Application of a Financial Quantitative Risk Model to Information Security Risk Assessment

Liuxuan Pan

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Information Security Group
School of Mathematics and Information Security
Royal Holloway, University of London
2018

Declaration of Authorship

I Liuxuan Pan hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signature: Liuxuan Pan

Date: 01/05/2018

Abstract

ISRA has its roots in documents like the Orange Book and the Anderson Report. Even recent standards such as the ISO 27000 series make assumptions similar to those made in this early work. With the advent of globalisation, cloud computing and BYOD, the assumptions made by the early guidelines on risk assessment no longer hold. For example, for many organisations it may be impossible even to identify assets far less calculate associated risk. This thesis argues that a new approach to risk assessment is needed and presents an alternative based on financial models. Instead of taking a bottom up approach, we apply the theory of 'value at risk' to provide a macroscopic view of the risk to an organisation based on the potential financial loss due to a cyber attack.

We present a thorough and systematic review of ISRA research and provide a taxonomy of approaches to the problem. Since knowledge of the probability distribution of attacks is necessary to build the VaR model, we use data provided by Spamhaus in an attempt to identify the distribution of attacks by malware. Our findings show that the feature of non-uniformity distribution of malware attacks in 24 hours. This work also demonstrated a novel approach to malware analysis using circular statistics and presented results of analysis using rose and helix diagrams. Based on these findings we constructed a novel 'Malware' VaR model to estimate the worst case financial loss due to malware based data exfiltration from an organisation.

Acknowledgement

I hope to express my genuinely grateful gratitude to my supervisor, Dr Allan Tomlinson, for providing me many helpful academic opinions. He accepted me as his student when I have to change a supervisor, and supports me to find out a new research direction. He takes time to sort out our meeting notes and shares with me.

Many thanks to Professor Lizzie Coles-Kemp, my advisor, for guiding me on the correct path of ISRA. She always pinpoints the drawbacks of my study. Also, I would like to thank Dr Alexey Koloydenko gratefully for supporting the knowledge of statistics and helpful guidance in the published paper.

Nevertheless, I would like to thank Professor Dusko Pavlovic for giving me the initial opportunity to undertake this research.

Thanks also to Wanpeng Li for helping me to extract the data from a big dataset. Many thanks to Konstantinos Mersinas for having wonderful chats on life and academic and offering me an excellent opportunity to be a project supervisor.

I thank my family for all their support spiritually throughout writing this thesis and my life in general. Special thanks to my husband Lei Zhong for his help and advice. This thesis completes because of his great encouragement in the final stage of writing. I also immensely appreciate my mother-in-law Jinhua He for helping me take care of my daughters.

Contents

List of Figures

List of Tables

List of Abbreviations

ALE	Annual Loss Expectancy
AHP	Analytic Hierarchy Process
ARO	Annual Rate of Occurrence
ASN	Autonomous System Number
ATA	Attack Tree Analysis
BYOD	Bring Your Own Derive
CC	Common Criteria
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDF	Cumulative Distribution Function
C.I.A	Confidentiality, Integrity, Availability
CyberVaR	Cyber Value-at-Risk
CESG	Communications-Electronics Security Group
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CWG	Conficker Working Group
CIA	Confidentiality, Integrity, Availability
DDoS	Distributed Denial of Service
ePHI	Electronic Protected Health Information
ETA	Event Tree Analysis
ES	Expected Shortfall
FTA	Fault Tree Analysis
FMEA	Failure Mode and Effect Analysis
FAIR	Factor Analysis of Information Risk
GBM-OA	Genre-based method-OCTAVE Allegro
Haz-Op	Hazard and Operability Analysis
HHM	Hierarchical Holographic Modelling
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISRA	Information Security Risk Assessment
ISRM	Information Security Risk Management
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria

JSA	Junior Security Analyst
LEF	Loss Event Frequency
MVaR	Malware Value-at-Risk
OCTAVE	Operationally Critical Threat, Asset, Vulnerability Evaluation
OECD	Organization for Economic Co-operation and Development
PLM	Probable Loss Magnitude
PII	Personally Identifiable Information
RA	Risk Assessment
RMI	Risk Management Insight
SEI	Software Engineering Institute
SLE	Single Loss Expectancy
SR	Systematic Review
SSA	Senior Security Analyst
TOE	Target of Evaluation
TCSEC	Trusted Computer System Evaluation Criteria
TDSC	Transactions on Dependable and Secure Computing
VaR	Value at Risk
MLE	Maximum Likelihood Estimate

Chapter 1

Introduction

Information security risk assessment (ISRA) is a widely used method in industries which require keeping their information secure. In the information age, securing data is becoming a hot issue and moving from physical to electronic risk assessment [136]. Information exists everywhere and has a very close relationship to our life. Private and public sectors collect personal information and store this in the cloud. More and more individuals share their daily life on social networks such as Facebook, Instagram and WeChat. Therefore, the network and platform providers should maintain the security of all users' information. ISRA helps the providers to identify risks associated with information systems and implement the security controls by following the information security standards and regulations [29].

1.1 Research Questions

There are several reasons for organizations to make an ISRA. On the one hand, organizations want to avoid information risks like information leakage or unauthorised manipulation. On the other hand, they want to obtain external trust that they can protect the privacy of customers well. Most organizations commission a third party to implement ISRA, because they have no idea how to collect and deal with the data to satisfy the requirements of risk assessment professionally, or they have no such human resources to do it.

With the advent of cloud services and 'bring your own device' (BYOD), it is becoming increasing difficult for organizations to identify assets and thus carry out a risk assessment based on current established techniques. It may be useful then, to look at a new approach to ISRA. Thus, if we can provide a professional and systematic tool to collect and analyse risk assessment data, then many companies can assess their in-

formation security risks professionally by using the device. The companies know more details about their own information systems better than a third party and can assess information security risks thoroughly by themselves. Therefore, there is an interest about what are risk assessment data and how to provide a professional and systematic tool to help organizations manage the assessment data in a practical risk assessment of information security. By reviewing the literature on the risk assessment development in information security, we find that researchers prefer to study the theoretical methods of risk assessment. They know the importance of data management in risk assessment, but fewer authors provide efficient methodologies to manage data in a practical implement project.

It is difficult to automatically assess information security risks in some assessment software systems by using the current risk analysis methods. Because these methods significantly focus on the general threats, and are not to be proposed for certain relevant type of threats. In fact, different quantitative, qualitative or hybrid risk analysis models require different information as the input data in this software. For instance, Chang and Lee use the information of threat or vulnerability levels and the related the values of CIA (Confidentiality, Integrity, Availability) to obtain risk scores [35]. Khanmohammadi considers the weight of the process and control effect on a vulnerability in the process-based risk analysis model [89]. Lo and Chen pay attention to the interrelations among security control areas in the hybrid model of risk analysis [107].

Furthermore, most of these approaches consider the impacts of threats as three ranks such as high, medium and low, and then assign scale scores to these three levels such as 5 representing a high impact and 1 representing a weak effect. But there are no standards of setting these scores. For instance, we do not know that why five presents the high impact. Why we do not use 4 to express highest risks. Or 5 could equally represent a low impact and 1 denotes a high impact. The likelihood is another vital parameter for assessing risk. And frequency is an essential factor when calculating the probability. To the best of our knowledge, it is hard to obtain the data of frequency for some threats such as insider threats. But some approaches to risk analysis do not consider this real problem. In the extreme case where likelihood cannot be computed due to the lack of frequency data for specific threats. This could lead to an incomplete ISRA. Therefore, a risk analysis model could focus on a particular type of information security risks such as cyber threats. The cyber threats could be insider threats, threats from malware, or threats from external attacks.

