Teddlie, 1998).

There were pros and cons in terms of the compatibility of quantitative and qualitative methodologies. Some scholars were against the compatibility, claiming that they were derived from two different paradigms with conflicting assumptions (Bednarz, 1985; Kuhn, 2012; Sale, Lohfeld, & Brazil, 2002). Different ontological and epistemological

positions of the paradigms did not allow the combination of them for validation or triangulation purposes (Sale et al., 2002). This notion argues that quantitative and qualitative methodologies cannot study the same phenomena due to paradigmatic differences.

On the contrary, other scholars (Bryman, 2016; Creswell, 2014; Johnson & Onwuegbuzie, 2004; Robson & McCartan, 2016) held that both methodologies were compatible each other with the possibility of integration. Although they are associated, respectively, with different paradigmatic assumptions, the association is not deterministic (Bryman, 2016). It is possible that qualitative research is connected to positivism and that quantitative researchers take an interpretivist and constructionist stance. Beyond the possibility of consolidation, mixed method research was considered another type of research paradigm along with qualitative research and quantitative research (Creswell & Plano Clark, 2011; Johnson et al., 2007; Tashakkori & Teddlie, 1998).

4.3.2. Research design

This study adopted a mixed methods approach as the research design. The mixed methods research design is not limited to using more than one research methods but involves the combination of the two research strategies (Bryman, 2016). The combination of the quantitative and qualitative approaches can produce distinctive benefits such as triangulation, comprehensiveness, and stronger inferences that cannot be generated from an individual approach (Johnson et al., 2007; O'Cathain et al., 2007; Robson & McCartan, 2016).

Mixed methods research draws on the strengths of both quantitative and qualitative research and neutralises the weaknesses of an individual research strategy (Creswell & Plano Clark, 2011). Bryman (2006) pointed out offsetting the weaknesses as one of rationales in mixed methods research. In quantitative research generalisation of the findings is highly emphasised. Reliability and validity of the research are very important

criteria so that similar research can be replicated by other researchers. However, quantitative research does not capture the subtleties and complexities of research subjects within a context. In addition, quantitative research does not have much flexibility after a research design is chosen, as it is mostly performed in fixed designs (Robson & McCartan, 2016). On the contrary, qualitative research provides rich explanations on complex relationships among the subjects and the related processes, although it is criticised for a lack of objectivity, generalisation, and transparency (Bryman, 2016). Therefore, mixed methods research can provide a comprehensive illustration of research subjects as well as statistical inferences by combining both approaches. From the research design point of view, this allows the study to have a more robust research process.

Like other research methods, a mixed methods approach has its own challenges. One challenge is that a researcher should be knowledgeable in both qualitative and quantitative methodologies and have more time and resources to complete the research (Creswell & Plano Clark, 2011). There are several types of mixed methods research depending on priority and sequence between the quantitative and qualitative methods (Bryman, 2016). The complexity of the research design models requires a more rigorous approach by the researcher. Another challenge is that it is difficult to fully integrate research findings from the quantitative and qualitative research. Integration means “comparing, contrasting, building on, or embedding one type of conclusion with the other” (Creswell & Tashakkori, 2007, p. 108). Simply presenting quantitative and qualitative findings separately undermines the quality of mixed methods research. When conducting mixed methods research, it is important for a researcher to follow the logic. The logic is explained that qualitative and quantitative methods should compensate for each other to create complementary strengths and diminish weaknesses (Johnson et al., 2007). This logic allows for a researcher to adopt mixed methods research strategically in a way that satisfies research purposes.

When using a mixed methods approach, a justification for this choice needs to be clearly provided (Creswell & Plano Clark, 2011). This approach was selected for this study to increase exploratory power and to enhance the robustness of the research process. The decision to connect both strategies was largely guided by the research problem. The research problem, '*how is cyber security managed in South Korean SMEs?*', could not be comprehensively understood without using both the quantitative and qualitative strategies.

Firstly, the quantitative phase was used to assess cyber security situations for SMEs. This was because there was an obvious lack of situational assessment on SMEs in South Korea. More importantly, it identified relationships or correlations among organisational variables. This investigation helped the researcher to identify organisational factors which were associated with increasing cyber security. This quantitative approach explored general cyber security situations for SMEs, allowing for a statistical balance for this study. The findings produced in this stage laid foundation for the next stage.

Secondly, the qualitative phase addressed unanswered questions from the quantitative phase by interviewing not only IT managers and owners of SMEs but also officials in government agencies. This data collection process helped to capture the complexity of the contexts surrounding SMEs. The scope of this research was broadened because this strategy presented an in-depth understanding of the research problem. The qualitative findings eventually aimed to provide interactions between internal arrangements and external influences by shedding light on organisational relationships with external entities.

Table 4.3: Mixed methods research for this study

Research strategy	Research methods
Quantitative research (1st)	● A self-completion (online) questionnaire of SMEs' IT managers and owners (328 samples / convenience sampling)
Qualitative research (2nd)	● Semi-structured interviews with SMEs' IT managers and owners (16 interviewees / generic purposive sampling) ● Semi-structured interviews with cyber security officials in the KISA, SMBA, and NPA (9 interviewees / snowball sampling)

In a mixed methods design there are three basic types except other advanced types (Creswell, 2014, p. 15).[52] The first type is 'convergent parallel mixed methods'. It is to merge both qualitative and quantitative data in a way that presents comprehensive results. The second type is 'explanatory sequential mixed methods'. Quantitative research is conducted before qualitative research is embarked upon. Quantitative analysis is explained in more detail with the qualitative data. The last one is 'exploratory sequential mixed methods'. The research sequence is the reverse from the second model. The researcher first explores concepts or variables through qualitative research and uses them in the follow-up quantitative research.

Among the three types, the second was employed in this study. The procedure involved collecting and analysing survey data in the first phase, followed up with semi-structured interviews. The main reason for this approach was that the quantitative phase provided an overall understanding of the research problem (Ivankova, Creswell, & Stick, 2006). Quantitative results could be clarified and analysed further with open-ended questions

52 Creswell and Plano Clark (2011, p. 69) suggested six major mixed methods research designs, which were the embedded design, transformative design, multiphase design along with the three basic types. Creswell (2014) claimed that the former three designs were advanced strategies which derived from the basic models.

in the qualitative stage (Creswell, 2014). In this aspect, this approach was useful for the exploration of the research problem. It suited the aim of this study which was to have a comprehensive understanding of SMEs' cyber security management. The follow-up qualitative research after the quantitative analysis offered a detailed layer of information, helping the researcher to answer the research questions.

However, a researcher needs to be cautious in that qualitative analyses in some studies might not add values but merely describe quantitative findings (Robson & McCartan, 2016). Avoiding mere reiteration of quantitative findings was of great concern for this study. The researcher made an effort in order for the qualitative phase to add substantial values by exploring participants' views in more depth.

4.4. Research methods

4.4.1. Documentary research

Documentary research has not been recognised as an established research method (Platt, 1981). Documents keep records of events in detail which normally people cannot have an experience of, providing researchers with access to unobservable actions or events. Payne and Payne (2004, p. 60) define documentary research as "the techniques used to categorise, investigate, interpret and identify the limitations of physical sources, most commonly written documents, whether in the private or public domain" (p. 60). Documents form a significant source of data, but also this research method is applicable at various stages of the research process (Finnegan, 2006). Denzin (1970) argues that documentary research is useful as an independent research method, but also takes a crucial part in conducting a triangulation. Due to these advantages, documentary research is used as a versatile method in many disciplines, for both quantitative and qualitative research. The scope of documents is very large, covering public, private, and personal records. Examples are official records, letters, diaries, photographs, the media, biography, and visual documents (Macdonald, 2008).

This research intended to incorporate national cyber security mechanisms regarding protecting SMEs along with internal cyber security arrangements of SMEs. For this, documentary research was employed to provide contextual information by utilising government and private documents and records. This method allowed for the researcher to contextualise cyber security arrangements and mechanisms.

McCulloch (2004) suggests four established rules when appraising documents: authenticity, reliability, meaning, and theorisation. As a fundamental criterion, documents should be verified as having the genuine origins and provenance. Scott (1990) contends that this criterion is applied to documentary research as well as all social research. Second, reliability refers to trustworthiness of documents. To examine reliability, whether a document contains bias or unfaithful accounts from an author needs to be considered. McCulloch (2004) interprets the concept of reliability broadly by including representativeness as a subset of reliability. Compared to this, Scott (1990) classifies representativeness which involves survival and availability as a separate criterion. Third, meaning involves providing a clarity and comprehensibility to a researcher. Fourth, theorisation concerns a theoretical framework through which documents are analysed. Three main traditions are positivist, interpretive and critical approaches.

Documents need to be read cautiously. Documents on the same event are produced with different orientations or purposes, consequently, presenting different meanings to the same phenomenon. In addition, some documents may not disclose social context which is necessary to construct social settings surrounding an event. For these reasons, a documentary researcher needs to adopt triangulation as a research strategy to achieve validity in a way that examines documentary data from various angles (Macdonald, 2008). Finnegan (2006) provides practical guidelines for researchers. When searching for documentary data, the researcher took eight questions from Finnegan (2006, pp. 146-149) into consideration. These are:

(1) Has the researcher made use of the existing sources relevant and appropriate for his or her research topic?

(2) How far has the researcher taken account of any 'twisting' or selection of the facts in the sources used?

(3) What kind of selection has the researcher made in her or his use of the sources and on what principles?

(4) How far does a source which describes a particular incident or case reflect the general situation?

(5) Is the source concerned with recommendations, ideals or what ought to be done?

(6) How relevant is the context of the source?

(7) With statistical sources: what were the assumptions according to which the statistics were collected and presented?

(8) Having taken all the previous factors into account, do you consider that the researcher has reached a reasonable interpretation of the meaning of the sources?

Chapter 2, the Literature Review, and Chapter 3, the Empirical Field of Inquiry, are the results of documentary research. In particular, Chapter 3 which presented a socioeconomic overview of South Korea relied upon this method to look at South Korean literature. In order to attain high reliability and representativeness, the researcher mainly referred to documents and records by international organisations and Korean and the UK governments. Those documents include trend analysis reports, statistics reports, white papers, policy reports, and investigation reports. They also include some unpublished government documents or circulars. The researcher endeavoured to obtain primary sources rather than secondary sources in that the former conveys the basic and original data, while the latter copies and interprets original materials (Macdonald, 2008). Although the researcher was a Korean police officer, the researcher's status as a Senior Inspector in the NPA did not contribute to obtaining any Korean documents. All of the documents acquired for this research were gathered from official channels.

4.4.2. Quantitative approach (survey questionnaires)

No other research method has become more prominent as survey research in social science disciplines within a short period of time (Blair, Czaja, & Blair, 2014). Festinger and Katz (1953) stated, “It is this capacity for wide application and broad coverage which give the survey technique its great usefulness in the behavioural sciences” (p. 16). The broad applicability of the survey research to social problems has itself given a dominant position in addressing issues from many fields.

The survey research collects data from a sample of respondents who were drawn from a well-defined population. In this respect, how to select samples is a major concern. If the representativeness of the sample is not guaranteed, it is hard to claim generalisation from a sample to a population. Therefore, choosing a right sampling method depending on research purposes is essential in the survey research. The survey research is employed to acquire a body of quantitative data at a single point in time (Bryman, 2016). This is why it is closely related to the cross-sectional design. It means that results from surveys do not present trends over time, but provide a snapshot of phenomena. A researcher asks questions to respondents and the questions are vehicles that measure variables of interest. Usually, a number of variables are to be investigated and patterns of association (e.g., correlations or causal relationships) among the variables are identified via statistical analyses.

Survey questionnaires contain a set of predetermined questions mostly in a closed format. The identical questions are given to respondents to reduce variations that may come from using different words in questionnaires. The standardised manner of the survey research corresponds to the use of a fixed design. The standardisation increases the reliability of quantitative findings in regard to measurement, but there is little room for flexibility after the research design is decided (Babbie, 2007). Another downside in relation to this aspect is that the survey research is less appealing to exploratory studies but appeals more to descriptive or interpretive studies (Robson & McCartan, 2016).

Questionnaire and structured interviews are the two predominant methods in conducting surveys (Bryman, 2016). A researcher can contact respondents in person, by mail or phone, or through the Internet. Survey data collection methods evolve over time, especially reflecting technological innovations (Krosnick, 1999). Computer-assisted personal interviewing and audio computer-assisted self-administered interviewing are the examples. Internet survey is being increasingly used in research. Traditional approaches, such as face-to-face interview, telephone interview, and self-completion questionnaire via mail, require a huge amount of time and money. Moreover, it is challenging to recruit respondents due to their modern lifestyle and privacy issues.

Self-completion questionnaires were administered via the Internet in this study. Survey participants gained access to the survey through an URL from a web-based program, Bristol Online Survey (BOS)[53], which is designed for academic research. Compared to an e-mail approach, web-based programs allow for more response options and flexible survey designs. Robson and McCartan (2016) compare the Internet survey approach to other approaches as shown in Table 4.4. Compared to the traditional methods, the Internet survey has desirable advantages especially in terms of cost and length of data collection period. Also, respondents can be supported by visual aids to assist in following the order of questions.

On the other hand, the response rate of the Internet survey may be lower than that of other methods. People tend to ignore survey emails or delete them because no rapport was created between the researcher and respondents. Another downside may be response bias. People with higher education and socioeconomic status are more likely to have Internet access than poorer people. It is possible that the poor are underrepresented in the Internet survey.

Having said that, in this research the advantages were expected to outweigh the disadvantages in that low response rate and high response bias did not seem to pose

53 www.onlinesurveys.ac.uk

serious harm on the quality of this study. Firstly, Krosnick (1999) argued that according to recent studies surveys with low response rates could yield more accurate results than those with higher response rates. It is supported by the argument that representativeness is not in direct proportion to response rate. Secondly, almost all SMEs in South Korea, research subjects in this study, were connected to the Internet. Most of them had their own websites for advertisement and sales purposes. Also, banking services and administrative processes were undertaken electronically on computers. Considering the high level of connectedness of SMEs to the Internet, the response bias was not a huge concern in this study.

Table 4.4: Comparison of data collection methods in the survey research (Robson & McCartan, 2016, p. 251)

Aspect of survey	Postal Questionnaires	Internet Surveys	Face-to-face Interviews	Telephone Interviews
Cost	Low	Very low	High	Low/Medium
Length of data collection period	Long	Short	Medium/Long	Short
Use of visual aids	Very good	Very good	Good	Fair
Rapport	Fair	Poor/Fair	Very good	Good
Control of question order	Poor	Poor/Fair	Very good	Very good
Response rate	Poor/Medium	Poor/Medium	Medium/Very high	Medium/High
Response bias	Medium/High	Medium/High	Low	Low

4.4.3. Qualitative interviews

The interview is probably the most widely used data collection method and one of the most invaluable sources to obtain information in research. Given the research problem and questions, it was imperative to conduct an interview with managers and owners in SMEs and officials in relevant government agencies. There are three main types of interview, which are distinguished by the extent of structure or standardisation of the interview: (1) the structured interview, (2) the semi-structured interview, and (3) the unstructured interview (Robson & McCartan, 2016).

The structured interview is the least flexible form among the three types. This type of interview is applicable especially when the researcher has a good understanding of the research topic. The interviewer gives each respondent exactly the same questions in the same sequence and respondents have a limited range of answers. By using a standardised format of asking questions, it is easy for a researcher to quantify interview responses. This allows for the maximisation of the validity and reliability of measurement (Bryman, 2016). A trade-off of imposing a standardised manner is that there is a risk of losing vast meanings in responses.

The semi-structured interview intends to reflect the point of view from respondents. It allows the researcher to have his or her latitude to modify interview questions or their order during the interview. Based on an understanding of respondents and the flow of the interview, the interviewer can ask impromptu questions. This enables the interviewer to elicit detailed answers from each respondent. If a particular response is considered significant, the interviewer can probe for more information. One major difference from the unstructured interview is that an interview guide has a series of questions in advance. This means that the latitude of the researcher in the semi-structured interview is much less than that in the unstructured one.

Lastly, the unstructured interview is the most flexible type in the interview process. It aims to “find out what kinds of things are happening rather than to determine the frequency of predetermined kinds of things that the researcher already believes can happen” (Lofland, 1971, p. 76). A distinctive difference from the structured interview is that the unstructured interview intends to uncover the interviewee’s experience of a topic or situation (Lofland & Lofland, 1984). The interviewer keeps an area of interest only and a list of topics in mind which require to be addressed. Phrasing questions and asking them in any sequence are under the discretion of the interviewer. Sometimes, an interviewer can share their opinion on the topic with respondents if the conversation is deemed appropriate. Flexibility of this type enables an interviewee not only to freely articulate ideas and opinions but also express emotions, beliefs, and values. In this context, building good relationships between the researcher and interviewees is very important. Therefore, it is advised that a researcher interviews subjects in person rather than hiring a third person (Burgess, 1984).

The structured interviewing is mostly adopted in quantitative research due to its high validity and reliability. On the contrary, the semi-structured interview and the unstructured interview are described as qualitative interviewing (Bryman, 2016; Robson & McCartan, 2016). Through qualitative interviewing a researcher enquires into experiences, opinions, and viewpoints of others in specific social settings (Rubin & Rubin, 2012; Turner III, 2010). Given the nature of this method, qualitative interviewing is also referred to as in-depth interviewing (Taylor, Bogdan, & DeVault, 2016). It is beyond a simple data collection method, but supports the researcher to reconstruct a whole picture of complicated contexts and process in question. Data collection is conducted through active engagement and interaction between the interviewer and interviewees. The interview is carried out as an informal conversation rather than a formal question and answer session. It implies that interviewees are treated as being equal with the interviewer.

In qualitative research, the semi-structured interview and unstructured interview are widely adopted because of their flexibility in garnering detailed information. Qualitative interviewing has long been used with other research methods, such as participant observation and documentary research. Of the two interviews, the semi-structured interview was finally selected for the data collection method in the qualitative phase. This was due to the research design and research orientation of this study. First of all, survey findings from the quantitative stage informed a set of questions that needed to be asked during the interviews. This brought about some structure to the interview. Second, the qualitative phase was oriented to explore research questions in more depth while clarifying and explaining the quantitative findings. The interviewer probed for more information by changing the order and even the wording of questions, following up the responses from the interviewees.

4.5. Data collection and analysis

4.5.1. Data collection

4.5.1.1. Sampling strategy

It is important for a researcher to clearly define the unit of analysis and the level of analysis before carrying out the research. The former is what or whom is being studied and the latter concerns the scale of the research. The unit of analysis in this study was SMEs and the research fell into a meso-level analysis. In addition, it is worth distinguishing the unit of analysis from the unit of observation. It is usual that they are identical in a study (Babbie, 2007), but that is not the case in this research. Although this study was on organisations, organisational data were empirically drawn from individuals. In other words, the research collected data at the individual level of observation, but the level of analysis was at the organisation level. Characteristics and behaviour of SMEs were measured by quantitative questionnaires and qualitative interviews.

Sampling techniques are categorised broadly as probability sampling and non-probability sampling. Probability sampling guarantees the equal chance of each unit to be included in a sample, while non-probability sampling does not entail a randomised selection method. It is hard to argue which, if any, is better than the other. The choice of sampling techniques depends on various vectors such as research questions, design and methods.

Probability sampling is generally preferred by quantitative researchers. In quantitative research, it is vital to elicit statistical inferences about the population from the sample. The inferences are drawn upon for the generalisation of the research findings to an entire population. The generalisation is possible in probability sampling because the sample is selected as representative of the population. It should be guaranteed that samples are chosen in a random fashion. Even though probability sampling cannot get rid of sampling error, this randomised selection process has a better chance of reducing sampling error than non-probability sampling (Bryman, 2016). On the other hand, non-probability sampling does not have logical grounds to make statistical inferences (Robson & McCartan, 2016).

In qualitative research, there is a greater preference by researchers to use purposive sampling as a non-probability form of sampling (Bryman, 2016). This is mainly because qualitative research gives more emphasis on the context and process. Qualitative researchers attempt to provide thick descriptions on research subjects in the setting being investigated and how interactions among the subjects evolve over time in context. Thus, it is needed to intentionally select samples that fit into research purposes and questions.

In this study, each stage utilised different sampling strategies. A quantitative data collection process used convenience sampling. This was followed up by qualitative interviews with a subset of the survey respondents. The interviewees were chosen

through generic purposive sampling. Lastly, government officials were selected via snowball sampling for additional qualitative interviews.

Firstly, the survey of IT managers and owners in SMEs used convenience sampling. As a type of non-probability sampling method, this technique is usually used when there is a high accessibility to potential samples. Convenience sampling has no inclusion and exclusion criteria in terms of selecting samples and does not require high costs and long duration of time. Due to the ease of research, this technique is adopted by many social science researchers. In particular, in the field of organisation studies convenience sampling is more commonly used than probability sampling (Bryman, 2016).

The data collection of survey questionnaires was possible due to support from the K-BIZ. This organisation is an interest group whose members include almost all SMEs in South Korea. Thus, it has contact details of its members, communicating with them on a regular basis. This organisation also has an online platform which enables constant exchanges of information with SMEs. The researcher contacted the organisation for support in this research. The K-BIZ is known for its openness to researchers and experts who wish to approach SMEs as academic interest from outsiders are considered important elements to gain supports for SMEs. After obtaining official approval from the K-BIZ, the researcher asked for the K-BIZ to pass on an invitation letter and survey questionnaires to SMEs via email. The researcher relied on the K-BIZ contact list by virtue of its accessibility.

As SMEs are dispersed around the nation, it is almost impossible to conduct random sampling method without full support. Instead, convenience sampling method was an appropriate choice for this research. In South Korea, there are eight provinces and nine self-governing areas. Of these, four provinces and five self-governing areas[54] were randomly selected in order to narrow down the geographical scope for data collection.

54 These include Gyeonggi-do, Gangwon-do, Gyeongsang buk-do and Gyeongsang nam-do, Seoul, Busan, Daegu, Daejeon and Ulsan.

Using convenience sampling method, emails which contained research introduction and the survey link were sent to 5,028 SMEs in those nine administrative areas. A total of 352 SMEs returned the questionnaires online for a response rate of 7% (Appendix 6). The survey data were collected for about two months (28 Oct 2016–27 Dec 2016). Although 352 samples were collected, 24 samples were discarded because of the poor quality of responses.

Secondly, it was followed up by semi-structured interviews with IT managers and owners in SMEs, using generic purposive sampling. This sampling technique is often used in a mixed methods context in that quantitative data are used as the basis for selecting qualitative samples (Bryman, 2016, p. 414). In this study, a group of respondents in the quantitative phase became a sampling frame from which qualitative samples were drawn. In the survey questionnaire guide (Appendix 1), it was mentioned that they were also invited to participate in a further interview. Survey respondents who expressed their willingness to join constituted the sampling frame for the qualitative interview phase. Thirty-five survey respondents accepted the invitation and 16 SMEs were selected from them. The selection depended upon the research questions which needed to be answered. The researcher also tried to reflect variation in organisational characteristics, such as business sector and size. This process followed the idea that data collection in the qualitative stage is based on the quantitative results (Creswell, 2014, p. 224).

In the generic purposive sampling, there are established criteria in selecting cases or contexts and the criteria are mostly informed by the research questions (Bryman, 2016). The unanswered questions and newly-emerged questions from the survey findings were important guidelines for deciding the criteria. Questionnaire answers of the respondents were reviewed in light of the criteria in order to identify proper samples that fitted into those criteria. It was a purposive process from finding the criteria to choosing samples. The researcher continued to collect samples until the research questions were fully answered.

Thirdly, when it comes to a sampling method for semi-structured interviews with government officials, snowball sampling was used. Government agencies related to this research were the NPA, KISA, and SMBA. At first, the researcher identified one or more initial participants relevant to the research topic and then the identified participants recruited other individuals who were relevant to the research. This sampling process continued until the researcher had enough samples.

In terms of interviewing government officials, the researcher intended to interview officials working in the headquarters of the NPA, KISA, and SMBA. These agencies directly or indirectly addressed cyber security issues of businesses, although each agency took a different approach. Because cyber security polices and schemes for SMEs were mostly drawn up and formulated in the headquarters, and officials in local offices were not aware of ongoing issues and severity of the problems on the national scale.

Snowball sampling is useful when it is difficult to identify appropriate participants (Bryman, 2016, p. 415). This difficulty was also applied to this study. Since the researcher had no experience in working in the cyber security field, there were no initial acquaintances within those agencies. Thus, the first contact was found on the official website of the organisations. All public organisations in South Korea provide specific roles and contact lists of sub-departments on their websites in order to enhance public accountability and transparency. Subsequently, the researcher asked the first contact person for more contacts in his agency relevant to the study. All interviews were carried out for one month (02 Feb 2017–28 Feb 2017).

To sum up, both the quantitative and qualitative phases used non-probability sampling techniques. In the mixed methods research, using non-random samples in both quantitative and qualitative phases is the most frequent combination, regardless of research goal, objective, purpose, and question. (Onwuegbuzie & Collins, 2007). The quantitative and qualitative data in this research cannot be generalised because samples drawn from non-probability sampling do not exhibit a proportional representation of

the population. The research findings are valid within the social settings germane to the study, which means that the application of the findings to other contexts might not be appropriate. This indicates that these sampling techniques might entail weak external validity. However, non-probability sampling was considered an appropriate choice for this research because this study aimed to be exploratory rather than representative.

4.5.1.2. Population and sample size

The total population of this study is all the SMEs in South Korea. In this study, SMEs are referred to as a company whose number of employees is more than 9 and less than 300 employees (see: p. 84). As discussed in the previous chapter, the number of SMEs in this category was on the rise annually with a total of 479,349 in 2014 (see: Table 3.4). At the time of data collection the number of SMEs was estimated to be around 0.5 million.

There is no hard and fast rule in terms of deciding sample size in a study. One misunderstanding might be that quantitative research involves large samples whereas qualitative research uses small samples. In fact, the sample size varies according to the research questions, purposes, and the research design (Onwuegbuzie & Collins, 2007). It is also true that a larger variation exists between quantitative and qualitative research than variations within either quantitative research or qualitative research. Due to the differences of research orientation, both research strategies have their own criteria when deciding sample sizes.

Large sample size is mostly applauded in quantitative research. This is because raising sample size increases validity and representativeness of the research while reducing sampling error. Determining the appropriate sample size in quantitative research largely depends on confidence levels and confidence intervals (Babbie, 2007). This study followed a general standard, which is 95 percent confidence level and plus or minus 5 percent confidence intervals. This means that the researcher can be 95 percent

confident that the study findings are accurately within the interval. The sample in the quantitative phase consisted of 328 out of a total of 0.5 million SMEs.

In a similar vein, a variation exists in the size of sample in the qualitative research (Bryman, 2016, p. 417). Unlike the quantitative research which has numeric criteria in choosing the appropriate sample size, the choice of sample sizes in qualitative research is decided largely by the researcher. It does not mean that the choice of sample size is purely subjective. When it comes to the minimum number of samples, there is no unified standard. Warren (2002) argued that interviewees between 20 and 30 are the minimum number in qualitative research, while Adler and Adler (2012) suggested that samples between 12 and 60 are appropriate. In the case of using interview as a data collection procedure, Guest, Bunce, and Johnson (2006) asserted that 12 interviewees were sufficient if a selected group is not particularly heterogeneous.

Taking a considerable variation of qualitative research into account, Bryman (2012) suggested five criteria in deciding sample size: (1) theoretical or data saturation, (2) minimum requirements for sample size, (3) the style or theoretical underpinnings of the research, (4) the heterogeneity of the population, (5) the breadth and scope of research questions. These criteria are useful guidelines not only when making a decision on sample size, but also when providing a justification for the decision. Among these criteria data saturation (theoretical saturation in studies using grounded theory) is considered the most important one. Data saturation suggests that samples should be collected up to the point at which new themes are not found in the data. It is ideal for sample sizes not to be too small to acquire data saturation (Onwuegbuzie & Collins, 2007). This is the reason why the minimum number of samples is included in the five criteria. In this research, the exact number of interviewees was decided during the data collection process. The decision was guided by the survey findings and research questions that needed to be answered. The researcher ceased further sampling when similar themes were repeated and new themes were not identified. It was decided that 16 IT managers

and owners from SMEs and 9 government officials were the proper number of interviewees to provide meaningful findings and analyses.

4.5.2. Data analysis

4.5.2.1. Data analysis process

The survey questionnaires contained nominal and numeric data on a range of issues regarding cyber security situations of SMEs. Numeric data were measured by the 5 Likert scale. The quantitative data collected was coded and analysed by statistical software, STATA (version 14). STATA has a vast array of statistical functions, carrying out analyses of complex quantitative data.

The quantitative data was used in two ways. Firstly, descriptive statistics such as frequencies and percentages presented rudimentary information on each survey question. Secondly, inferential statistics such as chi-square tests, one-way Analysis of Variance (ANOVA) and two sample t-tests were run to see whether there was an association among different categorical groups. These tests were undertaken mostly by business size and categories of business sector.

To analyse the interview data, thematic analysis was used to identify patterns or themes within data. This is one of the most widely adopted approaches among qualitative analytic methods. As other analytic methods, thematic analysis has both advantages and disadvantages. Braun and Clarke (2006) argue that one of the advantages of thematic analysis is its flexibility which enables it to be applied across different types of epistemological paradigms. However, compared to other analytic methods such as grounded theory, thematic analysis is not an identifiable technique (Bryman, 2016). As such, there are no clear procedures of conducting thematic analysis despite its universal applicability. In addition, Bazeley (2013) argued that thematic analysis tends not to clearly explain the processes through which themes are identified and emerged from

data. Therefore, it is important to articulate the way that themes are identified and how they relate to other themes (Bryman, 2016). These processes need to be justified. It needs to be clearly explained how themes are associated with research questions and literature. The choice of an analytical method comes down to research questions, which implies that research questions should inform a proper method (Holloway & Todres, 2003).

This research used a thematic analysis process proposed by Braun and Clarke (2006). There are six phases of analysis, which is recursive process: (1) familiarizing yourself with your data, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing a report. The researcher transcribed interview conversations in Korean first and then translated them into English. One Korean-American reviewed the whole transcription to check the quality of the transcription. After a couple of readings of the data, the coding process started to generate descriptive codes, analytic codes, sub-themes and finally themes[55]. Analytic codes were examined closely to identify relationships and patterns. This thorough examination let the sub-themes and themes emerge from the data.

The qualitative data was analysed through QSR NVivo (version 11.3) which is a qualitative data analysis computer software package. The software contains a wide range of functions such as data management, coding, and categorising of data from interviews, observations, and multimedia sources. Using software for data management is becoming the standard in qualitative research. It is essential to organise and manipulate large amounts of data in a way that enriches the analysis. Using software also supports transparency in a research process. Having the data organised in accessible dataset for others to be able to access and interpret from supports the broad goal of transparency.

55 The coding process generated 116 analytic codes, 15 sub-themes, and five main themes – for more details (see: Appendix 7).

4.5.2.2. Triangulation

In social science, triangulation refers to the examination of the research problem from at least two different perspectives or by using multiple research methods. It aims to increase the validity of the procedures and results of research as well as to improve the research rigour. This strategy is based on the premise that a research topic can be better comprehended if the researcher incorporates multiple perspectives (Denscombe, 2014). The concept of triangulation was originally used by navigators and surveyors to pinpoint exact locations of objects in space by combining measurements from several distinct points (Rothbauer, 2008). Researchers in social science also have accepted and developed triangulation for studying social phenomena. Because every research method has its own disadvantages, an examination of several sources provides benefits such as neutralising the disadvantages and strengthening research findings and interpretations. In this respect, triangulation has a substantial presence in the sphere of mixed methods research (Denscombe, 2014). Denzin (1978, as cited in Flick, 2004, p. 178) recognised triangulation as a validation strategy, distinguishing the four different types:

(1) triangulation of data: using data from different sources,
(2) investigator triangulation: using different observers or interviewers,
(3) triangulation of theories: using different perspectives and theoretical points and
(4) methodological triangulation: using multiple research approaches.

However, there is another perspective on triangulation. Triangulation is seen as a strategy for substantiating and justifying knowledge by adding additional knowledge rather than as a validation strategy (Flick, 1992). This perspective argues that combining different theories or methods helps researchers obtain a comprehensive picture, adding breadth and depth, not accuracy (Fielding & Fielding, 1986). Rothbauer (2008) in a similar vein acknowledges that this strategy allows for exploration and understanding

different dimensions of research subjects in a way that underpins their findings and interpretations.

This strategy was used in this study not only as a data collection technique but also as a data analysis technique. It was intended to maximise the validity of research findings as well as to gain additional knowledge. This study relied upon three different research methods (see: Section 4.4). The employed methods were documentary research, quantitative questionnaires and qualitative interviews. Among the four types of triangulation, this study adopted data and methodological triangulation as it used the data from different sources and combined both quantitative and qualitative approaches. In addition, when discussing all research questions in Chapter 7 triangulation was used as the main strategy to juxtapose the quantitative and qualitative research findings along with the existing literature.

4.6. Research ethics

Various questionable practices in social research can be broken down into four main ethical principles as indicated by Bryman (2016). The first principle was 'no harm to participants'. Not only physical harm but also psychological harm should be avoided to the participants. Any particular ethical harm was found for the survey respondents and interviewees in this research. Especially, this study did not involve vulnerable groups such as children or people with disabilities. In order to prevent any harm, several measures were taken.

- All participants were voluntary.
- Considering the organisations that participants were employed, consent for their participation was gained from the host organisation.
- Participants were clearly informed that they could withdraw at any time (also, they could withdraw their permission to use the data until data collection process ended).

The second principle was 'informed consent'. All the participants were fully informed on the goal, purposes, and the nature of the study. According to the British Society of Criminology (2006), it also needed to be explained why the research was being carried out and how the findings would be diffused. Comprehensive information was offered to the participants so that they could make an informed decision on the participation of the research.

- Participants were alerted to potential risks in invitation information.
- Participants were reminded of the risks before the start of survey and interview.
- Participants were informed that data would be published but would be untraceable and anonymous.
- Signed consent was acquired.
- Participants were provided with the University supervisory details for making a complaint.

The third was 'no invasion of privacy'. This principle was also referred as 'anonymity and confidentiality' (Robson & McCartan, 2016). Respondents could refuse to answer private questions even though they agreed to participate. The statement of the British Sociological Association (2002) suggests that the privacy principle may be undermined by covert methods. This research did not use any covert methods and no particular privacy issues were expected. It was ensured that both the survey respondents and interviewees were protected under anonymity and confidentiality.

- Participants and employing organisations were coded anonymously
- All data not in the public domain was anonymous
- Data in the public domain, traceable to an anonymous participant, was anonymised or discarded
- Participants were fully aware that their participation was known to the employer and the data gathered was visible to the employer
- Raw data was not shared with anyone else including colleagues in the University

The fourth principle was 'no deception'. Experimental research often uses deception to encourage natural responses of participants (Bryman, 2016). This study did not involve any experimental settings but sought verbal and written answers based on their pre-existing perceptions and knowledge of their organisations. The researcher had no reason to use any deceptive methods to affect either the survey respondents or the interviewees in this study.

Although the researcher explained these principles to interviewees thoroughly, it was noted that some of them were uncomfortable with recording their voices. In fact, among 25 interviewees, seven[56] of them brought up this issue in the middle of an interview or after the interview. They asked not to keep their interview recordings. Instead, they allowed for transcribing their recordings, but wanted to discard the recorded files after the transcription process. The researcher made sure that their interview recordings were deleted after transcribing them. Therefore, their requests did not affect the data collection and analysis phases. This example demonstrates that the researcher respected the ethical requirements and privacy of all research participants.

The researcher had a dual role throughout the research.[57] It was necessary to consider the implications of the police officer-researcher role. In principle, the police officer is obliged to abide by the law, while the researcher has the ethical obligation to keep respondents' anonymity and confidentiality. The former and the latter may produce different responses when they are informed of a crime by a respondent. In this regard there may be a role conflict during the research process. In this situation, the researcher would have followed his professional sense. In other words, any disclosure of an unreported crime during the research would have led the researcher to report it to both

56 Two interviewees were from officials from the public sector organisations and five were from SMEs.

57 The researcher has worked as a police officer in the National Police Agency in South Korea for about 10 years. He was officially permitted to take extended leave from the job to pursue a Ph.D. in the UK for 3-5 years.

the host organisation and the authorities. However, the researcher did not face any situations related to a conflict within his role.

There was a concern that the dual status could have a negative impact on the reliability of the study. For example, respondents might have tried to give the answers that the researcher wanted. For this reason it may be argued that the status as a police officer should not have been revealed. However, the researcher gave accurate information on the status of the researcher to research subjects by disclosing his dual status. In addition, it was emphasised that the researcher was officially exempted from his police duty until his research finishes and that the research would not be influenced by his role as a police officer. Another concern that required attention was that his police uniform might have had improper influence over the respondents and interviewees. As the researcher was not on official duty, there was no need to wear his uniform during the research.

These aforementioned measures were expected to greatly minimise the possible undue influence of the police status on the subjects. However, it should be admitted that the significance of this research was pointed out to the survey respondents and interviewees before any form of participation started. This was intended not to elicit responses that the researcher wanted but to elicit valid answers from them.

4.7. Conclusion

This chapter summarised the research process that was adopted in this study. The development of this chapter followed a logical order from suggesting research paradigms and methodology to presenting the data collection and analysis processes. In particular, considerable attention has been paid to the justification on why mixed methods research and, subsequently, explanatory sequential mixed methods have been chosen for this research, drawing on the research questions, aim and orientation.

The integration of quantitative and qualitative approaches was designed to effectively address the research questions by using survey questionnaires and qualitative interviews. There was a limitation in generalisation and replication of the findings in that both quantitative and qualitative phases were dependent upon non-random sampling techniques. Although the inability to generalise findings is a weakness of this research, this could be compensated for by using the mixed methods approach (Creswell & Plano Clark, 2011). Also, the choice of the research design in this study was the result of calculated decision-making, acknowledging the trade-off between generalising the findings and satisfying research aims and questions. Lastly, this chapter discussed research ethics germane to the researcher and this study. Ethical issues included the role conflict between a researcher and a police officer. The following chapters present the findings and analyses of empirical data.

CHAPTER 5: QUANTITATIVE FINDINGS - CYBER SECURITY IN SOUTH KOREAN SMES

5.1. Introduction

This chapter discusses the results of the survey and provides detailed analysis of the results. The primary purposes of the survey were: (1) to assess current situations that SMEs face in relation to cyber security and (2) to identify whether there are some differences depending on business sectors and sizes. The survey consisted of two sections which included 37 questions[58]. Section A focuses on delivering assessment of SMEs' current situation. Section B includes questions for backgrounds of a company and socio-demographic questions. The survey questionnaire is attached in Appendix 1.

The survey questionnaire contained both nominal data and numeric data. Using the statistical package STATA (version 14.0), this analysis consists of descriptive statistics and inferential statistics. Descriptive statistics (e.g., frequencies and percentages) illustrated the basic features of the data, while inferential statistics (e.g., chi-square tests, one-way Analysis of Variance (ANOVA), and two sample t-tests) were used to see whether there was an association among different categorical groups.

As explained in Chapter 1, the five research questions of this thesis served as reference points to guide the organisation of the survey questionnaire. The questions in the questionnaire were built upon a set of questions that HM Government (Department for Digital, Culture, Media and Sport, 2016, 2017, 2018) used to explore the cyber security situation in the UK. The research questions are explored through an examination of survey responses. Profiles of the SMEs surveyed are provided in Section 5.2 and results and analyses are presented in Section 5.3. Lastly, Section 5.4 suggests the main themes found from the analyses.

58 Section A includes 26 questions, section B includes 11 questions.

5.2. Profiling the survey respondents

This study is built on a sample of 328 respondents from SMEs selected from the population described in the previous chapter. Creating a profile is a first stepping stone to analysing survey data in that respondents and their SMEs could then be formally classified through various characteristics based on the profile. A profile of the respondents consists of two organisation-specific characteristics. Those are the type of business organisation and the number of employees.

Business sector classification followed 'Industry classification by company size' (SMBA, 2016) as suggested in Chapter 3 (see: Table 3.4). The number of missing responses was very small: five (1.5%) in the question on business sector and two (0.6%) in the question on business size. There was much variation among business sectors. Only 0.9% of SMEs were in the transportation and storage or the real estate sectors but as many as 38.1% in the manufacturing sector (see: Table 5.1). In this chapter we reduce this variation by also grouping businesses according to the orientation of their services:

(1) services largely directed at the public,
(2) services largely directed at organisations,
(3) public services and
(4) manufacturing and construction.

In terms of business size, 40 more samples of small businesses (184 cases) were collected than medium businesses (142 cases). However, the proportion gap between small businesses (56.1%) and medium businesses (43.3%) is not disproportionately large. Tables 5.1 and 5.2 present the two types of groupings within the sample.

Table 5.1: Sample profiles by business sector and size

	Small firms	Medium firms	Missing	Total	Percen-tage	Categories
Wholesale/retailing	21	3	0	24	7.3%	**Services largely directed at public (18.0%)**
Transportation and storage	2	1	0	3	0.9%	
Real estate	3	0	0	3	0.9%	
Arts, entertainment and recreation	3	1	0	4	1.2%	
Repair and extra service activities	7	5	1	13	4.0%	
Financial and insurance activities	6	6	0	12	3.7%	
Administrative and support service activities	7	4	0	11	3.4%	**Services largely directed at organisations (20.1%)**
Information and communication	20	9	0	29	8.8%	
Professional, scientific and technical activities	12	14	0	26	7.9%	
Education service activities	12	4	0	16	4.9%	**Public services (14.9%)**
Human health and social work activities	8	7	0	15	4.6%	
Environmental service activities	7	11	0	18	5.5%	
Manufacturing	59	65	1	125	38.1%	**Manufacturing and construction (45.4%)**
Construction	14	10	0	24	7.3%	
Missing	3	2	0	5	1.5%	**(1.5%)**
Total	184	142	2	328	100%	**100%**
Percentage	56.1%	43.3%	0.6%	100%		

Table 5.2: Sample profiles by business sector categories and business size

	Small firms	Medium firms	Missing	Total	Percen-tage
Services largely directed at public	42	16	1	59	18.0%
Services largely directed at organisations	39	27	0	66	20.1%
Public services	27	22	0	49	14.9%
Manufacturing and construction	73	75	1	149	45.4%
Missing	3	2	0	5	1.5%
Total	184	142	2	328	100%
Percentage	56.1%	43.3%	0.6%	100%	

5.3. Results and analysis

In this section, SMEs' cyber security situation is assessed. In the survey, questions were categorised into five groups which represent differing themes. Overall, these categories are intended to explore the current cyber security context in which SMEs operate their business. The objective of the survey is to have an awareness of management arrangements and surrounding contexts of SMEs because there is an obvious lack of situational assessment on SMEs in South Korea. These are the five categories:

(1) business connectedness to ICTs and their significance,
(2) incidence and impact of cyber security breaches,
(3) approaches to cyber security risks,
(4) dealing with cyber security breaches and
(5) information acquisition and relationship with external organisations.

5.3.1. Business connectedness to ICTs and their significance

The vast majority of Korean SMEs adopted online services in some form (Figure 5.1). 'Email addresses for organisation or employees' (87.2%) was identified as the most prevalent online service, followed by 'a website or blog' (64.9%) and 'online business bank account' (39.0%). There was a noticeable distinction in the use of online services. Most businesses used online services for communications (i.e., email addresses) and advertising (i.e., website or blog and accounts on social media sites) purposes. By contrast, online services for business transactions (i.e., ordering or booking by customers) and financial transactions (i.e., bank accounts) were used by around a third of businesses (respectively, 27.4% and 39.0%).

1. Which of the following, if any, does your company currently have or use? (multiple choice)

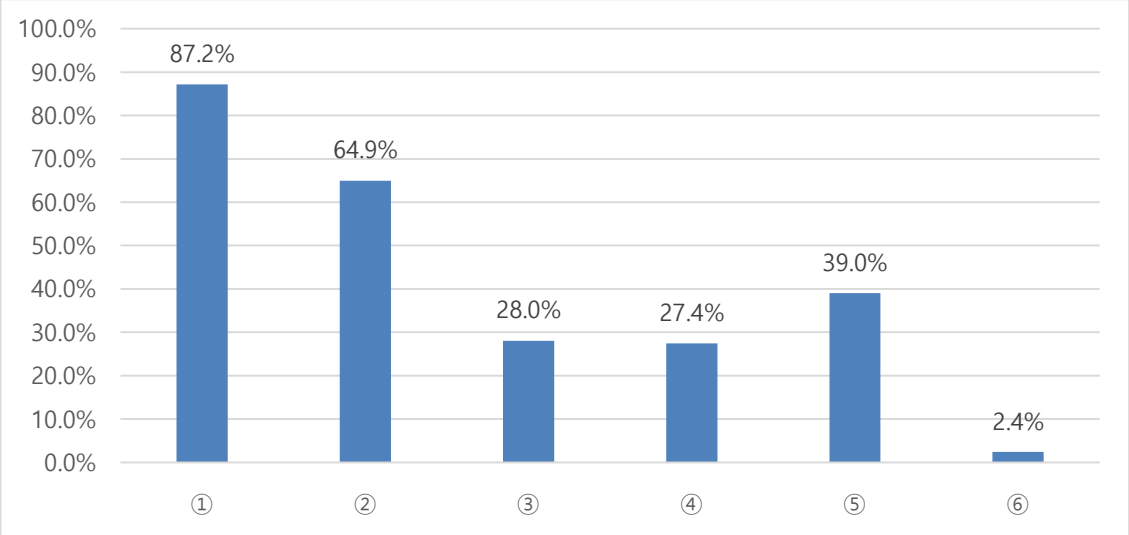


Figure 5.1 Types of online services that SMEs use

Keys

①	Email addresses for your company or its employees
②	A website or blog
③	Accounts or pages on social media sites (e.g., Facebook or Twitter)
④	The ability for customers to order, book or pay for products or services online
⑤	An online business bank account your company pays into
⑥	Other

About a third (32.6%) of the respondents replied that online services were either 'important' or 'very important' elements in their businesses (Figure 5.2). On the other hand, approximately half (46.0%) of the SMEs did not consider online services as a core part of their business offering (i.e., 'not at all important' or 'not very important'). About a fifth (21.3%) gave a neutral reply. There were 44 more negative responses than positive ones, which was translated into a 13.4 percentage point difference. The fact that negative answers outnumbered positive ones may be counterintuitive when considering that South Korea is one of the most connected societies in the world (ITU, 2015b; OECD, 2017b; UN, 2014a). However, it highlights that SMEs did not recognise their business dependence upon online services as much as they actually used them (Figure 5.1).

2. To what extent, if at all, are online services a core part of the goods or services your company provides?

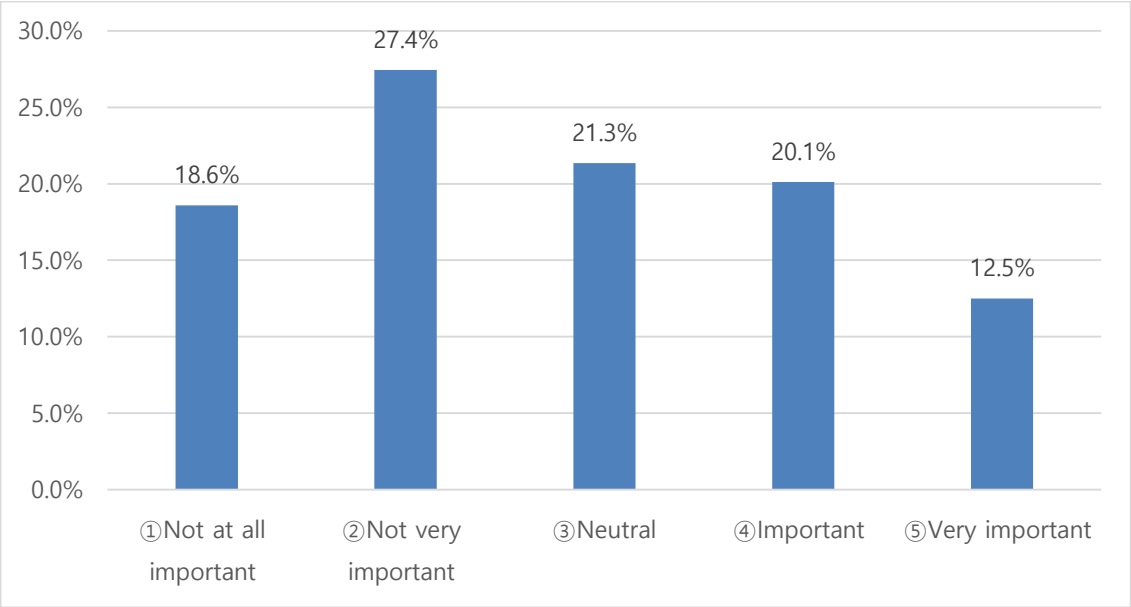


Figure 5.2 SMEs' perception on online services

The extent to which SMEs considered online elements within their businesses varied considerably by business size. Medium firms were more likely to consider online services as significant business elements than small firms. While slightly less than a fifth (19.0%) of medium firms recognised online services as 'very important', only 7.6% of small firms

viewed in the same way. Similarly, a 14.1 percentage point more of medium firms answered 'important' than small firms did (28.2% versus 14.1%). The *t*-test[59] showed that medium and small businesses had a significantly different perception of online services ($p<0.001$)[60].

Table 5.3: *t*-test statistics on the perception on online services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.54	0.09	1.21	2.36	2.71
Medium	142	3.16	0.11	1.34	2.94	3.38
diff	326	-0.62	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0		*t* value	df
			.000		-4.41	324

The use of personally-owned devices for regular work within a firm is a widespread phenomenon in Korea. Although the widespread use of personally-owned devices at work brings convenience to staff, this also means that firms face another set of cyber security risks. Staff in the overwhelming majority (77.7%) of businesses used their own devices to some extent (Figure 5.3). However, it was notable that the median in the proportion of staff who used their own devices was '1-20%' and this proportion went down as the value went up. The results highlight that the extent of actual use of personally-owned devices by staff was not considerably high within a firm.

59 A *t*-test is used when a researcher wants to compare two different groups on a variable of interest (by comparing the means of the two groups) or the same group before and after some event (Emerson, 2017).

60 In statistical hypothesis testing, the *p* value is the probability that a researcher would get the result by chance if the null hypothesis is true (Acock, 2016). In this case, the null hypothesis is that medium businesses' perception on online services is not different from small businesses'. The result that $p < 0.001$ means that there would be less than one time in 1,000 by chance of obtaining the result if the null hypothesis is true. Thus, it rejects the null hypothesis, concludes that medium businesses' perception on online services is different from small businesses'.

3. How many employees in your company use personally-owned devices such as smartphones, tablets, home laptops or desktop computers to carry out regular business-related activities?

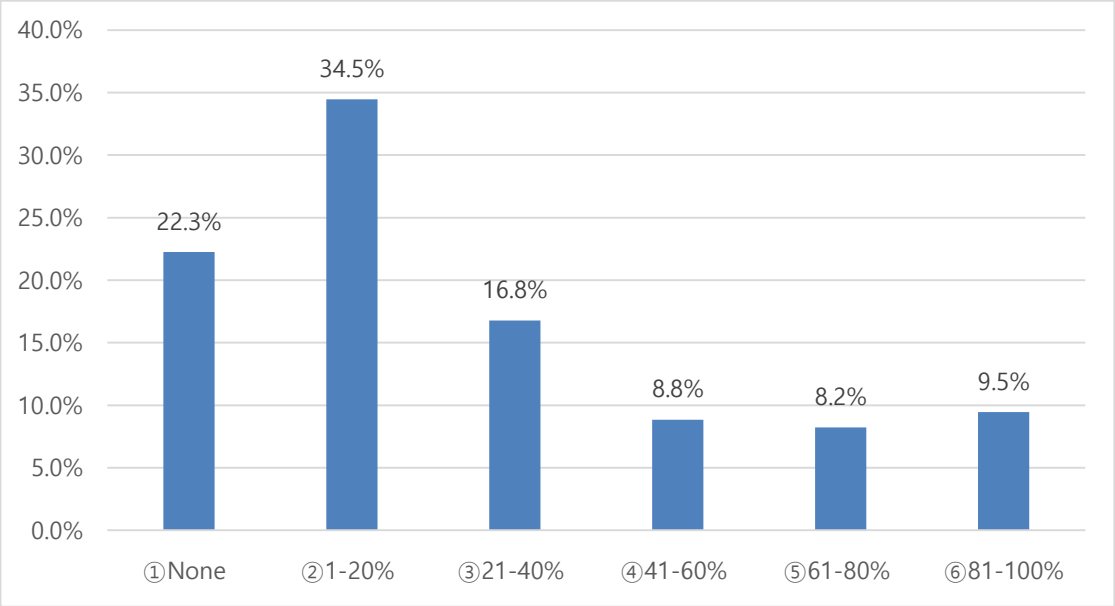


Figure 5.3 Proportion of staff who use personally-owned devices for regular work

Also, there was a difference by business sector. Over half (58.3%) of businesses in the financial and insurance sector and less than half (41.4%) of businesses in the information and communication sector replied that more than 80% (‘81–100%’) of staff used their own devices at work. On the contrary, manufacturing and construction sectors showed the opposite tendency. Over a fifth (23.2%) and a half (50.0%) of businesses, respectively, in manufacturing sector and construction sector answered that no staff used their own devices at work.

Cloud computing was widely adopted by Korean businesses, with about four fifths (83.2%) of businesses using some sort of externally-hosted web services (Figure 5.4). Only a minority (16.8%) of businesses did not use them in any form. Over a third (39.4%) of the SMEs used them either ‘often’ or ‘very often’.

4. Does your company currently use any externally-hosted web services, for example to host your website or corporate email accounts, or for storing or transferring data?

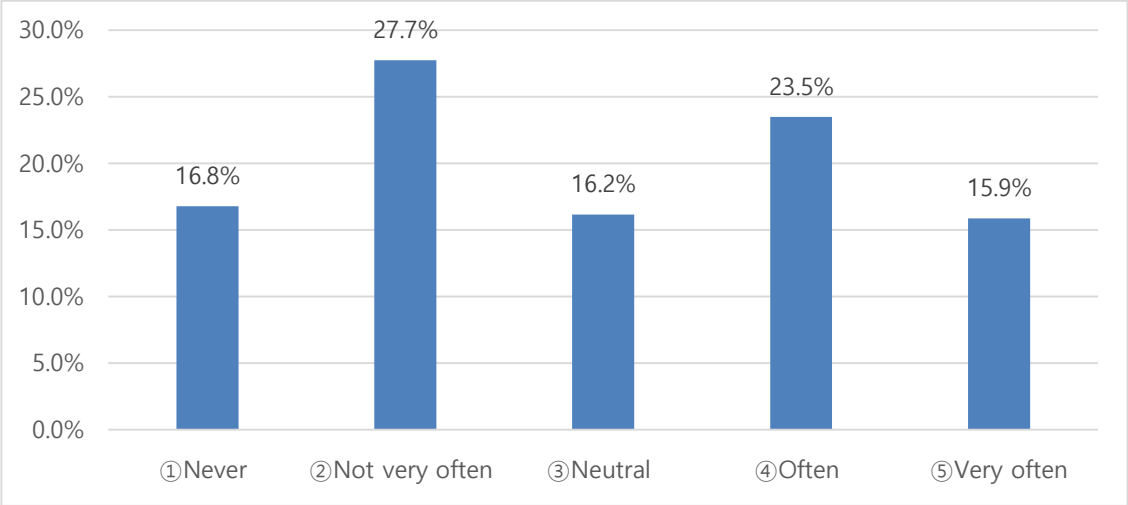


Figure 5.4 SMEs' use of externally-hosted web services

The use of cloud computing differed by business size. Medium companies were more likely to use externally-hosted services for any reason than small companies. Less than a third (27.2%) of small companies used these services more than 'often', compared to over half (55.6%) of medium companies. According to the *t*-test result, medium businesses used externally-hosted web services more often than small businesses (p<0.001), which supports the argument that cloud computing tends to be more acceptable as the company size grows (Brender & Markov, 2013; Truong, 2010).

Table 5.4: *t*-test statistics on the use of externally-hosted web services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.55	0.10	1.30	2.37	2.74
Medium	142	3.45	0.10	1.25	3.25	3.66
diff	326	-0.90	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0		*t* value	df
			.000		-6.28	324

Less than half (42.4%) of businesses considered externally-hosted web services were more than 'critical' to their businesses. It should be noted that the frequency distribution of answers in Figure 5.5 was quite similar to that of answers in Figure 5.4. The similar pattern of the frequency distribution graphs may imply that these two variables were associated. As a proof of the association, the correlation value between these two variables was .65 which was statistically significant at the .05 level. This indicates that the perception of whether these externally-hosted web services were critical to the respondents' companies (Figure 5.5) was highly related to the actual use of these services (Figure 5.4).

5. How critical, if at all, are these externally-hosted web services to your company?

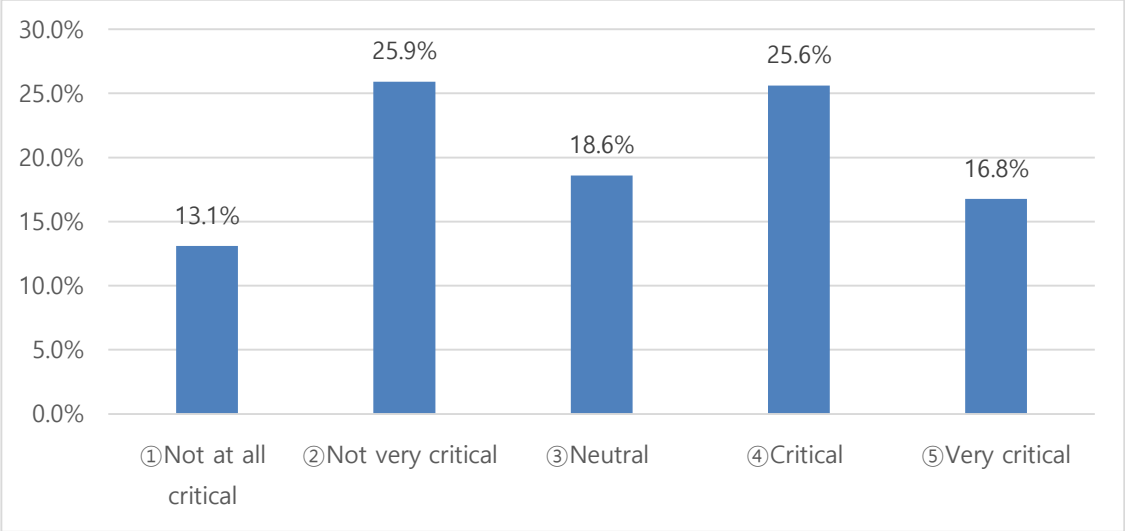


Figure 5.5 Criticality of externally-hosted web services

Perception on the criticality of cloud computing services varied by size band. Over half (53.5%) of medium firms viewed these services as more than 'critical' to their businesses, compared to about a third (34.2%) of small firms. The *t*-test analysis confirmed that the criticality of cloud computing services increased as business size expanded ($p<0.001$).

Table 5.5: *t*-test statistics on criticality of externally-hosted web services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.81	0.09	1.28	2.63	2.99
Medium	142	3.43	0.11	1.26	3.22	3.64
diff	326	-0.62	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0		*t* value	df
			.000		-4.37	324

5.3.2. Incidence and impact of cyber security breaches

Over half (55.4%) of the SMEs have experienced one or more cyber security breaches in the last 12 months. Among the affected businesses (*n*=182), the vast majority (76.4%) suffered fewer than 5 breaches and the proportion of the affected businesses went down dramatically as the number of breaches increased. As a consequence, SMEs can be formed into two broad groups:

(1) a group which did not suffer any breaches and
(2) a group which suffered a few breaches.

In addition, it is worth mentioning that a tenth (10.1%) of the respondents did not know whether their businesses experienced cyber-attacks. Businesses which answered 'Don't know' consisted of 18 small firms (9.8% of the total small firms) and 15 medium firms (10.6% of the total medium firms), which did not show any meaningful difference.

6. Approximately, how many cyber security breaches or attacks have you experienced in total over the last 12 months?

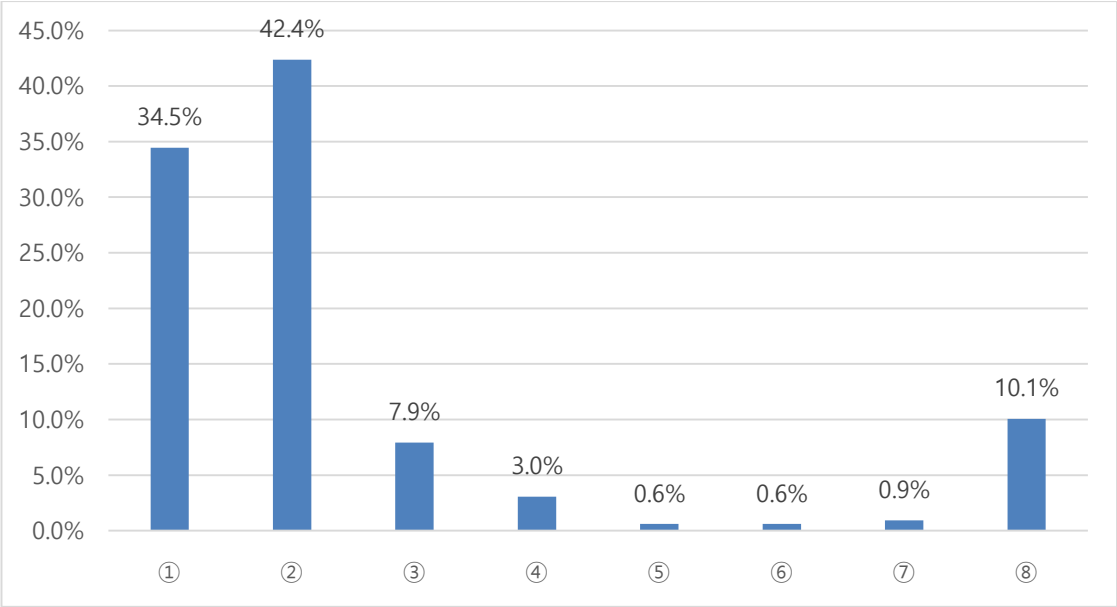


Figure 5.6 Experience of cyber security breaches or attacks

Keys

①	None	⑤	15 to fewer than 20
②	Fewer than 5	⑥	20 to fewer than 50
③	5 to fewer than 10	⑦	50 or more
④	10 to fewer than 15	⑧	Don't know

Overall, there was a negative relationship between breach experience and the size of a firm (Table 5.6). The incidence of breaches was found to be significantly different by business size, with over two thirds (68.1%) of small firms and about half (52.8%) of medium firms having experienced breaches over the last 12 months[61]. The association between breach experience and business size was statistically significant (p=.008). STATA showed that tau-b was -.160, which showed a weak relationship.[62] The asymptotic standard error (ASE) for tau-b was .058. And if tau-b is divided by this estimated standard error, the z test value is obtained. Here, z=-.160/.058=2.76. This z

61 'Don't know' responses were excluded from this analysis.
62 Values of tau-b less than 0.2 signify a weak relationship.

value was significant at the .05 level.[63] It means that the weak relationship was statistically significant.

Table 5.6: Cross-tabulation of Cyber security breach experience and business size

	Cyber security breach experience		
	No	Yes	Total
Small	53	113	166
Medium	60	67	127
Total	113	180	293
	Pearson chi2(1) = 7.124		Pr=.008
	Kendall's tau-b = -.156		ASE=.058

Among those SMEs (*n*=132) which claimed online services were 'not very important' and 'not at all important' to their business offer, less than two thirds (64.4%) experienced any form of breach[64]. On the contrary, among businesses (99 SMEs) that considered online services were 'important' and 'very important' to their business offer, about half (53.5%) have experienced breaches. A *t*-test confirmed that businesses which had no breach experience considered online services as more essential than businesses which had breach experience (*p*=.025).

Table 5.7: *t*-test statistics on the perception on online services by breach experience

	Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Breach experience	No	113	3.02	0.13	1.33	2.77	3.26
	Yes	182	2.71	0.10	1.30	2.52	2.90
	diff	295	0.31	0.16			
diff = mean(No) - mean(Yes)				Ha: diff > 0		*t* value	df
				.025		1.97	293

63 If z > ± 1.96 then it is significant at the .05 level and if z >± 2.60 it is significant at the .01 level.
64 'Don't know' responses were excluded from this analysis.

Another factor related to breach experience was the business sector that a firm belonged to (Table 5.8). A chi-square test showed that cyber breach experiences and categories of business sectors were associated (*p*=.008). Businesses that provided 'public services' were either more targeted by offenders or unprepared for cyber threats than businesses in other sectors. The opposite interpretation could be given to businesses that provided 'services largely directed at organisations'.

Table 5.8: Cross-tabulation of cyber security breach experience and categories of business sector

			Categories of business sector				
			1	2	3	4	Total
Cyber breach experience	No	Frequency	22	30	8	51	111
		Expected frequency	20	23	17	51	111
	Yes	Frequency	31	29	36	83	179
		Expected frequency	33	36	27	83	179
Total			53	59	44	134	290
Pearson chi2(3) = 11.704 Pr=.008							

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

The most common type of breaches experienced (Figure 5.7) were infections with viruses, spyware or malware (75.8%, 138 out of 182) and stealing money through fraudulent emails or fake websites (33.5%). There was a very large gap between the two. Other noticeable types were unauthorised access (19.2%) and denial-of-service attacks (17.6%). Figure 5.7 was comparable to Figure 5.8 in that the most prevalent source of the breach was reported as emails, email attachments, or websites (53.8%, 98 out of

182), followed by malware authors (38.5%). This reaffirmed that Korean SMEs were plagued by massive viruses and malware via email attachments or websites (Symantec, 2017). Against this backdrop, malware authors were seen as the main source of these attacks. Considering that the vast majority of the SMEs used emails and websites for their business (see: Figure 5.1), it was clear that they were constantly exposed to cyber security breaches.

7. Which of the following have happened to your company in the last 12 months? (multiple choice)

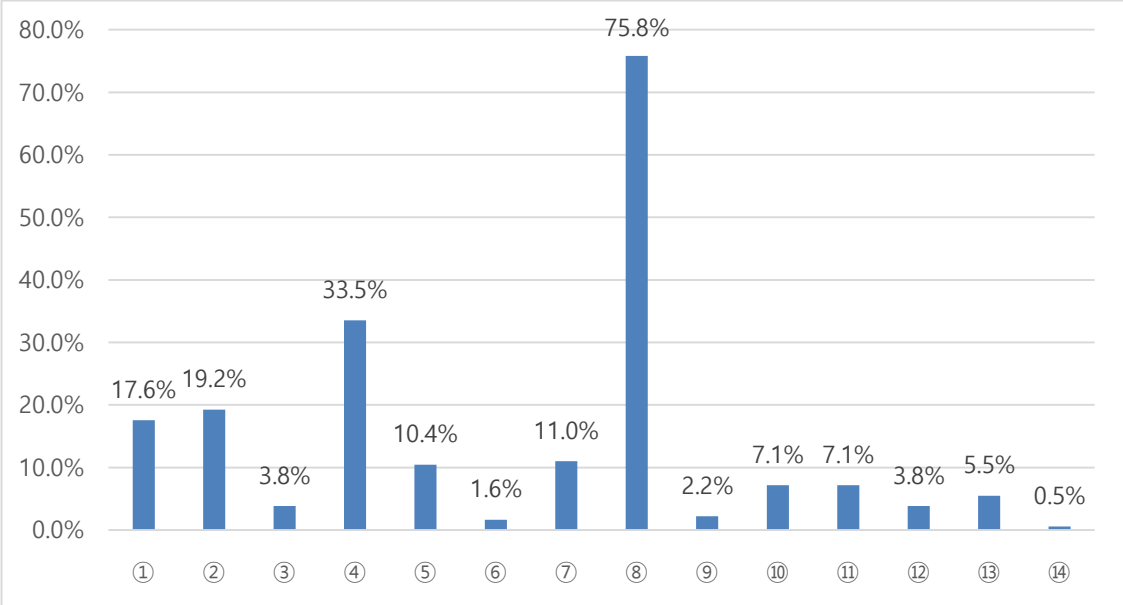


Figure 5.7 Types of breaches experienced

Keys

①	Denial-of-service attacks
②	Access to computers, networks or services without permission (i.e., hacking)
③	Money stolen electronically (e.g., through online banking)
④	Money stolen through fraudulent emails or fake websites
⑤	Personal information (e.g., customer data) stolen electronically
⑥	People damaging or stealing software from your computers or network
⑦	People downloading unlicensed/stolen software to computers or network
⑧	Computers becoming infected with viruses, spyware or malware
⑨	Theft of intellectual property

⑩	Others impersonating company in emails or online
⑪	Breaches from personally-owned devices
⑫	Breaches from externally-hosted web services
⑬	Breaches on social media
⑭	Other

8. As far as you know, who or what was the source of the breach or attack? (multiple choice)

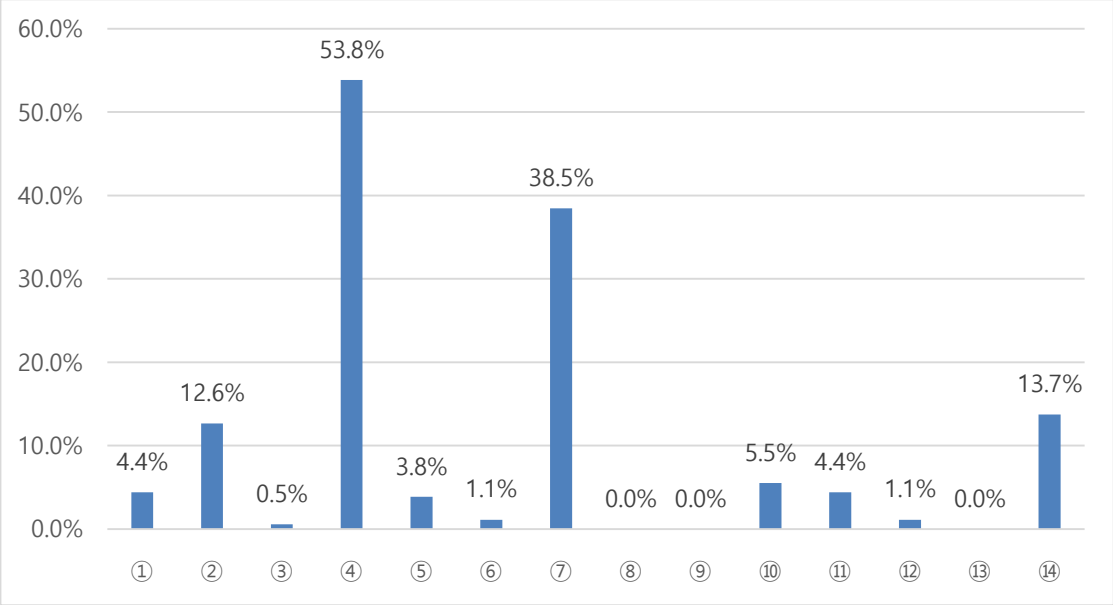


Figure 5.8 Sources of breaches or attacks

Keys

①	Third party suppliers	⑧	Nation-state intelligence services
②	Activists	⑨	Natural (e.g., flood, fire, etc.)
③	Competitors	⑩	Non-professional hackers
④	Emails (attachments) / websites	⑪	Organised crime
⑤	Current employees	⑫	Terrorists
⑥	Former employees	⑬	Other
⑦	Malware authors	⑭	Don't know

The direct costs of breaches include repair costs for business continuity, extra work hours of staff for handling a breach, and necessary investment for future protections

against incoming attacks. In the long term, other impacts include loss of revenue, lawsuit costs, and reputational damage. These long-term costs are difficult to measure. Slightly over a third (34.1%) of SMEs did not know the financial costs, with a similar number (33.5%) estimating the impacts as under £500. Although the average cost of a breach could not be accurately calculated due to insufficient information, the mean cost was expected to be low. This was because, excluding 'don't know' responses, most cases (70.8%, 85 out of 120) cost under £1,000 and about half (50.8%, 61 out of 120) under £500.

9. Approximately how much, if anything, do you think the cyber security breaches or attacks you have experienced in the last 12 months have cost your company financially?

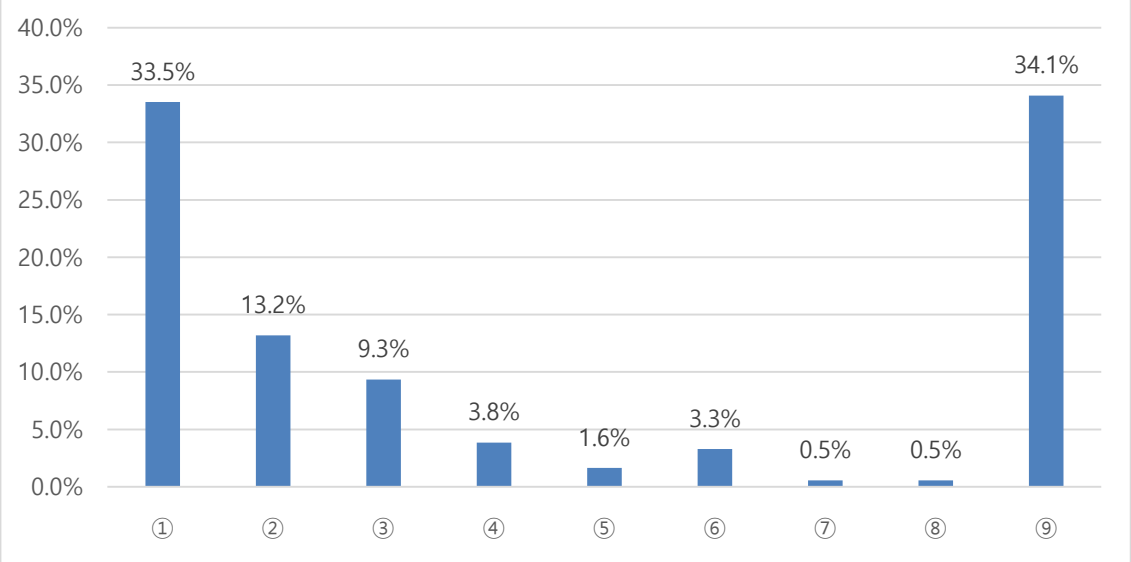


Figure 5.9 Estimated costs of breaches or attacks

Keys

①	Less than £500	⑥	£20,000 to less than £50,000
②	£500 to less than £1,000	⑦	£50,000 to less than £ 100,000
③	£1,000 to less than £5,000	⑧	£100,000 or more
④	£5,000 to less than £10,000	⑨	Don't know
⑤	£10,000 to less than £20,000		

Slightly under half (48.4%) of breaches were detected by anti-virus or anti-malware software. As these software are regularly updated by providers, they provide convenience for business users at low cost. These software are a one-size-fits-all approach, as once installed no further configurations or efforts are needed. The second and third most prevalent ways for detection were disruption to business (22.5%) and by accident (21.4%). These ways are reactive rather than proactive. Being aware of attacks upon disruption to business may be the worst scenario in that damage from a breach has already occurred. The fact that a fifth (21.4%) of businesses identified breaches by accident indicates that there were a large number of attempted attacks which were not detected. All the aforementioned detection methods did not involve any internal control mechanisms or security management processes.

On the other hand, identification by reports from staff or contractors (14.8%) and routine internal security monitoring (13.2%) are more proactive methods. These methods indicate that there is an organisational structure for cyber security. In other words, internal control mechanisms are, to some extent, active in a company. It is expected that a business will be willing to adopt these proactive methods as their business management becomes more structured. Adopting proactive methods is recommended in that they are more likely to detect not only breaches but also attempted attacks earlier than reactive methods.

10. How was the breach or attack identified? (multiple choice)

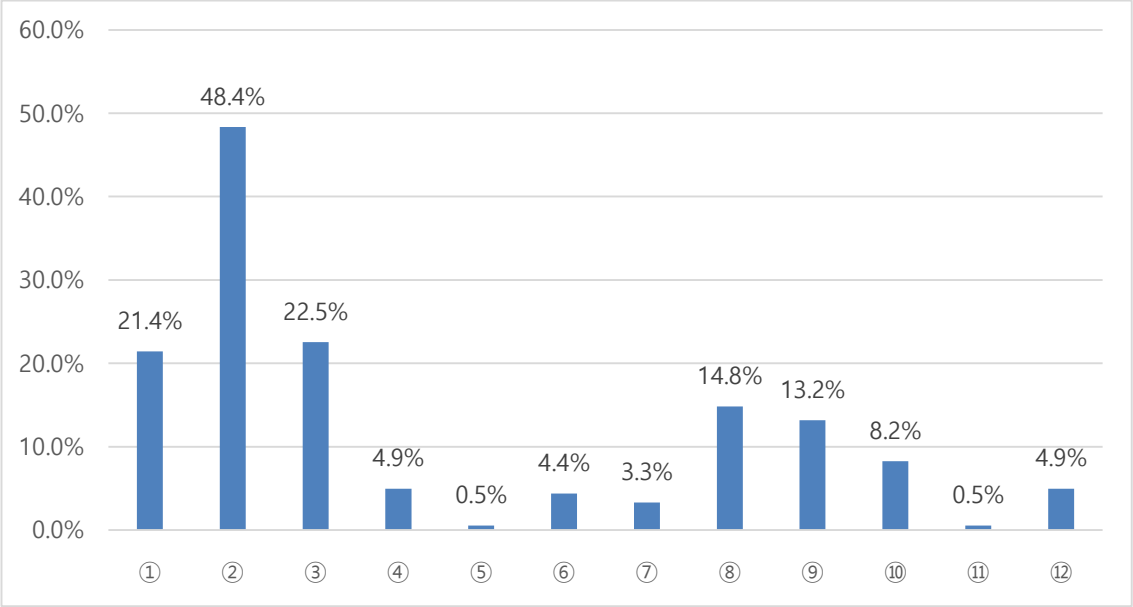


Figure 5.10 Methods for identifying breaches or attacks

Keys

①	By accident
②	By antivirus/anti-malware software
③	Disruption to business/staff/users/ service provision
④	From warning by government/law enforcement
⑤	Our breach/attack reported by the media
⑥	Similar incidents reported in the media
⑦	Reported/noticed by customers/customer complaints
⑧	Reported/noticed by staff/contractors
⑨	Routine internal security monitoring
⑩	Other internal control activities not done routinely (e.g., reconciliations, audits)
⑪	Other
⑫	Don't know

Regarding the impact of breaches, there was a considerable variety in replies (Figure 5.11). Two impacts that stood out were stopping staff from carrying out their day-to-day work (53.8%) and any other repair or recovery costs (46.2%). These impacts are direct consequences of disruption to business continuity. In addition, implementing new

measures for protecting against future attacks (22.0%) is a necessary follow-up response after the business disruption. These impacts are classified as direct or short-term impacts which require organisational responses within a short period of time. In contrast, some respondents did not think their firms experienced indirect or long-term impacts such as loss of revenue (1.6%), fines from regulators (0.0%), and reputational damage (6.6%) as often as direct or short-term impacts.

11. Thinking of all the breaches or attacks experienced in the last 12 months, have these impacted your company in any of the following ways? (multiple choice)

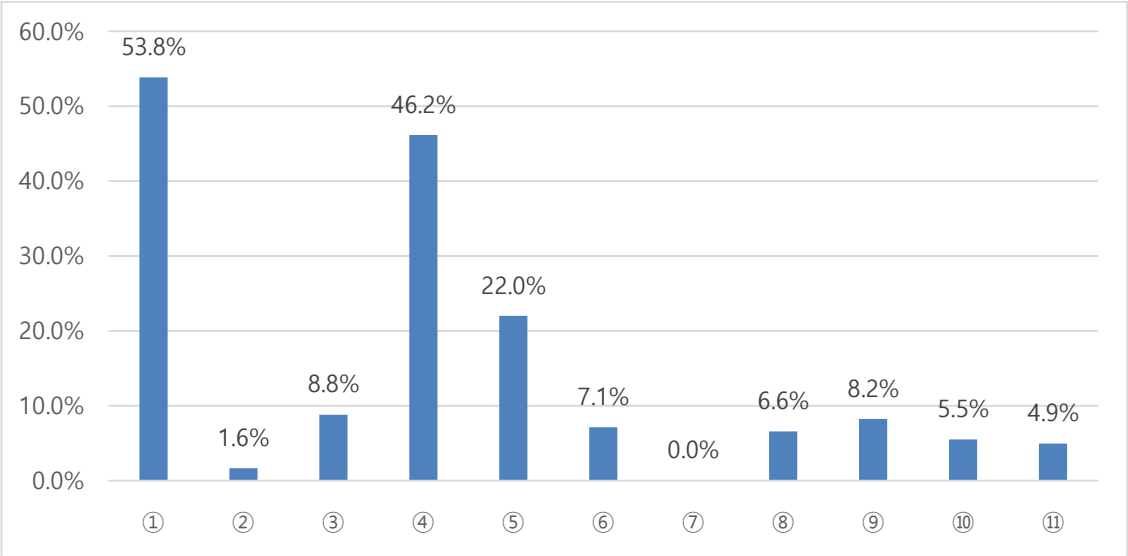


Figure 5.11 Types of the impact of breaches or attacks

Keys

①	Stopped staff from carrying out their day-to-day work
②	Loss of revenue or share value
③	Additional staff time to address the breach, or to inform customers or stakeholders
④	Any other repair or recovery costs
⑤	New measures needed to prevent or protect against future breaches or attacks
⑥	Lost or stolen assets
⑦	Fines from regulators or authorities, or associated legal costs
⑧	Reputational damage
⑨	Prevented provision of goods or services to customers
⑩	Discouraged you from carrying out a future business activity you were intending to do
⑪	Other

Even though 'reputational damage' (6.6%) was not recognised as a crucial impact on overall businesses, it was perceived differently depending on business size. Medium firms were more likely to suffer reputational damage than small firms (6.3% versus 1.6%). And, the association between reputational damage and business size was statistically significant (*p*=.025). However, no association was found between reputational damage and business sector categories (*p*=.903).

Table 5.9: Cross-tabulation of reputational damage and business size

		Business size		
		Small	Medium	Total
Reputational damage	Yes	3	9	12
	No	181	133	314
	Total	184	142	326
Pearson chi2(1) = 5.010				Pr=.025

Table 5.10: Cross-tabulation of reputational damage and categories of business sector

		Categories of business sector				
		1	2	3	4	Total
Reputational damage	Yes	2	3	1	6	12
	No	57	63	48	143	311
	Total	59	66	49	149	323
Pearson chi2(3) = 0.569						Pr=.903

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

5.3.3. Approaches to cyber security risks

Less than half (42.4%) of businesses did not have formal cyber security policies (Figure 5.12). Businesses that did not dictate the policies were distributed equally across all size bands (p=.980) and business sector categories (p=.101). Security aspects on removable devices (44.5%) and acceptable behaviours of staff (32.9%) were more commonly included in their policies. Alongside these two security aspects, use of personally-owned devices (29.6%) involved risks occurring within a company. On the other hand, risks coming from outside were derived from aspects such as remote or mobile working (29.9%) and use of cloud computing (24.1%). These aspects were not included in policies as often as the aspects of inside risks. This indicates that Korean businesses were more aware of, and prepared for, risks from inside than from outside.

12. Which of the following aspects, if any, are covered within your cyber security-related policy, or policies? (multiple choice)

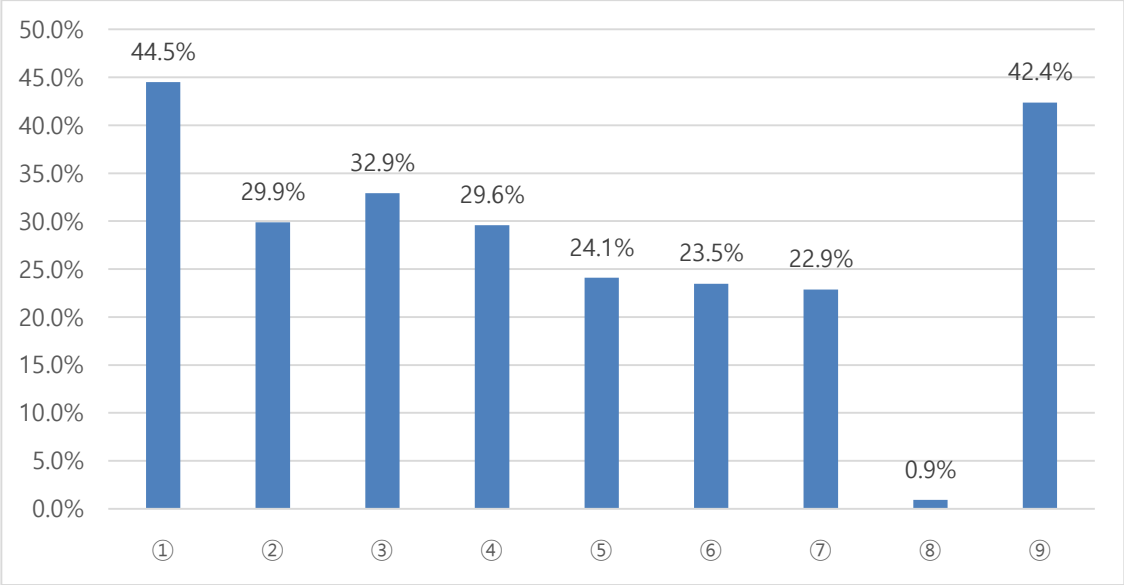


Figure 5.12 Adoption of cyber security-related policies

Keys

①	What can be stored on removable devices (e.g., USB sticks, CDs etc.)
②	Remote or mobile working (e.g., from home)
③	What staff are permitted to do on your company's IT devices

④	Use of personally-owned devices for business activities
⑤	Use of new digital technologies such as cloud computing
⑥	Data classification
⑦	A Document Management System
⑧	Other
⑨	No policy adopted

Slightly more businesses (35.4%) said that cyber security was a 'low' or 'very low' priority to senior management than those (32.1%) whose senior managers treated it as a 'high' or 'very high' priority (Figure 5.13). The remainder (32.6%) gave a neutral reply.