The systematic review of ISRA, presented in chapter 3, illustrates that risk analysis is a relevant research field. ISRA method is made up of three categories: quantitative, qualitative and synthetic. A quantitative approach constructs complex mathematical

models to obtain more accurate results, but it is not easy to collect the historical data to support the models [99]. With a qualitative method, it is easy to assemble the data by experts' opinions or questionnaires but it is too subjective [99]. Additionally, with the qualitative approach, it is complicated to assess the risks frequently(daily/weekly) and address the relative security controls in the light of updated risk scores. In other words, the nature of the qualitative method affects the daily information security risk assessment. The synthetic risk analysis methods can overcome the limitations of traditional quantitative and qualitative approaches by applying the fuzzy and AHP theory [128]. AHP is a decision-making model including identifying, organizing and evaluating decision objectives [149].

Furthermore, most existing studies of risk analysis methods mainly focus on constructing hybrid models by the theories of fuzzy and AHP [128]. These hybrid models provide more accurate data like experts opinions for quantitative tools, and reduce the subjectivity of qualitative methods [40]. In other words, the hybrid approaches apply the experts opinions as input data and then assess the risk levels of all information security assets.

However, these hybrid approaches still have the shortcomings of traditional risk analysis methods. First, they are proposed to deal with general information security risks rather than specific threats. Second, the risk scores given by experts opinions are not intuitive for managers to understand the risk levels. According to ISO27001:27005, the risk level of an asset is scaled by 1 to 5 score and the higher score, the riskier level [5]. Finally, the total risk levels of all information security assets are presented by a summed score in a scale from 50 to 60. We haven't a clear picture of what is the real difference between 59 and 60 to an organisation. These scores are hard to compare among different companies due to the nature of subjectivity of experts' opinions. In fact, the comparison helps us to understand which company has better information security protection under some constraints such as the same firm size and type.

Given that current ISRA standards are difficult to implement in practice, can we find a new approach to ISRA? Therefore, our primary research question is

Can we map a risk model from finance to a certain type of information security risk when the traditional ISRA methods are not always valid, and relative data of risks are not clear?

This big research question can be divided into the following sub-questions:

1. Can we apply a financial risk model to routinely assess particular type of information security risks such as cyber threats under assumptions and limited data?

2. Can the results of such a model be compared between different companies?

To answer the research questions, we focus on the features of cyber threats and construct a suitable approach which is based on a financial risk model Value-at-Risk (VaR). In fact, the application of VaR in ISRA is proposed to make available comparisons among companies. VaR is a classical financial risk model, which computes the worst loss over a target time horizon [85]. In 2001, VaR was applied first in ISRA by Jee and Jaisingh [80]. The ISRA VaR method evaluates the risk levels of attacked information assets by the worst loss instead of a simple summed score. Jee and Jaisingh take the logs of unauthorised external access as the input data of estimating the likelihood of threats [80]. However, their studies have not mentioned the details about how to connect the likelihood with VaR calculation.

Until 2013, Raugas et al. [141] provided the detailed model for cyber threats called CyberVaR. CyberVaR is an improved ISRA VaR model, which focuses on cyber threats. It analyses the risk level of information assets such as intellectual property by the theory of dynamic Bayesian network and attack tree. Whereas, the CyberVaR model can't be compared well between different companies due to various values of the same asset. For example, personal information has the higher sensitivity for a bank and will be assigned a higher value which is compared with that of a supermarket.

MVaR (Malware value-at-risk) is a new model we propose that can be used to analyse malware attacks from the standpoint of portfolio VaR theory. It is also an improved CyberVaR model. The portfolio VaR is "constructed from a combination of the risks of underlying securities" [85]. In financial risk management, the securities could be the stocks or options which consist of financial derivatives. The computers, and the data held on them, are analogous to the underlying securities and a company consists of all computers is the portfolio in the MVaR model. Thus, the MVaR model assesses the worst loss of computers in a company portfolio due to the risk of malware.

The reason to model a computer as a stock is that their values may have a more significant change during a particular period. For example, the stock prices fluctuate with the effect of financial risks in the trading session. Likewise, the values of attack targets (company computers) may vary in the working hours due to the active malware attacks and the data stored on the computer in that period [129]. It is possible to calculate the successfully attacked loss of each computer under a fixed successful attack rate and loss rate for a specific threat. Thus, we can deduce the mean and variance of each loss. Hence, all the losses are assumed as a sequence of independent random variables and have finite mean and finite positive variance. Based on this assumption, we can deduce the quantile of the total loss by the central limit theorem. Hence, such quantile is the VaR that we want to find out for a company portfolio.

Moreover, the MVaR model discusses the worst loss of cyber threats from a portfolio

standpoint, and it is more understandable for managers compared with CyberVaR. In practice, a computer is often the direct target for the cyber attacks, but it is also feasible to value the data in a network. Determining the data value of computers allows us to arrange the defence source in a more suitable strategy. For instance, the machines of finance department will focus on the payment login more frequently than the other units. In that case, we may allocate more ID authentication sources or strengthen the ID security mechanisms to the computers of this department.

Overall, the most important reason for applying the concept of the financial VaR to ISRA is that the ISRA VaR model provides a monetary figure which is easy to understand the consequences of cyber attacks for the managers. Thus, managers can decide whether increasing the security investments such as buying new cyber insurance or improving the defence systems.

1.2 Layout of the Thesis

The thesis consists of 7 chapters, and the content of each section is described as follows.

Chapter 1 In this chapter, we have described the importance of ISRA for all kinds of companies, and the research questions and the motivation of this study.

Chapter 2 This chapter makes a brief introduction to the fundamental concepts of information security and information security risk management (ISRM). It also introduces ISRM standards including ISO family and Common Criteria. Additionally, the chapter describes the relationship between risk assessment (RA) and ISRA and four commonly used ISRA standards. It compares the advantages and disadvantages of the standards. The comparison provides a basis for designing the data management system. The chapter also discusses the detailed process of data management in ISRA, including data collection, data analysis and data verification. These three steps of data management are the one-to-one relationship with the actions of ISRA.

Chapter 3 This chapter applies a systematic review method to study the state of the art in ISRA. The systematic review provides a classification framework for research studies over the past ten years (2004-2014). The framework classifies the current studies of ISRA into several parts in academic literature. The classification assists researchers to understand the state of art of ISRA and find out the entry points for academic research.

Chapter 4 In this chapter, we analyse the time patterns of malware infections by circular statistics. The analysis provides a visual overview of daily and weekly variations, which assist decision makers to allocate resources or estimate the cost of system monitoring during high-risk periods.

Chapter 5 This chapter presents the background of VaR and its evolution in ISRA. It also introduces one of its applications in ISRA called CyberVaR. CyberVaR builds on Bayesian Dynamic Network and attack three. The chapter also discusses the loss categories of cybercrime for a company. The loss can be divided into a direct loss, indirect loss and defence cost.

Chapter 6 In this chapter, we construct an MVaR model, which aims at assessing the worst loss due to malware attacks from the standpoint of the portfolio VaR theory. In simple terms, the MVaR model treats each computer as a stock and a company as a portfolio and then assesses the worst loss to this company portfolio when the machines are attacked by malware. The MVaR model assumes that the malware attack follows a Poisson distribution and the computers are attacked independently. Hence, the losses caused by each attacked machine are independent and summed to the total loss of the company portfolio. The final goal of the MVaR model is to assess the worst loss with a certain confidence level over a fixed time horizon. For example, there is 95% probability that the loss of the company will not exceed MVaR over ten days.

Chapter 7 This chapter concludes all the results, presents the main contributions and discuss the future research directions. The systemic review of ISRA is the first contribution which assists researchers to have a complete knowledge of ISRA. The thesis further applies the method of circular statistics to study the time patterns of malware. The analysis of the time patterns of malware provides the innovation of a new ISRA VaR model. Hence, the MVaR model is the third contribution we have made in this study. The MVaR model assesses the losses of cyber threats from the standpoint of the portfolio VaR theory.

1.3 Publications

This thesis is partly based on the following publications:

1. L.Pan and A.Tomlinson. A systematic review of information security risk assessment. International Journal of Safety and Security Engineering, 6(2):270281,2016.

   This paper is based on the work presented in chapter 3.

2. L.Pan, A.Tomlinson, and A.A.Koloydenko. Time pattern analysis of malware by circular statistics. In Proceedings of the Symposium on Architectures for Networking and Communications Systems, pages 119130.IEEE Press, 2017.

   This paper is based on the work presented in chapter 4.

3. L.Pan and A.Tomlinson. Risk Assessment in Information Security - An Alternative Approach. Information Security Magazine, 20 Nov 2017.

This article is based on the chapter 2.

4. L.Pan and A.Tomlinson. Malware Value-at-Risk (MVaR). (Submitted to WEIS [1] 2018).

   This paper is based on the contents of chapter 6.

1.4 Main Contributions

There are three primary contributions in this thesis.

1. We present a thorough and systematic review of ISRA research and provide a taxonomy of approaches to the problem. This systematic review provides us the research emphasis in the field of ISRA.

2. The first time we analyse the time pattern variance of malware around a 24-hour circle by circular statistics. The time pattern analysis reveals the feature of non-uniformity distribution of malware attacks. This feature is very important for constructing a financial quantitative risk model.

3. We constructed a novel 'Malware' VaR model to estimate the worst case financial loss due to malware based data exfiltration from an organisation. It is the first time to apply a portfolio VaR theory at a risk analysis of cyber security.

[1] The Workshop on the Economics of Information Security

Chapter 2

Background

This chapter begins at the introduction of information security, followed by the discussion of the relevant standards of ISRA. Information security is indeed an essential subject in all walks of life and any country. There are many ways to keep information safe, including encryption, malware detection, ID authorisation, risk management and so on. Notably, ISRA is the core part of information security risk management (ISRM) and a systematic tool to secure the whole information systems. Information security risks are various and difficult to identify without systematic methods. In this case, ISRA provides the approach to identify the risks efficiently and avoid risky behaviours. Furthermore, ISRA translates information security risks into transparent reports which help related managers mitigate these risks [29].

2.1 Information Security (IS)

Information can be private, public, sensitive, internal and external. In the information age, more and more organizations or individuals achieve their goals by big data. However, the insecurities of information contain leaking, tampering or stealing information by illegal use or unauthorized access. It is universally accepted that these insecurities are information security risks. Hence, some questions of information security may arise as follows:

- How do we assess these risks that are at the accepted or unaccepted level?
- How do we identify the types of risks that exist in the organizational or individual information system?

ISRA could be an answer to solve these problems with systematic methods. Before going to ISRA, it is necessary to discuss the content of information security. Risk assessment has been applied to many subjects, but information security is an extraordinary

field. In the era of big data, information security is required in various industries. And information security risks are unique due to their universality and complexity. Therefore, when information security becomes an independent field, it is not easy to measure its risks. That means an accurate understanding of information security benefits ISRA. We start with the evolution of IS definition in the early studies.

In 1984, IBM data security support programs proposed a definition of information security: "The protection of information assets form accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information" [1]. In 1991, Information Technology Security Evaluation Criteria (ITSEC) mentioned that "Information Technology (IT) security means confidentiality-prevention of the unauthorised disclosure of information; integrity-prevention of the unauthorised modification of information; availability-prevention of the unauthorised withholding of information" [79]. In 2005, ISO 27002 defines it as "the preservation of the confidentiality, integrity and availability of information" [173].

Compared with all definitions above, we could conclude that information security is to keep information confidential, integrate and available, and minimise its risks by various measures. Moreover, these definitions of different standards illustrate the application of information security could follow specific criteria to gain a united international agreement for organizations of different countries [72].

With the development of the Internet and the increments of cyber attacks, the term of information security is often entitled to cybersecurity [173]. In fact, they are not very analogous in definition and ranges of application. Cybersecurity is defined by the International Telecommunications Union as "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" [173]. Solms and Niekerk state that cybersecurity protects not only the information assets but also the non-information assets such as humans [173].

2.2 ISRM Standards

Information security has a vital effect on protecting the information of organizations and individuals. They expect to keep safe and private for their information held by IT products or systems. However, it is impossible to guarantee 100% security of information for any IT product or system. Thus, a series of standards ensure an appropriate level of security. According to Siponen and Willison, organizations apply information security risk management (ISRM) standards to certify the security of business practices

and obtain an international authorisation for their products and practices [162]. So far, there have been many developed risk management standards of information security. This section will make a brief introduction about two primary ISRM guidelines: the ISO 27000 family and Common Criteria (CC).

ISO 27000 family is the popular and best known international ISRM standards in managing information security risks and implementing the related security controls [41]. Siponen and Willison propose that "the Common Criteria has been used primarily for evaluating security properties of IT products" [162]. Therefore, we will demonstrate these two common standards, and compare them with the scope of application and contents of assets, threats and vulnerabilities.

2.2.1 The Evolution of ISO 27000 family

ISO 27001 and ISO 27002 are two critical standards in ISO 27000 family. They are dated from BS 7799. BS7799 was "Code of Practice for Information Security Management" and published by the UK Government's Department of Trade and Industry in 1995 [3]. It consisted of three parts. Part 1 was revised in 1998, adopted as ISO 17799 in 2000 by International Organization for Standardization (ISO) and incorporated as ISO 27002 in 2007. The emphasis of BS7799 Part 1 was a code of practice in Information Technology. BS7799 Part 2 was published in 1999 and adopted by ISO as ISO 27001 in 2005. Part 2 was well known as the "Plan-Do-Check-Act" process, which focuses on guidance for use in ISMS. BS7799 Part 3 was published in 2005. Figure 2.2 describes the time line of ISO 27000 family. Figure 2.1 depicts the evolutions and relationships between BS7799 and ISO 27001/2. ISO 27001 shows the process of information security management systems (ISMS), and ISO 27002 provides the guides for security management controls in ISMS.

BS 7799 and its derivatives focus on securing information systems and certifications of these standards [162]. Broderick describes that BS 7799 is "the first widely adopted management standard that was developed purely for the information security world" [31]. In addition to ISO 27001 and ISO 27002, the other ISO 27000 standards play a significant role in managing information security. For example, ISO 27005 focuses on ISRM and its related instructions of the ISRA process.