13. How high or low a priority is cyber security to your company's directors or senior management?

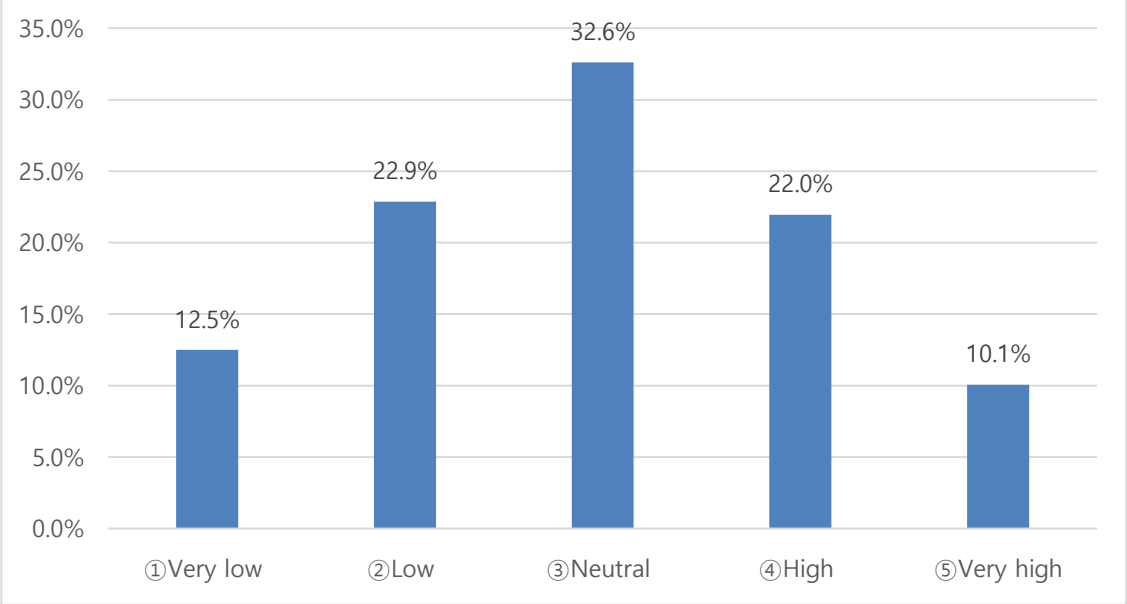


Figure 5.13 Cyber security as a priority to directors or senior management

A *t*-test showed there was no difference in senior management's perception on cyber security between small and medium firms (p=.744). However, a noticeable difference was found when a business sector was allowed for. As might be expected, senior managers in the majority of financial and insurance firms (83.3%) and information and communication firms (72.4%) perceived cyber security as a 'high' or 'very high' priority,

whereas only a small minority of manufacturing firms (13.6%) and construction firms (4.2%) showed the same tendency.

Table 5.11: *t*-test statistics on senior mangers' perception on cyber security by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.93	0.09	1.16	2.76	3.10
Medium	142	2.97	0.10	1.16	2.78	3.16
diff	326	-0.04	0.13			
diff = mean(Small) - mean(Medium)			Ha: diff != 0		*t* value	df
			.744		-0.33	324

There was a difference in priorities between business sector categories. As to the mean of those categories, the mean of businesses that provided 'services largely directed at organisations' heavily outnumbered that of businesses in 'manufacturing and construction sectors' (3.8 versus 2.5). ANOVA test confirmed the overall group differences (p=.037). However, the ANOVA test itself does not show which group is different from which. Therefore, a set of independent tests were needed to see the detailed nature of group differences. A multiple-comparison procedure, *Bonferroni*, found out that all individual group differences were statistically significant except the difference between 'services largely directed at public' and 'public services' (p=1.000).

Table 5.12: ANOVA on senior managers' perception on cyber security by categories of business sector

Source	SS	df	MS	F	Prob > F
Between groups	83.85	3	27.95	25.30	0.0000
Within groups	352.45	310	1.105		
Total	436.30	322	1.35		
Bartlett's test for equal variances:		chi2(3) = 8.50		Prob>chi2 = .037	

Table 5.13: Bonferroni test between categories of business sector

Row mean – Col Mean	1. Services largely directed at public	2. Services largely directed at organisations	3. Public services
2. Services largely directed at organisations	.75[65] .000[66]		
3. Public services	.09 1.000	-.66 .006	
4. Manufacturing and construction	-.57 .003	-1.33 .000	-.67 .001

One hypothesis was that the importance of online services to their businesses was associated with senior management's perception of cyber security. It could be explained that SMEs that said online services were core to their goods or services tended to regard cyber security as a high priority. Businesses that regarded cyber security as 'high' or 'very high' said that their goods or services were 'important' or 'very important' rather than 'not at all important' or 'not very important' (56.2%, versus 27.6%). The correlation value of .37 showed that the two variables (business' dependence upon online services in Figure 5.2 and treatment of cyber security on agendas in Figure 5.13) were moderately associated.

Table 5.14: Correlation between business' dependence on online services (question2) and the treatment of cyber security as a priority (question13)

	Question 2	Question 13
Question 2	1.000	
Question 13	.367 .000	1.000

65 This figure is the mean difference of the two business sector categories.
66 This figure is the p-value associated with the two business sector categories.

Just over a third (36.9%) of businesses did not provide cyber security training to their staff in the last 12 months, whereas over half (55.8%) businesses provided their staff with some cyber security training. Among businesses (*n*=183) which offered training, the frequency of training centred on either 'less than once a year' or 'annually' (81.4%) rather than more than 'quarterly' (18.6%).

14. Over the last 12 months, has your company provided employees with internal cyber security trainings?

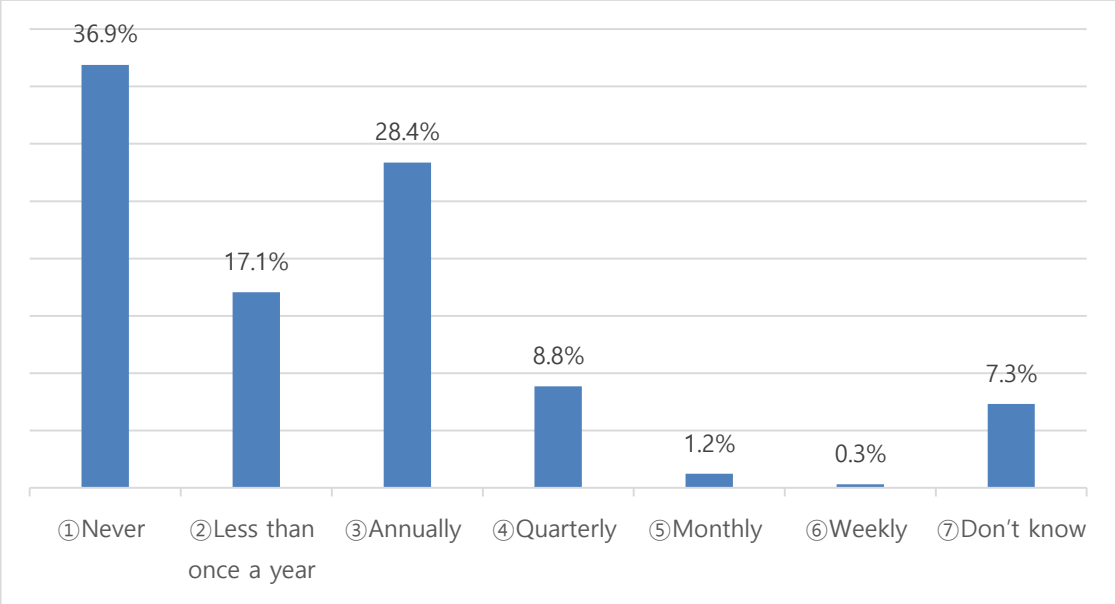


Figure 5.14 Provision of internal cyber security trainings

Provision of cyber security training was associated with how important cyber security was to senior management (Figure 5.13). Among businesses (*n*=24) whose answer was 'don't know' in question 14, exactly two thirds (66.7%) of them replied that cyber security was either a 'low' or 'very low' priority to their senior managers. Similarly, among businesses (*n*=116) whose cyber security was either a 'low' or 'very low' priority to their senior managers, slightly less than two thirds (63.8%) of them had never asked their staff attend cyber security training.

The association between staff training and the treatment of cyber security as a priority was supported by the correlation value of .61[67]. This indicates that the two variables had a moderate positive relationship which was statistically significant (p<.001). By size band, cyber security training was more prevalent in medium firms (63.4%) than small firms (50.0%).

Table 5.15: Correlation between the treatment of cyber security as a priority (question13) and staff trainings (question14)

	Question 13	Question 14
Question 13	1.000	
Question 14	.613 .000	1.000

Under a third (28.0%) of businesses did not have any governance or risk management arrangements in place (Figure 5.15). The most common type of governance was using staff members whose job role included cyber security or governance (41.8%), followed by having board members with responsibility for cyber security (36.0%). These risk management arrangements were dependent upon human resources, taking advantage of insiders within a company. This means that cyber security was mainly governed by internal mechanisms involving human factors.

This reflected a widespread aspect of organisational culture of Korean businesses. Korean businesses have a strong tendency to point out who is responsible for a certain issue. They consider the proverb, “Everybody's business is nobody's business”, as an axiom for business management. However, it should be studied further whether the responsible staff or board members had expertise in cyber security or whether the assigning responsibility primarily aimed to penalise someone in case of a damage incurred from a breach. This is discussed further in Sections 6.2.2 and 7.2.3.1. Under a

67 ‘Don’t know’ responses were excluded from this analysis.

third (30.2%) of businesses had policies covering cyber security risks and one in five (22.6%) depended on outsourced providers. A business continuity plan was only adopted by a small minority (14.0%).

15. Which of the following governance or risk management arrangements, if any, do you have in place? (multiple choice)

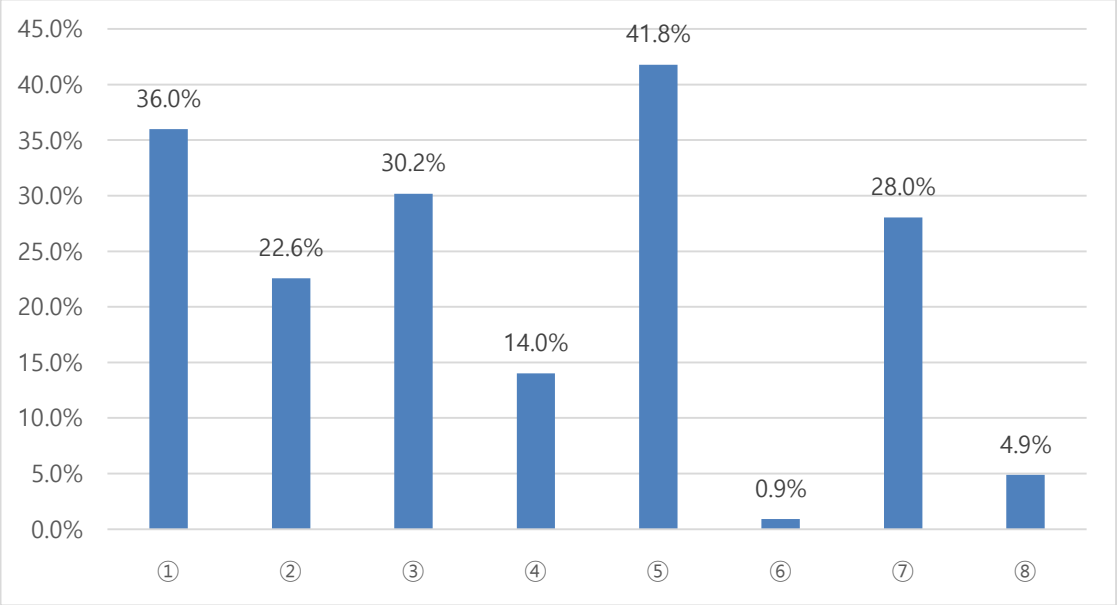


Figure 5.15 Governance or risk management arrangements

Keys

①	Board members with responsibility for cyber security
②	An outsourced provider that manages your cyber security
③	A formal policy or policies in place covering cyber security risks
④	A Business Continuity Plan
⑤	Staff members whose job role includes cyber security or governance
⑥	Other
⑦	None of these
⑧	Don't know

Senior managers in over a third (38.7%) of businesses were never given an update on any actions taken around cyber security (Figure 5.16). The obvious lack of reporting within a company was most serious in arts, entertainment and recreation (100%),

followed by manufacturing (49.6%), wholesale/retailing (45.8%), and construction (41.7%) businesses. All financial and insurance firms had an internal reporting structure on cyber security updates at least quarterly. Across the board, no senior management was given updates on a daily basis. Businesses (*n*=5) that reported weekly were all medium firms and three of them belonged to the financial and insurance sector.

16. Approximately how often, if at all, are your company's directors or senior management given an update on any actions taken around cyber security?

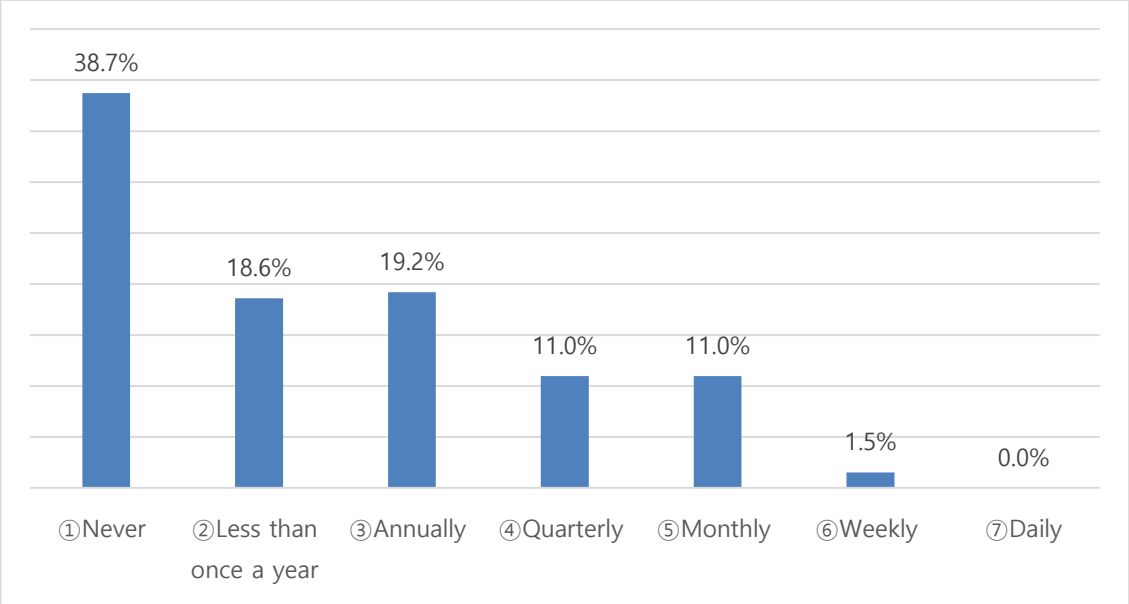


Figure 5.16 Cyber security updates for directors or senior management

Among businesses (*n*=127) whose senior managers were never updated on cyber security actions taken, slightly over half (53.5%) of them rated cyber security as a 'low' or 'very low' priority and one in ten (12.6%) of them considered cyber security a 'high' or 'very high' priority. It was highly likely that senior managers were not keen to be updated if they did not perceive cyber security as a high priority, and the positive relationship between cyber security updates and acceptance of cyber security as a priority was moderate (correlation value=.43).

Table 5.16: Correlation between the treatment of cyber security as a priority (question13) and cyber security updates (question16)

	Question 13	Question 16
Question 13	1.000	
Question 16	.430 .000	1.000

A small number of businesses (*n*=16) showed the opposite tendency. Those businesses replied that their senior managers were never given an update, although they viewed cyber security as more than a 'high' priority. This underlines that their senior management's perception on cyber security (i.e., acceptance as a priority) was detached from their actual engagement (i.e., cyber security updates). There was a large difference between the perception and engagement.

Some form of action to identify cyber security risks was taken by the large majority (82.0%) of SMEs (Figure 5.17). Among the choices suggested, regular health checks (68.3%) were shown as the most widely adopted action, while ad-hoc health checks beyond regular processes (27.4%) or an internal audit (22.6%) were adopted by less than a third of SMEs.

Chi-square tests showed that internal audit (*p*=.009), ad-hoc health checks (*p*=.001), and risk assessment (*p*=.011) were associated positively with business size. Medium firms had a greater tendency to implement these measures than small firms (internal audit: 29.6% versus 17.4%, ad-hoc health checks: 36.6% versus 20.7%, risk assessment: 23.9% versus 13.0%). However, no group difference was found in adopting regular health checks (*p*=.409). This indicates that business-as-usual health checks were widely used by all business sizes as a generic prescription, while other measures were more likely to be adopted as business size increased.

Table 5.17: Cross-tabulation of measures taken to identify risks (an internal audit) and business size

		Small	Medium	Total
An internal audit	Yes	32	42	74
	No	152	100	252
	Total	184	142	326
Pearson chi2(1) = 6.783				Pr=.009

Table 5.18: Cross-tabulation of measures taken to identify risks (ad-hoc health checks) and business size

		Small	Medium	Total
Ad-hoc health checks	Yes	38	52	90
	No	146	90	236
	Total	184	142	326
Pearson chi2(1) = 10.225				Pr=.001

Table 5.19: Cross-tabulation of measures taken to identify risks (risk assessment) and business size

		Small	Medium	Total
Risk assessment	Yes	24	34	58
	No	160	108	268
	Total	184	142	326
Pearson chi2(1) = 6.511				Pr=.011

Table 5.20: Cross-tabulation of measures taken to identify risks (regular health checks) and business size

		Small	Medium	Total
Regular health checks	Yes	123	101	224
	No	61	41	102
	Total	184	142	326
Pearson chi2(1) = 0.683				Pr=.409

17. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your company? (multiple choice)

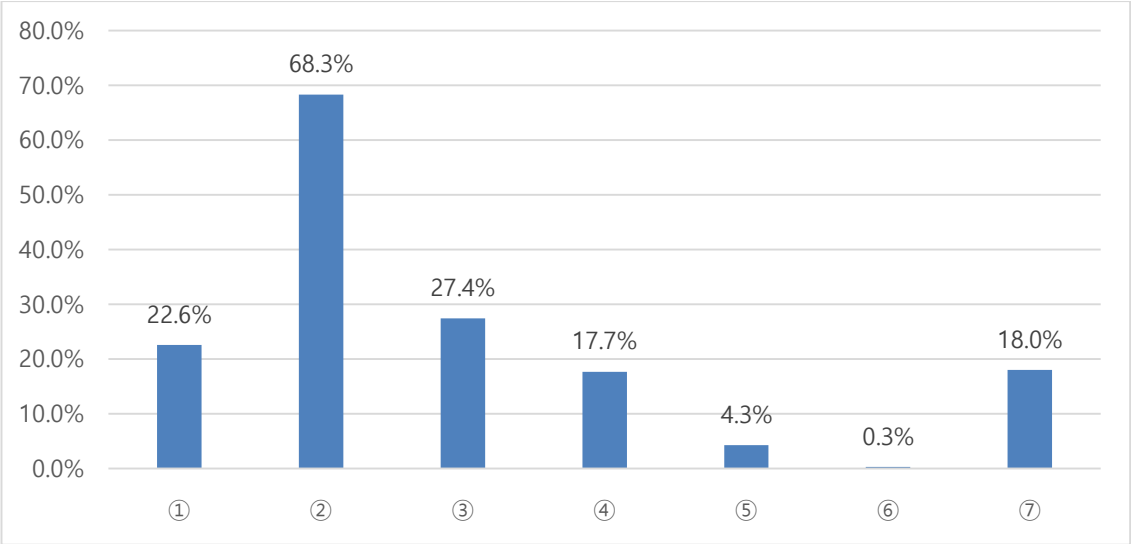


Figure 5.17 Measures taken to identify cyber security risks

Keys

①	An internal audit
②	Any business-as-usual health checks that are undertaken regularly
③	Ad-hoc health checks or reviews beyond your regular processes
④	A risk assessment covering cyber security risks
⑤	Invested in threat intelligence
⑥	Other
⑦	None of these

5.3.4. Dealing with cyber security breaches

Cyber security rules and controls could be classified into three groups depending on the responses. Over half of businesses said they applied software updates (66.5%) and malware protection updates (74.4%), and configured firewalls appropriately (50.9%). These types of controls were intuitive to adopt in that they require low resources. A set of updates were intended mainly to prevent infiltration of viruses and malware. Other controls widely adopted were restricting IT administration and access rights (46.6%) or encryption of personal data (39.6%). Finally, less common types of controls included

monitoring of user activity (26.2%), security controls on company-owned devices (26.8%), and only allowing access via company-owned devices (28.7%). A segregated guest wireless network (19.8%) was the least common form of control. Adopting these unpopular types of controls requires not only financial support but also managerial support in that they need to reconfigure their systems.

18. Which of the following rules or controls, do you have in place? (multiple choice)

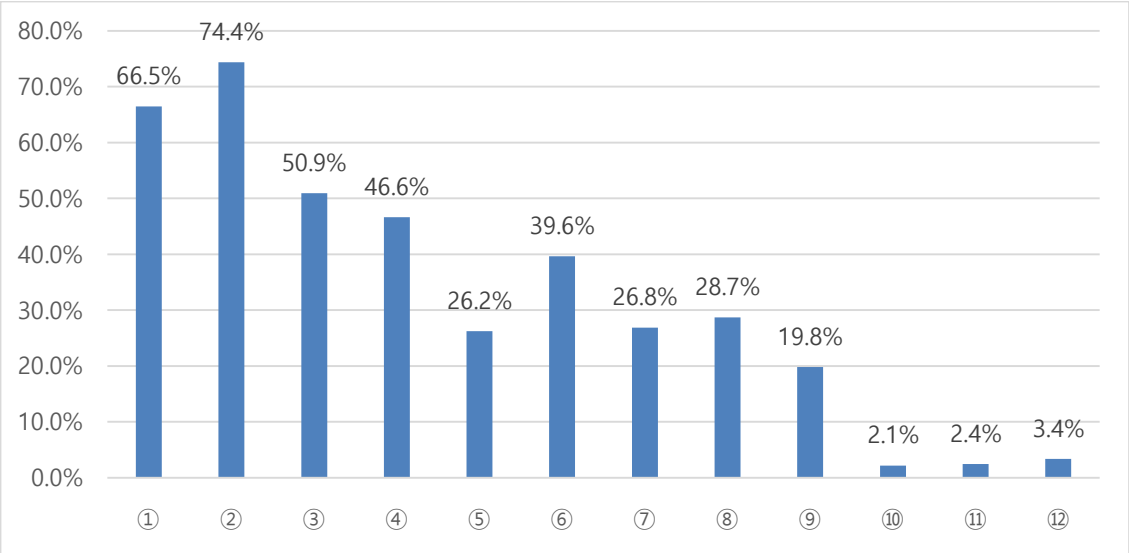


Figure 5.18 Adoption of rules or controls

Keys

①	Applying software updates when they are available
②	Up-to-date malware protection
③	Firewalls with appropriate configuration
④	Restricting IT admin and access rights to specific users
⑤	Any monitoring of user activity
⑥	Encrypting personal data
⑦	Security controls on company-owned devices (e.g., laptops)
⑧	Only allowing access via company-owned devices
⑨	A segregated guest wireless network
⑩	Other
⑪	None of these
⑫	Don't know

Most SMEs (94.5%) did not have formalised incident management processes to deal with breaches (Figure 5.19). This result indicates that Korean SMEs were not prepared to manage potential incidents. Although this statement applied to both small and medium businesses, there was a difference between the two groups. Medium firms were more likely to have the process than small firms (8.5% versus 3.3%, *p*=.042). However, it does not necessarily mean that in the vast majority of businesses any sort of plans were not ready. This will be investigated further in the qualitative analysis in Chapter 6 (see: Section 6.2).

Table 5.21: Cross-tabulation of incident management process and business size

		Business size		
		Small	Medium	Total
Incident management process	Yes	6	12	18
	No	178	130	308
	Total	184	142	326
		Pearson chi2(1) = 4.138		Pr=.042

Among business sectors, financial institutions stood out. Under half (41.7%) of financial and insurance firms had these processes, followed by information and communication firms (20.7%). By contrast, sectors such as wholesale/retailing, transportation, real estate, administrative and support services, arts, entertainment and recreation, repair and extra services did not have a single business that adopted an incident management process.

Businesses that provided 'services largely directed at organisations' had the highest rate of having incident management processes compared to other categories (12.1% versus 5.6% overall). Businesses in 'manufacturing and construction sectors' had the lowest rate (1.3%). The group difference was found to be statistically significant (*p*=.010).

Table 5.22: Cross-tabulation of incident management processes and categories of business sector

		Categories of business sector				
		1	2	3	4	Total
Incident management process	Yes	5	8	3	2	18
	No	54	58	46	147	305
	Total	59	66	49	149	323
Pearson chi2(3) = 11.418 Pr=.010						

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

19. Is there any incident management processes in your company?

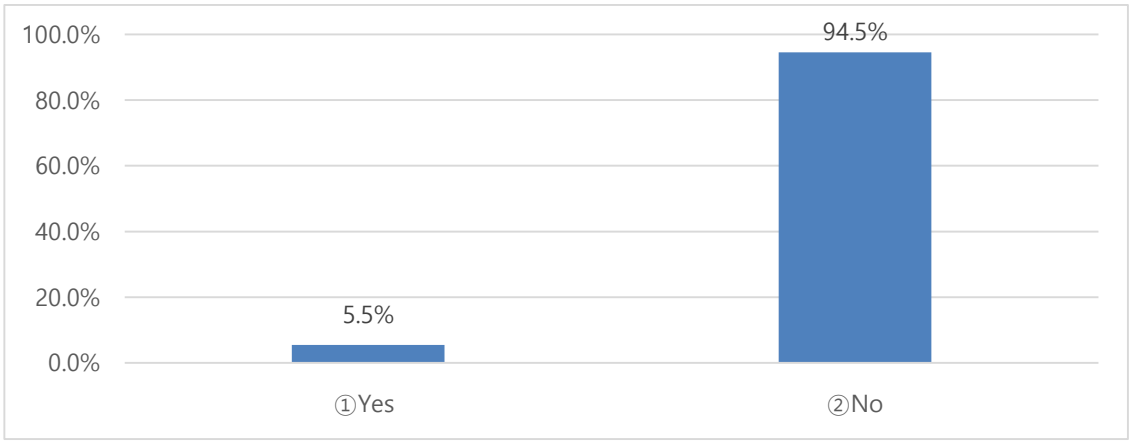


Figure 5.19 Adoption of incident management processes

As a means of risk management, insurance gives businesses an additional layer of protection from financial loss. From a financial point of view, insurance is a good tool to hedge against the risk of damages from cyber breaches. However, insurance was not found to be a widely accepted means of risk management in relation to cyber security. Under a tenth (9.1%) of businesses had insurance to cover damage from cyber security breaches.

20. Do you have insurance which would cover you in the event of a cyber security breach or attack?

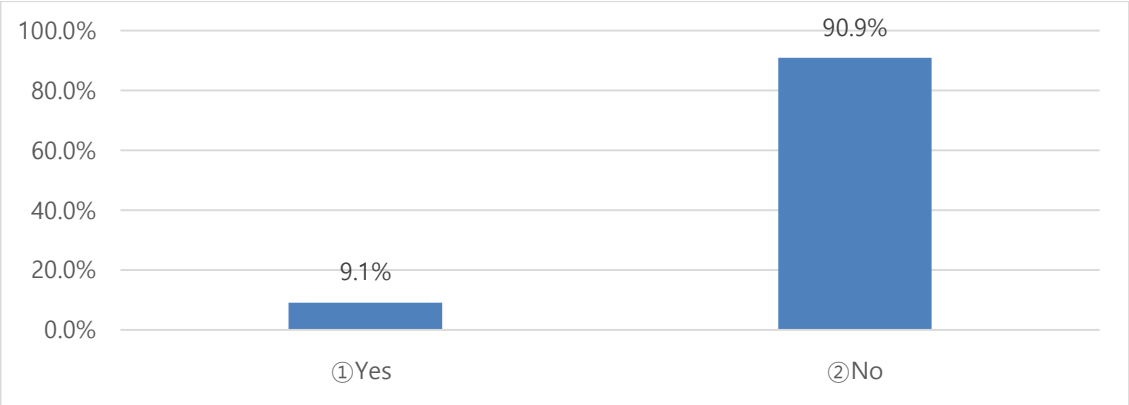


Figure 5.20 Insurance to cover cyber security breaches or attacks

There was a big difference between medium and small firms. Fewer small than medium firms were covered by any type of insurance (1.6% versus 19.0%). A chi-square test showed the group difference was statistically significant (p<.001). Over half (58.3%) of financial and insurance firms and a third (36.4%) of administrative and support service firms were covered by insurance when a breach entailed financial damage. By contrast, no business in education services, arts, entertainment and recreation services, and repair and extra services, had insurance.

Table 5.23: Cross-tabulation of insurance and business size

		Business size		
		Small	Medium	Total
Insurance	Yes	3	27	30
	No	181	115	296
	Total	184	142	326
Pearson chi2(1) = 28.986				Pr=.000

Businesses that provided 'services largely directed at organisations' were insured the most (16.7%), followed by businesses which were 'largely directed at public' (11.9%). The other two categories (i.e., 'public services' (6.1%) and 'manufacturing and

construction' (6.0%)) were covered by insurance the least. A chi-square test rejected the association between business sector categories and insurance coverage at the 0.05 level (*p*=.066).

Table 5.24: Cross-tabulation of insurance and categories of business sector

		Categories of business sector				
		1	2	3	4	Total
Insurance	Yes	7	11	3	9	30
	No	52	55	46	140	293
	Total	59	66	49	149	323
Pearson chi2(3) = 7.178						Pr=.066

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

When asked where to report a breach, just over half (51.2%) of businesses replied that they would report to the Police: other public sector agencies such as NIS (17.4%) and KISA (30.2%) were also mentioned (Figure 5.21). As for the private sector organisations, antivirus companies (30.5%), bank/credit card companies (19.2%), outsourced cyber security providers (27.1%), ISPs (18.9%), and website administers (17.7%) were mentioned. Businesses tended to report to more than one organisation[68]. Reporting destinations were also evenly distributed between public sector agencies (98.8%) and private sector organisations (113.4%)[69]. It may indicate that SMEs reported to both a private company and a public agency. The duplicated reporting practice needs to be investigated further to ascertain whether it was redundant or necessary.

68 742 choices were made in this question, although the sample size was 328.
69 The combined value was over 100% because this question had multiple choices.

21. Who is a breach or attack reported to? (multiple choice)

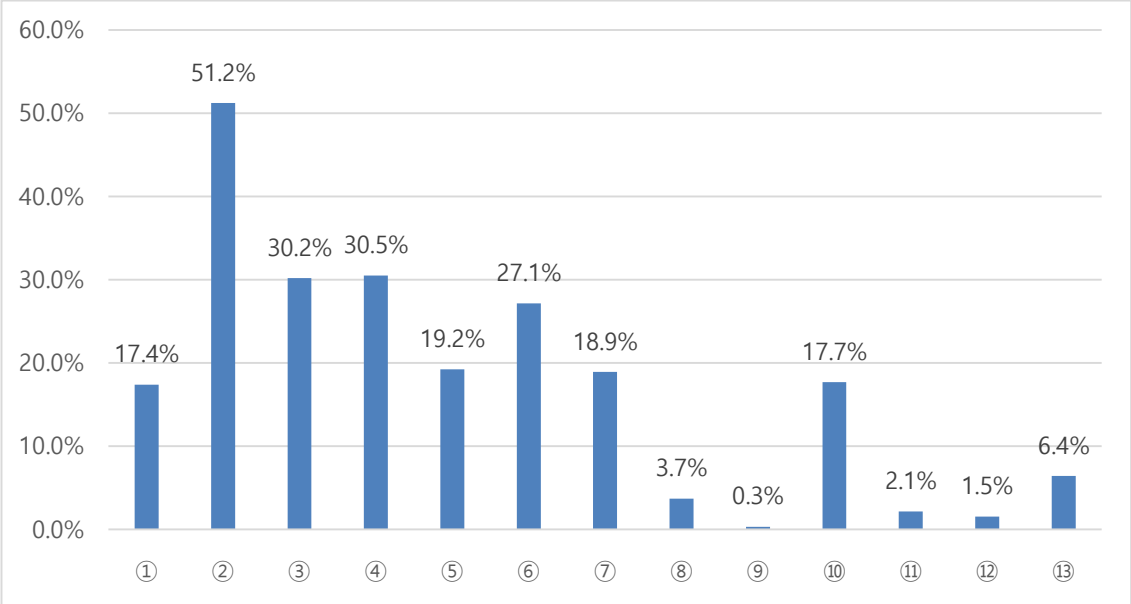


Figure 5.21 Destination for a breach or attack report

Keys

①	National Intelligence Service	⑧	Professional/trade/industry association
②	Police	⑨	Media
③	Korean Internet & Security Agency	⑩	Website administer
④	Antivirus company	⑪	Other
⑤	Bank or credit card company	⑫	No intention to report
⑥	Outsourced cyber security provider	⑬	Don't know
⑦	Internet service provider (ISPs)		

5.3.5. Information acquisition and relationship with external organisations

General online searching through major web portals (54.3%) was the most widely used method to seek information on cyber security threats (Figure 5.22). Under a third (29.6%) of businesses tapped into government websites (i.e., go.kr). A similar proportion (29.9%) acquired information from colleagues or experts within their company. The percentage of businesses that sought information from senior management in their company (12.2%) did not reach even half of that from colleagues or experts. This illustrates that information sharing of cyber security threats was more frequent among staff than

between staff and senior management. Among public organisations, KISA (22.0%) was the organisation businesses relied upon the most. Other agencies: Police (6.7%), NIS (6.4%), and SMBA (7.0%) were little used. The overall picture highlights that businesses were twice as dependent upon the private sector organisations (567 counts) than public sector agencies (282 counts) for information.

22. From where have you sought information, advice or guidance on the cyber security threats that your company faces? (multiple choice)

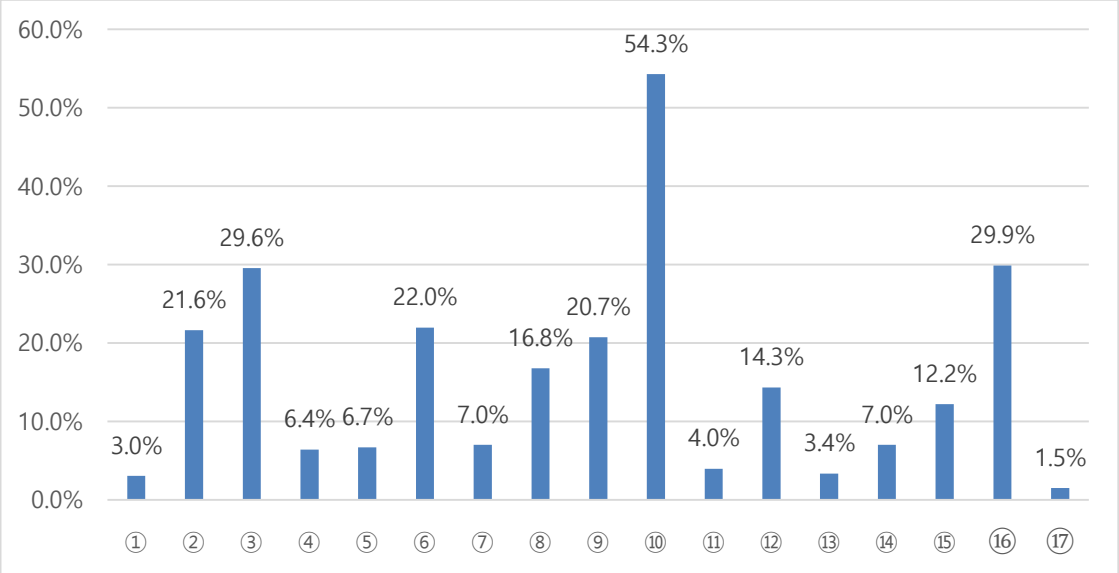


Figure 5.22 Destination for advice or guidance on cyber security threats

Keys

①	Business bank/bank's IT staff	⑩	Online searching generally
②	External security/IT consultants	⑪	Professional/trade/industry association
③	go.kr	⑫	Regulator
④	National Intelligence Services	⑬	Security product vendors
⑤	Police	⑭	Other companies
⑥	Korean Internet & Security Agency	⑮	Within your company – senior management/board
⑦	Small and Medium Business Administration	⑯	Within your company – other colleagues or experts
⑧	Internet Service Provider	⑰	Other
⑨	Newspapers/media		

Under a half (44.8%) of businesses were unaware of any suggested accreditation schemes and standards relating to cyber security (Figure 5.23). The overall picture represents a large discrepancy among choices. The ISO 27001 (31.4%) from an international organisation and Korean ISMS (44.8%) from the KISA were widely known to businesses, while Government's guidance (6.7%) and Security Operation Centre (13.1%) by the SBMA were not. The obvious lack of awareness on any Government's guidance may indicate that either guidance did not exist or it was poorly constructed so that businesses were unaware of it.

23. Are you aware of any of the following initiatives and standards? (multiple choice)

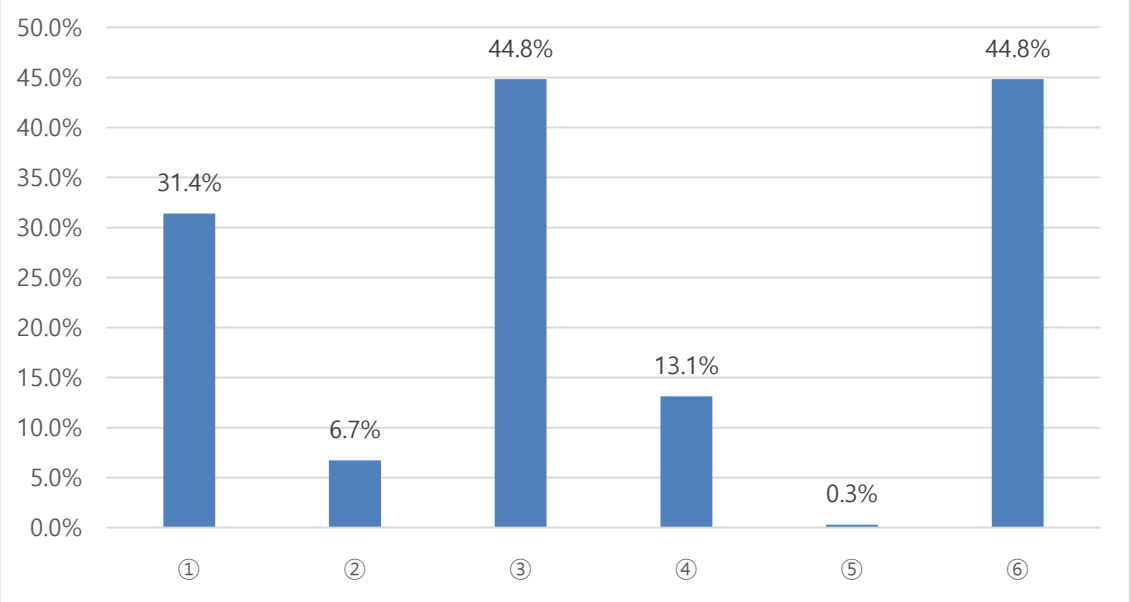


Figure 5.23 Awareness of domestic or international standards

Keys

①	International Standard for Information Security Management (ISO27001)
②	Any government's guidance
③	K-ISMS from KISA
④	Security Operations Centre from SMBA
⑤	Other
⑥	None of these

A large difference was found when factoring in business size. There was much higher awareness among medium firms than small firms both of ISO 27001 (39.4% versus 25.5%) and Korean ISMS (68.3% versus 27.2%). This difference was found to be statistically significant both in ISO 27001 (p=.007) and Korean ISMS (p<.001).

Table 5.25: Cross-tabulation of awareness of standards (ISO27001) and business size

		Small	Medium	Total
ISO27001	Yes	47	56	103
	No	137	86	223
	Total	184	142	326
Pearson chi2(1) = 7.158				Pr=.007

Table 5.26: Cross-tabulation of awareness of standards (Korean ISMS) and business size

		Small	Medium	Total
Korean ISMS	Yes	50	97	147
	No	134	45	179
	Total	184	142	326
Pearson chi2(1) = 54.777				Pr=.000

More than half (57.0%) of businesses reported that they had not contacted any government agencies in relation to cyber security (Figure 5.24). Among those (n=141) who contacted them, the KISA (22.6%) was the most widely mentioned, followed by the Police (19.8%). A minority (8.2%) of businesses mentioned the SMBA although the SMBA was the public agency that directly provided many services to small and medium firms. This will be examined further in the qualitative analysis in Chapter 6 (see: Sections 6.4 and 6.5).

24. Which any government agencies have you contacted in relation to cyber security? (multiple choice)

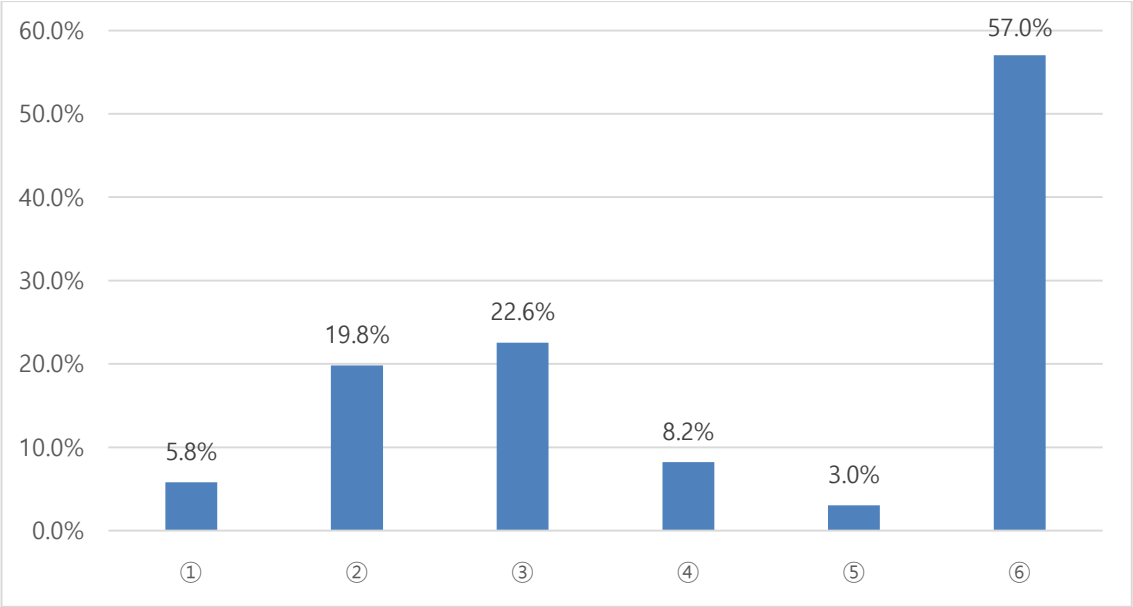


Figure 5.24 SMEs' contact on government agencies

Keys

①	National Intelligence Services
②	Police
③	Korean Internet & Security Agency
④	Small and Medium Business Administration
⑤	Other
⑥	None of these

The frequency distribution of Figure 5.25 was similar to that of Figure 5.24. Just over half (50.6%) of businesses mentioned they had not been contacted by suggested government agencies. Similar to Figure 5.24, the KISA was said to have contacted or provided under a third (26.8%) of businesses with any information. One notable difference came from the SMBA. In contrast to the meagre presence in Figure 5.24, the SMBA (17.7%) stood out against other agencies except the KISA in Figure 5.25. Disproportionately more contact was made by the SMBA than by SMEs (17.7% versus 8.2%). This implies an asymmetric relationship existed between SMEs and the SMBA.