Figure 2.2 demonstrated that ISO 27005 was published in 2008 and revised in 2011. The revision of ISO 27005:2011 correlates with two vital standards of IT security managements including ISO TR 13335-3:1998 and ISO TR 13335-4:2000 [74]. ISO 27005 is a critical standard for assessing information security risks. It has a very close relationship to the other ISO 27000 members such as ISO 27001. In reality, ISO 27001 defines the ISMS about the content and extent [74]. Figure 2.3 reveals that the ISMS

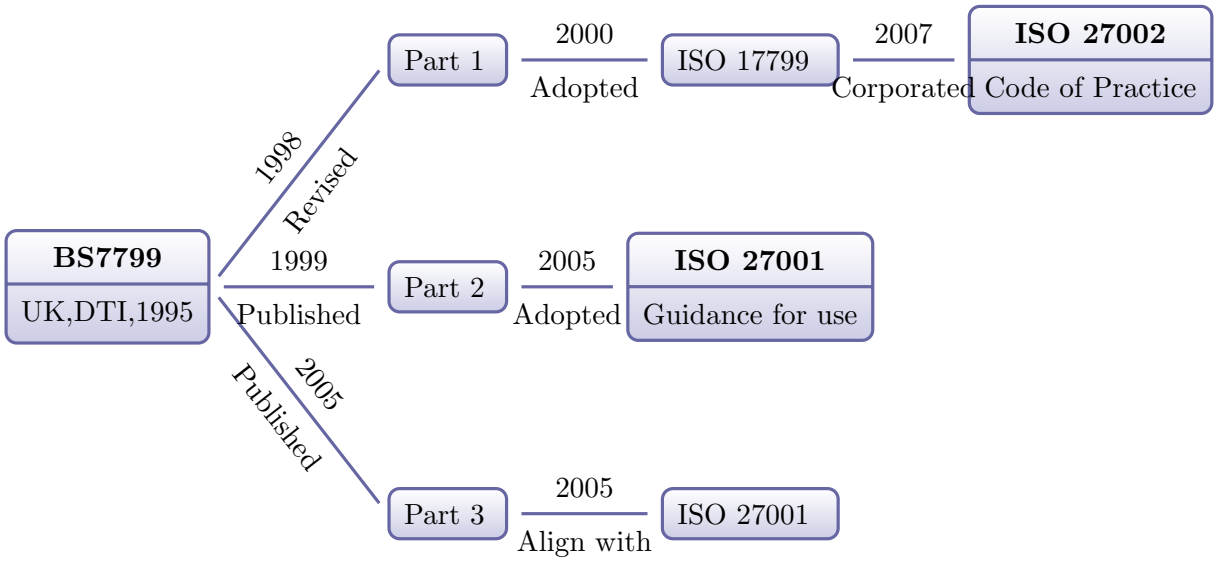


Figure 2.1: Evolution of ISO 27000 family Standards

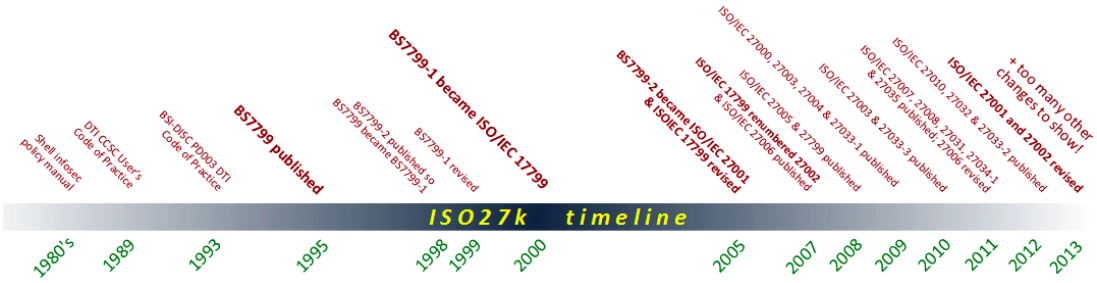


Figure 2.2: Timeline of ISO 27000 family [78]

process correlate with ISRM.

2.2.2 The Evolution of Common Criteria

The security objectives like asset, threat and vulnerability have very close relationships in ISMS. The vulnerabilities expose the value of assets and lead to the risk increases of information systems [51]. Farn et al. state that CC provides functional requirements to the security objectives and protects the ISMS by these requirements [51].

Common Criteria also called ISO 15408 is an international standard and composed of three guidances: ITSEC [1], CTCPEC [2] and TCSEC [3]. ITSEC is an European stan-

[1]ITSEC: Information Technology Security Evaluation Criteria
[2]CTCPEC: Canadian Trusted Computer Product Evaluation Criteria
[3]TCSEC: Trusted Computer System Evaluation Criteria

ISMS Process	Information Security Risk Management Process
Plan	Context Establishment (7) Risk Assessment (8) Risk Treatment Planning (9) Risk Acceptance (10)
Do	Implementation Plan of Risk Treatment (9)
Check	Continuing Risk Monitoring and Reviewing (11)
Act	Maintaining and Improving Information Security Risk Management Process (12)
Notes: a) (*n*) is a session number of ISO/IEC 27005:2011(E). b) Risk treatment implementations are not regulated in ISO/IEC 27005: 2011(E).	

Figure 2.3: Relationship between ISRM and ISMS [74]

dard which unifies two UK approaches of Green Book and CESG [4]. CTCPEC was a Canadian standard and published in 1993. TCSEC was released by the United States Department of Defence and commonly known as 'Orange Book' in the 1980s. We examine their relationships in Figure 2.4.

'Orange Book' is an important part of CC to provide the guidelines in keeping the computer system safe. The concept of 'Orange Book' comes from three earlier reports including 'Ware Report', 'RAND Report R-609' and 'Anderson report' [12, 175, 176], which provide the security models of computer systems. In the early time of computer development, the security of computer systems did not cause a great concern until the 1960s. At that time, the US military/government realised not only one user would use the computer after "the emergence of time sharing". Time sharing is a new way operating to allow users to interact with a computer at the same time without waiting [170]. With a time-sharing system, the other users might be malicious like overwriting another user's computer code or data [170]. Thus, the US military/government encouraged more academic research about computer system security.

'Ware Report' [5] was a relatively early paper to propose security controls. Security controls are "micro technical methods for avoiding risks and protecting information safe" [6]. Ware points out the necessity of identifying major threats due to the emergence of time-sharing system [170]. Hence, the threats Ware identified still existed in the computer systems such as assess controls to files, unauthorised copying of files

[4]CESG (Communications-Electronics Security Group) is national technical authority for information assurance of the UK government. https://www.gov.uk/government/organisations/cesg

[5]Security and Privacy in Computer Systems, came up in 1967 by Wills Ware [175]

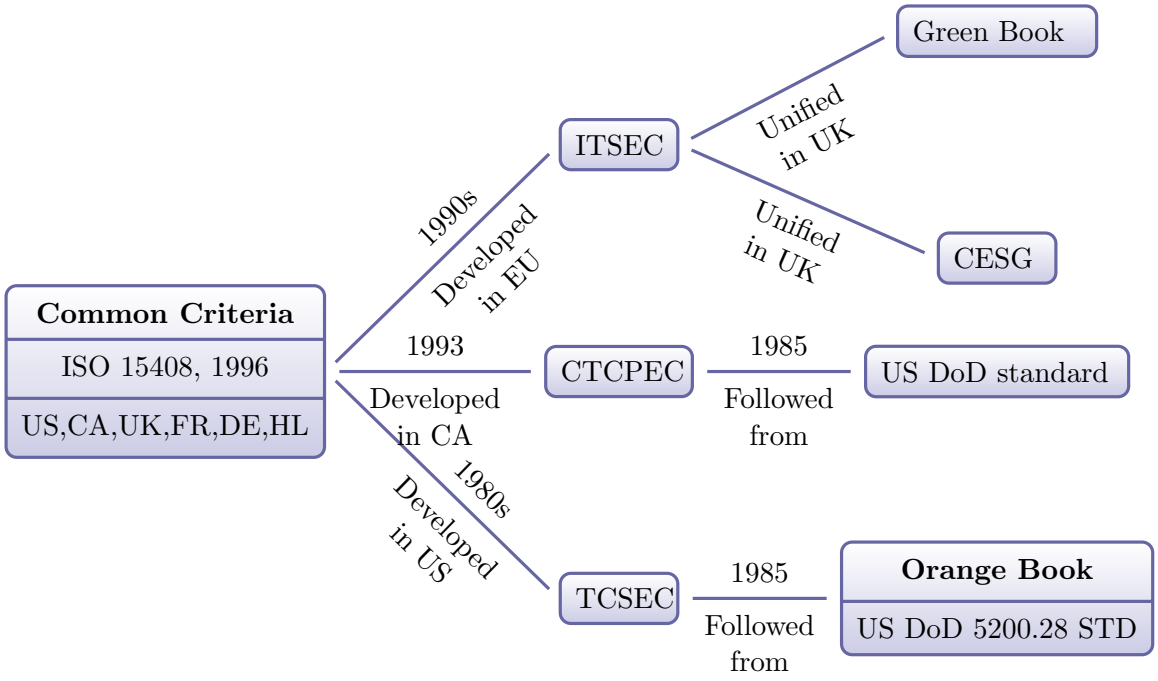


Figure 2.4: Evolution of Common Criteria

[170]. RAND Report R-609 is a report to discuss security requirements or controls in resource-sharing computer systems [176]. These documents published in the 1970s provide the basis to the current ISRA standards. However, Ware report and RAND Report R-609 did not provide a formal and complete security models for computer systems. "Without a model, it is difficult/impossible to translate security requirements into technical specifications" [170]. 'Anderson report' provides the guides for designing the security models [12, 170]. Overall, these reports present identification and security controls to risks, and the relative vulnerabilities of computer systems.