25. Have you been contacted or provided with any information by any government agencies in relation to cyber security? (multiple choice)

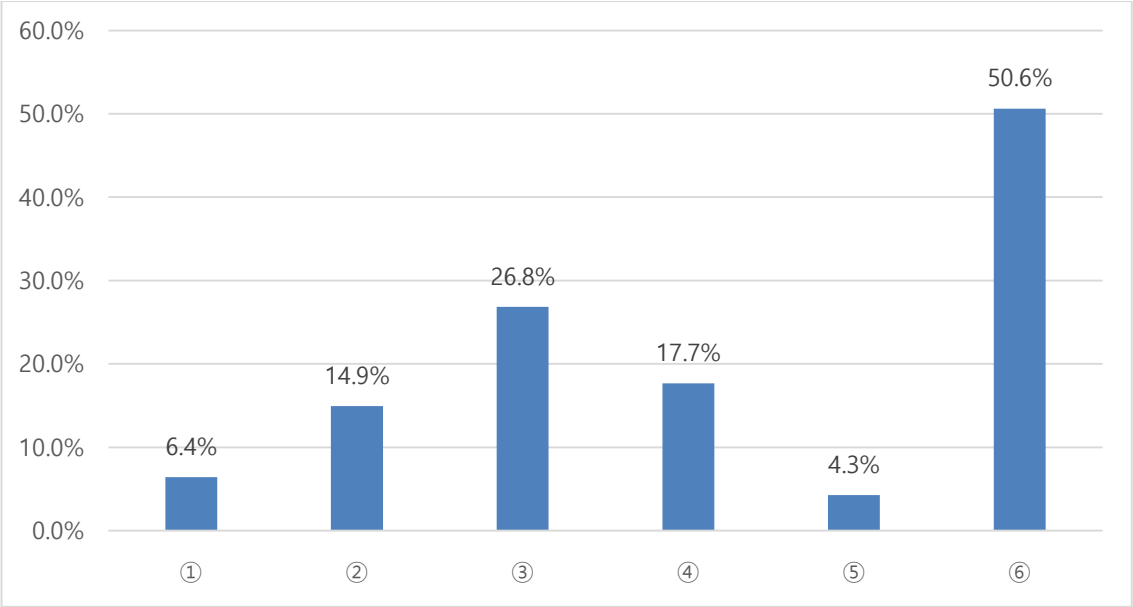


Figure 5.25 Government agencies' contact on SMEs

Keys

①	National Intelligence Services
②	Police
③	Korean Internet & Security Agency
④	Small and Medium Business Administration
⑤	Other
⑥	None of these

Figure 5.24 and Figure 5.25 showed that the KISA was the most frequently mentioned public organisation in terms of not only being sought by businesses but also reaching businesses. However, the relationship with the KISA was not equal to every business sector. It was noticeable that two business sectors had stronger relationships with the KISA than any other sectors. Information and communication (69.0%) and administrative and support services (45.5%) firms more frequently contacted the KISA compared to businesses in other sectors (22.9% overall). Conversely, the KISA provided information mostly to businesses in administrative and support services (54.6%) and information and communications (55.2%) (26.9% overall). On the other hand, financial

and insurance sectors had a weak or moderate relationship with the KISA (33.3% and 25.0%).

Korean SMEs frequently work for large companies as a subcontractor. Under two thirds (63.7%) of SMEs were not required to adhere to any cyber security standard when they worked for their clients. Government's scheme (26.8%) and Korean ISMS (18.0%) were more common types of requirements than renowned international ones (7.0%), which implied that domestic standards were more preferred by clients. Among SMEs (*n*=119) that said there was a requirement from their clients, over a dozen of SMEs were asked to adhere to more than two standards or schemes.

26. Which of the following, if any, do your clients require you to have or adhere to? (multiple choice)

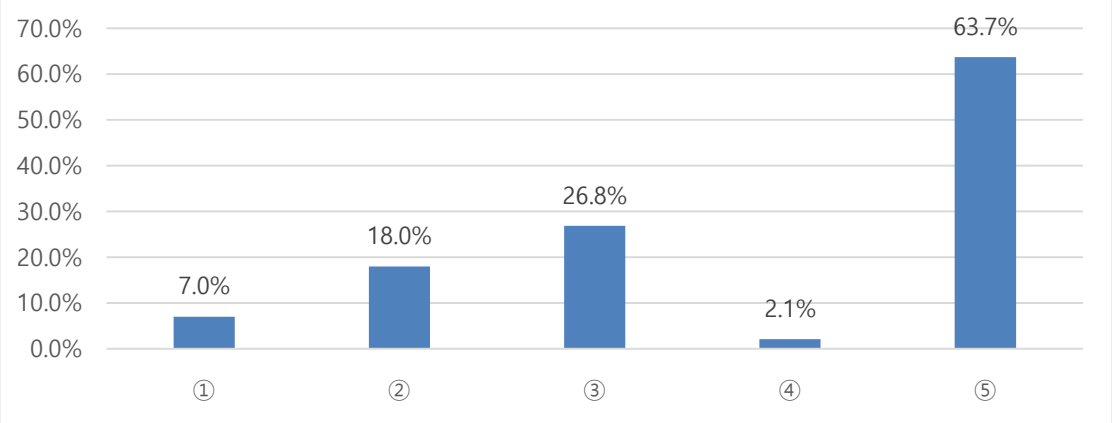


Figure 5.26 Clients' requirements for standards or schemes

Keys

①	A recognised international standard (e.g., ISO 27001/PCIDSS)
②	K-ISMS from KISA
③	Any government's scheme
④	Other
⑤	None of these

Adherence to suggested schemes was consistent across size bands. As business size increased, it was more likely that a firm was required to adhere to a standard or scheme.

Medium firms were more likely to be required to have international standards than small firms (12.0% versus 3.3%), and the same result was applied to Korean ISMS (30.3% versus 8.7%). The group difference of adherence to the two types of standards was statistically significant (respectively, *p*=.002 and *p*<.001). However, even though slightly more proportion of medium firms adhered to Government scheme (30.3% versus 23.9%), there was no statistically significant association between business size and adherence to Government schemes (*p*=.197). These results highlight that business size was a significant factor when choosing international standards or K-ISMS, but not when choosing Government schemes.

Table 5.27: Cross-tabulation of clients' requirements for standards (international standards) and business size

		Business size		
		Small	Medium	Total
International standards	Yes	6	17	23
	No	178	125	303
	Total	184	142	326
Pearson chi2(1) = 9.274				Pr=.002

Table 5.28: Cross-tabulation of clients' requirements for standards (Korean ISMS) and business size

		Business size		
		Small	Medium	Total
Korean ISMS	Yes	16	43	59
	No	168	99	267
	Total	184	142	326
Pearson chi2(1) = 25.195				Pr=.000

Table 5.29: Cross-tabulation of clients' requirements for standards (Government scheme) and business size

		Business size		
		Small	Medium	Total
Government scheme	Yes	44	43	87
	No	140	99	239
	Total	184	142	326
Pearson chi2(1) = 1.662				Pr=.197

On a related note, it was shown that the extent of requirements by clients varied by business sector. As expected, the financial and insurance sector was the most heavily required to have suggested standards: 50.0% for international standards and 75.0% for Korean ISMS.

5.4. Conclusion

Korean SMEs were highly connected to ICTs, but perception of their significance did not correspond to the actual adoption of ICTs.

A sizable majority of Korean SMEs relied upon online services in some form. The adoption of online services was mainly for communications and advertisement rather than business or financial transactions. Online services were used not only by business-owned devices, but also via personally-owned devices at work (77.7%). In particular, the use of externally-hosted web services was a widespread phenomenon in Korea. However, SMEs' perception of ICTs' significance did not necessarily match the high extent of actual usage of them. A 13.4 percentage point more of businesses replied negatively when asked whether their online services were a core part of their business offering. In addition, the number of positive answers (42.4%) was almost equal to that of negative answers (39.0%) when asked whether externally-hosted web services were critical to their business.

Cyber security breaches affected all kinds of SMEs and costs were not clearly measured.

It was notable that one in two businesses (55.4%) have experienced cyber security breaches, the majority attributed to viruses and malware (75.8%). Most of them were funnelled through emails, email attachments, or websites (53.8%). Two features of cyber-attacks using viruses and malware are the indiscriminate nature as to victim selection and low cost (Wall, 2007). Despite the prevalence of a breach, its financial impact was not well measured. Among businesses which suffered from breaches, about a third (34.1%) did not know the cost and a third (33.5%) estimated the total costs to be under £500. Business disruption (53.8%) and direct costs (i.e., repair or recovery costs: 46.2%) were found to be the most crucial impacts of cyber-attacks on businesses.

When it comes to approaches to risks, many businesses did not have a structural mechanism.

Under half (42.4%) of businesses had no formal cyber security policies. In line with this, more senior management viewed cyber security as a 'low' or 'very low' priority than 'high' or 'very high' (35.4% versus 32.1%). In addition, senior managers in over a third (38.7%) of businesses were never updated on cyber security. It was more likely that the perception on this subject by senior managers was positively related to communications between staff and senior managers. Likewise, the low perception of senior management on cyber security was translated into a lack of staff training. Staff in over a third (36.9%) of businesses did not experience any sort of cyber security training in the last 12 months. In addition, the dominant frequency of training was less than once a year (17.1%) or annually (28.4%). In terms of risk management arrangements, Korean SMEs heavily relied upon insiders, using staff members (41.8%) and board members (36.0%) rather than organisational artefacts such as policies or plans.

Most of SMEs were not prepared to deal with cyber security breaches, depending upon basic technical controls or actions.

The vast majority of businesses were not prepared to deal with breaches. They did not have incident management processes (94.5%) and were not covered by insurance (90.9%). What they employed mostly were malware protection updates (74.4%) and software updates (66.5%). These types of controls were provided online with high convenience to users. Also, regular health checks (68.3%) were shown as the most widely adopted action when businesses tried to identify cyber security risks. When it comes to reporting a breach, businesses were more likely to report to more than one organisation and reporting destinations were quite evenly distributed between public and private sector organisations.

Public sector organisations were not identified as a main contributor to SMEs in relation to information acquisition or information sharing.

Businesses acquired cyber security information mostly from online sources, such as major web portals (54.3%) and government websites (29.6%). Public sector agencies played a small role in contributing to SMEs' information acquisition. Among initiatives and standards, businesses were well aware of ISO 27001 (31.4%) and Korean ISMS (44.8%). In contrast, only 6.7% of businesses were aware of the Government's guidance which should have been accepted as a generic form of initiatives. Around half of businesses either did not contact any government agencies (57.0%) or have not been contacted by them (50.6%). Given that large companies contract for their services or products with SMEs in Korea, SMEs as a subcontractor are required to adhere to a set of standards. However in the cyber security domain slightly less than two thirds (63.7%) of SMEs were not required to have any standards. It highlights that there was not much pressure from client organisations in terms of cyber security standards.

CHAPTER 6: QUALITATIVE FINDINGS - SMES IN SOUTH KOREA

6.1 Introduction

This chapter provides findings of qualitative interview data, using thematic analysis. Raw data from field interviews was analysed, relevant extracts chosen and then structured to convey meaningful information. These extracts act as the basis of the themes suggested in the sections below.

In total, there were 25 interviewees. Among these, 16 were IT managers or owners in SMEs (13 managers and three owners) and the remaining 9 were officials from the public sector organisations (i.e., the NPA, the KISA, and the SMBA). The 16 interviewees from SMEs (see: Table 6.1) were chosen among the survey respondents who volunteered to participate, while the 9 public officials (see: Table 6.2) were selected using snowball sampling. How the researcher conducted the interviews is addressed in Chapter 4. Acronyms are used to denote the status of interviewees. 'CM', 'CO', and 'GO' are acronyms for 'Company Manager', 'Company Owner' and 'Government Official', respectively.

Braun and Clarke (2006) argued that rigorous application of thematic analysis allows for producing an insightful analysis which addresses research questions. Following this suggestion, the researcher tried to apply thematic analysis in a systematic and rigorous way. Finding themes is a sequential process. The course of finding themes, starting from identifying descriptive codes and developing analytic codes, was largely driven by the research questions mentioned in Section 1.2.4. Some descriptive and analytic codes were discarded because of their lack of relevance to the research questions. Themes emerged without reliance upon preconceptions, but were based on descriptive and analytic codes. The guideline which governed the coding process was the research questions.

Not all codes pointed at the main themes. There were dozens of codes which contradicted the themes. However, the researcher did not ignore the contradicting codes. Instead, they were carefully examined and interpreted to provide alternative readings of data. The researcher tried to present contradictions and contrasts among codes in order to enrich descriptions and discussions for this research.

After an extensive coding process, five themes were identified:

(1) unstructured cyber security management,
(2) culture resistant to cyber security,
(3) fragmentation of public organisations,
(4) overdependence on private organisations and
(5) influential external conditions.

These themes are substantiated by relevant sub-themes which gave structure to each theme.

Table 6.1: Profiles of interviewees from SMEs (*n*=16)

	Affiliation	Business sector	Category of Business sector	Size	Position
CO1	IT	Information and communication	Services largely directed at organisations	Small	Owner
CO2	Broadcasting services	Information and communication	Services largely directed at organisations	Small	Owner
CM3	Construction engineering	Professional, scientific and technical activities	Services largely directed at organisations	Medium	Low manager
CM4	Education/ event-planning	Education services	Public services	Small	Senior manager
CM5	Education	Education services	Public services	Medium	Low manager
CM6	Health	Human health and social work activities	Public services	Small	Senior manager
CM7	Manufacturing	Manufacturing	Manufacturing and construction	Medium	Middle manager
CM8	Manufacturing	Manufacturing	Manufacturing and construction	Medium	Middle manager
CM9	Construction	Construction	Manufacturing and construction	Medium	Middle manager
CM10	Real estate	Real estate activities	Services largely directed at public	Small	Low manager
CM11	Research institute	Professional, scientific and technical activities	Services largely directed at organisations	Medium	Low manager
CO12	IT	Information and communication	Services largely directed at organisations	Small	Owner
CM13	Manufacturing	Manufacturing	Manufacturing and construction	Medium	Middle manager
CM14	Finance	Financial and insurance	Services largely directed at public	Medium	Senior manager
CM15	Insurance	Financial and insurance	Services largely directed at public	Medium	Middle manager
CM16	Online shopping	Wholesale/retailing	Services largely directed at public	Medium	Senior manager

Table 6.2: Profiles of interviewees from public agencies (*n*=9)

	Affiliation	Position
GO1	National Police Agency	A manager in cybercrime investigation team
GO2	National Police Agency	A manager in cyber threat analysis team
GO3	National Police Agency	A manager in cyber security planning team
GO4	Korean Internet & Safety Agency	Staff in intelligence cooperation team
GO5	Korean Internet & Safety Agency	An organiser of IT training programmes for SMEs
GO6	Korean Internet & Safety Agency	A manager in breach investigation team
GO7	Small and Medium Business Administration	A manager in technology information protection team
GO8	Small and Medium Business Administration	Staff in technology assistance team
GO9	Small and Medium Business Administration	Staff in risk assessment team

6.2 Unstructured cyber security management

This theme starts from suggesting SMEs' awareness of breaches and threats to understand how SMEs perceive cyber threats. It continues to examine how the perception plays out in businesses. The theme, unstructured cyber security management, consisted of three sub-themes:

(1) awareness of risks and breaches,
(2) approaches to cyber security risk[70] and
(3) breach responses.

70 This sub-theme included a discontinuity between perception and engagement, no internal support, a factor that changes the dynamics and a lack of interest from senior management.

The latter two sub-themes were manifestations of the first sub-theme. While the second sub-theme involved general preparedness before a breach occurred, the third sub-theme related to responsive measures after a breach. It is important to note that these three sub-themes appeared in a sequential order and were connected to each other. The awareness influenced approaches to cyber security and breach responses, and the approaches were linked to the breach responses.

Interview data showed that SMEs' approach to cyber security was poorly constructed, ranging from no internal support to a lack of interest from senior management. In line with these, no formal guidelines or protocols were ready regarding breach responses.

6. 2. 1 Awareness of risks and breaches

Having awareness of risks and breaches is a rudimentary stepping stone in preparing for future responses. However, in general, Korean SMEs had a low awareness of breaches of their computer systems. The lack of awareness mainly resulted from a technical difficulty in identifying beaches as well as from a lack of imagination that SMEs can be victimised. The moment that SMEs became aware of the risks and breaches was when they identified damage to their computer systems. This means that damage experience as a victim was a direct cause for raising awareness.

CO1

Most SMEs do not know whether a security breach has occurred.

CM4

Previously, I saw statistics which said that over half of SMEs in other countries suffered attacks because SMEs were easy targets. But many Korean SMEs do not think that they can be targets of cyber-attacks. This perception, or attitude, also increases the possibility of not knowing of damage even if an attack occurred.

Although some SMEs (12.5%, 2 out of 16) recognised that there were many attempted attacks before a breach materialised, this knowledge did not lead to raising awareness or taking any preparatory action. They were negligent of the attempted attacks based on the assumption that most of the attempted attacks did not lead to damage. Along with the naïve perception, SMEs did not have a proper event detection system. This was due to the lack of resources, as it requires financial resources and attention to set up a system to forewarn and prevent an upcoming malicious event. The insufficient organisational support for cyber security was a reflection on how poor the awareness was. The extracts below illustrated the general mentality of SMEs:

CO12

We did not suffer from cyber breaches. There are a lot of attempted hackings but there was no actual damage.

CM14

We did not experience any form of cyber breaches until now, but there are a lot of attempted breaches for sure.

Even though SMEs had a low awareness on the risks and breaches, they were afraid of cyber threats. Over half (56.2%, 9 out of 16) of interviewees from SMEs replied that the most prevalent and dangerous types of cyber threats were carried out via viruses and malware, especially ransomware. The viruses and malware are malicious codes which automatically initiate damaging activities against targeted computer systems. Of various damaging activities, SMEs viewed information leakage as the most catastrophic scenario for their business.

Information that SMEs wanted to protect came in two types: business information and personal information. The type of information to be protected depended upon the nature of their business. For example, some manufacturers had confidential

technologies to take an advantage over competitors, while banks or online shopping businesses regarded customers' personal information as extremely sensitive data.

Information leakage can be perpetrated by insiders as well as external actors. Karagiannopoulos (2016) presented several high-profile cybercrime cases in the UK and the US. Those cases involved stealing corporate information by insiders for pecuniary reasons. Coinciding with Karagiannopoulos (2016) twice as many SMEs were afraid of information leakage by insiders than by external cybercriminals (Table 6.3). Not all interviewees were included in the table because some interviewees (43.8%, 7 out of 16) did not suggest awareness of any threats.

Table 6.3: Classification of perceived threats of SMEs

	Insider threats	**External threats**	**Total**	**Category of Business sector**
Business information	CO2, 12, CM3, 7, 8, 13,	CM3	6	- Manufacturing(3) - Services largely directed at organisations(3)
Personal information	CM14, 16	CM4, 14, 16	3	- Public services(1) - Services largely directed at public(2)
Total	8	4		

The classification revealed two interesting patterns. The first was that SMEs perceived insider threats more seriously than external threats (8 versus 4). This pattern was largely driven by the businesses which emphasised business information. SMEs that valued business information concerned themselves more with insider threats than those that treasured personal information (6 versus 2). Except for CM4, senior managers from SMEs which valued personal information (CM14 and 16) gave an even weight to both insider threats and external threats. The illustrations below show how the interviewees mentioned the perceived threats.

CM3

I am afraid of information leakage, for sure, because classified documents should not be disclosed to outside companies.

CM13

We are more afraid of information leakage by insiders than by external hacking. Our business might be interrupted for a couple of days by external attacks or we may suffer some financial damage, but if classified information is leaked to our competitors, the whole business will be in jeopardy. We consider data leakage as the worst scenario for our business.

CM14

Banks are targeted by hackers or malware for sure, but I also worry about breaches by insiders… insiders know loopholes in our system, so it is possible to take advantage of the system.

CM16

As with external infiltration, I am also afraid of information leakage by insiders. Most of employees are young people in their 20's to early 40's. Not every employee is suspicious…. We have experienced quite a lot of breaches by insiders and by outsiders. To my company, personal information leakage is the worst case. Due to the nature of our business, which is online shopping, our customer information is the most important asset.

The second pattern was that the threat perception was associated with which parties SMEs sold their services or products to. Business information was considered valuable by businesses in 'manufacturing' (CM7, 8 and 13) and by businesses whose 'services largely directed at organisations' (CO2 and CM3, 12). Given that around half of Korean manufacturers made products for large companies (Cho, 2014), most of SMEs in this category (i.e., businesses which valued business information) provided their products or services to 'organisations'. These SMEs perceived insider threats as more dangerous. On

the contrary, businesses which provided services to the public (CM4, 14 and 16) valued personal information, and recognised personal information should be protected from both inside and external threats. This pattern highlights whether SMEs' customers were organisations or members of the public was closely related to their threat perception.

6. 2. 2 Approaches to cyber security risks

This sub-theme involved SMEs' attitude to cyber security risks. For senior managers, media outlets were the main channels for acquiring information on cyber security threats. An exposure to major cases from media outlets drove them to feel the sense of the seriousness of cyber threats. However, how managers and owners of SMEs actually took action on cyber security issues did not match their perceptions. This implies that there was a discontinuity between their perception and engagement. First and foremost, senior managers did not act upon cyber security issues even though they viewed cyber security as a priority. In particular, this applied to the situation in which they had to make a decision in relation to investment (CM5 and 11) and giving up work-related conveniences (CM15).

CM5

Based on my impression, senior management know that cyber security needs more attention, but, well... this does not lead to investment.

CM15

Our senior managers share the idea that cyber security is important. But, they do not want to sacrifice their interests when they actually need to choose between security controls and giving up their convenience.

CM11

The good thing is that, more recently, our senior managers have interests in cyber security, not very high, though… I guess they heard of some bad incidents from news

media. The bad thing is that it does not necessarily lead to investment yet. They understand the severity of cyber breaches, but do not know what they need to do step-by-step.

The interviewees were all directly or indirectly involved in IT matters within a firm. In a business, they were positioned to get their cyber security agenda across to general staff and senior managers. However, there were several barriers to actual engagement in cyber security agendas. The main reason was an absence of internal support. To run training or to set up a security control requires organisational resources. Not only resources, but also the problem of a heavy workload. SMEs normally do not have an IT team or even a single IT professional solely responsible for IT matters. The large majority of SMEs' interviewees (81.3%, 13 out of 16) agreed with this point by suggesting that they were engaged in non-IT matters. They perceived IT matters as extra responsibilities. Among those 13 interviewees, 6 of them (46.2%) belonged to a management/business support team. This shows that IT matters within a firm were classified as a supporting role for business. Under this working condition, it is understandable that SMEs were not ready for acting upon cyber security matters. Some interviewees (18.8%, 3 out of 16) expressed their inability to carry out an action despite a perceived need to do so. See below for one example:

CM3

*As you might expect, we do not have dedicated cyber security staff. I do this job along with other IT supporting jobs, but cyber security is not the main job for me. Also, I have some other non-IT jobs I should deal with. I think this is normal… (**What do you mean by 'normal'?)** Well.. I see most of small and medium companies do not have proper cyber security staff, not even IT staff.. If there is no issue, cyber security is not the priority in my company at all. I have to constantly monitor information systems in the company, but I have no time to monitor them. I do check them when I have time or when some anomies are identified, for example, heavy payload of packets.*

SMEs often run their business without enough resources. Thus, generally, teams and departments within a business needed to fight against each other to tap into their limited resources. IT staff and managers had to provide justifications to senior management or an owner as to why they needed more resources. This was considered as internal politics. Senior managers and owners treated cyber security as a small part of IT matters and as a cost, not contributing to their revenues. In this competitive circumstance, it was difficult to garner expected investment in cyber security, not even in general IT systems.

The lack of support was represented in various forms, ranging from insufficient budgets and training to an absence of cyber security policies. Exactly half of the SMEs (50.0%, 8 out of 16) replied that they did not have an internal cyber security policy. And, less than half of them (43.8%, 7 out of 16) said that staff training was not provided by their firms. It is notable that policy adoption and staff training were associated. Among 9 SMEs which had either staff training or the cyber security policy, over half (55.6%, 5 out of 9) had both of them. On the contrary, about a third (37.5%, 6 out of 16) of SMEs did not have either of them. In total, more than two thirds (68.8%, 11 out of 16) of the total SMES either had both or neither. This finding supports the assertion that cyber security policy and staff training are manifestations of internal support. IT managers felt the shortage of business support on cyber security as follows.

CM10

Even though cyber security awareness by most employees is very low, we do not make an extra effort to increase their awareness. It is disappointing that no one thinks any form of training is needed and it is hard for us to step up to ask for it because there is no precedent.

CM11

Our team does not have the power to push our agenda. Our team is getting busier and busier… so, it is like having more responsibility without proper rights… which means.. we need to cover our systems more deeply, but they do not allow us to take proper actions.

In some cases (37.5%, 3 out of 8), the cyber security policy was not established in a separate format. The policy was included as part of a general security policy. The staff who made the policy were not cyber security experts, at times, not even IT staff. CM5 described the member of staff in charge of the general security policy as a 'layman'. A written policy is the backbone of business management. The treatment of cyber security policy as a subset of general security policy reflects a lack of recognition of cyber security as an independent area.

CM5

We have staff who make all sort of policy, including cyber security. There is no separate cyber security policy. It is included in the general security policy. Yeah.. cyber security is only a small part.. The funny thing is that he is a layman… I mean…general staff, not a cyber security expert.

CM7

Ye…, we also have an internal policy, but this is not noticeable if you look for it first time, because the cyber security policy is mixed up with other security policies. When someone made the security policy, he/she probably tried to jot down everything.. I need to upgrade it, but I did not have enough time to do it.

Across the board, it was still relatively uncommon for senior management to treat cyber security as a priority. Half of the SMEs (50.0%, 8 out of 16) have seen cyber security as a low or very low priority, whereas less than a third (31.3%, 5 out of 16) have given it a high or very high priority (Table 6.4). The tendency of low interest from senior management corresponded to other sub-themes, such as a discontinuity between their

perception and engagement, a lack of internal support, and contrasting values. These sub-themes represented the unfavourable atmosphere against cyber security.

Table 6.4: Cyber security as a priority to senior management

Priority by senior management	Businesses	Total	Percentage
Very high	CM14, 16	2	12.5%
High	CM4, 11, 15	3	18.75%
Neutral	CO2, 12, CM5	3	18.75%
Low	CO1, CM3, 7, 8, 10, 13	6	37.5%
Very low	CM6, 9	2	12.5%
Total	16	16	100.0%

However, there was a noticeable difference by the business sector. The difference came from the level of business connectedness to ICT. The more a business incorporated online elements, the higher chance it had to take cyber security as a priority. A stark contrast came from comparison between manufacturing/construction sector and financial/insurance sector. All four SMEs in manufacturing/construction sector (CM7, 8, 9 and 13) indicated that cyber security was either a low or very low priority to senior management. In contrast, senior management in financial/insurance sector (CM14 and 15) considered cyber security as a high or very high priority. On the other hand, no obvious distinction was made by size band. A few extracts below illustrate a low priority of senior management.

CM7

Our CEO and senior managers do not have interests in cyber security and pay attention to it. Cyber security is put at the back of the queue compared to other business agendas.

CM10

For senior managers, cyber security is on the back burner. Most of them treat cyber security as just a small part of IT matters. They do not share the idea that we need more investment on cyber security as our business adopts more ICTs.

CM13

I don't think our senior managers put much value on cyber security. Because our business is manufacturing headlights, we don't really use the Internet or connected software. The senior managers are more into how to make a better product or how to sell more, these sorts of things.

Having IT staff and managers responsible for cyber security was a widespread approach to manage the risks to SMEs. There was a consensus within organisations that IT staff and managers were responsible for cyber security risks and breaches. On any issues, assigning responsibility to a person or group was described as a widely used management strategy in Korean businesses. However, IT staff and managers did not welcome cyber security responsibilities because insufficient support and authority were given to them. They perceived the *buck-passing* as one of defensive behaviours of their companies as was noted by Robbins and Judge (2013, p. 431). This responsibility entailed negative connotations from some interviewees as follows.

CM11

(What do you think of having more responsibility? Doesn't it mean that you will have more support from your company?) *Not really. It is just putting the burden on IT staff and managers. This does not mean that my company is dedicated to cyber security. Giving responsibilities to someone is just a typical way of managing businesses by owners.*

CM5

Well,,,, it is just a superficial thing, no substance to it,,, I mean there is no appropriate amount of money or proper manpower to deal with it. Giving me the responsibility is

like,,, putting pressure to me, or giving me another burden. It looks unfair, but this is a normal thing on any agenda or issue in Korean companies and public organisations. This implies that if there is a big breach I should be a scapegoat. There can be legal consequences as well.

In total, the word, *damage*, was used 34 times throughout interviews of SMEs' managers and owners. Beyond the word frequency, the word had a meaningful contextual position in terms of cyber security approaches. Basically, the word was used for two reasons: (1) to give a sense of relief and (2) to prepare against a future breach. The first reason applied to when there was no damage up to that point in time. The manager, CM11, used words, "luckily" and "thankfully" to describe the relief. The fact that SMEs did not experience any damage or serious damage gave them a good reason to believe that they were properly protected. It was assumed that they did not have any problem because no damage was reported. This thought process was used to justify their current cyber security approach, causing SMEs to have a false sense of security (CM6). The feeling that they were safe acted as a restraining factor for internal support on cyber security.

CM11

There was another incident. Our messenger server was hacked, but luckily the server did not have important data, so no damage was entailed…… Thankfully, we didn't have to contact the police for investigation as no damage occurred and as we thought they were purely random malware.

CM6

Our business does not have many IT elements. I have never thought of cyber security in my business. There was no problem at all until now. I feel we are quite safe. Frankly, no reason to invest in cyber security things....

The second reason applied to a supposition, imagining a future damage. Over a third (37.5%, 6 out of 16) of SMEs revealed that they would take action if damage materialised.

The future action upon a potential cyber-attack was conditioned by the existence or extent of damage they suffered. SMEs changed their passive approach into a proactive one if damage was known to them. The damage identification was a turning point to reverse their hesitant approach. When it comes to a decision-making process in relation to future management actions, such as investment, support and breach reporting, the damage experience was regarded as a dominating referent point. However, there was no formal procedure or protocol on how to act upon the damage. SMEs knew that they should do something, but did not have an established plan as to what and how they should do it. Their approaches and responses were largely decided on a case by case basis, depending on the situation.

CO2

They seem to follow my words. Until now, it was recommendation, but if any damage incurs after a breach, then that will be a turning point. From then on, there will be only orders not recommendations.

CM5

Some staff clicked on attachments from emails and their account information has been leaked. And then, a massive amount of emails have been sent from our webmail server through this account, ending up putting our webmail server on the blacklist. As no actual damage has been materialised and the situation was resolved with the help of an IT vendor, our senior management was not informed of that attack. ***(So, you did not report the incident to your senior management?)*** *No, I didn't. I didn't have to. That was not serious enough to do reporting. If I report this kind of things, they will look at me and say like "so what?".*

6. 2. 3 Breach responses

The absolute majority of SMEs (93.8%, 15 out of 16) did not have a formal procedure for breach responses. There were no predetermined guidelines or protocols on how to

manage breaches. This does not mean that they did not have responses in any form. The unstructured responses to a breach indicated that response measures were sporadic and reactive rather than derived from a structured procedure. SMEs were not ready for forthcoming breaches, but simply reacted to them with having no response pattern or order. In fact, decisions on breach responses were made at the moment when they needed to take actions. As a consequence of this IT staff or managers needed to rely on a judgement call by their seniors, expecting some direction for handling the situation.

CM15

If our personal information is leaked, I am not sure what my boss will do about it. It is not a straightforward process.

CM10

One employee tried to download whole business data this year and he was caught before he quit the job. It ended as a minor incident... My senior manager covered this incident, giving him a warning.

As one of important elements of breach responses, public reporting was not well adopted by SMEs. SMEs did not think that reporting a breach to public organisations was a necessary measure for them, without recognising public reporting as one of continued steps of managing a breach. They treated public reporting as a means only for arrest and prosecution of offenders. Instead, what SMEs were interested in was business continuity. In interviews of SMEs, the term, *damage*, was interpreted in their own language. The damage was referred to as a disruption to business continuity. As long as their business runs as usual without major disruptions, they had no reason to be engaged in public reporting. These findings, in line with Yar's (2013, p. 13) claim on "dark figures" of cybercrime, suggest that SMEs had a tendency of no public reporting. The following excerpts show that damage and business continuity were important criteria for public reporting decisions.

CO1

As long as offenders have no intention of disrupting my business or of stealing our money, no official reporting will be made and I will just fix the problem to prevent similar attacks.

CM11

Thankfully, we didn't have to contact the police for investigation as no damage occurred and as we thought they were purely random malware.

CM8

If huge monetary damage is not materialised, no reporting will be made to the authorities.

In addition, whether to report to the authorities needed to go through a decision-making process from a business management point of view. There was no set of procedures for when they should initiate public reporting. In fact, public reporting involved several non-IT factors such as media attention and business reputation, thus requiring a business management decision. The reporting issue should not be viewed as part of IT issues, but from a larger perspective, involving a company-wide risk management decision. There was a small chance that the process reflected the needs or agendas from the cyber security perspective. This was because IT staff and managers were marginalised from the decision-making process. Although IT managers were responsible for cyber security issues, they were not the primary decision-makers. The following extracts explain how public reporting decisions were made by senior managers.

CM11

Reporting to the authorities is not a simple matter for us, because we might have to face unnecessary media attention, which is related to business reputation.. I need to talk to my boss and senior managers will ponder over this issue. There are a lot of factors they need to consider from the business management point of view. If we have suffered

serious damage, we will report definitely. Or… if another attack is about to happen… we might report..

CM15

We cannot simply call the police. I think whether to call the police will be decided by the senior management. Calling the police means the incident will be publicised in the media, for sure. And this will attract attentions from other government bodies and, more importantly, from current customers and potential customers, too. Thus, this is basically… a risk management decision.

GO2

But firms are not willing to report it because they are afraid of media attention and reputation loss. If they are caught for not reporting it, they end up paying a small fine.

Despite the business-wide pervasiveness of unstructured breach responses, there were a few outliers which were good examples. The two medium firms (CM14 and 16), one in the banking sector and the other an online shopping business, had internal breach management processes. Both firms provided 'services largely directed at public', thus treating customers' personal information as highly sensitive data. Thanks to the formalised processes, they could act upon a breach without relying on a judgement call by senior managers and owners. A senior manager from the banking sector (CM14) emphasised a business recovery throughout the breach management process, whereas a senior manager from an online shopping business (CM16) illustrated how a formal discipline process played out as follows.

CM14

We have our own protocols. Once a breach happens we assess the situation and contain the situation so as not to spread it through networks. Then, I report it to the CEO to be aware of the situation and we call our external IT security vendor immediately to find out an exact cause of the problem. If our banking system is shut down, we will try our

best to restore it. If some damage is found or personal information is leaked, then we contact the police for official investigation. More importantly, during this process, we should make sure banking systems is *not disrupted.*

CM16

In every case, we have a small hearing and decide the level of discipline. We do not fire the staff unless information is leaked intentionally. Most cases end up giving a warning. There were a few cases of intentional leakage. In these cases, we report to the police and go through criminal justice process.

6.3 Culture resistant to cyber security

Each group has its own unique culture. Culture in a group contains a set of values which are derived from a pattern of basic assumptions (Schein, 2010). Even though the values and assumptions are invisible, they are manifested through artefacts. The interaction among artefacts, values, and assumptions is not exclusive to a small number of groups, but universally identified in any group.

The weak cyber security management suggested in Section 6.2 was analysed as a manifestation of culture resistant to cyber security and IT staff within a company. Without studying underlying assumptions and values of individual agents in an organisation, it is difficult to comprehend artefacts, which were summed up as the unstructured cyber security management in this research. Resistant culture to cyber security as a theme was composed of a set of different sub-themes: contrasting values, miscommunication, leadership of an owner, and a negative perception. These sub-themes acted as undercurrents which formed the culture resistant to cyber security.

6. 3. 1 Contrasting values

Business managers should be well aware of their business orientation towards profit-making, staff trust, work efficiency, and convenience. These fundamental corporate values were fully accepted by staff and managers and positioned as a norm in businesses. However, cyber security was not compatible with these values in that it naturally entailed layers of security controls and tighter rules.

It was difficult to identify a commonality between cyber security and those corporate values. Interview data showed that cyber security was understood as a conflicting value against those corporate values. Half of the IT managers and owners (50.0%, 8 out of 16) were concerned about the value conflicts. This was why several interviewees viewed the choice of security controls as a trade-off between cyber security and business effectiveness. The basic assumption was that adopting an additional security control was at odds with those business values. This means that IT managers had to go through a difficult battle with the majority of teams and departments to pursue cyber security agendas. They needed to win over those competing values. As a consequence, cyber security management was inherently situated in a weak position. Excerpts below illustrate how the assumption played out in an unfavourable manner.

CM4

As a small business, we emphasise more on sharing information to efficiently finish our commissioned work than tightly controlling access points to fortify security. This is a matter of choice. I think risk from cyber security breaches is definitely lower, so there is no point of increasing security which inevitably lowers work efficiency.

CO12

Maybe I could install a hacking-prevention system, but it slows down traffic too much… As a CEO, it is not easy to keep raising security due to trust issues. If I adopt additional security controls, staff perceive that I do not trust them. In turn, it decreases staff morale.

CM15

They (senior managers) do not want to sacrifice their interests when they actually need to choose between higher security controls and more convenience for work efficiency.

Due to this contrasting situation, IT staff and managers (50.0%, 8 out of 16) found themselves sandwiched between cyber security and corporate values. They also understood that overall business culture was tuned into business profits and individual work performance. Recognition of this difficult situation was reflected in the motto, *strengthening security, but at the same time reducing inconvenience of other employees*, which was provided by CM3. The motto itself was paradoxical in that his team tried to achieve both strong security and inconvenience reduction. The paradoxical motto not only reflected the conflicting situation that the IT team faced, but also could be understood as a neutralising strategy to adapt to the internal intricacies. As a manifesto, the motto signified that the IT team was willing to get along with non-IT teams and that it would factor in those corporate values when deciding the level of security. This demonstrates how the IT manager balanced the two different needs from different parties. The following extracts provide illustrations on this point.

CM14

Bankers work until 10pm usually. And they have to sell banking products and attract customers under his or her name. These things comprise their work performance, which translates into promotion or other incentives. In this situation, it is not easy to coerce security too much to other employees.

CM3

Our team's motto is "strengthening security, but at the same time reducing inconvenience of other employees". But there is a certain point that we cannot yield. We cannot take the risk that can lead to business disruption. If the business is disrupted, it is me who is responsible for it. I do not want to be labelled as an incompetent employee.

6. 3. 2 Miscommunication

Communication is considered a crucial element in constituting corporate culture. Likewise, communication was embedded in the formation process of cyber security culture. A small owner (CM10) directly mentioned the importance of communication among teams. Some managers used different means of communication to reach a certain purpose. While a middle manager in a manufacturing company (CM13) said formal or informal events were held to increase loyalty of staff, a senior manager in an online shopping business (CM16) adopted a visual approach to convey cyber security messages to non-IT staff. The excerpts below show how various means of communication were utilised to raise cyber security elements across a company.

CM10

And on top of that active communication between separate teams is really important.

CM13

Senior managers and a CEO emphasise loyalty to employees and try to communicate with them. The main strategy is to host family events or casual 'beer parties' so that they feel the company is their home. It is basically making a strong bond so that they cannot betray our company.

CM16

We cannot handle about 300 employees by 5 IT staff. So we had to try all sorts of ways to reach all of them in a visual manner. We use bulletin boards, posters, TVs in corridors, PC screen protectors. We try to make all employees see cyber security notices as often as possible.

Despite the importance of communication, a lack of communication was a noticeable phenomenon within a firm. The lack of communication was noticed both horizontally and vertically. This implies that a communication problem occurred not only between IT

staff and non-IT staff or among different teams (12.5%, 2 out of 16) but also alongside the hierarchical structure (25.0%, 4 out of 16). By business size, horizontal miscommunication tended to be suggested in small businesses (CM10 and CO12), whereas vertical miscommunication was conspicuous in medium businesses (CM3 and 15). The vertical miscommunication was represented in two different relationships: (1) the relationship between IT staff and senior managers (CM3) and (2) the relationship between IT staff and an owner (CM10 and 15). See below for three examples.

Horizontal miscommunication

CO12

We don't have an employee solely for cyber security. As my business is the IT-related one, every employee has good understanding of cyber security. All of them have computer science backgrounds from high school or college. Because staff don't really tell me everything… I might not know what they are thinking.. But I know that my staff in charge of cyber security matters has some difficulty talking to others. Every staff in my firm think himself or herself as a computer expert, so they do not listen to others when they are advised about computer things. So, I let the cyber security staff directly come and talk to me if he finds any problem, then I can do something. It is an easier way to take action against vulnerabilities.

Vertical miscommunication

CM3

We try to make senior managers think cyber security is crucial for business, but they do not want to hear us because they don't understand what we are trying to say. At some point, we gave up, especially when we found out that they had absolutely no understanding on how the computer system works or its basic mechanisms.

CM10

Recently, there was an alarm call…one employee tried to download whole business data this year and he was caught before he quit the job. It ended as a minor incident so we didn't report it to our CEO. We can't talk to everything to our CEO.

Internal reporting within an organisation is a method of formal communication. Reporting is a step-by-step process from staff to managers, and to an owner. A reporting mechanism is structured along a chain of command, thus being classified as hierarchical communication. Staff and managers should report their work or important issues to senior managers, so that they go through a decision-making process based on the reports from non-managerial employees. If there are no cyber security reports, senior management should make a decision without sufficient evidence. As a consequence, an outcome from decision-makings is prone to be biased. The excerpts above (CM3, 10) illustrated a lack of regular reporting on cyber security issues to senior management. In fact, reporting occurred on a limited scale. Major incidents which accompanied damage or business disruption were likely to be reported to senior management. This type of reporting was limited only to breach management rather than the whole cyber security management.

6. 3. 3 Leadership of an owner

The essence of leadership is influencing others (Yukl, 2002). In Asian businesses, position, authority and seniority are fundamental features which underlie leadership (Lok & Crawford, 2004). Drawing on this, Korean companies are based on paternalistic leadership which emphasises bureaucratic control and centralised decision-making (Cheng et al., 2014; Lok & Crawford, 2004; Swierczek, 1991). Less than two thirds of SMEs' interviewees (62.5%, 10 out of 16) primarily depicted an owner as an ultimate decision-maker as well as a controller on most internal business affairs. This depiction demonstrates that an owner had a tremendous influence on every corner of their business based on their authority which derived from his/her official position. This was also the case with cyber security agendas.

CM13

If a CEO changes, senior managers should change their ideas according to the CEO. This is Korean business culture. And, this change trickles down to general staff.

CM3

In SMEs, a CEO is the key who controls everything and decide from minute matters to bigger ones… Also, we are thinking about applying for ISMS certificate. Because this certificate is expensive and requires a lengthy process, I am not sure our CEO would say yes.

The 10 SMEs which mentioned the heavy influence of an owner consisted of six small and four medium businesses. Considering the sample size, significantly more interviewees from small businesses (100.0%, 6 out of 6) concurred with the statement than those from medium businesses (40.0%, 4 out of 10). Not only managers but also small owners (CO2 and 12) themselves perceived the influential role of an owner. Having said that, an owner's influence was viewed predominantly in a negative sense. IT managers expressed a sceptical opinion against their owners' support for cyber security agendas. Compared to this, very few extracts were found which mentioned an owner in a positive light. See below for two examples.

CM4

If our business gets larger, we may need to rent a server from IDC and add some layers for cyber security. We… maybe… my worry is the cost. I am not sure whether our CEO would be favourable to this idea.

CM5

Our CEO changes basically every year. A new CEO wants to show that he or she is different from his or her predecessor. Thus, a new CEO mostly focuses on short-sighted performance with high visual effects. However, cyber security is a supporting role rather

than cash-generating area, so it is hard to expect any short-term performance from cyber security.

Due to its strong authority, leadership of an owner was recognised as a significant factor which changed cyber security culture. One middle manager in a medium business (CM13) presented a successful case of how a mind-set change of an owner brought about cultural changes within a company. This was an outlier case.

CM13

I think the mind-set of a CEO is really important. A year ago, our CEO joined a seminar provided by the SMBA. From then on, he started to stress that cyber security should be one of our priorities. This has changed our corporate culture a little bit. Other teams tried to pay attention to what we said, at least...pretended to do. Now, we train staff once a year on how much our business information is important...

There can be some downsides from a strong leadership. One of them was a structural bias in decision-making processes. The processes were supposed to involve discussions among senior management. Managers avoided engaging in the processes because their owners' decision was deemed as a verdict without proper discussion. Some managers in small businesses (33.3%, 2 out of 6) agreed this point. They showed their reluctance to talk to an owner regarding cyber security decisions, deferring most of decisions to their owner. See below for an example.

CM10

But, our owner has an extensive authority, I mean, too much. Basically, he decides on most of things, even on cyber security, although he does not know anything about that. It is difficult to have some meaningful discussions with him because of his strong character. This situation makes me avoid suggesting anything about it. I just wait for his decisions and just follow them.

6. 3. 4 Negative perception

Negative perception was pervasive throughout the whole interview data. In detail, “a lack of understanding”, “marginalised”, “do not know”, “hassle”, “discourages”, and “against” were the exact terms used to denote the negative perception against cyber security and IT staff. It was apparent that there was a dichotomy between IT staff and non-IT staff. Interestingly, this negative perception was identified on several levels: staff, manager, and organisation levels. Non-IT personnel treated IT professionals as supporting staff for them and deemed cyber security as a cost. Overall, each level had a negative tendency against cyber security agendas. In consequences, the overall culture showed, to some extent, an unfavourable propensity against it.

CM3

Senior managers and most of employees consider cyber security a cost. Cost is something they should reduce, which means that cyber security needs to be reduced, not enhanced.

CM5

IT business is booming, but… Still IT professionals are marginalised within the company... We are treated as supporting staff for others. No proper attention is given to us. And cyber security is the thing we have to handle without proper attention by the company itself.

CM7

Most employees do not think of cyber security seriously. Sometimes, they are against us.

As with the aforementioned negative perception, non-IT personnel had insufficient understanding on cyber security. The managers in medium firms (CM3, 5, and 7) who expressed concern over the negative perception above also mentioned a lack of understanding of cyber security. This clearly indicates that the negative perception and the lack of understanding were linked. Although it is difficult to confirm causality

between these two, it would be more intuitive to argue that the negative perception was based on the lack of understanding than vice versa.

CM3

Easily speaking… most employees do not understand cyber security. They just complain about additional procedure. They only think that this is a hassle which discourages their work efficiency.

CM5

Our senior management does not understand what the IT team does and they look at us as just IT professionals. They do not know that there are professional subareas such as software, hardware, and security.

CM7

Haha… nope, not really... most staff do not even know what cyber security is, and only a few will know what they should do for cyber security.

The negative perception, or disregard for cyber security was not only maintained by individuals, but also permeated in the organisational structure. And, the negative sentiments on cyber security have spread into disregard for individual agents, IT staff, who were involved in cyber security matters. As a comparable response, IT staff and managers also contained some negative feelings against non-IT staff. The abovementioned extracts (CM3, 5, and 7) illustrated how much animosity IT managers had towards non-IT staff and managers. Phrases, such as “against us”, “they just complain”, and “do not even know” conveyed strong negative emotions against them. The negative feelings and attitudes were not directional perceptions between IT staff and non-IT staff, but bidirectional ones. A low manager from a medium firm (CM3) provided an example of non-IT staff resistance on cyber security and IT staff.

CM3

Due to cyber security risks, we do not use wifi. If we adopt wifi, we need to do more network segmentation and buy another security solution. Because of the cost, we gave up, finally. But, some employees still ask for wifi. Though we try to explain why we cannot adopt it, they keep asking and ignoring our explanation. They do not want to accept that additional security controls need to be equipped to use wifi. They want just a convenience, but we have to think about security.

In spite of the awareness of disregard for cyber security, most businesses (50.0%, 8 out of 16) could not act upon it due to the lack of internal support. Changing negative perceptions requires a long-term commitment with multi-faceted support. Instead, IT staff and managers who suffered internal disrespect figured out ways to neutralise the negative perception. They tried to adjust to this hostile environment by utilising an adaptive strategy. This strategy was not a by-product of management decisions, but an intentional product of IT staff and managers themselves. Aiming at getting cyber security messages across to non-IT staff and managers, this strategy took advantage of the fact that non-IT staff and managers did not have knowledge of IT matters. A low manager in a construction engineering business (CM3) described how this adaptive strategy was carried out in a real situation. According to the description below, an ostensible reason for this strategy was testing and alarming non-IT staff, but the real intention was to increase the dependency of non-IT staff on IT personnel.

CM3

*Well… sometimes we do some things cautiously….. We intentionally make an incident. We shut down a server or disable some systems. This is a way of informing employees of the importance of cyber security, but also it is a good way of giving the impression that IT team does an important job. Some employees seem to neglect us, so that we need to make them feel that they rely on us for their efficient work. (**When you did that, people don't complain about that? or aren't they suspicious of the disruption?**) No. They don't know anyway. They do not tell whether the disruption is because of malware or.. done*

by us. And, we have a good reason to do this, because this is another form of testing our staff and alarming them to be careful of their computers.

Even though the negative perception was dominant feelings across businesses, some businesses (18.8%, 3 out of 16) identified positive sentiments against cyber security. Non-IT staff in those businesses were aware of the importance of cyber security and showed positive attitudes towards cyber security. In line with the positive feelings, they favourably accepted cyber security rules and policies. The following excerpts illustrate this point.

CM4

Our staff know that securing personal information is a critical element for our company, so they are aware of the importance and basically know what to do... I am sure that most of staff understand the importance.

CM14

Sure, they know the importance of cyber security definitely. They should follow what they should do, of course, because they are fully aware that there are consequences for not following rules.

CM15

All staff know how important it is to keep to the rules in the policy…. Most of employees understand that personal information of customers are important.

Some investigation is needed to find out why these three SMEs were different from the rest. There were two commonalities. The first common feature was that cyber security was considered a priority by senior management. It was assumed that an emphasis by senior management on cyber security contributed to the increase of the awareness of general staff. The second commonality was related to the nature of their business. Those three businesses relied heavily upon ICTs in any form in order to provide education

services, banking services and insurance services, respectively. Their services were provided to the public rather than organisations, which meant that protection of customers' personal information was the first priority. These commonalities indicate that non-IT staff and managers' perception on cyber security was influenced by various factors on the organisational level.

6.4 Fragmentation of public organisations

Public sector organisations in cyber security have their own aims and roles. Cyberspace has the nature of surpassing time and geographical boundaries. This nature causes a new set of difficulties that public sector organisations have never encountered. Compared to this, public organisations are inherently bounded by geographic locations or jurisdiction. This is why coordination among relevant public organisations and with international counterparts cannot be overemphasised. However, relationships among the Korean public organisations were fragmented in three ways. Firstly, the level of cooperation was weak and they competed with each other to some extent. Secondly, information was not shared among them in an appropriate manner. Thirdly, two different approaches to cyber security were identified. These three were identified as sub-themes for the theme, fragmentation of public organisations.

6. 4. 1 Weak cooperation and competitive milieu

It is a normal expectation that public sector organisations in the same area work side-by-side. However, this was not the case among Korean public organisations working to secure cyberspace. To start a discussion on this, it was necessary to identify which public organisations were participating actors in the cyber security area. Interviewees recognised that the KISA, SMBA, NPA, and NIS were the main agencies. There was no dispute that the four entities were engaged in protecting SMEs regarding cyber security and cybercrime. The question centred on to what extent they were engaged in cooperation. When it comes to cyber security, the KISA took the leading role since it was

the IT professional public body which aimed to secure the whole public and private network across the nation. Due to its technical and strategic expertise in cyber security, KISA had the role of supporting a handful of public organisations. Two government interviewees described it as follows,

GO2

KISA is the core government organisation when we frequently talk about cyber threats… They are IT professionals both in technical point of view and policy point of view... They have a fairly good picture about general cyber threats... KISA has the expertise in cyber security, so basically they have no expectation from other relevant government agencies. No agency knows cyber security more than the KISA, so to speak. Thus, it is the KISA that supports other agencies in many ways.

GO5

We (KISA) send out Internet data or other materials in cyberspace to a variety of organisations. I think most of government organisations have some sort of connection with us. We support them by providing information they need... Indeed, Police, NIS, military, Korea Communications Commission (KCC) are all our (KISA) partners in the aspect of security breaches.

Interview data illustrated how their working relationships looked. There were three types of relationships: (1) cooperation, (2) no cooperation and (3) unofficial cooperation. Firstly, different extents of cooperation were found between the NPA and KISA, and the NPA and SMBA. Some interviewees from the NPA (66.7%, 2 out of 3) described the cooperation between the NPA and KISA was based on an operational and tactical level. The two agencies had an overlapping area in that they were responsible for cyber-attacks and breaches. The police interpreted them as cybercrime because any form of cyber-attacks and breaches were criminalised under the Korean law[71]. In order to

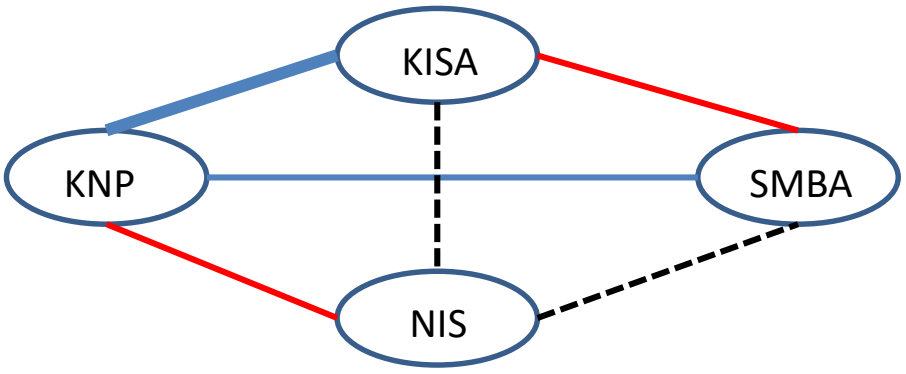
71 the Act on the Promotion of Information and Communications Network Utilisation and Information Protection

facilitate a transfer of victims' reports, the NPA deployed three cybercrime investigators to the 118 call centre in the KISA (GO3). If an inquiry was judged to be worth investigating, the call centre transferred the inquiry to one of the police investigators. This was cooperation on the operational level. On the tactical level, the NPA and KISA cross-examined malicious codes in order to reaffirm the nature of codes (GO1). These two examples show that the two agencies carried out substantial cooperation, but there was no indication that the cooperation was based on strategic guidance. Compared to this, the cooperation between the NPA and SMBA was weak. No substantial level of cooperation was found except occasional information sharing.

Secondly, no cooperation was found between the NPA and NIS, and the KISA and SMBA. Interviewees from these agencies did not recognise the other agency as a partner. The NPA was in competition with the NIS, which will be explained below. On the other hand, the SMBA and KISA were involved in different frameworks. One interviewee from the SMBA was aware of the different roles between them. This will be explained further in Section 6. 4. 3. Thirdly, the NIS had an unofficial cooperation with the KISA and SMBA. Due to the secret nature of the NIS, the extent of the cooperation between the KISA and NIS was almost hidden from public view.

GO9

Roughly speaking, we (SMBA) try to protect business secrets, whereas KISA aims to promote a safe internet environment for everybody. So, we target SMEs directly, but KISA targets the whole cyberspace.



- Red line : No cooperation
- Blue line : Cooperation
- Dash line: Unofficial cooperation

Figure 6.1 A diagram on the relationships among the main agencies

The diagram above shows that the extent of overall cooperation was significantly weak. Some interviewees (22.2%, 2 out of 9) even suspected whether public cooperation was needed. This implies that these government agencies did not have or, if they had, shared common ground which justified cooperation among them. It was noted that there was a lack of official framework for cooperation on the organisational level. Rather, their relationships were based on private connections on the individual level. The informal relationships between government officials reflected the extent and level of cooperation.

GO4

Relatively speaking, there is not much cooperation going on with other public organisations. We (KISA) often talk to the NIS, the Police, the military and maintain fairly good relationships, but do not have official cooperation framework. We have official relationships, of course, but not the level of close cooperation if I can say... I would say that we have more personal relationships rather than official ones. When we go to a conference or meeting, we meet people from other government bodies and easily become friends.

In addition, they were under competition to stand out in the league and outperform others. In Korean government, organisational performance was evaluated on how effectively an agency solved a problem rather than the extent of cooperation. This evaluation criterion spurred competition among government agencies working in the same area. If organisation A did not do anything when organisation B responded effectively and then made their achievement public, the organisation 'A' would not only lose face but also lose credits from higher government bodies, such as the Prime Minister's Office or the Presidential Office. This hierarchical government structure lay behind this competitive milieu. The two excerpts below provide an example of a difficulty in the cooperation between agencies.

GO1

I had an experience which embarrassed me quite a lot. My team was doing an investigation on a high-profile case involving customers' information leakage of an online shopping company. Because I had a lot of connections with officials in the KISA, they expected me to ring them up and do some co-work if I saw some big cases. If I don't, they will be disappointed, surely. But, at that time, the case was sensitive and, also, I was ordered not to share the information, I did not let them know. After finishing the investigation, I felt very sorry for that.

GO6

Well, this is due to the fact that they are working in the overlapping area and there is a bit of competition going on among us,, basically we need to fight for limited credits… like getting credits,, so the relationship is tense and we need to be cautious…… but there is no competition with private firms. Both of us can win-win.

Another reason behind the competition was related to organisational power struggle. The NIS which was, technically, in charge of cyber terrorism was viewed as trying to extend its hegemony over total cyber security. In particular, relationships between the NPA and NIS were the least cooperative compared to relationships between other

agencies. The NIS attempted to pass the 'Anti-cyberterrorism Act' which could provide the legal footing to the NIS. The NPA was afraid the Act would pass because, as a consequence of that, the NPA thought its investigatory role in cyber security could be significantly diminished. GO1 explained in detail how the two agencies competed against each other to expand or maintain their boundary.

GO1

But, the NIS is not our partner… The NIS keeps making every effort to pass the impending 'Anti-cyberterrorism act'. This bill dictates that the NIS is in charge of cyber terrorism incidents. The police chiefs will be held accountable to the NIS in any cyber terrorism cases or cases suspected as having links to cyber terrorism. If this bill is approved in the Congress, it will change the whole dynamics of how cyber terrorism cases are dealt with. The problem is that there is a grey area that general cybercrime and cyber terrorism incidents intersect. If we do not draw a fine line between them, the NIS has the possibility to invade our cybercrime area, too.

6. 4. 2 A lack of information sharing

Information sharing is a critical element to efficiently address cyber security issues. However, no interviewees from the government agencies mentioned an information sharing framework. It was evident that there was no overarching framework which aimed to share information among them. Rather, information sharing occurred occasionally among several agencies with similar needs. Although there were some meetings in place to discuss current issues among relevant agencies, those meetings centred on resolving the incumbent issues rather than sharing information. Also, the extent of information sharing was limited. The competing milieu was pointed out as the contextual factor which debilitated information sharing. Information sharing should have been based on trust among participants. It was therefore difficult to expect trust under the competing milieu. Even the low level of information sharing happened in an

unbalanced and asymmetric manner. Officials felt that the information sharing meetings did not function properly. The interview extract below points out this malfunction.

GO7

The meeting is a bit superficial. I feel that they are not willing to show or share what they have and just try to listen to what others say.

There should be several reasons for the failure of information sharing, but around half of interviewees (44.4%, 4 out of 9) pointed out that the existence of the intelligence agency, the NIS, in information sharing meetings was problematic. The inherent nature of an intelligence agency was its secrecy, which translated into *no information sharing*. It is quite an irony that the secret agency was in these meetings because the NIS was not expected to share their information with other public organisations. In addition, the NIS was allegedly engaged in internal politics in various ways, and one of them was dispatching intelligence agents to public and non-public sector organisations to collect their internal information (YTN, 2017).[72] If an intelligence agency of this character sits on the information sharing table, this would create different dynamics. In consequence, the existence of the NIS impeded information sharing, but also information sharing occurred in an asymmetric manner. GO5 phrased this situation as "the structural hindrance". These excerpts provide a detailed illustration on the overwhelming existence of the NIS as follows.

GO2

What I felt during that time was that there was no information sharing. The NIS could gather information from relevant government agencies through deployed staff. But, what the NIS shares with other government agencies is just, simply, threat levels and the way of informing is unilateral notification...We have a National cyber security framework, but, it is hugely affected by the NIS. Because the NIS is, by its nature, against information

72 However, a new Director Suh Hoon abolished the domestic information officer system on the same day (1 June 2017) he was appointed as the chief of the NIS (YTN, 2017).

sharing and disclosure. The problem is that the NIS is the main actor in the framework. You can probably imagine how the framework will work…

GO5

The NIS does not share their information, even though the NIS exclusively dominates information on North Korea or on the public sector. But, the point is that the NIS is deeply involved in the information sharing platform…This is the structural hindrance. Due to this limitation, our information sharing platform is largely divided.

It was the KISA which took the role of distributing cyber security information to other public organisations. This was why the KISA was recognised as a hub among the related public organisations. In this aspect, the KISA was equivalent to the GCHQ, a signals intelligence agency in the UK. They were both responsible for providing signals information to other public organisations. Therefore, dependence upon the KISA by other public organisations was disproportionately greater than vice versa. Despite the high centrality, the KISA was viewed as conducting a supporting role rather than a leading role. This may have reflected a general social milieu on IT professionals. In Korean society IT professionals have not been well respected (Ryu, 2003). This social milieu lingered on although the extent of disrespect slowly diminished. IT staff and managers in SMEs were treated as supporters as shown in Section 6. 3. 4. In a similar vein, the KISA was treated as a supporting agency for other public organisations (see: Section 6.4.1).

6. 4. 3 Two different approaches

It was found that there were two approaches to SMEs' cyber security: (1) general cyber security and (2) technology information protection. The first centred around overall cyber security threats, while the second focused on protection of technology and business information. Each approach was taken by a different set of public organisations. The KISA, NPA, and NIS involved general cyber security, whereas the technology

information protection was taken by the SMBA, the NPA, and the NIS. It was notable that the NPA and NIS were involved in both approaches. In case of the NPA, each approach was dealt with by different bureaus. Foreign Affairs Bureau concerned technology information protection, whereas Cyber Bureau involved overall cyber security threats and cybercrime as is described by GO2 below.

GO2

One funny thing is that two Bureaus in the Police do the similar job. Foreign Affairs Bureau is in charge of business information leakage incidents. Its public partner is the SMBA. On the other hand, we, Cyber Bureau deals with cybercrime and cyber security and its public partner is the KISA.

Conceptually, the former approach is broader than the latter one. Separating the latter one from the former one is a unique phenomenon. This was because the Korean government provided special attention to technology information protection. As mentioned in Section 3.4.3, protecting technology information was one of the government's principal interests in that the economy depended heavily on exports, and technology-oriented industries. The public organisations which were involved in one approach were ignorant of public bodies in the other approach. Largely, public actors in the two approaches were divided and did not interact each other. The two sides worked under a different framework. It is surprising to find out that there has not been any discussion on these two different approaches among related public organisations. In particular, the SMBA which involved the business information approach did not have a clear idea on how their approach related to cyber security. Each interviewee from the SMBA had his own version of interpretation on the difference between the two approaches.

GO7

Our role does not directly deal with cyber security. We call it business and technology information protection. Cyber security and technology information protection may have

some overlapping areas. Or I can say in this way. Cyber security is a means to protect business information. What we are doing is, in some sense, increasing cyber security. Without cyber security, business information cannot be protected. But, we do not say that we are doing cyber security. Rather, we say that we protect business information of SMEs.

GO8

I don't know much... But, maybe what we are doing can be captured by the concept of cyber security? Or do they involve totally different area? Well… as far as I know, cyber security is about technical things, but we are more like managing insiders.

GO9

We basically work for SMEs and our team assesses and prevents business information leakage of SMEs. Very few cases of information leakage happen offline and in almost 95% of all cases, business information is leaked online or via external devices. So, to large extent, cases that we deal with are related to cyber security. But, viewpoints from us and KISA are different.

The relation between the two approaches has never been discussed publicly. Public bodies in one approach did not envisage that other bodies in the other approach could be their partners. With having no formal or informal relationships, there was no engagement or cooperation between the two sides. However, the excerpts above hint at the possible intersection between the two approaches, as they mentioned, "overlapping areas", "captured by the concept of cyber security", and "related to cyber security". This highlights that there may be overlapping elements or sub-areas that require attention from both sides. In fact, there was once an internal discussion over this issue in the NPA. Some senior officers were aware of the common nature of these two approaches. However, the discussion ended to no avail. This example indicates that the Korean government needs to assess and discuss the rationale of keeping the two different frameworks.

GO2

Some high-ranking officials in the headquarters thought it was redundant to handle similar works in different bureaus. Once there was a discussion on the possible takeover of business information leakage incidents by Cyber Bureau. It did not work well, did not change anything. Well, I don't know how it needs to be changed, but, what I suggest is that both sides should work together. Because they are managed separately, it entails a waste of public resources. There is no communication whatsoever between these two bureaus. I think we need a sort of a framework which can encompass both cyber security and technology information protection.

6.5 Overdependence on private organisations

It was recognised that both public organisations and SMEs relied heavily upon the private sector organisations. But groups of private firms that the public organisations relied upon were different from those the SMEs rested upon. So did the reasons for the reliance. Findings below indicate that there were more organisations which required attention for this research and relationships among participating entities were complex. This section consists of two sub-themes, which are 'dependence upon private firms by public organisations' and 'dependence upon IT vendors by SMEs'.

6. 5. 1 Dependence upon private firms by public organisations

Compared to the weak cooperation and competitive milieu among public organisations, public bodies maintained intense and close cooperation with private organisations. This indicates that the private sector organisations were located in a core part in relations among the whole cyber security actors. The NPA and KISA had different reasons for cooperating with private organisations. The NPA created a working group with ISPs, antivirus companies, and IT security companies, etc. The creation of the working group was driven by the NPA for their own purposes. Two interviewees from the NPA (GO1 and 3) suggested two reasons: (1) to efficiently gather evidence and (2) to catch up with

recent trends. The former reason indicates that gathering digital evidence required the cooperation of some private companies which retained this. This is a new set of difficulties for law enforcement agencies compared to gathering physical evidence. The latter reason suggests that cybercrime investigators were keen to acquire external knowledge on cyber security. This level of cooperation was not a must, but an important facilitator for cybercrime investigation. This cooperation model can be viewed as an adaptive strategy in that this was developed out of need from the NPA. It opened a gate for cybercrime investigators to utilise informal connections with the private parties via the formal channel.

GO1

To efficiently resolve criminal cases, we invest in cooperation with private companies. If we do not have good relations with ISPs or online social media companies, it is difficult to collect evidence during investigations. ***(What about antivirus companies, and IT security companies?)*** *They are more like information providers to us, because they have recent news on cyber-attacks and source code of malware…*

GO3

Private firms such as antivirus firms or IT security firms have abundant information on recent trends. Their state-of-the-art information helps us to set up a new tool or tactic to prevent that. We have a working group with private firms and we meet once in two months. This is a good platform to take in outside knowledge. If we don't know what's going on outside, we can't see what is a new type of cybercrime and how it is changing.

In case of the KISA, cooperation with private parties was necessary to meet their organisational goal which was 'creating a secure cyberspace'. The KISA was able to identify cyber security attacks either by itself or from public reports to the 118 centre, but it could not develop a vaccine or disable a certain server. These should be carried out, respectively, by antivirus companies and ISPs. The KISA's cooperation with antivirus companies, IT security vendors, and ISPs was a crucial part of its breach management

process. These private parties engaged in implementing the KISA's policies as active participators, following a work protocol. Compared to the NPA's cooperation model, this model was based on an official partnership to reach KISA's organisational goal.

GO4

We are very close to private entities, like antivirus companies, IT security vendors, and ISPs. They are important to us. Once we identify malicious codes or viruses, we directly report them to antivirus companies so that they can make vaccines. Then, antivirus vendors will update their software. Also, following the analysis of a malicious code, we need to cut off orders from the controlling server. To do this, we have to contact ISPs to ask for cut-off of certain IPs or domains.

GO6

But, with private firms conversation is more formalised. Based on MoU, we cooperate with private firms to share information and to execute our policies. They will not work with us if we do not formally recognise them as formal partners. It is much closer and deeper.

In stark contrast, the SMBA did not engage with private organisations. This was due to the nature of their work. The SMBA dealt with technology information protection which rested on business secrecy. Instead, the SMBA's partners were confined to the public sector organisations, such as Ministry of Trade, Industry and Energy, Korean Intellectual Property Office, Fair Trade Commission, the NPA, and the NIS. Except the NPA and NIS, the first three public organisations addressed technology and business information protection from slightly different perspectives. The Ministry of Trade, Industry and Energy concentrated on protecting core technologies that significantly impacted on Korean exports, while the Korean Intellectual Property Office aimed to protect intellectual property rights. Lastly, the Fair Trade Commission, an antitrust watchdog, regulated unfair deals between large companies and SMEs. In this respect, the antitrust watchdog monitored whether large companies took advantage of their superior position

to take away SMEs' proprietary information. The protection coverage of the SMBA was larger than these three public bodies in that it protected not only business information but also technology information which should not be exposed to outsiders. An excerpt below illustrates the skewed partnerships that the SMBA had.

GO7

I would say that we do not cooperate with private companies because we are dealing with technology information protection. There is a bit of secrecy in this area. Business information inherently are secrets or intellectual property.

6. 5. 2 Dependence upon IT vendors by SMEs

The extent of dependency of SMEs upon IT vendors was overwhelming. In fact, almost all SMEs (93.8%, 15 out of 16) used IT services from IT vendors and those services, to some extent, contained cyber security elements. IT vendors were recognised as instantly sought-after parties when a technical anomaly or a security breach was suspected. For example, an IT vendor that managed a server for an SME was the most frequently contacted party by the SME. In addition, an IT vendor acted as an information provider when an SME needed to extend its cyber security capabilities. The SMEs' overdependence was predicated on the assumption that cyber security was a sub-set of general IT matters so that a general IT vendor could resolve cyber security problems as well. The following extracts describe SMEs' dependent attitudes towards IT vendors.

CO2

Our IT vendor provides us a server along with other services, but also supports us with the average level of cyber security. Cyber security is part of their job.

CM10

I contacted a commissioned IT vendor and the vendor fixed it within a few hours... Because the vendor knows the server and IT environment of our company, it is the right choice for us to contact the vendor if something happens.

CM13

*We are using a groupware from Hanbiro. Before, we got infected with a virus and the server was shut down. At that time, Hanbiro contacted us and resolved the situation very well. Our data were fully recovered. That was a huge relief…(**Do IT vendors provide enough cyber security, too?)** Yeah, I think, to a large extent, yes…. They provide IT services as a package, including cyber security.*

Then, why did SMEs rely upon IT vendors for cyber security matters? Primary reasons for this were: (1) immature market and (2) practical benefits to SMEs. The first reason involved a market environment of an IT sector. The interviewees below (CM9 and 16) suggested that there were only a few IT vendors which specialised in cyber security of SMEs. An immature market referred to the fact that cyber security was not a recognised sub-area in the IT sector. This was mainly because businesses in the IT sector perceived that provision of cyber security controls to SMEs did not yet generate profits. Currently, most cyber security vendors targeted large businesses and public sector organisations because these entities had a larger sum of budgets allocated for cyber security than SMEs.

CM9

When we work with field staff, we use clouding system. We work together in the cloud. This makes me worried sometimes. I tried to get a consultation about it, but it seems that there is no proper security vendor which provides security services on clouds for SMEs.

CM16

*I can rarely find any cyber security solutions or services targeting SMEs. In Korea, IT security vendors tilt toward serving government organisations, large companies mostly in financial institutions, gaming companies, or major web portal providers**. (Why is that?)*** *Because they have money.*

Secondly, for SMEs practical benefits by using IT vendors outweighed downsides associated with it. The benefits included convenience, efficiency and responsiveness. IT staff and managers were able to deal with an unexpected situation through supports from IT vendors. SMEs perceived that IT vendors were responsive and resolved an urgent issue in an efficient manner. It is important to bear in mind that business disruption was the greatest concern in breach management (see: Section 6.2.3). These benefits helped IT staff and managers to have a chance to disclose their work expertise to non-IT staff and managers. The resistant culture and negative perceptions against IT staff and managers were widespread within SMEs (see: Section 6.3). In fact, IT professionals were marginalised from the majority of non-IT staff. Against this unfavourable working environment, successful support from IT vendors gave IT professionals an opportunity to show their presence in their companies.

CM7

Frankly, I rely on our IT vendors… one which administers the IDC server and the other which administers our firewall system. They monitor our systems and contact us if something wrong happens. Very convenient for me… ***(Can you give me an example?)*** *Yeah, for example, the firewall vendor sends us a monthly report and lets us know the amount of traffic, the total number of attempted viruses and malware. Because we use static IPs, once I get the report, I inform some staff that their computers were infected. Then, general staff think that I am doing something! It is a great way to show them that I do something…*

CM9

We can use IT services from external parties… IT vendors… and they do basically everything. We simply need to choose products and services according to our budget.

CM13

They (IT vendors) bring us more efficiency. Employing one cyber security professional costs much more than using an IT vendor.

On the contrary, some SMEs (12.5%, 2 out of 16) cast doubt on the trend of overdependence upon IT vendors. When using services from IT vendors, SMEs normally allowed for them to have full access to computer and network systems. This also opened the door for accessing corporate data by the IT vendors. The authorised access by IT vendors was viewed as a high risk, generating nervousness for some SMEs. This was a trade-off between work efficiency and data protection. Although most SMEs were satisfied with the use of IT vendors, it is worth noting that there were some risks involved in it. The worry for IT vendors is illustrated as follows.

CM13

It is great to have an external party which can support us professionally, but on the other hand, it makes us nervous because the external party is able to access all of our data. If they maliciously leak our data or disrupt our system for any reason, that will be a very bad incident for us.

6.6 Influential external conditions

The aforementioned main themes were not formulated by themselves, but were conditioned by socioeconomic environments. They were outcomes of interactions with external environments. Three substantial external factors emerged from the interview data. These socioeconomic factors directly or indirectly influenced dynamics of cyber security management in SMEs as well as relationships among the public and private sector organisations involved. These were identified as sub-themes in this section: tough

business environment, ineffective penalty system, and client-driven contractual mechanisms.

6. 6. 1 Tough business environment

Survival could be the most serious risk to any business (Borodzicz, 2005, p. 62). Likewise, Korean businesses have struggled to win over competitors and increase their survivability (Jin & Gu Suh, 2005; Lee, 2004; Wright & Kwon, 2006). In this respect, severe market competition was one of the most mentioned codes from SMEs' interviewees (31.3%, 5 out of 16). Tough business environment has been created not only by domestic competitors but also by overseas ones. Korean SMEs make stringent efforts to keep their competitive edge in a way that outperforms foreign companies, especially, China, Japan, and India. Excerpts below illustrate heavy pressures from the competition. Due to the tough competition, SMEs placed emphasis on cultivating staff's creativity, providing high quality service, and attracting customers. In contrast, applying additional security controls was depicted as being in contradiction to those emphases. This implies that the severe market condition was an inhibiting factor to the increase of cyber security in SMEs.

CO1

I focus more on keeping ahead of our competitors with brilliant ideas. So, I try to encourage my staff to be creative and brilliant. Regulating or controlling their behaviour is killing their creativity… it is the worst thing.

CM14

Banks in our size, or banking sector in general, face very fierce market competition. Bankers work until 10pm usually. And they have to sell banking products and attract customers under his or her name.

6. 6. 2 Ineffective penalty system

Ineffective penalty system has emerged as an important contextual factor. Interestingly, this factor was not mentioned by SMEs, but only by public organisations. In the US, lawsuits related to corporate cyber security have surged recently, and this led senior managers to pay more attention to legal risks involving cyber security (Yoon, 2016). However, it has been continuously pointed out that Korean businesses have received low penalties on their illegal activities (Park, 2004). This also applied to SMEs' cyber security practices. The law[73], which regulated substandard cyber security practices of businesses, was also known for its lenient penalties (Lee, 2016). In addition, the judiciary was known for its tendency to sentence a small fine for illegal or substandard corporate practices on various aspects, including cyber security.

It is of importance that relevant law is revised to effectively regulate inappropriate cyber security practices of businesses (Yoon, 2016). Interviewees from government agencies perceived that SMEs did not invest in cyber security. Some of them (33.3%, 3 out of 9) mentioned that ineffective penalty system contributed to the lack of cyber security investment. When SMEs carried out risk assessment, a penalty from a court was one of elements which constituted legal risks. In many cases, SMEs were placed in a situation which involved a choice between accepting the fine and spending budgets to meet regulations. Based on the rational choice theory, SMEs were highly likely to accept the small fine rather than investing in cyber security to abide by regulations. This tells us that the penalty system was not effective in changing SMEs' behaviour. Let's propose a supposition. If the law suggests a large amount of fine or imprisonment, this will increase legal costs, raising the legal risks accordingly. Heavier penalties are expected to change the dynamics of SMEs' risk assessment. As a consequence, this will propel SMEs to

73 The law, Act on Promotion of Information and Communication Network Utilization and Information Protection, stipulates an array of activities that a person in charge of managing customers' personal information or a company should abide by (see: Section 28). Section 73 dictates that such a person or a company in violation of Section 28 shall be subject to imprisonment for up to 2 years or a penalty of not more than 20 million won (£13,465).

choose the cheaper option, which may be an investment in cyber security. How SMEs carried out risk assessment is set out below.

GO5

For businesses, everything is about risk management. There are financial risks, management risks, legal risks, cyber security risks, and so forth. How to deal with all sorts of risk is the major question for them. The basic equation when thinking about risk is cost and benefit analysis. Cyber security is not an exception. If estimated risk from cyber security breaches is not high, which means 'acceptable', they do not need to invest. ***(How do they know that it is acceptable or not?)*** *Considering risk assessment, one important dimension is lawsuit or court fines. For them, it may be cheaper to pay a fine than buying servers and software. For this reason, they are not motivated to invest money for upgrading IT systems.*

GO6

Still, SMEs consider that damage from a breach is not serious. Even if personal information is leaked, the amount of fines decided in a court is small.

6. 6. 3 Client-driven contractual mechanism

Subcontracting has been a very popular business practice in Korean industries, with about half of SMEs in manufacturing sector being subcontractors (Cho, 2014). The practice unfolds in the following way. When large companies make products or provide services, it is not the large companies that actually carry out those things. Instead, they hire a small company, which is called a subcontractor, to do their works. In the Korean subcontracting practice, large companies become contractors and SMEs become subcontractors (Cho, 2014). In the dual relationship, a large company becomes a client to an SME. This practice is deeply entrenched in Korean economy. As suggested in Table 3.3, 81.1% of Korean exports were driven by large companies. To expand in overseas markets, large companies pay special attention to the quality of their products and

services. In consequence, when subcontracting, the contractors try to maintain the high quality of products or services provided by subcontractors.

It is a recent trend that subcontractors' cyber security is included as one of the elements in the quality control process. Some SMEs (37.5%, 6 out of 16) identified themselves as subcontractors. Increasingly, contractors demanded subcontractors for a certain level of cyber security. This was a significant external pressure for SMEs. SMEs had no choice but to consider cyber security seriously to win contracts from large companies. This can be conceptualised as a client-driven mechanism. Most of the subcontracting SMEs (83.3%, 5 out of 6) noted pressures from their clients. This mechanism was an offspring of contractual relationships between large companies and SMEs. It changed or was reshaped according to the relationships. Interviewees below suggest that clients' requirements on cyber security had a direct impact on SMEs. These were an influential factor that changed their decisions on cyber security management. However, there is a caveat. Some business sectors can be distanced from the client-driven mechanism if they do not recognise subcontracting as the dominating practice. Two excerpts below show how the client-driven mechanism was accepted by SMEs.

CM8

We are quite sensitive to business information leakage. As a second-tier subcontractor, we have to abide by certain rules from a contractor. A previous client asked us for evidence that we met minimum standards that they required. Fortunately, our current contractor does not stress general security matters too much.

CM13

My company is the second-tier subcontractor. We sell our products to the first-tier subcontractor which sells its products to large car companies in Korea. The contractor sends a policy concerning cyber security and information leakage to the first-tier subcontractor which also refers the policy to us. The policy from the contractor is what we should abide by during the manufacturing process.

Although large clients put pressure on the subcontracting SMEs to pay attention to cyber security issues, they did not require the subcontractors to adhere to any known international standards or government schemes. The reason was that international standards were not applicable to SMEs and that there was no known public guidance. Instead, the clients used broad terms and set arbitrary criteria that required subcontractors to comply with. In reality, these methods were used to indicate the responsibilities of subcontractors if something went wrong.

CM7

Well,,, not really. They do not say specifically what we have to adhere to. International standards are out of our league. And, what public guidance are you talking about? I haven't heard of any. What they do is to use some broad sentences. This is to transfer cyber security responsibilities to subcontractors, I mean,,, us. Or sometimes, staff from some clients come to me and talk about minimum criteria that they think we need to have. But they are quite arbitrary.

CM9

International standards are too much. They are for really big companies. And, there is no government guidance that we are aware of,,, frankly. Our large clients do not clearly specify what we have to do. Instead, they use comprehensive phrases or ambiguous terms in a contract. It is like having us take responsibility for security breaches. If nothing happens, it is okay, but it can be bad if something does happen.

6. 7 Conclusion

This chapter has explored the main findings that emerged from the field interviews. Firstly, internal security management was unstructured in many ways. Overall, SMEs were not ready for potential risks or breaches as indicated by a lack of awareness of risks and threats, unprepared approaches to the risks, and no formal procedure for breach responses. Secondly, there was a culture resistance to cyber security. There was an

underlying conflict between different sets of values. Some corporate values, such as profit-making, efficiency and convenience, contradicted cyber security. Miscommunication among staff and negative perceptions against IT staff were pervasive. Authoritative leadership of an owner was recognised as having a negative impact on cyber security. Thirdly, public organisations which composed the cyber security governance were fragmented. The fragmentation was manifested in three ways: competition, a lack of information sharing and two divergent approaches. Fourthly, overreliance upon private organisations was identified. Not only public organisations, but also SMEs depended upon private sector organisations. This is a conspicuous difference of policing cybercrime from traditional crimes. Finally, as influential external factors, tough business environment, ineffective penalty system and client-driven mechanism were found to have a significant influence on SMEs' decisions regarding cyber security management.

The five themes can be grouped into two categories: (1) risk management mechanism (within a business) (2) risk management governance (including public and private sector organisations). The first category involves internal handling of cyber security by SMEs and includes two themes, which are unstructured cyber security management and culture resistant to cyber security. Considering the terms, such as *unstructured* or *resistant*, these two themes indicate negative points of view on the internal risk management mechanism within an SME. The second category includes three themes, which are fragmentation of public organisations, overdependence on private organisations, and influential external conditions. This category concerns relationships among public and private sector organisations as well as external factors that influence those relationships. The themes under this category highlight that risk management governance needs to be understood with relational terms. As opposed to the belief that the risk management governance posits harmony and cooperation among associated organisations, the findings showed that it was not the case. The themes suggested in this Chapter will be developed further in Chapter 7 by amalgamating the findings of the quantitative and qualitative research with the literature.

CHAPTER 7: DISCUSSION OF RESEARCH QUESTIONS

7.1. Introduction

This chapter aims to comprehensively understand cyber security management in Korean SMEs by integrating the quantitative and qualitative research findings with the existing literature, including the qualitative results describing the empirical field of enquiry. The research questions defined in Chapter 1 are considered in turn. In this way it is shown that the research has progressed in a consistent manner from setting the research questions, constructing a proper methodology, and moving to data collection and analysis.

The triangulation strategy improves the validity of interpretation and adds research rigour. This analysis technique will minimize disadvantages from using only one source or research method. Furthermore, this strategy fits into the orientation of this study, which is exploratory, by adding additional knowledge from different sources.

The quantitative and qualitative findings shed light on different aspects and identify different factors. There are agreements in some areas, and conflicts in others. Furthermore, in many cases, the findings support the existing state of the literature.

Although this chapter is kept as short as possible, some interview excerpts are used in Sections 7.2.1 and 7.2.2 to illustrate the actual voices of interviewees.

7. 2. Integration of findings

7.2.1. Research question 1: The extent to which South Korean SMEs are exposed to cyber security risks?

The Internet has become a vital medium for individual communications, business management, and provision of government services. Both Korean SMEs and Korean society have a high rate of connection to ICTs (ITU, 2015b; OECD, 2017b; UN, 2014a). Quantitative surveys measured SMEs' exposure to cyber security risks with three elements:

(1) their dependence upon online service,
(2) use of personally-owned devices at work and
(3) use of externally-hosted web services.