The evolution of the ISO family and Common Criteria could help understand ISRM standards. ISRM guidelines help organisations achieve the international security authorisation for their information systems. However, current management standards still have some unavoidable problems. For instance, the management scopes are too generic due to the uniqueness of organisations in different countries. Organizations have to tailor the guidelines to fit their circumstances [162]. Additionally, the instructions appeal to common practice and are not validated by some rigorous steps [162]. ALL in all, many existing standards cannot be unified. In this case, we could use the similarity and allow the existence of differences of these standards when applying them.

2.2.3 Discussion

'Ware Report', 'RAND Report R-609' and 'Anderson report' are the initial standards for the security of computer systems. When these reports were published, computers were stand-alone mainframes and often kept in rooms guarded by soldiers. With the advent of the Internet, and more recently BYOD [6] and cloud services, the models of the 1970s break down. It is no longer a simple exercise to identify all an organisations' assets, and determine who has accessed to the assets where data might be stored. Consequently, this raises some questions about whether the existing standards are fit for the purpose and whether it is time now to look for an alternative approach to ISRA.

Information security is a big topic with different definitions from various standards. These definitions show the similar meanings that information security minimises the risks and keeps confidentiality, integrity and availability of information by certain technical methods and guidelines. So far, many approaches have been applied to secure data such as encryption, ID authorisation, malware removal and network trust mechanism. These specific techniques protect information from a micro level, while some international standards and policies secure information from a macro view.

It is not our goal to study all ISRM standards, but we focus on the most accepted ones. Thus, we have an overview of two well known guidelines of ISO 27000 family and Common Criteria and compare them. In order to study ISRM well, we only foucs the most important part of ISRM, named ISRA [6]. In the discussion of ISRM standards, we find that ISO 27005 of the ISO family has a clear picture of ISRA. In the later section, we make a further study of ISRA standards including ISO 27005.

2.3 Information Security Risk Assessment (ISRA)

We have discussed two popular ISRM standards in the last section. ISRA, as the most critical process of ISRM, is becoming more and more importance for organizations in an information age. ISRA standards are helpful to guide the institutions to assess information security risks systematically. More and more agencies are required to follow the international ISRA standards to evaluate their information systems. In order to understand the ISRA and its standards, we choose four commonly and widely used frames including OCTAVE, FAIR, ISO 27005 and NIST SP800-30. This section introduces the relationship between risk assessment (RA) and ISRA. We further discusses these four standards and compares their strengths and weaknesses respectively.

[6] Bring Your Own Device

2.3.1 RA and ISRA

Risk assessment is a critical systematic method of analysing risks and applied initially been in nuclear and aeronautical systems [136]. Now it has been involved in many industries such as finance, transportation, power system, workplace, public health, shipping and fish industries. Risk assessment is defined as "a systematic methodology for analysing a system" and tries to answer three questions [136]:

1. What can go wrong?
2. How likely is it?
3. How serious are the consequences?

However, it is not distinct to say risk assessment because it has different roles in different industries or subjects. For instance, system adequacy and system security are two primary tasks in power system risk assessment [104]. Enterprise risk assessment is "a systematic process for identifying and evaluating events that could affect the achievement of objectives, positively or negatively" [137]. According to ISO 27005:2011, information security risk assessment (ISRA) is defined as "the overall process of risk identification, risk analysis and risk evaluation" [8]. ISRA can identify the prime information security risks and help an organization understand these significant risks to business operation, and then avoid risky behaviour [29].

ISRA standards provide an efficient and systematic process to assess information security risks. Different standards have different requirements to ISRA. These provisions have respective merits and demerits.

2.3.2 Standards of ISRA

Before starting the introduction, it is necessary to point out some essential terms of ISRA. All these relevant standards are talking about information security risks rather than the other types of risks. So what is information security risks? ISO 27005:2008 defines information security risk as "a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation" [6]. The information security risk has a close relationship with likelihood and impact. Likelihood is defined as "chance of something happening", and impact is "adverse change to the level of business objectives achieved" [6, 7].

OCTAVE (Operationally Critical Threat, Asset, Vulnerability Evaluation) is a risk-based and self-directed assessment framework. SEI (Software Engineering Institute) of Carnegie Mellon developed OCTAVE by the CERT program in 2003. Organizations would like to apply OCTAVE to implement ISRA due to its flexibility. OCTAVE has

very detailed steps about the process of risk assessment. However, these steps are complicated to follow in a daily risk assessment and some small projects [166]. The computation of risk in OCTAVE is equal to threat plus impact [166]. This calculation is not explicit to compute the most critical factor likelihood when obtaining risk scores.

FAIR (Factor Analysis of Information Risk) pays high attention to the methods of risk calculation. RMI (Risk Management Insight) developed FAIR to analyse and manage information security risks in 2005 [84]. The Open Group and ISACA (Information Systems Audit and Control Association) group highly recommend it owning to the attention of objectivity [166]. However, FAIR is difficult to assess risk levels if there is no objective data concerning a loss degree [166]. FAIR does not provide a detailed threat or vulnerability catalogue. Without a threat catalogue, the assessment term is hard to identify risks objectively and completely. Moreover, an asset is a vital term for ISRA. FAIR defines an asset as "any data, device, or other components of the environment that supports information-related activities, and which can be affected in a manner that results in loss" [84].

NIST SP800-30 (Risk Management Guide for Information Technology Systems) is a flexible and widely used framework. In 2002, the US Federal Government developed SP800-30 as a high-level risk management document. It is widely adopted by federal, local government and organisations, especially FISMA or HIPAA, to conduct their risk assessment processes [166]. NISP SP800-39 provides the definition of RA for SP800-30 as "the process of identifying risks to organisational operations (including mission, functions, image, reputation), corporate assets, individuals, other organisations, and the Nation, resulting from the operation of an information system" [9]. There are nine steps for the risk assessment of SP800-30 such as threat and vulnerability identification, likelihood determination, control and impact analysis and so on. Furthermore, SP800-30 provides a checklist to identify threat sources and related vulnerabilities. In this list, a threat is divided into three types: natural, human and environmental. Additionally, SP800-30 highlights that it is vital to conduct threat-vulnerability pair matrix after identifying threats. Then, SP800-30 calculates the level of risks by impact times likelihood. In the calculations, likelihood and impact are scaled into three levels: high, medium and low and relevant scores are assigned to each level. For example, 5 indicates high impact and 1 presents low one, and vice versa.