As illustrated in Section 5.3.1, virtually all Korean SMEs used online services in their business (see: Figure 5.1). However, online services were not incorporated into core parts of business management and were mainly used for communication and advertising purposes rather than for business and financial transactions. Also the use of personal devices and of externally-hosted web services was widespread among SMEs. Employees in over three quarters (77.7%) of SMEs used personal devices at work, although the extent of use varied by business sector (see: Figure 5.3). On a similar note, most SMEs (83.2%) used externally-hosted web services (e.g., cloud computing) (see: Figure 5.4). Personal devices at work and externally-hosted web services were not exclusive to each other, but stimulated the use of ICTs by SMEs. These practices corresponded with the fundamental corporate values of work efficiency, profit-making and staff trust (see: Section 6.3.1), which was why the adoption of online services was fully accepted by business management.

Despite the high connectedness to ICTs, quantitative findings showed inconclusive results on SMEs' perceptions of the significance of ICTs (see: Section 5.3.1). SMEs which did not think online services important part of their business outnumbered those which did (46.0% versus 32.6%) (see: Figure 5.2). This contrasted to their high use of online services. However, SMEs' perception on the criticality of externally-hosted web services (see: Figure 5.5) matched the actual use of them (see: Figure 5.4). The two figures

illustrated the similar pattern of the frequency distribution graphs. According to qualitative findings, over half (56.3%, 9 out of 16) of SMEs recognised ICTs as critical elements for their services (Table 7.1). A junior manager from a construction engineering company, CM3, explained the significance of the connectedness. This excerpt is an excellent example of how deeply computer and network systems were vital in business.

CM 3

It is very crucial for us. We use ERP, email, homepage and plan to use groupware, electronic authorisation system, and messenger. We have a server in our Internet Data Centre (IDC). Because we have sensitive information in ERP, we have one server in our headquarters. For us, design rendering is very important.

Do perceptions of the connectedness to ICT vary by business size?

Medium firms were more likely to perceive both online services and externally-hosted web services as an integral part of their business than small firms (see: Tables 5.3 and 5.5). However, this result was not supported by qualitative findings. The similar number of small and medium firms (4 versus 5) replied 'crucial' or 'very crucial' (Table 7.1). Therefore, it is difficult to argue there was a relationship between the significance of ICTs and business size.

Table 7.1: The extent of significance of ICTs to SMEs (from qualitative interviews)

Level of criticality	Businesses	Percentage	Small firms	Medium firms
Very crucial	CO1, 12 / CM3, 14, 16	31.3%	2	3
Crucial	CO2 / CM4, 11, 15	25.0%	2	2
Neutral	CM5, 9, 10	18.8%	1	2
Not very crucial	CM7, 8	12.5%	0	2
Not at all crucial	CM6, 13	12.5%	1	1
Total	16	100.0%	6	10

The high connectedness to the Internet exposed SMEs to cyber threats, such as economic espionage and cybercrime (see: Table 2.3 in Section 2.3.2.2). The Korean government considered economic espionage a serious problem undermining the export-driven economy (Choi, 2010; Park et al., 2013). This was why some government agencies, such as the SMBA, the NPA, and the NIS, focused on protecting business and technical information as a separate approach to general cyber security (see: Section 6.4.3). Based on the typology of cybercrime (United Nations Office on Drugs and Crime, 2013), economic espionage and cybercrime against SMEs (e.g., cyber trade fraud in Section 3.3.2) are computer-related acts for personal or financial gain or harm, and those acts can be perpetrated via acts against the confidentiality, integrity and availability of computer data or systems (see: Table 2.4).

The use of online services blurs temporal and spatial boundaries of traditional business management. This characteristic is also spurred on by the use of personal devices and externally-hosted web services. This can pose a great risk to SMEs. Private devices which retain business information can be left in public places, and as a consequence of this a company can lose intellectual property and sensitive data (Madzima et al., 2014). In other cases, the use of personal devices can provide a criminal opportunity to employees with malicious intentions. In terms of externally-hosted web services, all business information is stored in outside servers managed by third party vendors and is therefore vulnerable to outsider threats (Brender & Markov, 2013). Hackers or organised cybercriminals attempt to target the servers which store business information for pecuniary gains, economic intelligence or personal reasons.

What sort of threats concern SMEs the most?

In Section 6.2.1, SMEs (56.3%, 9 out of 16) viewed information leakage as one of the most damaging cases for their businesses. Theoretically, information leakage can be carried out by either insiders or outsiders. However, twice as many SMEs were concerned about insider threats as opposed to external threats (66.7% versus 33.3%)

and this result was driven by the SMEs which concerned business information rather than personal information (see: Table 6.3). Whether SMEs cherished business information or customers' personal information varied by the type of their customers. These results on perceived threats of SMEs can provide useful information to government agencies which create cyber security policies for SMEs.

Another implication from the qualitative results above was that insider threats required more attention from SMEs and public or private sector organisations. An employee in a business can be either an agent for dealing with technical vulnerabilities or an offender who commits a cybercrime and it is not reasonable to rule out such possibilities. To address insider threats, a balanced approach to cyber security is of vital importance (see: Section 2.5.2). Effective cyber security management cannot be completed only by technical solutions, but needs to incorporate human factors and management support (Rhee et al., 2012; Singh et al., 2013; Singh et al., 2014; Werlinger et al., 2009). To implement cyber security management in a holistic manner, corporate management practices, risk management tools, and cyber insurance (see: Section 2.5.1), should be taken into consideration in any decision-making processes.

7.2.2. Research question 2: How serious are cyber security breaches for South Korean SMEs?

Seriousness of cyber security breaches consists of two elements. The first is the frequency of breaches and the second is the impact of breaches. It is important to bear in mind that the breach frequency alone is not a sufficient criterion because some breaches do more harm than others. Assessing the impacts and their harm allows for a deeper understanding of the seriousness of the situation.

Quantitative results revealed that over half (55.4%) of SMEs experienced at least one breach in the last 12 months (see: Figure 5.6). Among the affected 182 SMEs, over three quarters (76.4%) experienced less than 5 breaches, while 17 SMEs (9.3%) experienced

breaches over 10 times. Qualitative results in a similar vein supported the quantitative results in that over half (56.3%, 9 out of 16) of SMEs suffered a breach. The consensus in both findings was in line with results from the UK survey (Department for Digital, Culture, Media and Sport, 2017), which showed that 52% of small firms and 66% of medium firms identified breaches in the previous 12 months.

However, in an analysis of breach experience by business size and sector, some mixed results were identified. It is inconclusive to argue any relationship between business size and breach experience because three difference sources (columns in Table 7.2) presented different findings. On the other hand, both quantitative and qualitative findings agreed upon the findings in the analysis by business sector (Table 7.3). Both sources pointed out that SMEs in 'public services' were the most vulnerable among the categories of business sector.

Table 7.2: Breach experience by business size

	Quantitative finding	**Qualitative finding**	**UK's cyber Security Breaches Survey 2017**
Small business	68.1% (113 out of 166)	50.0% (3 out of 6)	52%
Medium business	52.8% (67 out of 127)	60.0% (6 out of 10)	66%

Table 7.3: Breach experience by categories of business sector

	Quantitative finding	**Qualitative finding**
Services largely directed at public	58.5%	50.0%
Services largely directed at organisations	49.2%	60.0%
Public services	81.8%	66.7%
Manufacturing and construction	61.9%	50.0%

Without further knowledge of business turnover or scale of business, it is difficult to measure the impact of breaches. Around a third (34.1%) of SMEs showed their ignorance of financial costs of breaches (see: Figure 5.9). In spite of insufficient information on the breach costs, over two thirds (70.8%) of SMEs (*n*=120) [74] which reported breaches cost under £1,000 in the last 12 months. Where did these costs originate from? These costs were closely associated with business disruption (see: Figure 5.11). Two crucial impacts (i.e., stopping staff from carrying out their day-to-day work: 53.8%, and repair or recovery costs: 46.2%) were considered to be direct consequences of business disruption. In contrast, indirect or long-term costs (e.g., fines from regulators (0.0%) and reputational damage (6.6%)) were not regarded as having a considerable impact. For SMEs, business continuity was the first priority when dealing with cyber security breaches. The excerpts below show how seriously SMEs were afraid of business disruption.

CM10

Last year computers of five employees were infected with ransomware. And all five infections happened at the same time, so our project files were encrypted by the infection. Fortunately, we had a backup, so there was not much impact. It just took a day to get back to the project again.

CM14

Banks like us,,, viruses, phishing and hacking are large threats. If these attacks affect our normal business and customers cannot use our system, this is the most serious case.

It is noted that cyber security breaches against SMEs were serious from the frequency and impact points of view. However, despite its seriousness, it was difficult for them to detect a breach in advance. Some SMEs (CO1 and CM4) acknowledged that they did not know whether their computers and networks were breached. There should be several reasons for the lack of breach awareness. First and foremost, SMEs did not have

74 This figure was calculated after excluding 'don't know' responses.

sufficient resources for detecting and preventing cyber threats (Bauer & Dutton, 2015; Harris & Patten, 2014; Singh et al., 2013; Truong, 2010). Secondly, this was attributed to the asymmetric nature of cyber-attacks. A disproportionately large number of cyber-attacks are attempted before one gets through security and damages a computer system. This was evidenced by the fact that a fifth (21.4%) of businesses in the survey identified breaches accidentally (see: Figure 5.10). SMEs therefore tended to accept a huge volume of attempted attacks as a norm and this could not be halted due to the nature of cyber-attacks. The lack of breach awareness was associated with how SMEs interpreted cyber threats. When it comes to a breach, they cognitively classified breaches into two groups:

(1) breaches with damage, and
(2) breaches without damage.

Most SMEs interviewed were concerned about breaches with damage and did not give proper attention to breaches with no damage. Damage was thus the reference point for taking a cyber-attack seriously and engaging in any responses. Purely attempted cyber-attacks without damage were largely ignored by SMEs. SMEs did not use cyber security management as a prevention tool but purely in a reactive way.

Quantitative and qualitative findings provided some commonalities in terms of types and modus operandi of breaches. Survey results showed that over three quarters (75.8%) of affected SMEs pointed out viruses and malware as the most frequent type of breaches (see: Figure 5.7). Similarly, according to qualitative data, the vast majority of affected SMEs (88.9%, 8 out of 9) found the same result. In terms of modus operandi, emails, email attachments, and websites have been identified as the most frequent forms of attacks. Over half (53.8%) of affected SMEs mentioned them as the source of attacks (see: Figure 5.8). Interview data substantiated this finding in that three businesses (CM3, CM4, and CM5) directly pointed out them as the source of the breaches. One

commonality of these three businesses was that they all suffered at least one breach over the past year.

CM3

It is also hard to imagine that there would be any all-in-one vaccine for this because ransomware is updated constantly… As ransomware is infected through email attachments or random downloads from websites…

CM4

This year one PC in a training room was infected with a ransomware, which sent spam emails to all staff.

CM5

Some staff clicked attachments from emails and their account information have been leaked. And then, a massive amount of emails have been sent from our webmail server…

In these excerpts, phrases such as "random downloads" (CM3), "sent to all staff" (CM4), and "a massive amount of emails" (CM5) were used to describe the nature of the modus operandi. These phrases denote randomisation, targeting indiscriminate victims, and disproportionate volume, respectively. Nothing can better capture these characteristics than *spamming*, which is a method of distributing unsolicited bulk emails. Spamming has become an effective source for cybercriminals as it is carried out automatically via machines. The automatic nature of spamming is considered a major factor for asymmetry of the offender-victim relationship (Wall, 2007). The asymmetric relationship refers to the fact that the relatively small number of offenders targets a disproportionately large amount of victims. This highlights transformative characteristics of cybercrime as cyber-attacks are increasingly asymmetric, automated, and global on a larger scale.

Both quantitative and qualitative data provided similar findings on the seriousness of cyber security breaches for SMEs. Those findings added more explanatory power to the argument that SMEs were targeted by cybercriminals and the scale of the threats cannot be ignored (Cabinet Office, 2011a; Department for Digital, Culture, Media and Sport, 2018; Ponemon Institute, 2017). However, there was a disparity between SMEs' actual breach experience and their interpretation of cyber threats. Although SMEs experienced real consequences from breaches, they perceived that breaches without damage were not within the preview of their interest. This was mainly due to their lack of awareness of cyber threats. The problem is that their narrow interpretation of the threats can limit choices and options for possible responses to cyber security management.

7.2.3. Research question 3: The extent to which South Korean SMEs are prepared to prevent or mitigate cyber security risks and breaches?

This research question was intended to understand an SMEs' preparedness to cyber security. Discussion on this question will develop through examining two dimensions: (1) approaches to cyber security risks and (2) dealing with breaches. The first dimension denotes a general readiness to the risks, which includes individuals' perceptions, internal policies and practices, organisational culture, and decision-making processes. Those approaches are intended for addressing overall risks. On the other hand, the second dimension involves arrangements to deal with breaches. This dimension can also be seen as part of an approach to cyber security risks, but there are two reasons why these two dimensions need to be separated.

The first reason involves qualitative findings. Two sub-themes emerged from interview data: approaches to cyber security risks (see: Section 6.2.2), and breach responses (see: Section 6.2.3). These sub-themes demonstrated that SMEs' approaches to the risks were not identical to responses to breaches. This was related to the SMEs' tendency that interpreted cyber threats in a narrow scope (see: Section 7.2.2). SMEs focused on dealing with breaches with damage, without much consideration on mitigating the risks.

Therefore, specific sets of rules, controls, and practices were taken to prepare for breach management.

The second reason is the scope of those concepts. Looking at the preparedness to the risks and breaches separately is necessary in that risk management is a more complex and broader concept than breach management. While risk management is an iterative process which consists of identification, assessment, and mitigation, with taking various factors such as assets, threats, and vulnerabilities into consideration (Raggad, 2010, p. 23), managing a breach requires temporal responses until a breach is resolved.

7.2.3.1 What are the main approaches of SMEs to cyber security risks?

Several questions[75] from the survey were asked in order to measure the extent of preparedness to the risks. Overall, results from the related survey questions indicate that SMEs were not prepared to manage cyber security risks. Virtually all questions were dominated by negative responses (see: Table 7.1). In particular, negative responses of no experience in training, risk management through responsibility, and no update to senior management recorded the highest percentage among suggested choices. It is self-explanatory that all these responses contained negative connotations except risk management through responsibility. In Chapter 6, it was asked whether putting IT staff and managers responsible for cyber security was a sign of encouragement or discouragement (see: Section 6.2.2). Qualitative data suggested that responsibility for cyber security was interpreted as holding negative connotations by IT staff and managers.

75 They included cyber security policies (Figure 5.12), cyber security as a priority (Figure 5.13), internal trainings (Figure 5.14), risk management arrangements (Figure 5.15), an update to senior management (Figure 5.16), and measures taken to identify the risks (Figure 5.17).

Table 7.4: Negative responses on the preparedness to the risks (from the survey data)

	Negative responses	Percentage
Question 12	No formal cyber security policies	42.4%
Question 13	Considering cyber security as a (very) low priority rather than (very) high	35.4% versus 32.1%
Question 14	No experience in any cyber security trainings	36.9%
Question 15	Risk management through responsibility	Over 41.8%
Question 16	No update to senior management	38.7%

Many aspects of the quantitative results (Table 7.4) were replicated in qualitative findings (Table 7.5), although all the same aspects were not covered by the interviewees. Qualitative findings illustrate how lacklustre approaches were formed and played out in an organisational context (see: Section 6.2.2).

Table 7.5: Negative responses on the preparedness to risks (from the interview data)

	Negative responses	Percentage
Section 6.2.2	No formal cyber security policies	50.0% (8 out of 16)
	- As part of a general security policy	37.5% (3 out of 8)
	Considering cyber security as a (very) low priority rather than (very) high	50.0% versus 31.3%
	No experience in cyber security trainings	43.8% (7 out of 16)

A lack of cyber security policies implied low perception of SMEs on their current cyber security situation. Those SMEs thought cyber security risks did not merit organisational responses. Without those policies, it is difficult to expect any structured arrangements within a firm. Another critical aspect relates to senior management. As an influential group of decision-makers, senior management has a significant role in every aspect of business management. Hence, it is important for senior managers to have some knowledge of the technical side of cyber security (Rainer Jr et al., 2007) in order to

understand the associated context and engage in decision-making. However, it was found that senior managers did not take the lead on cyber security agendas. Senior mangers' low perception of cyber security led to a lack of engagement (i.e., no update). Over half (57.3%) of SMEs reported that senior managers were updated on cyber security either 'never' or 'less than once a year' (see: Figure 5.16). Under this atmosphere, it is understandable that internal staff training was not emphasised. Only 10.3% of SMEs provided staff trainings more often than quarterly (see: Figure 5.14). Overall, the examination of quantitative and qualitative data revealed how seriously SMEs were unprepared for cyber security risks.

What was a major factor underlying the unpreparedness of SMEs to manage the risks? The qualitative data found a theme, or culture resistant to cyber security (see: Section 6.3). This theme demonstrated that cyber security culture was not embraced as part of organisational culture, marginalising cyber security management from mainstream business management. Non-IT employees and managers perceived cyber security issues to contrast with widely accepted corporate values, such as profit-making, efficiency, and convenience. Also, there was evidence of horizontal and vertical miscommunication, and negative perception against IT functions and staff was pervasive. Though business owners were depicted as having authoritative leadership, they were viewed as not supporting cyber security agendas.

The examination of the levels of culture revealed that SMEs' organisational culture was resistant to cyber security. Van Niekerk and Von Solms (2010) classified organisational culture into four distinct levels: artefacts, values, underlying assumptions, and knowledge. Artefacts are visible structures and processes. In this study, the lack of policies, little or no staff training, negative attitudes towards IT staff, and a lack of budget for cyber security were identified as main artefacts here. These artefacts were manifestations from the value conflicts (see: Section 6.3.1).

On a deeper layer, underlying assumptions are based on unconscious perceptions and thoughts. There was the general consensus among non-IT staff that an additional layer of security controls hampered work convenience and efficiency. The interview data shed light on negative feelings and perceptions against IT staff and security controls (see: Section 6.3.4). Non-IT staff and managers viewed IT staff as minor supporters and security controls as unnecessary measures. The assumption lying behind this perception was that cyber security was not compatible with business management.

Lastly, there was a knowledge disparity between IT professionals and non-IT staff. The knowledge gap and a lack of understanding of cyber security were identified as an underlying factor of negative perception on cyber security (see: Section 6.3.4). Technical mechanisms and jargons created a sense of difference between IT and non-IT staff. Bridging the knowledge gap is of pivotal importance (Rainer Jr et al., 2007) in that this can contribute to effective cyber security management by influencing decision-making processes (Asgharpour et al., 2007; Ben-Asher & Gonzalez, 2015).

7.2.3.2 What are the key arrangements to deal with cyber security breaches?

Cyber security breaches can be addressed from a preventative or responsive point of view. In other words, a SMEs' approach to cyber security breaches can be divided into two phases:

(1) pre-breach and
(2) post-breach.

The pre-breach phase denotes preparedness before a breach occurs, aiming to prevent breaches. On the contrary, the post-breach phase involves SMEs' responses after a breach occurrence. The two phases are distinctive in that aims and objectives, management processes, and evaluation criteria at the pre-breach stage can be different from the post-breach stage.

(1) Pre-breach

Due to the organisational culture resistant to cyber security, most SMEs relied upon convenient types of software updates rather than an array of technical controls which required long-term commitment. Malware protection updates (74.4%) and software updates (66.5%) were widely used technical controls because users only needed to click on the screen following instructions (see: Figure 5.18). On the contrary, some other controls which required extensive managerial and budgetary support were not popular. This implies that SMEs preferred quicker and less expensive types of controls to systematic and procedural types of controls which entailed heavy costs.

Interview data explained why it was difficult to make a long-term commitment for cyber security controls. Most of SMEs mentioned insufficient resources for cyber security (Bauer & Dutton, 2015; Harris & Patten, 2014; Kwon & Kim, 2017). Getting more financial support within a company entailed competition with other teams and fierce discussion among senior managers. In order to persuade an owner, IT managers had to provide clear justification as to why they needed to purchase a security control. A decision-making process regarding budget allocation was described as internal politics (see: Section 6.2.2). The second reason was that IT staff and managers did not have enough time to commit themselves solely to cyber security issues. Some interviewees complained of their heavy workload. Only less than half (43.8%, 7 out of 16) of interviewees from SMEs employed an IT professional and they were all medium businesses. Small businesses did not have resources to hire an IT professional. Although medium firms employed IT professionals, they were tasked with non-IT works alongside IT works. Cyber security was deemed as a side job within IT functions.

(2) Post-breach

Incident management processes and insurance are important preparatory set-ups to deal with breaches. The survey and interview data showed that the absolute majority of

SMEs (respectively, 94.5% and 93.8%) did not have incident management processes (see: Figure 5.19 and Section 6.2.3). This result showed that there were no established protocols or rules when SMEs managed breaches. The qualitative findings (see: Section 6.2.3) demonstrated that the way SMEs handled breaches was impromptu and instantaneous rather than following a structured procedure. Responses depended on snap judgements of an owner and senior managers without sufficient discussions, because decisions on breach responses were made at the last minute when the breach should be acted upon.

Therefore, the decision-making process was subjective in that even similar breaches ended up being handled differently. Also, cyber security decision-making was conditioned not only by the nature of the breach (i.e., harm or damage), but also by other factors such as available budget, perception of cyber security, or market conditions. An owner and senior managers made a decision considering situational factors as well as relevant information at hand, thus responses to a breach varied greatly. Similarly, 90.9% of SMEs did not have any insurance which covered breaches (see: Figure 5.20). Compared to this, UK's SMEs were more reliant upon cyber security insurance, with 38% of them being insured (Department for Digital, Culture, Media and Sport, 2017).

In economic terms, insurance is a means of hedging against future financial loss. To purchase insurance, it should be justified that expected reduction of financial loss outweighs insurance premiums. A Korean SMEs' reluctance to buy insurance reflected their expectation that future costs from breaches would not be greater than insurance premiums. This demonstrates SMEs' perception that costs from breaches were acceptable.

Another crucial aspect at the post-breach stage was the reporting mechanism. As suggested in Section 2.6.5, the UK reporting mechanisms consisted of public and private sector organisations as well as international partners. Wall (2007, p. 168) noted that

Police, governmental non-police agencies, ISPs, and other corporates engaged in Internet governance. Policing illegal behaviours in cyberspace requires the cooperation of a multiplicity of actors. This is a unique characteristic of cybercrime compared to traditional crimes. The plurality of reporting actors was also found in the quantitative data. When reporting a breach, SMEs were more likely to report to more than one organisation. Moreover, private sector organisations such as antivirus companies, banks or credit card companies, outsourced cyber security providers, and ISPs were sought after by SMEs as often as public sector ones (113.4% versus 98.8%) (see: Figure 5.21).

Except for engaging in the formal reporting mechanism, SMEs depended heavily upon IT vendors when a breach or technical anomaly occurred (see: Section 6.5.2). In fact, SMEs made more contacts with IT vendors than with public or other private organisations for breach management. IT vendors were pointed out as an important communication channel on any IT matters, ranging from general IT consultations, through diagnoses of abnormal cyber activities to breach responses. SMEs viewed IT vendors as first responders to security breaches. The high dependency on IT vendors was a choice of convenience. As most SMEs used basic IT services from the vendors in any form, it was efficient for SMEs to contact them for cyber security matters.

In this section, the quantitative findings supported two major themes from the qualitative findings: unstructured cyber security management (see: Section 6.2) and culture resistant to cyber security (see: Section 6.3). The unstructured cyber security management was identified in two dimensions:

(1) approaches to risks and
(2) responses to breaches.

Both quantitative and qualitative data showed that most SMEs did not have a structural mechanism to prevent or mitigate risks before breaches occurred. It was at the post-breach stage that SMEs' countermeasures were taken. However, even the

countermeasures were improvised without reference to any established protocols. In addition, the countermeasures were not an outcome from considerations in respect of cyber security management, but from a snap judgement of senior management. Therefore, different responses were taken to the similar breaches, making the choice of responses unpredictable. This demonstrates that no proper cyber security management framework was adopted by SMEs.

If the culture theory by Schein (2010) is applied here, the former theme or unstructured cyber security management (see: Section 6.2) is a collection of artefacts. Values and underlying assumptions behind these artefacts are summarised in the latter theme or 'culture resistant to cyber security' (see: Section 6.3). The contrasting corporate values to cyber security (i.e., work efficiency, profit-making, and staff trust) were upheld by non-IT staff and managers, and these values were assumed to be incongruent with cyber security. These three levels, or artefacts, values, and underlying assumptions, composed resistant culture to cyber security. In conclusion, the unstructured cyber security management is a manifestation of the 'culture resistant to cyber security'.

7.2.4. Research question 4: What are the characteristics of external influences and initiatives in South Korea?

Both quantitative and qualitative findings indicate that SMEs' cyber security management was not found to be an isolated mechanism, but affected by external influences and initiatives. When cyber security managers and owners were on the verge of making a decision, they put internal factors as well as external factors on the table for discussion or consideration. This corresponds with Dojkovski et al.'s (2007) claim that cyber security management in Australian SMEs can be seen as "a result of national and cultural influences" (p. 1563).

First and foremost, it was of importance to identify what sort of external influences and initiatives were related to SMEs' cyber security. Seven external influences and initiatives were discovered from quantitative and qualitative findings. These are:

(1) insurance,
(2) international and domestic standards,
(3) government guidance and schemes,
(4) IT vendors,
(5) SMEs' tough business environment,
(6) ineffective penalty system and
(7) client-driven contractual mechanism.

Of those seven external factors, quantitative findings (see: Section 5.3) listed insurance, international and domestic standards (i.e., K-ISMS from KISA), and government's guidance and schemes. The rest have emerged from qualitative interview data. Those which emerged were suggested as sub-themes under the two major themes: 'overdependence on private organisations' (see: Section 6.5) and 'influential external conditions' (see: Section 6.6). The sub-themes carried a significant weight in this research in that they shed light on:

(1) new actors (i.e., IT vendors, criminal justice actors, and other businesses),
(2) SMEs' relationships with the actors and
(3) socioeconomic factors.

This exploration enlarged the scope of this research by enabling an examination beyond organisational boundaries of SMEs.

(1) Insurance

Insurance was not found to be a popular initiative to protect SMEs from cyber threats. The absolute majority of SMEs (90.9%) did not have insurance to cover cyber security breaches or attacks. This finding corresponds with another survey result which found only 6.1% of businesses in Korea were insured (KISA, 2011). In fact, the cyber security market in Korea was immature. There were only nine insurance companies which sold cyber insurance to businesses (Ministry of Science, ICT and Future Planning, 2013). The unpopularity of cyber insurance was because both insurance companies and potential buyers were not sure whether the insurance costs were reasonable (Ministry of Science, ICT and Future Planning, 2013). The difficulty of setting the price was attributed to a lack of historical records as cybercrime was a new phenomenon (Gordon et al., 2003). Furthermore, SMEs did not have sufficient resources for cyber security and had distinctive organisational structures from large companies (see: Section 2.3.3). Therefore, to appeal to SMEs, cyber insurance needs to be customised based on organisational conditions and contexts of SMEs, but also a policy on the insurance cost needs to be substantiated by reasonable grounds.

(2) International and domestic standards / (3) Government guidance and schemes

In the survey less than half (44.8%) of SMEs did not have any awareness of the suggested schemes and standards (see: Figure 5.23). It is understandable that the ISO 27001 and Korean ISMS were quite well known to SMEs (31.4% and 44.8%) because of their high publicity. Compared to this, government guidance (6.7%) was not recognised by SMEs. The lack of awareness of the government's schemes evidenced in this research also echoed the UK situation, where little over 10% of SMEs were aware of the government's schemes, such as Ten Steps to Cyber Security guidance (15.9%) and Cyber Essentials scheme (13.5%) (Department for Digital, Culture, Media and Sport, 2017).

However, there is a difference in structuring the guidance and schemes between the two countries. The UK government embarked on the NCSP from 2011 and published schemes, such as Ten Steps to Cyber Security and Cyber Essentials based on the programme (Cabinet Office et al., 2015). Although the business community had a low awareness of the schemes, the UK government's schemes were well structured as part of the national cyber security framework. This demonstrates that there was a high level of alignment between cyber security strategies and operational schemes (see: Section 2.6.4). The existence of the national framework is of significance in that the framework itself provides clear goals and objectives. As such, the affiliated schemes could be managed, evaluated, and updated in a structured manner based on directions and guidance from the framework.

In contrast, the qualitative data showed that there was neither a publicised government framework for cyber security nor affiliated guidance and schemes in Korea (see: Section 6.6.3). No interviewees from SMEs mentioned their awareness of any government guidance. These findings correspond with Jang's (2014) claim that the Korean government did not have a comprehensive national cyber security strategy. The lack of a government framework is a reflection of the Korean government's lacklustre approach towards cyber security.

Qualitative findings demonstrated that relationships among the public organisations were fragmented (see: Section 6.4). Firstly, the public organisations in the cyber security domain was based on a weak cooperation model (see: Section 6.4.1). Rather, competitive milieu was identified. Secondly, no information sharing framework existed (see: Section 6.4.2). Information sharing took place occasionally to address an issue in hand. Thirdly, there were two different approaches to SMEs' cyber security: (1) general cyber security and (2) technology information protection (see: Section 6.4.3). The public organisations involved in one approach did not interact with others in the other approach. These three sub-themes demonstrated that there was no coordinated approach to cyber security at a national level.

The fragmentation of the public organisations in Korea is in marked contrast to the UK's cyber security structure. The UK structure was predicated upon a hierarchical consistency from the National Security Strategy down to Policing Vision 2025 (see: Section 2.6.1). The hierarchical consistency was maintained via a control tower, or the CGSD in the Cabinet Office. In order to realise these strategies, the UK government displayed its commitment by embarking on the NCSP with a substantial amount of resources. Also, the NCSP was evaluated for its progress by independent public authorities (see: Section 2.6.3.1). It is important to note that the higher body, the Cabinet Office, took the lead to establish a national framework which drove a coordinated approach to cyber security. This level of consistency was highly expected to increase cooperation and information sharing among the involved public organisations.

(4) IT vendors

Qualitative findings (see: Section 6.5.2) revealed that IT vendors emerged as the most sought-after parties by SMEs. Over 90% (15 out of 16) of the SMEs relied on general services of IT vendors for normal business operations and the services themselves included some elements of cyber security. These IT vendors were already familiar with computer systems of the SMEs as they were in a contractual relationship. In this circumstance, benefits from using the services of IT vendors were obvious. It was efficient and convenient for SMEs to take advantage of its existing ties to the commissioned IT vendors. Most SMEs were satisfied with their responsive services.

The dependence of SMEs on the existing ties is a reflection of two things. The first is related to a narrow perception of cyber security. SMES' non-IT managers assumed that cyber security was just a part of IT issues, thus treating cyber security issues as purely technical. This assumption justified that the commissioned IT vendors were capable of handling any cyber security issues. However, some interviewees wished cyber security could be recognised as an independent area from general IT issues. In fact, cyber security had a broader boundary than IT protection. As discussed in Section 2.2, cyber security

aimed to safeguard humans and society alongside information resources (Von Solms & Van Niekerk, 2013). On the contrary, the IT vendors were only concerned with technological issues, not taking the protection of insiders and of society into consideration.

Secondly, dependence on the existing ties for cyber security is seen as a realistic choice. Most SMEs did not have sufficient resources to invest in cyber security (Bauer & Dutton, 2015; Harris & Patten, 2014; Singh et al., 2013; Truong, 2010). Budget constraints discouraged them from purchasing IT services which specialised in cyber security. Even for profitable SMEs with willingness to buy such a service, there were not many available cyber security services for SMEs. This indicates that cyber security market targeting SMEs were immature (see: Section 6.5.2). Instead, cyber security vendors marketed a variety of services customised to larger firms and public organisations. Both insufficient resources of SMEs and the immature market prompted SMEs to rely on the existing ties to IT vendors.

Despite the SMEs' high dependence on IT vendors, their services for cyber security were limited to technological aspects. Technical support by IT vendors was intended for a breach response or problem solution rather than proactive measures (see: Section 6.5.2). Recent studies (Singh et al., 2013; Singh et al., 2014) claimed that human factors and managerial support were vital prerequisites to implementing cyber security management, emphasising a holistic approach (see: Section 2.5.2). However, IT vendors with the existing ties did not provide advice or recommendations on human and managerial aspects of cyber security. It is necessary that professional cyber security vendors provide customised services to SMEs. This seems to be quite far from reality at present.

Qualitative findings (see: Section 6.6) suggested that dynamics of cyber security management within SMEs were influenced by three socioeconomic factors:

(1) tough business environment,

(2) ineffective penalty system, and

(3) client-driven contractual mechanism.

The first two sub-themes are restraining factors for SMEs' involvement in cyber security management, whereas the last sub-theme, client-driven mechanism, is an facilitating factor which puts pressure on SMEs to engage in cyber security management.

(5) SMEs' tough business environment

The qualitative findings argued that fierce business competition prevented investment in cyber security in SMEs (see: Section 6.6.1). Among these three sub-themes, tough business environment was also identified as a significant external factor from the literature. However, findings from previous studies stood in contrast to the findings in this research. Chang and Ho (2006) contended that environmental uncertainty had a positive influence on implementing cyber security management. In line with this, Kearns and Lederer (2004) argued that environmental uncertainty increased dependence upon information technologies. The contrasting results seemed to be derived from conceptual differences between tough business environments and environmental uncertainty. The former phrase used in this study was interpreted rather narrowly as a reflection of severe market competition. Compared to this, the later phrase in the previous studies incorporated a variety of dimensions, possibly including market competition, although it was not clearly defined in those studies.

(6) Views on the effectiveness of the South Korean penalty system

To draw attention from senior management, it is of pivotal importance that the law effectively regulates inappropriate cyber security practices of businesses (Yoon, 2016). However, in general when Korean businesses were convicted of wrongdoings, they faced relatively low sentences in criminal courts (Park, 2004). This was also the case with

the law which governed substandard cyber security practices of businesses (see: Section 6.6.2). The law stipulated lenient penalties against those subpar practices (Lee, 2016). In addition, the purview of the legal framework was narrow in that the law regulated cyber security practices mostly regarding customers' personal information. This means that employees' personal information and general business information were not protected by the legal framework.

The importance of protecting personal information online has gained significant attention in recent years. Public and the media have been indignant at low penalties imposed by the courts on businesses which mishandled customers' personal information (Lee, 2016). In qualitative findings, one in three government officials (33.3%, 3 out of 9) echoed this public perception of the penalty system. They suggested that the penalty system was ineffective and discouraged SMEs from investing in cyber security. From a risk assessment point of view, it is a more economical choice for SMEs to accept the low penalty from courts than investing in cyber security. Interestingly enough, the argument about the ineffective penalty system was not mentioned by any single interviewee from SMEs. It may be that the researcher's dual status (see: Section 4.6) prevented the SMEs' interviewees from disclosing contentious aspects of criminal justice system against businesses.

(7) Client-driven contractual mechanism

The last socioeconomic factor was predicated upon the predominant contractual mechanism among Korean businesses, which is called subcontracting (Cho, 2014). Large companies hire SMEs as subcontractors to do much of their important work. This mechanism can also be explained as one that hinges on supply chain contracts. It was noted that supply chain contracts can be used to require small companies to be certified to a standard (Philpott, 2015). Qualitative findings found that slightly over one third (37.5%, 6 out of 16) of SMEs identified themselves as subcontractors which sold their products or services to large companies (see: Section 6.6.3). It was a recent

phenomenon that clients required subcontractors to meet some standards on cyber security based on this contractual mechanism. The cyber security requirements were suggested as part of the quality control process. In fact, a very large percentage (83.3%, 5 out of 6) of subcontracting SMEs experienced pressure for higher cyber security practices from their clients.

In terms of types of requirements, quantitative data (see: Section 5.3.5) found that about two thirds (63.7%) of SMEs were not required to comply with any standards (see: Figure 5.26). This finding corresponds with the claim from some SMEs' interviewees that their clients did not clearly mention a specific type of requirement. Rather, the clients tended to use ambiguous terms in the contract or set arbitrary criteria that SMEs were required to adhere to. It seems that even clients had no clear understanding of what needed to be done by subcontractors in respect of cyber security.

However, mixed results were found between quantitative and qualitative findings. The quantitative data reported that government's schemes (26.8%) were a relatively common type of requirement, but the SMEs' interviewees were not aware of any available public guidance. In fact, it was found that in South Korea no government guidance was published on a similar scale to Cyber Essentials of the UK. As evidence of this, Philpott (2015) proposed the possibility of rolling out a UK standard which includes Cyber Essentials in Korea for small businesses. It could be that the survey respondents who chose government schemes interpreted them as a large concept which encompassed law, public regulations, and policy.

On the other hand, the UK survey (Department for Digital, Culture, Media and Sport, 2017) captured a different type of contractual mechanism. The mechanism concerned relationships between SMEs and their suppliers. The UK survey reported that 21% of small firms and 30% of medium firms were concerned with the cyber security risk stemming from their suppliers. International standards, such as the Payment Card Industry Data Security Standard (48%) or ISO 27001 (42%), were the most widely

accepted requirements placed on suppliers. On the contrary, government schemes, such as Cyber Essentials (6%) and Cyber Essentials Plus (2%), were the least popular. This survey result showed that the UK businesses placed relatively stricter and more structured standards on suppliers than Korean large businesses did to SMEs.

These three socioeconomic factors (see: Section 6.6) demonstrate that SME's cyber security management was directly or indirectly associated with external influences and initiatives. As far as the researcher is aware, the two sub-themes, ineffective penalty system and client-driven contractual mechanism, have not been studied much in relation to SMEs' cyber security. This is why there was little literature to incorporate into the discussion. However, the lack of research in these aspects provided an opportunity to carry out this research. The fact that these sub-themes emerged from qualitative data can be considered as a contribution to the literature on cyber security management studies.

7.2.5. Research question 5: What is the nature of relationships in South Korea between SMEs and other public or private sector organisations?

As discussed in Section 7.2.4, SMEs' cyber security management was influenced by external factors. The extent and scope of these influences can be better understood if the nature of relationships between SMEs and public or private sector organisations is made clear. SMEs needed to contact those organisations for various reasons, such as to acquire information, to report breach or cybercrime, and to purchase services. In contrast, public organisations attempted to reach SMEs for protection from cyber threats, and some private organisations (e.g., ISPs, IT security companies, and antivirus companies) provided IT services to SMEs.

SMEs had weak relationships with public sector organisations. According to the quantitative findings (see: Figures 5.24 and 5.25), over half of SMEs have neither contacted nor been contacted by any public organisations (respectively, 57.0% and

50.6%). When seeking information, advice or guidance, SMEs were twice as reliant upon private sector sources as public sector ones (see: Figure 5.22).

The qualitative findings (see: Section 6.5.2) in a similar vein presented a more detailed picture on this. It was IT vendors that SMEs relied upon the most in case of cyber security breaches or anomalies. As explained above (see: Section 7.2.4), SMEs took advantage of IT vendors based on the existing contractual relationship. Although IT vendors brought many practical benefits to SMEs, this generated some nervousness as well. The fact that IT vendors normally had full access to corporate systems was considered a high risk for some SMEs which paid extra attention to customers' personal information or business proprietary information (see: Section 6.5.2). However, the nervousness did not seem to reverberate across the whole SMEs. Due to a lack of internal support and fierce market competition, they tended to opt for work efficiency and convenience at the cost of corporate information security.

Another dimension worth examining is the relationship between public sector and private sector organisations. The qualitative findings (see: Section 6.5.1) disclosed that each public sector agency intended to maintain cooperation with an array of private companies, such as ISPs, antivirus companies, and IT security companies, adopting its own approach. Hence, the extent of the cooperation varied considerably due to different purposes and intentions of the agencies. The NPA and KISA attempted to maximise the extent of cooperation for different reasons. However, it was not the case with the SMBA because of its involvement in a different approach, technology information protection (see: Sections 6.4.3 and 6.5.1). This demonstrates that there was no comprehensive framework for public and private partnerships in South Korea.

Dependence or overdependence is a core concept to understand the relationships of actors. According to social network theories, centrality on a certain actor by others is a good measure of the prominence or importance of the actor (Wasserman & Faust, 1994, p. 170). Both quantitative and qualitative data in this study indicated that both SMEs

and public agencies were significantly dependent upon private companies in a network. If this theory is applied here, private companies, especially IT vendors, were embedded in a central position within the network. The high centrality of IT vendors provided them with the prominence in the ties among relevant actors. A group of IT vendors can be called a hub in the relationships. In contrast, SMEs and public organisations were embedded in relatively weak positions. In social network research, it is generally assumed that the centralised position in the network generates power (Bonacich, 1987), as information is funnelled through an actor with high centrality. Power is a structural outcome in that the nature of relationships among actors determines where power resides (Frooman, 1999). Asymmetric relationships therefore cause power imbalance.

Due to the power imbalance, the cyber security domain in Korea was more likely to be driven and shaped by those private IT companies. They were creators of new cyber security technologies as well as frontline users of these technologies. SMEs and public organisations needed to go through those private IT companies to embrace these technologies.

This situation brings a critical policy implication. Those companies' choices will confine not just what SMEs purchase, but also how public agencies use it as a way to control cyber threats. This can be a huge problem if a few private IT companies dominate the cyber security market. As a consequence of this SMEs and public agencies could lose their bargaining power. For SMEs, it will be difficult to expect a high-quality product compared to the amount paid, and public agencies' practices will be conditioned by technical specifications of products or policies of those companies. One good example is police body cameras. In the US, three quarters of the body camera market is dominated by Taser International (Gelles, 2016). Due to its market dominance, most law enforcement agencies in the US have no choice but to accept the terms and conditions set by Taser and end up purchasing new technologies (e.g., data storage and facial recognition system) sold by the company (Joh, 2017).

If this situation continues or becomes worse, the cyber security domain will be dominated by market-driven initiatives. The private IT companies are more likely to churn out new products and services for business profits. This questions the role of the government. What should the government do within the cyber security domain? This will be addressed in the next chapter (see: Section 8.4.2).

CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

8.1. Summary of the key findings

Drawing on a mixed methods approach, this study used three research methods: documentary research, quantitative questionnaires, and qualitative interviews. Firstly, documentary research revealed that the government, large companies, and individual citizens were recognised as potential targets from cyber financial fraud as well as cyber terrorism perpetrated by North Korea (see: Section 3.3.1). In contrast, the government focused on protecting one third of SMEs which had high levels of technology. As a consequence of this, the majority of SMEs have not benefitted from the government's initiatives (see: Section 3.4.3).

Secondly, quantitative survey data found these: (1) Korean SMEs were highly connected to ICT, but perception of their significance did not correspond to the actual adoption of ICTs, (2) cyber security breaches affected all kinds of SMEs and costs were not clearly measured, (3) when it comes to approaches to risks, many businesses did not have a structural mechanism, (4) most SMEs were not prepared to deal with cyber security breaches, depending upon basic technical controls or actions, and (5) public sector organisations were not identified as a main contributor to SMEs in relation to information acquisition or information sharing (see: Section 5.4).

Thirdly, qualitative interview data identified five themes: (1) unstructured cyber security management, (2) culture resistant to cyber security, (3) fragmentation of public organisations, (4) overdependence on private organisations, and (5) influential external conditions. The first two themes indicated negative points of view on the internal risk management mechanism within a business, and the remaining three themes shed light on intricate relationships among public and private sector organisations as well as external factors that influenced those relationships (see: Section 6.7).

In order to comprehensively understand cyber security management in Korean SMEs, findings from the quantitative and qualitative research were integrated with the existing literature, including the qualitative results describing the empirical field of enquiry. In conclusion, this research has found that SMEs did not have a structural mechanism to prevent or mitigate risks at the pre-breach stage (see: Section 7.2.3.2). Instead, they involved responses at the post-breach stage. This indicated that SMEs were not prepared from a preventative point of view. Furthermore, it was found that management of cyber security within a business was not an isolated mechanism, but influenced by external organisations and factors (see: Section 7.2.4). However, there was an insufficient role of public sector organisations in protecting SMEs. The lack of national leadership in the Korean cyber security governance (see: Section 3.4.4) resulted in weak public and private partnerships (see: Section 7.2.5).

8.2. Evaluation of the research objectives

In Chapter 1, four research objectives were introduced to achieve the research aim: to empirically explore and evaluate the current state of cyber security management in SMEs in South Korea.

The first objective was to identify cyber security risks and threats against SMEs. Due to a lack of risk and threat assessment, this objective was intended to assess overall cyber security situations surrounding SMEs. It was addressed through the research questions 1 and 2. In order to fulfil a thorough assessment, a wide range of cyber security elements as well as organisational characteristics and behaviours, such as leadership, communication, managerial support and culture have been incorporated in the analyses. Beyond this, SMEs' perceptions on the significance of ICTs and the risks and threats have been examined in connection with security breaches. This approach sought to discover the extent and scope of the risks and threats against SMEs. The findings relating to this objective were discussed in Sections 7.2.1 and 7.2.2.

The second objective was to examine whether SMEs are prepared to address the risks and threats. It was found that SMEs did not have a structured mechanism to prevent or mitigate the risk before a breach occurs, focusing more on post-breach responses (see: Section 7.2.3). This internal management of cyber security in SMEs was examined in a broader sense by incorporating environmental aspects (see: Sections 7.2.4 and 7.2.5). It was analysed in two ways: (1) how external organisations had a relationship with SMEs and (2) how external factors had an influence on decision-making processes in the SMEs' cyber security management. This exploration could serve as a theoretical basis for the formulation of a conceptual framework in future studies.

The third objective was to suggest policy recommendations to strengthen cyber security management of SMEs. The examination carried out for the first and second objectives implied a set of policy recommendations which could be taken by the South Korean Government (see: Section 7.2.5). This indicates that these recommendations were derived from the research findings. Hence, they are greatly applicable to the Korean context, but not to other sociocultural settings. It was also suggested that these recommendations should not be adopted individually, but need to be addressed as part of an overarching government framework.

The fourth objective was to propose an effective framework for protecting SMEs from cyber security risks and threats. The comprehensive framework was suggested as an integrated model in Section 8.3.1 as a result of the investigation conducted in the study. The realisation of the research aim and the previous three objectives culminated in the proposal of the integrated model. As the final outcome of this research, this framework was produced through the research findings as well as rigorous research methodology. This model's underlying concepts and constructs could provide theoretical implications.

In conclusion, the overarching aim of this study has been successfully achieved in that the understanding of the cyber security management of SMEs has been enhanced throughout this study. The trustworthiness of the research findings and analyses rests

upon its scientific approach and design along with the research methodology adopted. The study's research findings could be used in future research and programmes which seek to resolve the problems associated with cyber security management of SMEs both in the Korean context and beyond.

8.3. Recommendations

8.3.1. Integrated cyber security risk management model in Korean SMEs

In Chapter 2, several risk management frameworks were suggested (see: Section 2.4). Main elements such as risk identification, assessment, responses, and monitoring were connected as part of an iterative process. Although these frameworks were concise, it was questionable whether they could be applicable to real situations of SMEs. Drawing on those frameworks, this research examined a comprehensive landscape of cyber security management of SMEs. Based upon the quantitative and qualitative data, how SMEs approached cyber security risks and threats and what sort of factors influenced SMEs' approaches were thoroughly explored. The extensive exploration could be summed up as a model. Figure 8.1 below provides an illustration of the functioning of the 'Integrated cyber security risk management model', as a means of understanding the security management process.

In this model, the term, *integrated*, implies that the approach being taken here combines a focus on the internal elements of the cyber security management process, in conjunction with external influences and initiatives. This integrated approach also signifies a holistic approach shared between public and private sector organisations involved in order to produce coordinated effects capable of addressing the associated risks and threats. This model is predicated on the two main arguments from this study: (1) organisational behaviours, such as culture, leadership, communication, managerial roles, decision-making, and group attitudes and perceptions have a direct influence on the cyber security management of SMEs and (2) external influences and initiatives have

significance in indirectly affecting the cyber security management of SMEs. Similar risk assessments may not lead to a choice of similar measures due to different organisational behaviours and external factors. In other words, although businesses may face a similar type of security threat with similar impacts, it is possible that those businesses decide to choose different types of security controls.

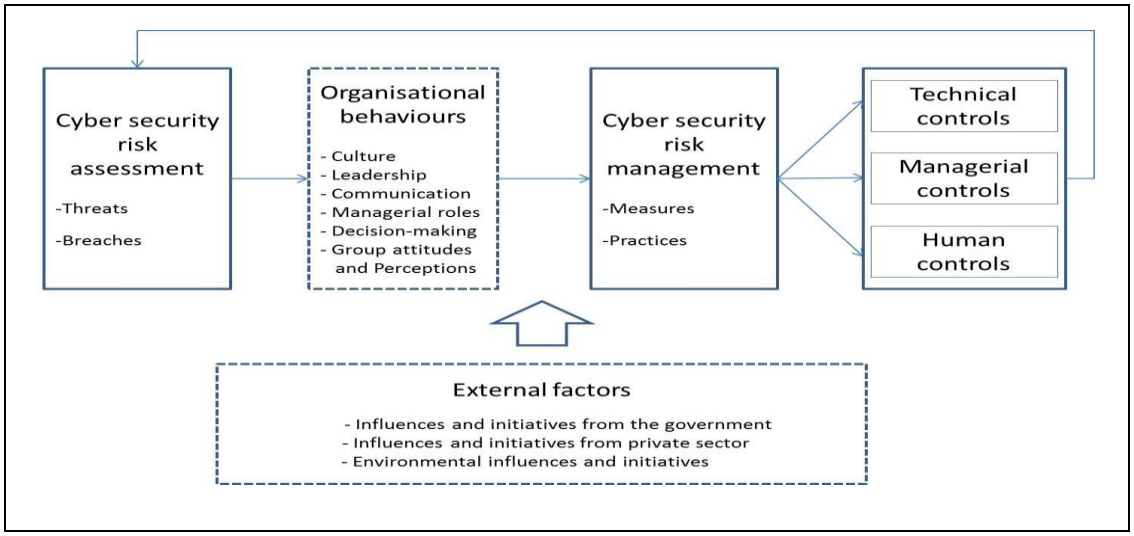


Figure 8.1 Integrated cyber security risk management model

This model can be explained in this equation:

$$Cyber\ \ security\ \ risk\ \ management = f(risk\ \ assessment * organisational\ \ behaviours * external\ \ factors)$$

Compared to the internal mechanisms of SMEs which focused primarily on dealing with breaches with damages without addressing the risks (see: Section 7.2.2), this holistic model could be productive in that it can shift SMEs' focus into prevention at the pre-breach stage. This is mainly because this model places emphasis on *risk*. Since risk management concerns a future event which causes the adverse consequences, it shifts human attention from past or present to future. Fischer, Halibozek, and Green (2008, p. 148) stated that security should be predicated upon analysis of the total risk potential to avoid one-dimensional and reactive approaches. As this model is conceptualised as

an iterative process which aims to prevent and mitigate the risks, the original intention of this model is to address the risks rather than to manage breaches. The iterative process within this model can be reviewed and applied to SMEs for assessment as well as for diagnostic purposes.

This model, in itself, is the key recommendation for South Korean SMEs. This research found that South Korean SMEs were not ready to address cyber security risks and threats (see: Section 7.2.3.2) and there was no known guidance for SMEs from the government (see: Sections 6.6.3 and 7.2.4). This model incorporates a wide range of elements for effective cyber security management which constitute an iterative process. Therefore, SMEs' owners and managers could take it as a conceptual map as well as guidance for the management of cyber security risks. More importantly, substantial gains can be made if SMEs consider how to change their organisational behaviours in a way that recognises cyber security as a core part of their business management.

The integrated model in this section will be suited to fully utilise the resources and expertise in SMEs and related public and private sector organisations. This will be conducive to mitigating the level of cyber security risks and threats against SMEs and to modifying a business environment in South Korea, in which SMEs will be able to feel safe and secure to carry out their business. It should be noted that its research findings are confined to the research context that was investigated, namely, South Korea. However, the integrated model represents a dynamic framework which can be improved and modified according to changing external circumstances and conditions. It is therefore contended that the integrated model as proposed in this study can have a broader application as a conceptual framework for SMEs as well as for future studies.

8.3.2. Recommendations for the government

There are several areas where the government could intervene in a constructive manner. Based on discussions in Sections 7.2.4 and 7.2.5, some recommendations are suggested here:

Firstly, public and private partnerships should be strengthened. This is mainly because cyber security can be achieved within plural policing environments due to the distributed nature of cyberspace (Broll, 2016). The UK's cyber security framework emphasised public and private partnerships (e.g., CiSP) for facilitating information and raising awareness (see: Section 2.6.3.2). It was of importance that the CiSP expanded its role in a way that supported SMEs by cooperating with Regional Organised Crime Units (Ring, 2013; UK-CERT, 2016). However, this research found that South Korean SMEs had weak relationships with public sector organisations (see: Section 7.2.5). Also, each public sector agency took its own approach to maintain cooperation with multiple IT companies without a comprehensive framework for public and private partnerships (see: Sections 6.5.1 and 7.2.5).

Secondly, the government can create public schemes to provide guidance for general cyber security. The schemes need to be publicised so that SMEs can be aware of them. The difficulty of raising awareness of the schemes was found in both the UK and Korea (see: Sections 5.2.3 and 7.2.4). One effective way is to adopt a policy. The UK government adopted the influential policy which stated that any government suppliers applying for contracts regarding personal information and ICT services should have Cyber Essentials (Crown Commercial Service, 2014). This sort of policy could be a powerful tool for the Korean Government.

Thirdly, the government could change the ineffective penalty system. Increasing penalties under law and strengthening sentencing guidelines will both raise the legal risks for SMEs (see: Section 6.6.2). This would be expected to shift SMEs' decision–making into more investment in cyber security agendas. Alongside the penalty system reform, the government needs to ponder over what sort of regulatory policies will

influence SMEs' decision-making. However, it should be cautious since strict regulations may ignore a variety of differences among businesses, incurring unnecessarily heavy costs. The regulations need to be based upon a legal framework which is aimed at the comprehensive protection of SMEs from cyber security risks and threats.

Fourthly, the government can influence the client-driven contractual mechanism among businesses. In most cases, SMEs as subcontractors were required to meet the criteria that their clients ask (see: Section 6.6.3). The problem lies in the fact that the clients used unclear and broad terms without specifying any known standards or schemes. It is possible that some large companies, to some extent, abuse their superior position as a client and unfairly transfer cyber security responsibilities to SMEs based on those broad terms. The government can take the role of overseeing this contractual mechanism. It is the Fair Trade Commission that regulates unfair business practices by large companies against SMEs. Therefore, it would be efficient if the Commission monitors the practices regarding cyber security by expanding its existing regulatory framework.

These four suggestions were derived from both quantitative and qualitative findings (see: Sections 5.3.5, 6.5.1, 6.6.2, and 6.6.3), which allowed the researcher to propose relatively concrete suggestions. It is worth mentioning that there should be an overarching government framework which can include these four suggestions. This argument is based upon the finding from documentary research that there was a lack of national leadership in the Korean cyber security governance (see: Section 3.4.4). Cyber security policies and strategies will be more effective if they are structured under an overarching framework in a consistent manner as in the case of the UK (see: Sections 2.6 and 3.4.4).

8.4. Research contributions

This study made distinctive contributions to knowledge of cyber security management studies. Previous research on businesses in South Korea tended to be technical in nature,

and very little research focused on cyber security management of businesses. Considering this, the social science approach taken by this study in this discipline is expected to provide researchers and practitioners with newly explored evidence relevant in the context of South Korea. It is also noted that this research is one of the very few comprehensive studies on SMEs' cyber security management internationally. Although some security management studies on Korean businesses have been carried out, there is currently no specific research focusing on SMEs.

In particular, this research differs from previous studies in that it has broadened the academic discourses by exploring the national context in which SMEs operate. This holistic approach was provided for an examination of cyber security management in SMEs in the national setting. This research investigated the nature of SMEs' relationships with external influences and initiatives from the government, private entities, and surrounding environments. The national setting as to SMEs' cyber security management has not been explored in the Korean context. As such, this study is the first primary research to be carried out on these issues on such a comprehensive scale in South Korea.

In the study, the central focus throughout was on the vulnerability of SMEs, internal handling of cyber security risks by SMEs, and relationships among public and private sector organisations as well as external factors that influence the relationships. These matters are of great interest to academic researchers but also to policy makers responsible for cyber security and cybercrime.

Firstly, researchers can benefit from this study. This empirical-based study shed light on how organisational behaviours and external factors interrelate with cyber security management. Findings and analyses discovered new patterns and associations between identified concepts or constructs. The integrated model (Figure 8.1) illustrates how those constructs and themes are associated. Although this study does not suggest any theory, it is recognised that this study contributes to the relevant field conceptually. As such, this study can provide some theoretical implications for future research.

Secondly, from the regulatory point of view this study provides policy implications for the government. There was the recognition that public sector organisations have a role to play in influencing the internal security management mechanisms within SMEs. As evidence of this statement, some suggestions for the Korean government were proposed in Section 8.3.2. The exploration of the role of public sector entities can be viewed as another contribution to this study. This indicates that cyber security breaches are not entirely SMEs' faults and that it is also important to nurture a constructive environment which encourages the internal security risk management mechanisms. In addition, it was discovered that there were two separate approaches to SMEs' cyber security (see: Section 6.4.3). Government agencies involved in one approach were unaware of the other approach and never considered overlaps or commonalities between the two approaches. It would change government policies if the possibility of engagement or collaboration between the two approaches were identified and carried out.

In cyber security, industry research collaboration between nations is greatly important (Trim & Youm, 2015). Despite the differences in the environmental contexts between South Korea and other countries, this research may benefit an international readership. Since cyber threats are transnational risks that transcend national boundaries, other countries are likely to face similar problems. The integrated model (Figure 8.1) can be compared and contrasted to their national contexts, although it should be undertaken cautiously.

8.5. Limitations of the study

This research provides meaningful results and insights on protecting SMEs from cyber security risks and threats, yet several limitations are also recognised. Firstly, there was a shortage of relevant theories and previous literature on SMEs' cyber security management. In cybercrime victimisation studies, a clear lack of attention is given to organisational victims, due to a difficulty in gaining access to businesses for data

collection (Holtfreter & Meyers, 2015). This, in part, has limited in-depth discussion of the existing literature in Chapters 2 and 7 and the construction of a research framework at the outset of this research. However, the lack of an extant literature provided a justification for advancing this research, thus prompting this research to be exploratory rather than representative.

Secondly, research findings were not generalised because both the quantitative and qualitative phases used convenience sampling, generic purposive sampling and snowball sampling (see: Section 4.5.1.1). These non-probability sampling techniques do not guarantee the representativeness of the sample. Therefore, generalisation from a sample to a population could not be claimed. However, this research was intended to be exploratory rather than proving or disproving a theory, which indicates that the researcher did not aim to achieve robust representative outcomes.

Thirdly, the researcher could not carry out focus group interviews for more exploration of the research questions. Focus group interviews were not intended when the research design was established before data collection. However, after completing the qualitative interviews the researcher felt the need to do so. For this reason, the researcher asked some interviewees whether they were willing to join focus group interviews, but virtually all of them gave negative responses. These responses were understandable in that Korean people are generally passive in terms of discussion or group talking. Also, this passive attitude may reflect the traditional and bureaucratic context of South Korea. Expressing individual opinions is not portrayed in a positive light in Korean society and it is preferred not to stand out in a group. In addition, costs and time constraints prevented further exploration of the research problem.

8.6. Future research

This study was based on the quantitative survey and semi-structured interviews conducted with managers and owners of SMEs and government officials. As was

suggested in Section 8.5, an inherent weakness of this research is that the findings of this study do not necessarily hold true for other national settings. However, it would be appropriate to apply the framework from this study to other studies with similar nature in different national contexts. The application to other settings will improve or refine the framework. Undertaking such studies is expected to highlight similarities as well as differences in the landscape of cyber security management on the international stage.

Future research might, for example, incorporate additional variables which may be associated with cyber security management of businesses. The incorporation of additional organisational and external variables would allow for a more comprehensive exploration and analysis of cyber security management processes. Such organisational variables could include annual turnover, credit rating, management structure, type of customers, and proportion of export in businesses. On the other hand, external variables such as economic conditions, business-wide initiatives, co-operation between companies, and government support could be expanded depending on the research contexts. Although this study was exploratory, future studies could investigate causal impacts of variables on cyber security management. An examination of causal impacts could provide different types of theoretical or policy implications which could not be gained from this study.

The emphasis on cyber security management has not, as yet, gained prominence in South Korea. Although small progress has been made with regard to policy guidelines in order to deal with emergency situations, the government was not prepared for addressing cyber security risks and threats from a preventative point of view. As such, there is now an urgent need for substantive and in-depth research to support businesses' and the government's preventative efforts. First and foremost, it is pivotal to monitor and evaluate mechanisms and processes of managing the risks and threats in businesses. In addition, broader studies using a macroscopic approach will be able to produce comprehensive recommendations for creating a desirable environment. This could contribute to mitigating cyber security risks and threats against businesses. The

opportunity therefore exists to carry out more research in this field with a potentially much larger impact.

BIBLOGRAPHY

Acock, A. C. (2016). *A gentle introduction to Stata* (5th ed.). Texas: Stata press.

Action Fraud. (n.d.). *Frequently asked questions*. Retrieved from https://www.actionfraud.police.uk/about-us-frequently-asked-questions

Adler, P. A., & Adler, P. (2012). Contribution to S.E. Baker, & R. Edwards (Eds.), *How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research* (pp. 8-11). National Centre for Research Methods Review Paper. Retrieved from http://eprints.brighton.ac.uk/11632/1/how_many_interviews.pdf

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal, 26*(3), 236-248.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. *Proceedings of the 8th Australasian Conference on Information Security: Vol. 105* (pp. 47-55). Brisbane, Australia: Australian Computer Society.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575.

AlHogail, A., & Mirza, A. (2014a). A framework of information security culture change. *Journal of Theoretical & Applied Information Technology, 64*(2), 540-549.

AlHogail, A., & Mirza, A. (2014b). Information security culture: A definition and a literature review. *Proceedings of 2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). Hammamet, Tunisia: IEEE.

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for understanding information security culture and practices in the Saudi context. *Proceedings of the 7th Australian information security management conference* (pp. 6-17). Perth, Western Australia.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265-300). Berlin, Heidelberg: Springer.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of security risks. In S. Dietrich, & R. Dhamija (Eds.), *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 367-377). Berlin, Heidelberg: Springer.

Babbie, E. (2007). *The practice of social research* (11th ed.). CA: Thomson Wadsworth.

Bae, S., Park, S., & Kim, S. J. (2015). A study on the Development for the National Cybersecurity Capability Assessment Criteria. *Journal of the Korea Institute of Information Security & Cryptology, 25*(5), 1293-1314.

Baek, M. J., & Sohn. S. H. (2011). A Study on the effect of information security awareness and behavior on the information security performance in small and medium sized organization. *The Journal of Small Business Innovation, 33*(2), 113-132.

Bank of Korea. (2014). *2016 Internet banking service usages*. Seoul: TSO.

Bank of Korea. (2015). *2016 Internet banking service usages*. Seoul: TSO.

Bank of Korea. (2016). *2015 Internet banking service usages*. Seoul: TSO.

Bank of Korea. (2017). *2016 Internet banking service usages*. Seoul: TSO.

Bass, B. M. (1985). *Leadership and performance beyond expectations*. New York: Free Press.

Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership* (2nd ed.). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Bauer, J. M., & Dutton, W. H. (2015). *The new cyber security agenda: Economic and social challenges to a secure internet*. (World Bank's World Development Report n.102965). Retrieved from the World Bank website: http://documents.worldbank.org/curated/en/689851467991972707/The-new-cybersecurity-agenda-economic-and-social-challenges-to-a-secure-internet

Bazeley, P. (2013). *Qualitative data analysis: Practical strategies*. London: Sage.

Beck, U. (1992). *Risk society: Toward a new modernity*, London: Sage Publications.

Bednarz, D. (1985). Quantity and quality in evaluation research: A divergent view. *Evaluation and Program Planning, 8*(4), 289-306.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61.

Bhattacharya, D. (2011). Leadership styles and information security in SMEs. *Information Management & Computer Security, 19*(5), 300–312.

Blackburn, R. (2012). *Segmenting the SME market and implications for service provision: A literature review* (Research Paper Ref: 9/12). London: Advisory, Conciliation and Arbitration Service.

Blair, J., Czaja, R. F., & Blair, E. A. (2014). *Designing surveys: A guide to decisions and procedures* (3rd ed.). London: Sage.

Böhme, R., & Schwartz, G. (2010). Modeling cyber-Insurance: Towards a unifying framework. *Proceedings of the 9th Workshop on the Economics of Information Security* (pp. 1–36). Cambridge, MA.

Bolot J., Lelarge M. (2009). Cyber insurance as an incentive for internet security. In M. E. Johnson (Ed.), *Managing Information Risk and the Economics of Security* (pp. 269-290). Boston: Springer.

Bonacich, P. (1987). Power and centrality: A family of measures. *American journal of sociology, 92*(5), 1170-1182.

Borodzicz, E. (2005). *Risk, crisis and security management*. Chichester: John Wiley & Sons.

Borodzicz, E. P., & Gibson, S. D. (2006). Corporate security education: Towards meeting the challenge. *Security Journal, 19*(3), 180-195.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society, 15*(5), 662-679.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management, 33*(5), 726–733.

British Society of Criminology. (2006). *Code of ethics for researcher in the field of criminology*. Retrieved from www.britsoccrim.org/docs/CodeofEthics.pdf

British Sociological Association. (2002). *Statement of ethical practice*. Retrieved from http://www.psi.uba.ar/academica/carrerasdegrado/psicologia/sitios_catedras/obligatorias/723_etica2/material/normativas/british.pdf

Broll, R. (2016). Collaborative responses to cyberbullying: preventing and responding to cyberbullying through nodes and clusters. *Policing and Society, 26*(7), 735-752.

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative Research, 6*(1), 97–113.

Bryman, A. (2012). Contribution to S. E. Baker, & R. Edwards (Eds.), *How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research* (pp. 18–20). National Centre for Research Methods Review Paper. Retrieved from http://eprints.brighton.ac.uk/11632/1/how_many_interviews.pdf

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford: Oxford university press.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Burgess, R. G. (1984). *In the field: An introduction to field research*. London: Allen & Unwin.

Button, M. (2008). *Doing security*. Basingstoke: Palgrave Macmillan.

Button, M., Tapley, J., & Lewis, C. (2013). The 'fraud justice network' and the infrastructure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice, 13*(1), 37-61.

Cabinet Office. (2011a). *The cost of cyber crime*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Cabinet Office. (2011b). *The UK cyber security strategy: Protecting and promoting the UK in a digital world*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Cabinet Office. (2015). *Major Projects Authority annual report 2014-15*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/438333/Major_Projects_Authority_Annual_Report_2015.pdf

Cabinet Office. (2018). *The CSQ Interview: Campbell McCafferty, Government Chief Security Officer*. Retrieved from https://quarterly.blog.gov.uk/2018/01/19/the-csq-interview-campbell-mccafferty-government-chief-security-officer/

Candiwan, C. (2014). Analysis of ISO27001 implementation for enterprises and SMEs in Indonesia. *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security* (pp. 50-58). Kuala Lumpur, Malaysia.

Castells, M. (2010). T*he rise of the network society: The information age: Economy, society, and culture Vol. 1* (2nd ed.). Oxford: John Wiley & Sons.

Centre for the Protection of National Infrastructure. (n.d.). *Critical national infrastructure.* Retrieved from https://www.cpni.gov.uk/critical-national-infrastructure-0

Chalmers, A. F. (2013). *What is this thing called science?* (4th ed.). Indianapolis: Hackett Publishing.

Chang, H. B. (2010). The design of information security management system for SMEs industry technique leakage prevention. *The Journal of Multimedia Information System, 13*(1), 111-121.

Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345–361.

Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Cheng, B. S., Boer, D., Chou, L. F., Huang, M. P., Yoneyama, S., Shim, D., ... & Tsai, C. Y. (2014). Paternalistic leadership in four East Asian societies: Generalizability and cultural differences of the triad model. *Journal of Cross-Cultural Psychology, 45*(1), 82-90.

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2003). Understanding organizational security culture. In M. Hunter, & K. Dhanda (Eds.), *Proceedings of Information systems: the challenges of theory and practice* (pp. 335–365). Las Vegas: Information Institute.

Cho, S. (2014). Welfare reforms, labour markets and inter-firm relations in South Korea since 1997: An inter-institutional approach. *Competition & Change, 18*(1), 20-36.

Choi, J.-H. (2010). A study on the institutional improvement directions of industrial security programs. *Korean Security Science Association*, (22), 197–230.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability, 8*(7), 638.

Choi, M. G., Jeong, J. H., & Kim, J. H. (2014). A study on the effects of the security perceptions of top managers and the education on the business performances. *The Journal of Small Business Innovation, 36*(2), 209-226.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Chung, M. K., Lim, J. I., & Kwon, H. Y. (2016). A study on North Koreas cyber attacks and countermeasures. *Journal of the Korea society of IT services, 15*(1), 67-79.

Clark, D., Berson, T., & Lin, H. S. (2014). *At the nexus of cyber security and public policy*. National Research Council, Washington DC: The National Academies Press.

Collin, B. C. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. *Crime and Justice International, 13*(2), 15-18.

Conway, M. (2008). *Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructures* (Working paper 5). Dublin: International Studies Centre of Dublin City University.

Council of Europe Cybercrime Convention. (2001). *Convention on cybercrime* (European Treaty Series – No. 185). Retrieved from http://www.europarl.europa.eu/m eetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. *Proceedings of the Conference on Usability, Psychology, and Security* (pp.1-15). San Francisco, California.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. London: Sage.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). London: Sage.

Creswell, J. W., & Tashakkori, A. (2007). Editorial: Developing publishable mixed methods manuscripts. *Journal of Mixed Methods Research, 1*(2), 107–111.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Crown Commercial Service. (2014). *Procurement policy note–Use of cyber essentials scheme certification* (Action Note 09/14). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368247/Cyber_Essentials_Scheme_draft_PPN_28_10.pdf

Danielson, M. (2009). Economic espionage: Framework for workable solution. *Minnesota Journal of Law, Science Technology, 10*(2), 503-548.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. In E. Lindon (Ed.), *Focus on terrorism* (pp. 71-76). Washington: Nova Science Publishers.

Denscombe, M. (2014). *The good research guide: for small-scale social research projects* (5th ed.). Berkshire: McGraw-Hill Education.

Denzin, N. K. (1970). *The research act in sociology: A theoretical introduction to sociological methods*. London: Butterworths.

Department for Business, Innovation and Skills. (2013). *Call for evidence on a preferred standard in cyber security*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf

Department for Business, Innovation and Skills. (2014). *Cyber Essentials Scheme: Summary.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

Department for Digital, Culture, Media and Sport. (2016). *Cyber security breaches survey 2016*. Retrieved from https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

Department for Digital, Culture, Media and Sport (2017). *Cyber security breaches survey 2017*. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

Department for Digital, Culture, Media and Sport (2018). *Cyber security breaches survey 2018*. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

Department for Digital, Culture, Media and Sport, & Vaizey, E. (2015, July 16). *New £5000 Government grant for SMEs to boost cyber security* [Press release]. Retrieved from https://www.gov.uk/government/news/new-5000-government-grant-for-small-businesses-to-boost-cyber-security

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of management Review, 25*(4), 850-863.

Devitt, K. R., & Borodzicz, E. P. (2008). Interwoven leadership: The missing link in multi-agency major incident response. *Journal of Contingencies and Crisis Management, 16*(4), 208-216.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20*(2), 165-172.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449–457.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. *Proceedings of the 15th European Conference on Information Systems* (pp. 1560-1571). St. Gallen, Switzerland.

Downing, E. (2011). *Cyber security - A new national Programme* (SN/SC/5832). House of Commons Library. Retrieved from http://researchbriefings.files.parliament.uk/documents/SN05832/SN05832.pdf.

Doyle, C. (2016). *Stealing trade secrets and economic espionage: An overview of the economic espionage Act* (R42682). Congressional Research Service, US Library of Congress.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Emerson, R. W. (2017). ANOVA and t-tests. *Journal of Visual Impairment & Blindness, 111*(2), 193-196.

Erbschloe, M. (2004). *Trojans, worms, and spyware: A computer security professional's guide to malicious code*. Oxford: Elsevier Butterworth-Heinemann.

European Union Agency for Network and Information Security. (2006). *Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools*. Retrieved from https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

Festinger, L., & Katz, D. (1953). *Research methods in the behavioural sciences*. New York: Dryden.

Fielding, N., & Fielding, J. L. (1986). *Linking data*. California: SAGE.

Financial Supervisory Service. (2013, December 3). *Comprehensive measures for the prevention of electronic financial fraud* [Press release]. Retrieved from http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp?seqno=17385&no=27&s_title=%C1%BE%C7%D5%B4%EB%C3%A5&s_kind=title&page=2

Financial Supervisory Service. (2017). *Statistics on banking practices*. Retrieved from http://www.fss.or.kr/fss/kr/bbs/list.jsp?bbsid=1207396624018&url=/fss/kr/1207396624018

Finnegan, R. (2006). Using documents. In R. Sapsford, & V. Jupp (Eds.), *Data collection and analysis* (2nd ed., pp. 138-151). London: Sage Publications.

Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to Security* (8th ed.). Oxford: Elsevier Butterworth-Heinemann.

Flick, U. (1992). Triangulation revisited: Strategy of validation or alternative?. *Journal for the Theory of Social Behaviour, 22*(2), 175-197.

Flick, U. (2004). Triangulation in qualitative research. In U. Flick, E. von Kardoff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 178-183). London: Sage.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44.

Flyvbjerg, B. (2001). *Making social science matter: Why social inquiry fails and how it can succeed again*. Cambridge: Cambridge university press.

Frooman, J. (1999). Stakeholder influence strategies. *Academy of management review, 24*(2), 191-205.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988.

Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62–70.

Gehem, M., Usanov, A., Frinking, E., & Rademaker, M. (2015). *Assessing cyber security: A meta-analysis of threats, trends, and responses to cyber-attacks*. The Hague Centre for Strategic Studies. Retrieved from https://hcss.nl/sites/default/files/files/reports/HCSS_Assessing_Cyber_Security.pdf

Gelles, D. (2016, July 12). Taser international dominates the police body camera market. *New York Times*. Retrieved from https://www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html

Ghobadian, A., & Gallear, D. (1997). TQM and organization size. *International Journal of Operations & Production Management, 17*(2), 121–163.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81-85.

Graham, R. S. (2017, October 19). The difference between cybersecurity and cybercrime, and why it matters. *The Conversation*. Retrieved from http://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654

Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). 'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management, 34*(2), 99-122.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N.K. Denzin & Y.S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117). London: Sage.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security, 22*(1), 21–35.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Gupta, V., Dhiman, L., & Sangroha, D. (2013). An approach to implement Bring Your Own Device (BYOD) securely. *International Journal of Engineering Innovation and Research. 2*(2), 154-156

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for SMEs: An empirical examination. *Information Management & Computer Security, 13*(4), 297–310.

Halfpenny, P. (1979). The analysis of qualitative data. *Sociological Review, 27*(4), 799–827.

Han, J., & Yoo, H. (2016). The effect of managerial information security intelligence on the employee's information security countermeasure awareness. *Information Systems Review, 18*(3), 137-153.

Harris, M., & Patten, K. (2014). Mobile device security considerations for small and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97–114.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Ullah Khan, S. (2015). The rise of 'big data' on cloud computing: Review and open research issues. *Information Systems, 47*, 98–115.

Hashim, J. (2015). Information Communication Technology (ICT) adoption among SME owners in Malaysia. *International Journal of Business and Information, 2*(2).

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Herbane, B. (2010). Small business research: Time for a crisis-based view. *International Small Business Journal, 28*(1), 43–64.

Her Majesty's Inspectorate of Constabulary. (2015). *State of policing: The annual assessment of policing in England and Wales 2015*. Retrieved from http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-2015.pdf

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems, 30*(3), 79-98.

HM Government. (2015). *National Security Strategy and Strategic Defence and Security Review 2015* (Cm 9161) [Electronic version]. London: TSO.

HM Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved from https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Hoffman, B. (2006). *Inside terrorism*. New York: Columbia University Press.

Holloway, I., & Todres, L. (2003). The status of method: Flexibility, consistency and coherence. *Qualitative Research, 3*(3), 345-357.

Holtfreter, K., & Meyers, T. J. (2015). Challenges for cybercrime theory, research, and policy. *The Norwich Review of International and Transnational Crime,* 54-66.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248.

House of Commons. (2017). *Protecting information across government* (HC 769). Retrieved from https://publications.parliament.uk/pa/cm201617/cmselect/cmpubacc/769/769.pdf

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660.

Hunton, P. (2010). Cybercrime and security: A new model of law enforcement investigation. *Policing*, 1–10.

IBM. (2014). *IBM Security services 2014 cyber security intelligence index*. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79.

International Monetary Fund. (2015). *World economic outlook database*. Retrieved from https://www.imf.org/external/pubs/ft/weo/2015/02/weodata/download.aspx

International Organization for Standardization & International Electrotechnical Commission. (2016). *ISO 27000: 2016. Information technology-security techniques-Information security management systems-Overview and vocabulary*. ISO.

International Telecommunications Union. (2008). *ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cyber security.* Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

International Telecommunications Union. (2011). *ITU national cyber security strategy guide.* Retrieved from http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

International Telecommunication Union. (2014). *ICT facts & figures*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

International Telecommunication Union. (2015a). *ICT facts & figures*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

International Telecommunication Union. (2015b). *Measuring the information society report.* Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

ISACA. (2013). *COBIT 5 For Risk*. Rolling Meadows, IL: ISACA

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods, 18*(1), 3–20.

Jang, S. (2016, December 15). South Korean military is defeated by North Korean cyber warfare…'Need to change an awareness of military operations'. *Special Economy*. Retrieved from http://www.speconomy.com/news/articleView.html?idxno=76451

Jang, Y. (2014). *A study on the national cybercrime strategy: Toward the improvement of Korean cyber policing policies applying a logic model* (Unpublished doctoral thesis). Korea University, Seoul.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993.

Jin, B., & Gu Suh, Y. (2005). Integrating effect of consumer perception factors in predicting private brand purchase in a Korean discount store context. *Journal of*

Consumer Marketing, 22(2), 62-71.

Jo, S. (2016, March 12). North Korea hacked smartphones of 40 South Korean government officials in foreign and security positions. *Korea Economic News.* Retrieved from http://news.hankyung.com/article/2016031185041?nv=o

Joh, E. E. (2017). The undue influence of surveillance technology companies on policing. *New York University Law Review*, 92, 101-130.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher, 33*(7), 14–26.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112–133.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Jung, P. W. (2011). A critical analysis on the concept of "cyber cecurity". *Yonsei Journal of Medical and Science Technology Law, 2*(2), 1-25.

Jung, B. S., Ryu, S. I., & Kim, H. S. (2012). Analysis of research trends in industrial security - Concentrated on academic research information services (Year 2000~2011). *Journal of Korean Public Police and Security Studies, 9*(2), 195-215.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the* econometric society*, 47*(2), 263-291.

Kang, J. H. (2015). Domestic SME industrial security promotion measures proposed. *Korean Journal of Industrial Security, 5*(1), 113-144.

Kang, J., Kim, H., Kim, S., & Yoo, J. (2016). Cyber warfare countermeasures by comparison of cyber warfare strategy and technology of North Korea and other major country. *Journal of Security Engineering, 13*(4), 287-298.

Karagiannopoulos, V. (2016). Insider unauthorised use of authorised access: What are the alternatives to the Computer Misuse Act 1990? *International Journal of Law, Crime and Justice, 47*, 85-96.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9*(3), 2012–52.

Kearns, G. S., & Lederer, A. L. (2004). The impact of industry contextual factors on IT focus and the use of IT for competitive advantage. *Information & Management, 41*(7), 899-919.

Kim, J. [Jihyun]. (2014). Proposal of cyber security control tower system in view of Korea's constitutional law. *Journal of Security Engineering, 11*(1), 25-40.

Kim, T. [Taekye]. (2014). Institutional issues and the corresponding measures of crime cyber terrorism. *Journal of Law and Politics Research, 14*(3), 1337–1381.

Kim, Y. [Yanghoon]. (2014). A correlation study of core technology leakage and security capability: Centric SMEs cases. *Korean Journal of Industrial Security, 4*(1), 97-108.

Kim, J. (2016, May 20). Youths face justice after joining voice phishing in China. *Mediapen*. Retrieved from http://www.mediapen.com/news/view/151036

Kim, B. (2017). A strategic approach for establishing Korea's cyber terrorism policy: Focusing on the UK's cyber terrorism policy. *Korea Security Science Association, 51*, 171-196.

Kim, S., Kang, J., & Kim, Y. (2015). Countermeasures against phishing/pharming via portal sites for general users. *The Journal of Korean Institute of Communications and Information Sciences, 40*(6), 1107-1113.

Kim, J., & Kim, S. (2016). Study on plans to improve small and medium corporations' technological protections using information security management system. *Journal of the Korea Society of Digital Industry and Information Management, 12*(3), 33-54.

Knapp, K. J., Marshall, T. E., Rainer, R.K., & Ford, F.N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Morrow, D.W. (2004). The top information security issues facing organizations: What can government do to help? *The 2004 International Information Systems Security Certification Consortium Survey Results*, Auburn University, Auburn, AL.

Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). Security governance: Its impact on security culture. *Proceedings of the 3rd Australian Information Security Management conference* (pp. 47-58). Perth, Australia.

Korea International Trade Association. (2015). *This is how to prevent trade fraud via email hacking* [Press release]. Retrieved from http://www.kita.net/info/press/view_kita.jsp?sNo=6484&pageNum=12&nGubun=3&s_con=&s_text=&sStartDt=&sEndDt=&sOr

der=&sClassification=01&search_word=&rowCnt=20&s_date1=&s_date2=&actionName=

Korea Internet & Security Agency. (2011). *A factual survey on information security*. Seoul: TSO.

Korea Internet & Security Agency. (2016). *A manual for Information Security Management System*. Seoul: TSO.

Korean Statistical Information Service. (2013). *Exports by company size*. Retrieved from http://kosis.kr/statHtml/statHtml.do?orgId=142&tblId=DT_B10062&vw_cd=MT_ZTITLE&list_id=142_100&seqNo=&lang_mode=ko&language=kor&obj_var_id=&itm_id=&conn_path=E1#

Krosnick, J. A. (1999). Survey research. *Annual Review of Psychology*, *50*(1), 537–567.

Kuhn, T. S. (2012). *The structure of scientific revolutions* (4th ed.). Chicago: University of Chicago press.

Kwon, J. (2016, March 11). North Korea hacked smartphones of South Korean government officials. *Arirang News.* Retrieved from http://www.arirang.co.kr/News/News_View.asp?nseq=189072

Kwon, Y. (2014). Problems of cyber criminal punishment regulations and how to deal with them. *Law Review, 53*, 177-193.

Kwon, J., & Kim, K. (2017). A study on Establishment of small and medium business information security plan under resource restrictions. *Journal of Convergence for Information Technology, 7*(2), 119-124.

Kwon, O., & Seok, J. (2016). A study of the major countries cyber terrorism response system and implications. *Korea Security Science Association, 49*, 185-214.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219–236.

Lee, C. (2017). A critical review of industrial security concepts. *Korea Security Science Association, 50*, 287-303.

Lee, D., (2013). A study on personal data hacking case to build corporate security and counter strategy: Focused on Hyundai Capital hacking case. *Journal of Security Engineering, 10*(4), 455-472.

Lee, M. (2016, August 1). Seoul YMCA to report 10.3 million personal information leak by Interpark to prosecutor's office. *Asiae Economy.* Retrieved from http://www.asiae.co.kr/news/view.htm?idxno=2016080108352216809

Lee, Y. I. (2004). South Korean companies in transition: An evolving strategic management style. *Strategic Change, 13*(1), 29-35.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1–17.

Levi, M., Morgan, J., & Burrows, J. (2003). Enhancing business crime reduction: UK directors' responsibilities to review the impact of crime on business. *Security Journal, 16*(4), 7-27.

Levy, M., & Powell, P. (2005). *Strategies for growth in SMEs: The role of information and information systems*. Oxford: Butterworth Heinemann.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Proceedings of the 7th Australian information security management conference* (p. 88-97). Perth, Australia.

Lofland, J. (1971). *Analysing social settings. A guide to qualitative observation and analysis*. California: Wadsworth.

Lofland, J., & Lofland, L. H. (1984). *Analysing social settings. A guide to qualitative observation and analysis* (2nd ed.). California: Wadsworth.

Lok, P., & Crawford, J. (2004). The effect of organisational culture and leadership style on job satisfaction and organisational commitment: A cross-national comparison. *Journal of Management Development, 23*(4), 321-338.

Loveday, B. (2017). The shape of things to come. Reflections on the potential implications of the 2016 Office of National Statistics crime survey for the police service of England and Wales. *Policing: A Journal of Policy and Practice,* 1-12.

Macdonald, K. (2008). Using documents. In N. Gilbert (Ed.), *Researching Social Life* (3rd ed., pp. 285-303), London: Sage Publications.

Madzima, K., Moyo, M., & Abdullah, H. (2014, August). *Is bring your own device an institutional information security risk for small-scale business organisations?* Paper

presented at the Information Security for South Africa (pp. 1–8). Johannesburg, South Africa: IEEE.

Magklaras, G. B., & Furnell, S. M. (2004). The insider misuse threat survey: Investigating IT misuse from legitimate users. *Proceedings of the 5th Australian Information Warfare & Security Conference*, Perth, Western Australia.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. A. (2017). A systematic literature review: Information security culture. *Proceedings of Research and Innovation in Information Systems (ICRIIS) 2017 International Conference* (pp. 1-6). Langkawi, Malaysia: IEEE.

Matlay, H. (1999). Employee relations in small firms: A micro-business perspective. *Employee relations, 21*(3), 285-295.

McAfee, A., & Brynjolfsson, E. (2012). Big data. The management revolution. *Harvard Business Review, 90*(10), 61–67.

McCulloch, G. (2004). *Documentary research in education, history, and the social sciences*. New York: RoutledgeFalmer.