ISO 27005 has two versions: ISO 27005:2008 and ISO 27005:2011. ISO 27005:2008 was developed in 2008 and revised in 2011. ISO 27005:2011 achieves a vast improvement in the contents of ISRA. These two versions are different in quoting definitions of the relevant terms of risk assessment. ISO 27005:2008 does not present explicitly about risk assessment, it just use the one defined in ISO 27000:2009. ISO 27000:2009

makes a brief introduction about information security management systems and related definitions for the ISO 27000 family of standards. It defines risk assessment as "overall process of risk analysis and risk evaluation" [8]. In practice, ISO Guide 73:2009 is a risk management vocabulary and provides a series of definitions on the terms of risk management. The definition used in ISO 27005:2011 is quoted from ISO Guide 73:2009. ISO 27005:2011 quotes risk assessment of ISO Guide 73:2009 as "overall process of risk identification, risk analysis and risk evaluation" [8]. This definition from ISO 27005:2011 is more explicit than that in ISO 27000:2009.

Risk identification is listed independently as the first and significant phase of ISRA. The process of ISRA can be implemented smoothly if the asset, threat and vulnerability are identified comprehensively. ISO27005:2011 states the detailed contents and the lists of assets, threats and vulnerability. Assets consist of primary assets and supporting assets, and the information is a part of prime assets. ISO 27005:2011 demonstrates that four methods of a vulnerability assessment are automated vulnerability scanning tool, security testing and evaluation, penetration testing and core review [8]. These four approaches collect and identify vulnerabilities by the interviews of people and users, questionnaires, physical inspection and document analysis. Likewise, ISO27005:2011 presents several qualitative methods for the risk analysis. Unfortunately, it does not mention the quantitative ways and has no specific or related measure methods for different risks. For risk evaluation, ISO 27005:2011 emphasises the risk evaluation criteria. However, fewer researchers are keen to study this direction [128].

In summary, ISO 27005 has been supported by the whole ISO 27000 family to secure the information systems. Additionally, the application of ISO 27005 has the consistency with the other ISO 27000 family members. In fact, ISO 27005 provides an explicit progress of the implementation of ISO 27001. Similarly, ISO 27001 and ISO 27002 support users to understand ISO 27005 easily and completely. Furthermore, the risk management documents of ISO such as ISO 31000:2009 and ISO 31010:2009, assist ISO 27005 in implementing the risk assessment. ISO 31000 is a risk management standard that manages risks by providing some principles and generic guidelines in any industry. However, ISO 31000 offers a general guidance for some audit programmes, but not for the certification purpose. In practice, it focuses on the selection of guidelines for risk assessment techniques.

2.3.3 Framework Comparisons

There are many different standpoints to compare ISRA standards. Shamala et al. compare and analyse six well-documented ISRA standards from the view of a conceptual framework [153]. Thus, we study four chosen frameworks from the view of contents

and approaches of risk analysis. We also display the comparison results in Figure 2.5.

Standards	ISO 27005	FAIR	NIST SP800-30	OCTAVE
Issued Time	2008	2005	2002	1999
Example lists of Threat & Vulnerability	YES	NO	YES	NO
Risk Assessment Definition	YES (Explicit)	NO	YES (Not Concise)	NO
Steps/Phases	3 (Easy Followed)	4 (More Conceptual)	9 (Complexity Not Concise)	3 (Complexity Self-directed)
Formula of Risk Computation	Risk = Consequence × Likelihood	LEF (Loss Event Frequency) & PLM (Probable Loss Magnitude)	Risk = Impact × Likelihood	Risk= Threat (Condition) + Impact (Consequence)
Consistency with anther same series standards	YES	NO	YES	YES
Implement In shorter/daily RA	Difficult	Difficult	Difficult	Difficult
Preferable Approach of RA	Qualitative and Quantitative	Quantitative	Qualitative and Quantitative	Qualitative
Organization (Used by)	Following security requirement of ISO27001	Any	Any	Large (300 employees or more)

Figure 2.5: Comparisons of ISRA Standards

Figure 2.5 shows that OCTAVE is the earliest standard, and ISO 27005 is the latest version. Once the old standards cannot satisfy the requirements of information security, then the new one will be developed to fulfil the new requirements. FAIR and OCTAVE do not mention an explicit definition of risk assessment in the field of information security. NIST SP800-30 defines ISRA as "the process of identifying risks to organisational operations (including mission, functions, image, reputation), corporate assets, individuals, other organisations, and the Nation, resulting from the operation of an information system" [9]. Whereas, the ISRA definition from NIST SP800-30 is not concise compared with that of ISO 27005. ISO 27005 provides the digestible ISRA concept and the easy-to-follow steps.

ISO 27005 and NISP SP800-30 provide the example lists of typical threats and

Framework	ISO 27005	FAIR	NIST SP800-30	OCTAVE
Definition of ISRA	Overall process of risk identification risk analysis and risk evaluation	NO	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system	NO
Phases	1. Risk Identification 2. Risk Analysis 3. Risk Evaluation	1. Identify scenario components 2. Evaluate LEF 3. Evaluate LPM 4. Derive and articulate Risk	1. System Characterization 2. Threat Identification 3. Vulnerability Identification 4. Control Analysis 5. Likelihood Determination 6. Impact Analysis 7. Risk Determination 8. Control Recommendations 9. Results documentation	1. Build Asset-Based Threat Profiles 2. Identify Infrastructure Vulnerabilities 3. Develop Security Strategy and Plans

Figure 2.6: Definitions and Phases of Four ISRA Frameworks

vulnerabilities, whereas FAIR and OCTVAE do not. Furthermore, NISP SP800-30 offers a list for identifying threats and vulnerabilities, and ISO 27005 provides the more detailed tables for categorising threats and relevant vulnerabilities. Figure 2.6 further describes the differences between each frame in the definition and phases of ISRA. For the stages of risk assessment, NIST SP800-30 has nine steps, but they are a little complicated to follow up. OCTAVE and ISO 27005 have three aspects to implement ISRA, through the steps of OCTAVE are self-directed and not easily observed.

Additionally, the formulas of risk computation in these standards are slightly different, particularly in FAIR. FAIR calculates the risk by Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM). LEF is "the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset" [84]. The magnitude of loss could be severe, high, significant, moderate, low and very low [84]. The ranges of loss could be assigned to each magnitude. For example, the severe magnitude is set up if the loss exceeds $10,000,000 [84].

ISO 27005 and NIST SP800-30 develop both qualitative and quantitative approaches for assessing information security risks. OCTAVE prefers to use qualitative approach due to self-directed process, while FAIR devotes itself to quantitative methods. In fact, Fair focuses on the risk analysis methods, not the improvement of the whole ISRA framework. Fair provides very detailed calculation ways of risk analysis.

From the comparison, we find that OCTAVE is more suitable for larger organisa-

tions like a scale of employees larger than 300 or more. NIST SP800-30 and FAIR are available for any size of organisations. ISO 27005 is chosen by the companies which have followed the ISO 27000 family. Likewise, NIST SP800-30 keeps the continuous relationship with its NISP families such as NISP SP800-37 and NIST SP800-39. OCTAVE develops OCTAVE-S and OCTAVE-Allegro for different scales of organisations. FAIR has no itself series as complementary standards.

To sum up, although these four frameworks have their respective benefits and drawbacks, there is a common problem that they are difficult to run a shorter or daily assessment. In reality, it is hard to monitor the new risks and patch the vulnerabilities in time an organisation. This problem tries to be solved by the privilege of information system managers. Nevertheless, it is not suitable to set up exorbitant privilege to a particular manager. Thus, We can only assign managers the access rights to the relevant datasets and assessment results. Then the information system can remind other managers and assessors the updates automatically.