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence* (Home Office Research Report 75). Retrieved from the UK Home Office website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Ministry of Science, ICT and Future Planning. (2013). *A study on estimating economic damages from Internet incidents for cybersecurity insurance*. Seoul: TSO.

Ministry of Strategy and Finance. (2015). *13 major export items* [Press release]. Retrieved from http://mosfnet.blog.me/220580493362

Mir, D. F., & Feitelson, E. (2007). Factors affecting environmental behavior in micro-enterprises: laundry and motor vehicle repair firms in Jerusalem. *International Small Business Journal, 25*(4), 383-415.

Mitchell, V. W. (1993). Handling consumer complaint information: Why and how? *Management Decision, 31*(3), 21-28.

Moradoff, N. (2010). Biometrics: Proliferation and constraints to emerging and new technologies. *Security Journal, 23*(4), 276-298.

Morgan, M.G., Fischhoff, B., Bostrom, A., Atman, C.J. (2002). *Risk communication: A mental models approach*. Cambridge: Cambridge University Press.

Nam, J. S. (2012). Actual condition of damage of industrial secrets leakage crime and its measures at small or medium sized business - Focusing on legal·systematic methods, *Journal of Korean Association of Public Safety and Criminal Justice, 21*(1), 44-75.

Nasheri, H. (2005). *Economic espionage and industrial spying*. Cambridge: Cambridge University Press.

National Aeronautics and Space Administration. (2007). *NASA systems engineering handbook* (SP-2007-6105 Rev1). Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook.pdf

National Audit Office. (2014). *Update on the National Cyber Security Programme* (HC 626). Retrieved from https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf

National Audit Office. (2016). *Protecting information across government* (HC 625). Retrieved from https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf

National Cyber Security Centre. (2017). *The launch of the National Cyber Security Centre.* Retrieved from https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%nc20launch%20of%20the%20National%20Cyber%20Security%20Centre.pdf

National Fraud Intelligence Bureau. (2013). *Action Fraud and National Fraud Intelligence Bureau* (User Guide). Retrieved from https://www.whatdotheyknow.com/request/187748/response/466202/attach/4/User%20Guide.pdf

National Institute of Standards and Technology. (2017). *Risk management framework for information systems and organizations* (Draft NIST Special Publication 800-37). Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf

National Intelligence Service. (2015). *National information protection White Paper*. Seoul: TSO.

National Police Agency. (n.d.). *Organisation chart*. Retrieved from http://www.police.go.kr/portal/main/contents.do?menuNo=200667

National Police Agency. (2012). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2013). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2014). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2015). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2016). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2017a). *National Police White Paper*. Seoul: TSO.

National Police Agency. (2017b). *An annual report of cyber one-stop centre 2016.* Seoul: TSO.

National Police Agency. (2018). *A report on trade fraud*. Unpublished internal document.

National Police Chiefs' Council. (2015). *Digital Investigation and Intelligence: Policing Capabilities for a Digital Age*. Retrieved from http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf

National Statistical Office. (2017). *Nationwide business statistics 2016*. Daejeon: TSO.

Nye, J. S. (2010). *Cyber power.* Retrieved from Belfer Center for Science and International Affairs website: https://www.belfercenter.org/publication/cyber-power

Observatory of Economic Complexity. (n.d.). *South Korea*. Retrieved from https://atlas.media.mit.edu/en/profile/country/kor/

O'Cathain, A., Murphy, E., & Nicholl, J. (2007). Why, and how, mixed methods research is undertaken in health services research in England: A mixed methods study. *BMC Health Services Research, 7*(1), 85.

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis, 31*(3), 497-512.

Organisation for Economic Co-operation and Development. (2017a). *Entrepreneurship at a glance 2017*. Retrieved from http://dx.doi.org/10.1787/22266941

Organisation for Economic Co-operation and Development. (2017b). *Fixed and wireless broadband subscriptions per 100 inhabitants (June 2017)*. Retrieved from https://www.oecd.org/sti/broadband/oecdbroadbandportal.htm

Office for National Statistics. (2017). *Crime in England and Wales: Year ending Sept 2016*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016

Onwuegbuzie, A. J., & Collins, K. M. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report, 12*(2), 281–316.

Onwuegbuzie, A. J., & Leech, N. L. (2006). Linking research questions to mixed methods data analysis procedures 1. *The Qualitative Report, 11*(3), 474–498.

O'Reilly, C., Chatman, J. (1996). Culture as social control: Corporations, cults, and commitment. In B. M. Staw, & L. L. Cummings (Eds.), *Research in Organizational Behavior* (vol.18, pp. 157-200), Greenwich: JAI Press.

Organ, D. (2015). Trust through certification in SME Cloud adoption. In P. R. J. Trim, & H.Y. Youm (Eds.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (pp. 32-46), Seoul: British Embassy in South Korea.

Osterman Research (2012). *Achieving rapid payback with mobile device management* (Osterman Research White Paper). Retrieved from https://www.ostermanresearch.com/whitepapers/orwp_0175.pdf

Park, K. (2004). A study on penal-sanction against corporation crimes. *Chungnam Law Review, 15*(1), 23-38.

Park, S., & Kim, S. J. (2013). A study on cyber security bills for the legislation of cyber security act in Korea. *Korea Convergence Security Association, 13*(6), 91–98.

Park, T.-H., Lim, C.-H., Lee, K.-O., & Lim, J.-I. (2013). Analysis on local governmental role for strengthening of industry security in small and medium-sized businesses. *The Journal of Digital Policy & Management, 11*(10), 1–16.

Parry, S. (2012). Going green: the evolution of micro-business environmental practices. *Business Ethics: A European Review, 21*(2), 220-237.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117-129.

Payne, G., & Payne, J. (2004). *Key concepts in social research*. London : SAGE.

Pfeffer, J. (1997). *New directions for organization theory: Problems and prospects.* New York: Oxford University Press.

Philpott, E. (2015). Cyber security in supply chains. In P. R. J. Trim, & H.Y. Youm (Eds.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership*. (pp. 54-56), Seoul: British Embassy in South Korea.

Platt, J. (1981). Evidence and proof in documentary research: 1. *Sociological Review, 29*(1), 31-52.

Ponemon Institute. (2017). *2017 Cost of Cyber Crime Study*. Retrieved from the Accenture website: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

Raggad, B. G. (2010). *Information security management: Concepts and practice*. New York: CRC Press.

Rainer Jr, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security, 16*(2), 100-108.

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Proceedings of the 13th ISSA annual meeting. Information Security for South Africa* (pp. 1-7). Johannesburg, South Africa: IEEE.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*(2), 221–232.

Ring, T. (2013). UK cyber-strategy suffers as spooks meet the suits. *Computer Fraud & Security, 2013*(11), 9–13.

Robbins, S. P., & Judge, T.A. (2013). *Organizational behaviour* (15th ed.). Boston: Pearson.

Robinson, N., Disley, E., Potoglou, D., Reding, A., Culley, D. M., Penny, M., . . . Millard, J. (2012). *Feasibility study for a European cybercrime centre*. Retrieved from RAND Corporation website: https://www.rand.org/pubs/technical_reports/TR1218.html

Robson, C., & McCartan, K. (2016). *Real world research* (4th ed.). Chichester: Wiley.

Rothbauer, P. M. (2008). Triangulation. In L. M. Given (Ed.), *The SAGE encyclopedia of qualitative research methods* (pp. 892-896). London: Sage.

Royal Society. (1992). *Risk analysis, perception, management.* London: Royal Society.

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). London: Sage.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Ryu, J. W. (2003, October 8). We need society which values science and technology. *Digital Times*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=029&aid=0000043754

Ryu, T. (2016). Just by changing the name of an email sender 'Trade scam'. *Segye News.* Retrieved from http://www.segye.com/content/html/2016/03/03/20160303004262.html?OutUrl=naver

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82.

Sale, J. E. M., Lohfeld, L. H., & Brazil, K. (2002). Revisiting the quantitative-qualitative debate: Implications for mixed-methods research. *Quality and Quantity, 36*(1), 43–53.

Sarantakos, S. (2013). *Social research* (4th ed.). New York: Palgrave Macmillan.

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). California: John Wiley and Sons.

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal, 31*, 46-52.

Scott, J. (1990). *A matter of record: Documentary sources in social research.* Cambridge: Polity Press.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27*(5), 644-667.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14*(4), 225–239.

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303–315.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal, 38*(6), 1573-1592.

Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis, 20*(1), 1-12.

Small and Medium Business Administration. (n.d.). *An information security operations service*. Retrieved from https://www.ultari.go.kr/portal/psi/techPreventControl.do

Small and Medium Business Administration. (2011). *New measures for the protection of intellectual properties of SMEs* [Press release]. Retrieved from http://www.smba.go.kr/board/

Small and Medium Business Administration. (2016). *Industry classification by company size 2014*. Retrieved from http://220.71.4.163:8000/statHtml/statHtml.do?orgId=142&tblId=DT_142N_A20500

Snijders, C., Matzat, U., & Reips, U.-D. (2012). Big data: Big gaps of knowledge in the field of internet science. *International Journal of Internet Science, 7*(1), 1–5.

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security, 2004*(1), 8–12.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 503–522.

Stebbins, R. A. (2001). *Exploratory research in the social sciences*. London: Sage.

Stroh, L. K., Northcraft, G. B., & Neale, M. A. (2002). *Organizational behavior: A management challenge* (3rd ed.). London: Lawrence Erlbaum Associates.

Symantec. (2017). *Internet security threat report*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Swierczek, F. W. (1991). Leadership and culture: Comparing Asian managers. *Leadership & Organization Development Journal, 12*(7), 3-10.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Applied social research methods series, Vol. 46). CA: Sage.

Taylor, S. J., Bogdan, R., & DeVault, M. (2016). *Introduction to qualitative research methods: A guidebook and resource*. New Jersey: Wiley.

Taylor-Gooby, P., & Zinn, J. O. (2006). Current directions in risk research: New developments in psychology and sociology. *Risk Analysis, 26*(2), 397-411.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Trim, P. R. J., & Lee, Y. (2015). Cyber security issues, challenges and the way forward. In P. R. J. Trim, & H.Y. Youm (Eds.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (pp. 11-14), Seoul: British Embassy in South Korea.

Trim, P. R. J., & Youm, H. Y. (2015). Increasing Korea-UK university and industry research collaboration in cyber security. In P. R. J. Trim, & H.Y. Youm (Eds.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (pp. 7-10), Seoul: British Embassy in South Korea.

Truong, D. (2010). How cloud computing enhances competitive advantages: A research model for SMEs. *The Business Review, 15*(1), 59–65.

Tucker, D. S. (1997). The federal government's war on economic espionage. *University of Pennsylvania Journal of International Economic Law, 18*(3), 1109-1152.

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report, 15*(3), 754-760.

UK-CERT. (n.d.). *Cyber-security Information Sharing Partnership (CiSP)*. Retrieved from https://www.cert.gov.uk/cisp/

UK-CERT. (2016). *Annual report 2015/2016* (CUK-24-05-16-PD). Retrieved from https://www.ncsc.gov.uk/content/files/protected_files/report_files/CERT-UK-Annual-Report-2015-16.pdf

United Nations. (2014a). *E-government survey*. Retrieved from https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf

United Nations. (2014b). *World urbanization prospects: The 2014 revision*. Retrieved from https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.pdf

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

Vlek, C. (1995). Risk assessment, risk acceptance and risk management: A psychological decision theorist's view. In W. J. van den Brink, R. Bosman, F. Arendt (Eds.), *Contaminated soil '95* (pp. 565-579). Dordrecht: Kluwer Academic Publishers.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Wall, D. (2007). *Cybercrime*. Cambridge: Polity.

Wall, D. (2007/11). Policing cybercrimes: Situating the public police in networks of security within cyberspace (Revised, Feb 2011). *Police Practice and Research, 8*(2), 183–205. Retrieved from SSRN: https://ssrn.com/abstract=853225

Wall, D. (2005/15). The Internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77–98). California: Sage.

Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review, 20*(2), 115-131.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101.

Warren, C. A. (2002). Qualitative interviewing. In J. F. Gubrium & J. A. Holstein (Eds.), *Handbook of interview research: Context and method* (pp. 83-101). California: Sage.

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*.

Cambridge: Cambridge university press.

Weber, R. (2004). Editor's comments: The rhetoric of positivism versus interpretivism: A personal view. *MIS Quarterly, 28*(1), iii-xii.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4–19.

Whitman, M., & Mattord, H. (2011). *Principles of information security* (4th ed.). Boston: Cengage Learning.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis, 27*(3), 597-606.

Willis, J. W., Jost, M., & Nilakanta, R. (2007). *Foundations of qualitative research: Interpretive and critical approaches*. London: Sage.

Wright, C., & Kwon, S. H. (2006). Business crisis and management fashion: Korean companies, restructuring and consulting advice. *Asia Pacific Business Review, 12*(3), 355-373.

Yar, M. (2013). *Cybercrime and society* (2nd ed.). London: Sage.

Yoo, J. (2014). Comparison of information security controls by leadership of top management. *The Journal of Society for e-Business Studies, 19*(1), 63-78.

Yoon, H. (2013). The current trends of voice phishing fraud: Legislation and policy implication. *Korean Association of Criminology*, *25*(2), 245-267.

Yoon, S. (2016). Corporate information security as a corporate governance issue - Focused on U.S. discussions. *Business Law Review, 30*(1), 9-37.

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems, 26*(1), 13.

YTN. (2017, June 1). The new Director Suh Hoon, the abolishment of the NIS' domestic intelligence officer system. *YTN News*. Retrieved from http://www.ytn.co.kr/_ln/0101_201706011723581031

Yukl, G. A. (2002). *Leadership in organizations* (8th ed.). New York: Pearson.

Yun, J. (2016). Developing reference model for national cybersecurity strategy establishment and improvement. *Convergence Security Journal, 16*(4), 53-61.

Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. *Proceedings of IFIP International Information Security Conference: Vol. 201* (pp. 437-441). Boston, MA: Springer.

Zinn, J. O. (2008). Introduction: The contribution of sociology to the discourse on risk and uncertainty, In J. O. Zinn (Ed.), *Social theories of risk and uncertainty: An introduction* (pp. 1-17). Oxford: Blackwell Publishing Ltd.

APPENDICES

Appendix 1 (Survey Questionnaires for Managers and Owners in SMEs)

(Survey Questionnaire Guide)

This is Jeyong Jung, a research student in the Institute of Criminal Justice Studies at the University of Portsmouth in the UK. I invite you to participate in an academic study of 'Cyber Security Management of SMEs in South Korea'.

My study is part of my PhD research. The first aim of this study is to assess current situations of SMEs in relation to cyber security. This is because there is an obvious lack of situational assessment on SMEs in South Korea. Secondly, it is to identify organisational factors that have an influence on the implementation of security controls and vulnerability to security breaches. Investigating relationships or correlations among factors will help the researcher to prioritise the factors that may be used to increase cyber security. Finally, the researcher finally intends to devise an effective framework for protecting SMEs from cyber security risks and cybercrimes.

Quantitative data for this research will be obtained from survey questionnaires. You can join this study by completing this web-based questionnaire. I do not need your name or any identifying details. The questionnaire is completed anonymously and all reasonable measures will be taken to ensure confidentiality. You will be asked about your previous experience of cyber security breaches or attacks. The breaches or attacks you mention should have been officially reported to and sanctioned by their organisations or the authorities. You should not disclose unreported cybercrime cases. Any such disclosures will be reported to the proper authorities.

Withdrawal from the research is possible at any time during the survey without any reason. Responses from completed questionnaires will then be collected for analysis. Once this is finished and my thesis has been submitted then the data from the questionnaires will be destroyed. Until this phase, completed questionnaires will be saved electronically in my personal computer.

I also invite you to join further interview. Voluntary participations for interview later are welcomed. If you want to participate in it, please contact me via email or phone (010-4335-5057). If you have any concerns regarding this research please contact me (jeyong.jung@port.ac.uk), or my supervisor, Dr. Victoria Wang (victoria.wang@port.ac.uk). If there are any ethical concerns, you can also contact the Chair of the Faculty Ethics Committee (ethics-fhss@port.ac.uk).

By moving to the next screen you display your agreement to participate in the survey.

<NEXT SCREEN>

Section A : Assessment of SMEs' situation

In the following section, you will be asked about five themes concerning cyber security of your company. These questions will be used to assess current situations of SMEs. Please state any relevant answers regarding the following statements.

1. Which of the following, if any, does your company currently have or use? (multiple choice)
   ①Email addresses for your company or its employees ②A website or blog ③Accounts or pages on social media sites (e.g. Facebook or Twitter) ④The ability for your customers to order, book or pay for products or services online ⑤An online business bank account your company pays into ⑥Other ( )

2. To what extent, if at all, are online services a core part of the goods or services your company provides?
   ①Not at all important ②Not very important ③Neutral ④Important ⑤Very important

3. How many employees in your company use personally-owned devices such as smartphones, tablets, home laptops or desktop computers to carry out regular business-related activities?
   ①None ②1-20% ③21-40% ④41-60% ⑤61-80% ⑥81-100%

4. Does your company currently use any externally-hosted web services, for example to host your website or corporate email accounts, or for storing or transferring data?
   ①Never ②Not very often ③Neutral ④Often ⑤Very often

5. How critical, if at all, are these externally-hosted web services to your company?
   ①Not at all critical ②Not very critical ③Neutral ④Critical ⑤Very critical

6. Approximately, how many cyber security breaches or attacks have you experienced in total over the last 12 months?
   ①None ②Fewer than 5 ③5 to fewer than 10 ④10 to fewer than 15 ⑤15 to fewer than 20 ⑥20 to fewer than 50 ⑦50 or more ⑧Don't know

7. Which of the following have happened to your company in the last 12 months? (multiple choice)
   ①Denial-of-service attacks ②Access to computers, networks or services without permission (i.e., hacking) ③Money stolen electronically (e.g. through online banking) ④Money stolen through fraudulent emails or fake websites ⑤Personal information (e.g. customer data) stolen electronically ⑥People damaging or stealing software from your computers or network, even if accidentally ⑦People downloading unlicensed or stolen software to your computers or network, even if accidentally ⑧Computers becoming infected with viruses, spyware or malware ⑨Theft of intellectual property ⑩Others impersonating company in emails or online ⑪Breaches from personally-owned devices ⑫Breaches from externally-hosted web services ⑬Breaches on social media ⑭Other ( )

8. As far as you know, who or what was the source of the breach or attack? (multiple choice)
①Third party suppliers ②Activists ③Competitors ④Emails/email attachments/websites ⑤Current employees ⑥Former employees ⑦Malware authors ⑧Nation-state intelligence services ⑨Natural (flood, fire, lightening etc.) ⑩Non-professional hackers ⑪Organised crime ⑫Terrorists ⑬Other ( ) ⑭Don't know

9. Approximately how much, if anything, do you think the cyber security breaches or attacks you have experienced in the last 12 months have cost your company financially?
①Less than £500 ②£500 to less than £1,000 ③£1,000 to less than £5,000 ④£5,000 to less than £10,000 ⑤£10,000 to less than £20,000 ⑥£20,000 to less than £50,000 ⑦£50,000 to less than £ 100,000 ⑧£100,000 or more ⑨Don't know

10. How was the breach or attack identified? (multiple choice)
①By accident ②By antivirus/anti-malware software ③Disruption to business/staff/users/ service provision ④From warning by government/law enforcement ⑤Our breach/attack reported by the media ⑥Similar incidents reported in the media ⑦Reported/noticed by customers/customer complaints ⑧Reported/noticed by staff/contractors ⑨Routine internal security monitoring ⑩Other internal control activities not done routinely (e.g. reconciliations, audits etc.) ⑪Other ( ) ⑫Don't know

11. Thinking of all the cyber security breaches or attacks experienced in the last 12 months, have these impacted your company in any of the following ways? (multiple choice)
①Stopped staff from carrying out their day-to-day work ②Loss of revenue or share value ③Additional staff time to deal with the breach or attack, or to inform customers or stakeholders ④Any other repair or recovery costs ⑤New measures needed to prevent or protect against future breaches or attacks ⑥Lost or stolen assets ⑦Fines from regulators or authorities, or associated legal costs ⑧Reputational damage ⑨Prevented provision of goods or services to customers ⑩Discouraged you from carrying out a future business activity you were intending to do ⑪Other ( )

12. Which of the following aspects, if any, are covered within your cyber security-related policy, or policies? (multiple choice)
①What can be stored on removable devices (e.g. USB sticks, CDs etc.) ②Remote or mobile working (e.g. from home) ③What staff are permitted to do on your company's IT devices ④Use of personally-owned devices for business activities ⑤Use of new digital technologies such as cloud computing ⑥Data classification ⑦A Document Management System ⑧Other ( ) ⑨No policy adopted

13. How high or low a priority is cyber security to your company's directors or senior management?
①Very low ②Low ③Neutral ④High ⑤Very high

14. Over the last 12 months, has your company provided employees with internal cyber security trainings?
①Never ②Less than once a year ③Annually ④Quarterly ⑤Monthly ⑥Weekly ⑦Don't know

15. Which of the following governance or risk management arrangements, if any, do you have in place? (multiple choice)
①Board members with responsibility for cyber security ②An outsourced provider that manages your cyber security ③A formal policy or policies in place covering cyber security risks ④A Business Continuity Plan ⑤Staff members whose job role includes information security or governance ⑥Other ( ) ⑦None of these ⑧Don't know

16. Approximately how often, if at all, are your company's directors or senior management given an update on any actions taken around cyber security?
①Never ②Less than once a year ③Annually ④Quarterly ⑤Monthly ⑥Weekly ⑦Daily

17. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your company? (multiple choice)
①An internal audit ②Any business-as-usual health checks that are undertaken regularly ③Ad-hoc health checks or reviews beyond your regular processes ④A risk assessment covering cyber security risks ⑤Invested in threat intelligence ⑥Other ( ) ⑦None of these

18. Which of the following rules or controls, if any, do you have in place? (multiple choice)
①Applying software updates when they are available ②Up-to-date malware protection ③Firewalls with appropriate configuration ④Restricting IT admin and access rights to specific users ⑤Any monitoring of user activity ⑥Encrypting personal data ⑦Security controls on company-owned devices (e.g. laptops) ⑧Only allowing access via company-owned devices ⑨A segregated guest wireless network ⑩Other ( ) ⑪None of these ⑫Don't know

19. It there any incident management processes in your company?
①Yes ②No

20. Do you have insurance which would cover you in the event of a cyber security breach or attack?
①Yes ②No

21. Who is a breach or attack reported to? (multiple choice)
①National Intelligence Service ②Police ③Korean Internet & Security Agency ④Antivirus company ⑤Bank or credit card company ⑥Outsourced cyber security provider ⑦Internet/network service provider ⑧Professional/trade/industry association ⑨Media ⑩Website administer ⑪Other ( ) ⑫ No intention to report ⑬Don't know

22. From where have you sought information, advice or guidance on the cyber security threats that your company faces? (multiple choice)
    ①Business bank/bank's IT staff ②External security/IT consultants ③go.kr ④National Intelligence Services ⑤Police ⑥Korean Internet & Security Agency ⑦Small and Medium Business Administration ⑧Internet Service Provider ⑨Newspapers/media ⑩Online searching generally ⑪Professional/trade/industry association ⑫Regulator ⑬Security product vendors ⑭Other companies ⑮Within your company – senior management/board ⑯Within your company – other colleagues or experts ⑰Other ( )

23. Are you aware of any of the following initiatives and standards? (multiple choice)
    ①International Standard for Information Security Management (ISO 27001) ②Any government's guidance ③K-ISMS from KISA ④Security Operations Centre from SMBA ⑤Other ( ) ⑥None of these

24. Which any government agencies have you contacted in relation to cyber security? (multiple choice)
    ①National Intelligence Services ②Police ③Korean Internet & Security Agency ④Small and Medium Business Administration ⑤Other ( ) ⑥None of these

25. Have you been contacted or provided with any information by any government agencies in relation to cyber security? (multiple choice)
    ①National Intelligence Services ② Police ③Korean Internet & Security Agency ④Small and Medium Business Administration ⑤Other ( ) ⑥None of these

26. Which of the following, if any, do your clients require you to have or adhere to? (multiple choice)
    ①A recognised international standard (e.g. ISO 27001/PCIDSS) ②K-ISMS from KISA ③Any government's scheme ④Other ( ) ⑤None of these

Section B: Questions over your company and socio-demographics

In the following section, you will be asked about background information of your company and yourself. These questions are used to identify various organisational features of your company and yourself.

1. What type of industry is your company in?
   ①Manufacturing ②Construction ③Wholesale/retailing ④Accommodation and food service activities ⑤Transportation and storage ⑥Real estate ⑦Financial and insurance activities ⑧Administrative and support service activities ⑨ Information and communication ⑩Education service activities ⑪Professional, scientific and technical activities ⑫Human health and social work activities ⑬Utilities ⑭Arts, entertainment and recreation ⑮Environmental service activities ⑯Repair and extra service activities

2. How many employees are working in your company? ( )

3. When was your company established? ( )

4. Approximately, how much was the annual turnover of your company last year? ( )

5. Approximately, how much did your company invest in cyber security last year?
   ( ) or ( ) % of the annual turnover

6. How many ICTs (ex, desktop computers and laptops) does your company have? ( )

7. Do you think your company is vulnerable to cyber security breaches?
   (If Yes → Q8 / No → Section E) ①Yes ②No

8. How much do you think your company is vulnerable to cyber security breaches?
   ①Very low ②Low ③Neutral ④High ⑤Very high

9. What is your position in your company?
   ①Low-level manager ②Middle-level manager ③Senior manager ④Owner

10. What is your gender?
    ①Male ②Female

11. What was your last education?
    ①Middle School or under ②High School ③Community college ④University ⑤Master's degree ⑥ PhD degree

<Thank you for your participation>

Appendix 2 (Semi-structured Interview Questions for SMEs' IT Managers or Owners)

(Interview Guide)

This is Jeyong Jung, a research student in the Institute of Criminal Justice Studies at the University of Portsmouth in the UK. I invite you to participate in an academic study of 'Cyber Security Management of SMEs in South Korea'.

The first aim of this study is to assess current situations of SMEs in relation to cyber security. This is because there is an obvious lack of situational assessment on SMEs in South Korea. Secondly, it is to identify organisational factors that have an influence on the implementation of security controls and vulnerability to security breaches. Investigating relationships or correlations among variables will help the researcher to prioritise organisational factors that may be used to increase cyber security. Finally, the researcher finally intends to devise an effective framework for protecting SMEs from cyber security risks and cybercrimes.

Qualitative data for this research will be greatly obtained from face-to-face interview. Participation in my research is entirely voluntary and I anticipate that your engagement will require approximately 60 minutes of your time through face-to-face interview. Withdrawal from the research is possible at any time prior to the data I am collecting being analysed. You can stop the interview at any time. In any event, your contribution to my research will be in confidence and references in my final published research will be anonymous. It should also be noticed that the data belongs to the researcher and the University of Portsmouth. And the data cannot be used for human resources or employment progression issues. If your permission is obtained and no withdrawal is requested, the researcher will include material from the interview for the researcher's PhD thesis and, possibly, other relevant publications.

If you have a concern on any aspect of this interview or study, you may contact me via e-mail (jeyong.jung@port.ac.uk) or by telephone on 010-9370-5057 (South Korea) or 44-75-2174-5683 (UK). If there are any ethical concerns, you can also contact my advisor, Dr. Victoria Wang (victoria.wang@port.ac.uk) or the Chair of the Faculty Ethics Committee (ethics-fhss@port.ac.uk).

If you have any further questions, please feel free to contact me. Thank you for sharing your time for this interview. Your participation is greatly appreciated.

Cyber security management of SMEs	
Intro-duction	Purpose and Nature of Study / Risk of Inadequate Disclosure Awareness / Confirming Consent
1	Would you tell me about your company? (the number of employees, the number of ICT, business sector, importance of ICTs to business, etc.)
2	What is your role in your company?
3	Has your company ever experienced any cyber security breaches? What sort of damage occurred?
4	What types of cyber-attacks are the most prevalent and dangerous to your company?
5	How did(or will) you deal with cyber security breaches when (or if) they happen(ed)?
6	What measures does your company employ to increase the standard of cyber security?
7	What does senior management think about cyber security? Do senior managers agree on the statement that cyber security requires more attention within a company?
8	Do normal employees understand the importance of cyber security? How do you approach them to share the understanding?
9	Where do you usually get cyber security information?
10	Have you been contacted by any government organisations as to cyber security for information, alerts, or other supports?
11	What role do government organisations need to take? What is your expectation from the public sector?
12	What should be done to increase the level of cyber security in your company?
Con-clusion	Anything Else, Open Questions and Answers / Any Concerns regarding Interview / Contact Details

Appendix 3 (Semi-structured Interview Questions for Public Officials)

(Interview Guide)

This is Jeyong Jung, a research student in the Institute of Criminal Justice Studies at the University of Portsmouth in the UK. I invite you to participate in an academic study of 'Cyber Security Management of SMEs in South Korea'.

The first aim of this study is to assess current situations of SMEs in relation to cyber security. This is because there is an obvious lack of situational assessment on SMEs in South Korea. Secondly, it is to identify organisational factors that have an influence on the implementation of security controls and vulnerability to security breaches. Investigating causal relationships or correlations among variables will help the researcher to prioritise organisational factors that may be used to increase cyber security. Finally, the researcher finally intends to devise an effective framework for protecting SMEs from cyber security risks and cybercrimes.

Qualitative data for this research will be greatly obtained from face-to-face interview. Participation in my research is entirely voluntary and I anticipate that your engagement will require approximately 60 minutes of your time through face-to-face interview. Withdrawal from the research is possible at any time prior to the data I am collecting being analysed. You can stop the interview at any time. In any event, your contribution to my research will be in confidence and references in my final published research will be anonymous. It should also be noticed that the data belongs to the researcher and the University of Portsmouth. And the data cannot be used for human resources or employment progression issues. If your permission is obtained and no withdrawal is requested, the researcher will include material from the interview for the researcher's PhD thesis and, possibly, other relevant publications.

If you have a concern on any aspect of this interview or study, you may contact me via e-mail (jeyong.jung@port.ac.uk) or by telephone on 010-9370-5057 (South Korea) or 44-75-2174-5683 (UK). If there are any ethical concerns, you can also contact my advisor, Dr. Victoria Wang (victoria.wang@port.ac.uk) or the Chair of the Faculty Ethics Committee (ethics-fhss@port.ac.uk).

If you have any further questions, please feel free to contact me. Thank you for sharing your time for this interview. Your participation is greatly appreciated.

Government policies that are related to cyber security of SMEs	
Intro-duction	Purpose and Nature of Study / Risk of Inadequate Disclosure Awareness / Confirming Consent
1	Would you tell me about your job? How is it related to protecting SMEs in terms of cyber security?
2	What types of cyber-attacks are the most prevalent and dangerous?
3	What do you think about current cyber security situations that SMEs face? (prevalent types of cybercrime, seriousness of impacts, vulnerable groups)
4	Which groups are identified as more vulnerable ones depending on business sector, size, etc? Is there any customized policy for the vulnerable groups?
5	What is the role of your agency in relation to cyber security? What are the main priorities?
6	What are the main strategies, tactics and policies to protect SMEs? (respectively, for prevention and response) How effective are they? How does your agency evaluate the effectiveness of the policies?
7	How does your agency cooperate with other agencies or private companies(e.g., IT security vendors or ISPs)?
8	What are the main difficulties in protecting SMEs? What is the uniqueness of protecting SMEs compared to securing other entities, such as large companies, individuals and public organisations?
9	What should be done to improve the level of cyber security in SMEs?
Con-clusion	Anything Else, Open Questions and Answers / Any Concerns regarding Interview / Contact Details

Appendix 4 (Ethical Approval from University of Portsmouth)

University of Portsmouth
Faculty of Humanities and Social Sciences
Ethics-fhss@port.ac.uk

20th September 2016

Dear Jeyong Jung

Study Title:	**Cyber security management of SMEs in South Korea**
Ethics Committee reference:	**16/17:01**

Thank you for submitting your documents for ethical review. The Ethics Committee was content to grant a favourable ethical opinion of the above research on the basis described in the application form, protocol and supporting documentation, revised in the light of any conditions set, subject to the general conditions set out in the attached document.

The Ethics Committee provides a favourable ethical opinion with the following requirements:

1. **The participant is clear that the researcher is a police officer**
2. **The documentation will be held for 10 years under DPA conditions**
3. **Participants must be made aware that it will not be possible to withdraw their participation once the on-line survey has been submitted, as all submissions are anonymous to the researcher.**

There is no need to submit any further evidence to the Ethics Committee; the favourable opinion has been granted with the assumption of compliance

The favourable opinion of the EC does not grant permission or approval to undertake the research. Management permission or approval must be obtained from any host organisation, including University of Portsmouth, prior to the start of the study.

Documents reviewed

Appendix 5 (FORM UPR16_Research Ethics Review Checklist)

FORM UPR16

Research Ethics Review Checklist

University of Portsmouth

Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information

Postgraduate Research Student (PGRS) Information			**Student ID:**	796356
PGRS Name:	Jeyong Jung			
Department:	ICJS	**First Supervisor:**	Dr. Victoria Wang	
Start Date: (or progression date for Prof Doc students)		**01/10/2015**		
Study Mode and Route:	Part-time ☐ Full-time ☒	MPhil ☐ PhD ☒	MD ☐ Professional Doctorate ☐	

Title of Thesis:	A study of cyber security management within South Korean Businesses – An examination of cyber risk, threats, and cybercrime
Thesis Word Count: (excluding ancillary data)	76,817

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

UKRIO Finished Research Checklist:
(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES ☒ NO ☐
b) Have all contributions to knowledge been acknowledged?	YES ☒ NO ☐
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES ☒ NO ☐
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES ☒ NO ☐
e) Does your research comply with all legal, ethical, and contractual requirements?	YES ☒ NO ☐

Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

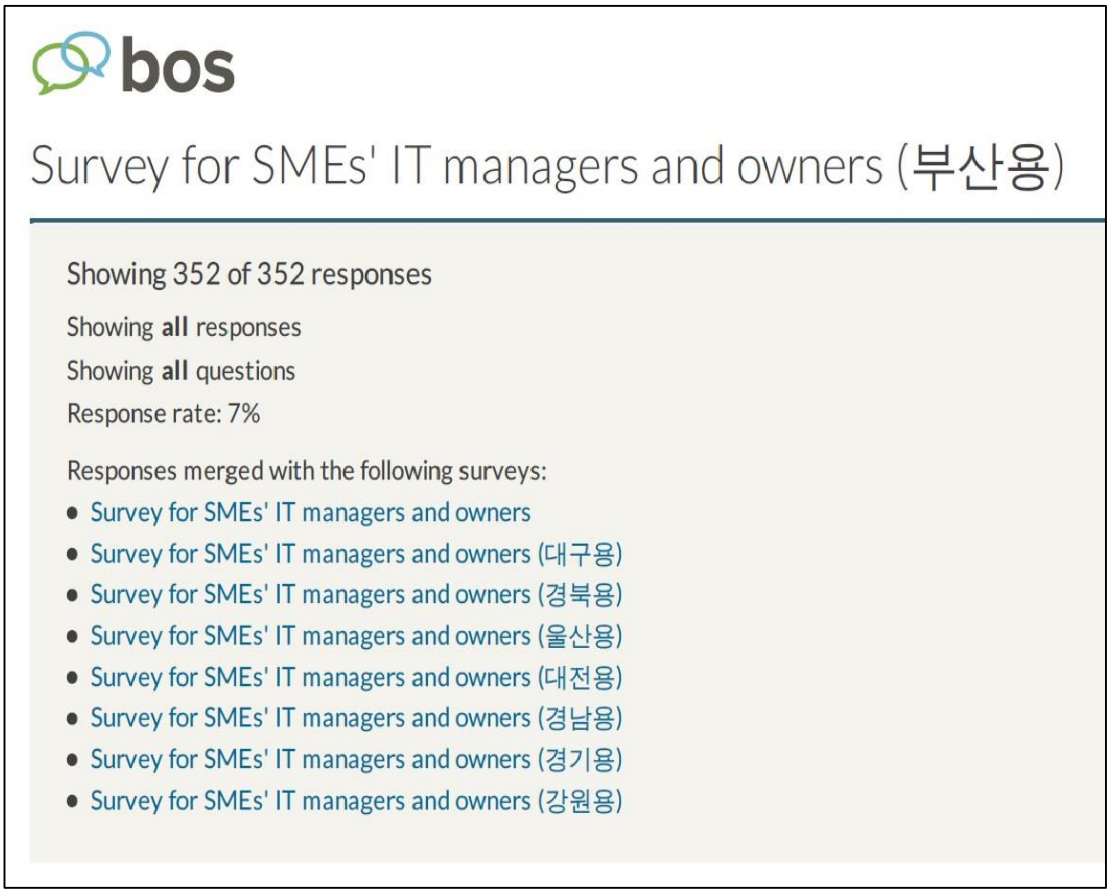
Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):	16/17:01

If you have *not* submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:

Signed *(PGRS)*:	Jeyong Jung	**Date:** 11/04/2018

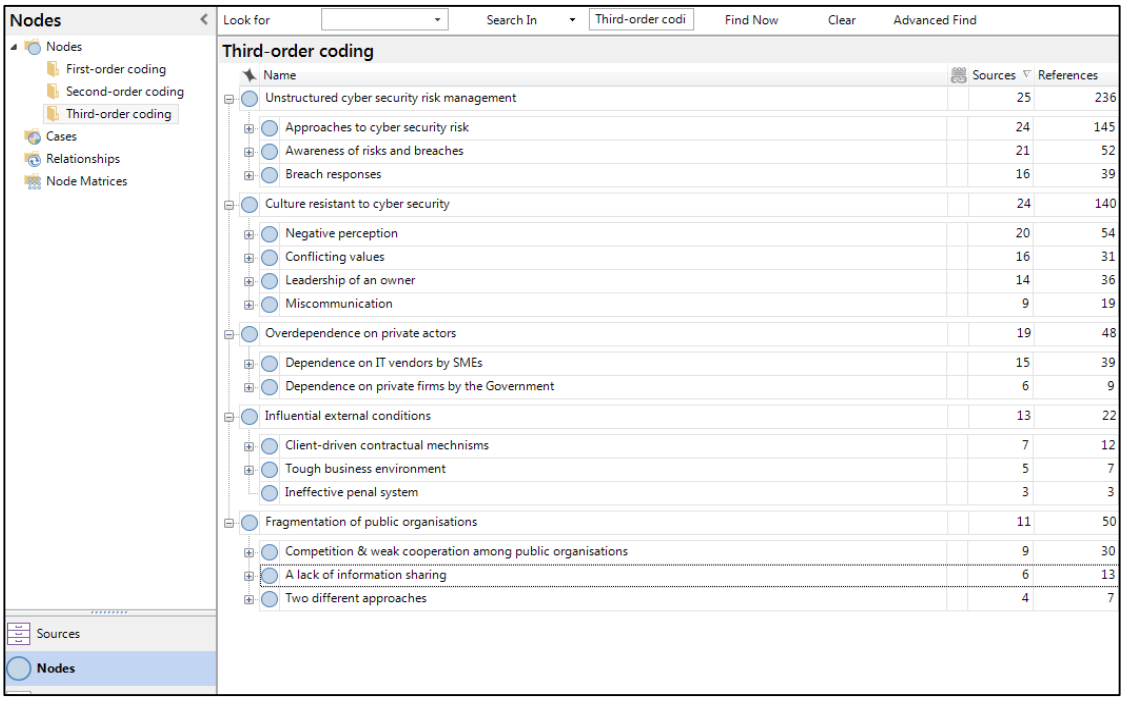
UPR16 – August 2015

Appendix 6 (Response Result of Online Survey)

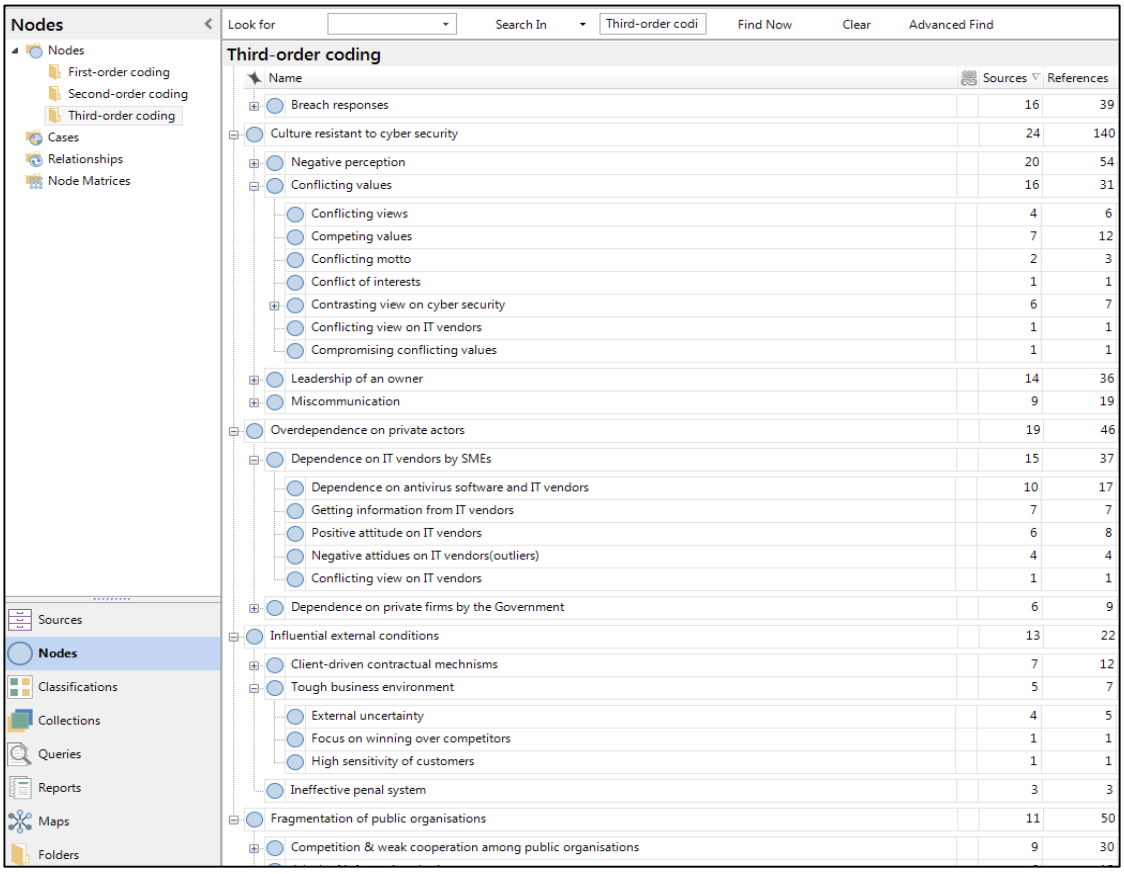


(The total number of responses and response rate / the first survey in the list which does not have a name was for Seoul.)

Appendix 7 (Coding Structure of Qualitative Data using NVivo)



(The structure of themes and sub-themes)



(The structure between analytic codes, sub-themes, and themes)