Moreover, the comparison indicates the ISRA processes of ISO 27005 and NIST SP800-30 are more comprehensive, while FAIR and OCTAVE concentrate on the methodologies of risk analysis. ISO 27005 states an explicit definition of ISRA and provides the detailed catalogues of threats and vulnerabilities. The whole process of ISRA in ISO 27005 is more accessible to follow compared with NIST SP800-30. Hence, ISO 27005 has the close relationships with other members of ISO 27000 families which are also used widely in international organisations. Across all the findings, ISO 27005 is deemed to the best one in these frameworks and the basis of this thesis.

2.4 Data and ISRA

One of the hottest research issues in information security is that risk factors cannot be evaluated accurately due to the lack of real-world data [18]. To the best of our knowledge, data plays a vital role in all kinds of risk analysis. Without data, even if the analytical method is perfect, ISRA cannot run successfully.

What is data? Ten persons or even a hundred will provide different ones due to their perspectives. Data is used everywhere and has many descriptions in various subjects. Tricker describes data “can be hard - that is precise, verifiable, often quantitative; or soft - that is involving judgemental, often qualitative assessments” [171]. OECD [7] guidelines state that data is “a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means” [2].

[7] OECD: Organization for Economic Co-operation and Development

Information is another term we often talked. What is the relationship between data and information? Triker mentions that "Information is a function of data available, the user of that data, and the specific situation in which it is used" [171]. OECD guidelines describe information as "the meaning assigned to data using conventions applied to that data" [2]. For instance, if we consider data as every brick of LEGO, then information is the different LEGO models by using these small pieces of data. Data is extracted to produce different information models. Therefore, we consider data as any text, number, description and symbols in the process of ISRA. Data is the basis of ISRA, and the quality of data determines the level of ISRA. Figure 2.7 exhibits the relationship between data and ISRA. We produce information by processing data, and then information is used to provide decisions. These decisions like increasing the investment of security controls become the support of improving the security of information systems [54, 184].

Figure 2.7: Relationship between Data and Risk Assessment

Some classifications of data are helpful for the analysis of ISRA. For instance, data consists of training data and test data in an information system [59]. For IT security systems, data is divided into "expected threat frequency data, countermeasure-effectiveness data, threat-to-impact transitions data and data concerning the financial loss form the impacts" [18]. From the view of sensitivity, data could be confidential, internal, public and individual industry data [166]. Confidential data "should only be released on a need to know basis" [166]. Internal data is "openly shareable within the organization" [166]. If the information is "openly shareable with the public" [166], then it is public data.

Except for three types above, there is still some special classification as follows: PII (Personally Identifiable Information) and ePHI (Electronic Protected Health Information) [166]. Ebenezer highlights that public and internal data are the primary data source in the traditional information security risk assessment [48]. In practice, an appropriate category can help managers arrange the right security controls. Nevertheless, the diversity of the classifications of data for different systems or subjects remind us that it is essential to declare definition and classification of data, and then make a high qualitative assessment. This thesis will follow the data category of confidential,

internal, public and individual industry data [166]. We find this classification is more explicit and suitable to classify the organisational data in a risk assessment process.

2.4.1 Data and Risk Assessment tools

It is well-known that ISRA has to deal with a great deal of data. In this case, it is a challenge to implement the ISRA process without an automated assessment tool. To the best of our knowledge, some small institutions apply spreadsheets to collect the data and run an ISRA for their information systems. However, it is not easy if the worksheets are too many. Some companies have developed self-assessment automated tools for collecting ISRA data and assessing the risks. These tools are quantitative and qualitative, free or chargeable.

Behnia et al. [22] compare the tools of current risk assessment and show the results of qualitative approaches in Figure 2.8. They discuss five qualitative risk assessment tools as follows: OCTAVE, CORAS, CRAMM, FRAP and COBRA [22]. Likewise, Figure 2.9 shows the consequences of four quantitative methods including ISRAM, CORA, IS and RiskWatch. However, their study does not provide a sufficient analysis for decision-making. For example, they do not mention ways for choosing the suitable means to different types and sizes of organisations. Antoniou et al. supplement the weakness and add the popularity to each tool in certain countries [13].

Some ISRA researches consider to manage data by an automated tool [128]. However, these articles have not a explicit definition of data management. To a great extent, the reliability and availability of data could determine the results of risk analysis [29]. Compared with other types of risks, it is more challenging to assess information security risks due to the changeable risk factors and limited relevant data [29]. Therefore, data management is essential for the process of ISRA. Many risk assessment tools such as CRAMM, COBRA, RiskWatch can collect and analyse ISRA data, but they are not entirely meeting the demand of organisations due to their respective drawbacks.

CRITERIA	QUALITATIVE				
	OCTAVE	CORAS	CRAMM	FRAP	COBRA
Method/Tools	Method/Tools	Tools	Method/Tools	Tools	Tools
Method or Tool Name	OCTAVE v2.0, OCTAVE-S v1.0	Coras editor v.1.1	CCTA Risk Analysis and Management Method	FRAP	Cobra
Vendor Name	Carnegie Mellon University, SEI (Software Engineering Institute)	European Commission	Insight Consulting	Tom Peltier Auerbach Publications	C&A Systems Security
Country of Origin	USA	Intracom (Greece), Solinet (Germany), Telenor (Norway);	United Kingdom	Canada	United Kingdom
Date of First Release	Version 0.9, 1999	January 2001	1985	1993	90s
Official Web Site	http://www.cert.org/octave/osig.html	http://www2.nr.no/coras/	http://www.cramm.com	http://www.peltierassociates.com/frap.htm	http://www.riskworld.net
Languages	English	English	English, Dutch, Czech	English	English
Price	Free	Free	Unknown	Free	Full Cobra Suite: $1995 Cobra for ISO17799: $895
Compliance to IT Standards	N/A	ISO 31000 ISO/IEC 17799 AS/NZS 4360	ISO/IEC 17799	ISO 17799	ISO 17799 : COBRA ISO17799 Consultant : Checking compliance with the ISO 17799 security standard
Skills Needed	Standard	Standard	Specialist	Standard	Standard
Availability	Trial version available, Registration required	Trial version available, Registration required	Registration required	N/A	N/A
Tools Supporting the Method	Commercial tools -Licensed materials -Trainings (Sector with free availability: Educational Support, Awareness trainings)	-An XML mark-up for exchange of risk assessment data. -A UML based specification language targeting security risk assessment	Commercial tools -CRAMM expert (Insight) -CRAMM express (Insight)	Standard	Standard

Figure 2.8: Comparison framework for qualitative automated tools [22]

The powerful and comprehensive tools of CRAMM and RiskWatch are too expensive, although they have enough countermeasures of risk calculation and databases for security controls. The automated device of CORAS is free and meets the requirements of ISO 31000 and ISO 17799. CORA is a quantitative criterion and has an expensive tool named CORA 5.0. But CORA has no explicit IT standards to support corresponding risk analysis methods. Data management plays a vital role in the ISRA process.

For instance, if data collection is efficient, then the ISRA process can be implemented smoothly and quickly. Fewer studies are about data management which is vital for ISRA to obtain the database of interviews and surveys. The further discussion of data management is in Appendix B. In the future study, we could conduct a new system of data management to ISRA, which is free, qualitative and more available.

CRITERIA	Quantitative			
	ISRAM	CORA	IS	RiskWatch
Method/Tools	Method/Tools	Tools	Method/Tools	Tools
Method or Tool Name	ISRAM	CORA 5.0	IS Risk Analysis Based on a Business Model	RiskWatch for Information Systems & ISO 17799
Vendor Name	National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology	International Security Technology, Inc	Korea Advanced Institute of Science and Technology	RiskWatch
Country Of Origin	Turkey	New York	Seoul, Korea	United States
Date Of First Release	December 2003	1978	2002	N/A
Languages	English	English	English	English
Price	Free	$7,000 to $85,000	Free	$15.000 Educational discount: 25%
Compliance To IT Standards	NIST SP 800-30 ISO/IEC 17799 ISO/IEC 13335	N/A	N/A	- ISO 17799: Control standards included - US-NIST 800-26: Control standards included
Skills Needed	Standard	Standard	Standard	To use : On-line help
Availability	Open	Licensing organization without limit	Open	Online demonstration Registration required
Tools Supporting The Method	Key Risk Management Tools for Information	N/A	N/A	Online and telephone Support, Help, FAQ

Figure 2.9: Comparison framework for quantitative automated tools [22]

Chapter 3

A Systematic Review of ISRA

Many standards provide the guides for the process of risk assessment, particularly in the field of information security [128]. These different ISRA standards have various definitions of risk analysis, evaluation and assessment. As a result, researchers often confuse these terms and disciplines, which lead to further confusion within the community [128]. In this sense, it is essential to come to a common understanding of the processes and terminology to clarify research in this area. A conventional approach to this goal is to carry out a systematic literature review. This chapter takes a formal proposal for the systematic review based on the idea of the Cochrane Collaboration [1].

3.1 Motivation

In different standards, the definitions or descriptions of the ISRA process are not the same. For instance, SP800-30 Revision 1 illustrates that "risk assessment is the process of identifying, estimating, and prioritising information security risks" [123]. ISO 27001:2005 defines ISRA as "the overall process of risk analysis and risk evaluation" [5]. ISO 27005:2011 further describes it as "the overall process of risk identification, risk analysis and risk evaluation" [8]. In fact, chapter 2 has compared four frameworks of ISRA and summarised their respective advantages and disadvantages. Based on the comparison, it is clear that ISO 27005:2011 provides a more explicit framework and accurate definitions for each stage. Thus, 27005:2011 is considered as the reference guideline to defend the results of a systemic review of stakeholders and auditors.

Most ISRA researches propose abundant different processes, structures and methods [151]. The differences could cause some doubts for academic freshers. In this case, it is worth to synthesise the existing literature to find out state of the art of ISRA and

[1] "The Cochrane Collaboration is an international, independent, not-for-profit organisation" [131].

its study directions. We apply the methodology of a systematic review not only to summarise the related research of ISRA but also propose a classified framework of them. The classification framework can help researchers obtain a clear picture of ISRA in the academic sector. When an academic fresher has a basic understanding of ISRA, then he or she can seek out specific entry points on this subject. Also, organisations can benefit about the advanced ISRA methods by the review, and connect the organisational and academic level.

3.2 Systematic Review

Medicine and healthcare are the original subjects of applying for a systematic review. The Cochrane Collaboration produces such application methods as Cochrane Review [131]. Cochrane Reviews are the unique systematic reviews in healthcare and reflect the findings of updated studies [49]. However, a systematic review is applied not only to healthcare but also to other subjects for collecting the published literature data and assessing the current development trend of defined topics [10]. The particular research questions of an assigned subject can obtain the answers in a systematic review by as many relevant research papers as possible [49].

By contrast with systematic literature reviews, traditional literature reviews have a bias. For instance, the authors who apply for the general literature reviews prefer to intercept the beneficial parts of the novel. However, systematic reviews adopt explicit and transparent methodologies and a standard process to synthesise all existing research works [49, 91], and present an unbiased result. Furthermore, the results of systematic reviews are accountable, replicable and useful for users [49, 91]. We synthesise and analyses 80 papers over ten years (2004-2014) in the field of ISRA, and execute the review as follows:

1. design the specific research questions.
2. construct the literature search.
3. select the relevant literature by title, abstract and keywords.
4. extract and synthesise the data from relevant papers.
5. classify the data.
6. report the review results.

Figure 3.1 shows the process of a systematic review [101]. Meanwhile, the detailed searching steps are described in Figure 3.2, including research questions' identification, protocol review, data extraction and synthesis.

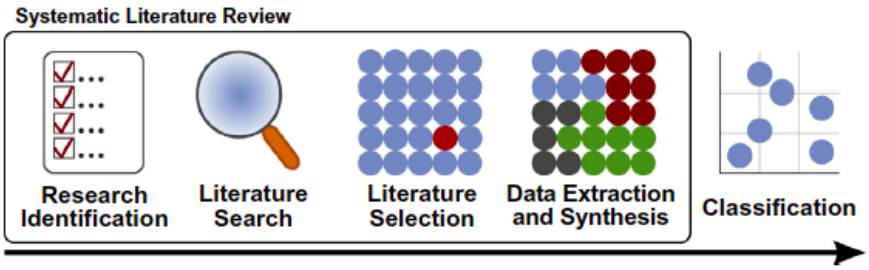


Figure 3.1: The Research Methodology of Systematic Review [101]

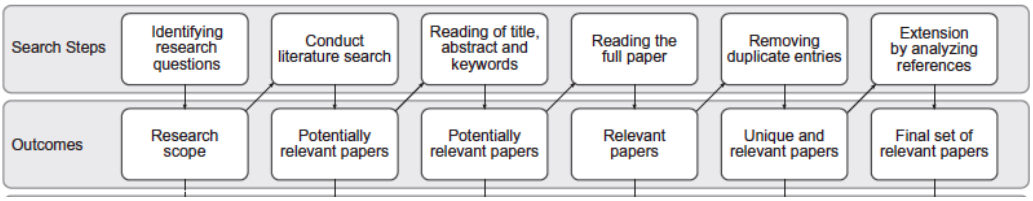


Figure 3.2: The Steps of Systematic Review [101]

3.2.1 Research Questions

By following the steps, we propose the research questions:

1. Which subjects are the main research direction of ISRA in the future?
2. What are the current research types?
3. What kinds of ISRA methods do researchers study?

3.2.2 Review Protocol

We select the papers from Google Scholar, ACM Digital Library, Science Direct, Web of Science, Wiley InterScience, DBLP, IEEE Digital Library, Springer Link and Elsevier. The related searching keywords contain information risk assessment, information security risk assessment, security risk assessment, and assessing the risk of information security. The review protocol also considers the publications between 2004 and 2014 due to limitations of reviewing time and human resources.

The next step after the literature search is to define the selection criteria of literature for answering the research questions better. The selection criteria are as follows.

1. Papers are published in English.

2. A paper title contains the similar meaning of risk assessment and at least one word of information security.
3. The paper should be downloaded for free.
4. A paper title mentions a research subject such as healthcare or cloud computing.
5. The paper specifies the method of risk analysis, risk identification or risk evaluation.

If a publication satisfies the chosen criteria above, it is selected to the systematic review. All papers are peer reviewed as they are collected from conferences and journals.

3.2.3 Data Extraction and Synthesis

The original search resulted in 107 research papers. According to the chosen criteria, 80 publications are the final dataset of the systematic review.

3.3 Review Results

This section will introduce the general statistical results of collecting ISRA literature and a classification framework of this literature. The analytical results will show the annual distributions of published papers over ten years and the types of application industries of ISRA.

3.3.1 General statistical description

Figure 3.3 describes that, of the 80 publications, 38 were from journals, 37 from conferences and five from symposia. In fact, these papers come from 78 different types of journals, conferences and seminars such as "Computer and Security" and TDSC [2] are on the list. The data sample is more convincing due to the diversity of paper collections. The limitation of this systematic review is without a paper from white papers and articles.

Figure 3.4 suggests that ISRA has begun to obtain more attention from 2010, and achieved a further development in 2013 and 2014.

Furthermore, the types of industries are becoming diversified and shown in Figure 3.5. These industries apply ISRA to reduce the leakage of information, including E-government [180], SCM (Supply Chain management) [148], E-healthcare [181],

[2]Transactions on Dependable and Secure Computing [82]

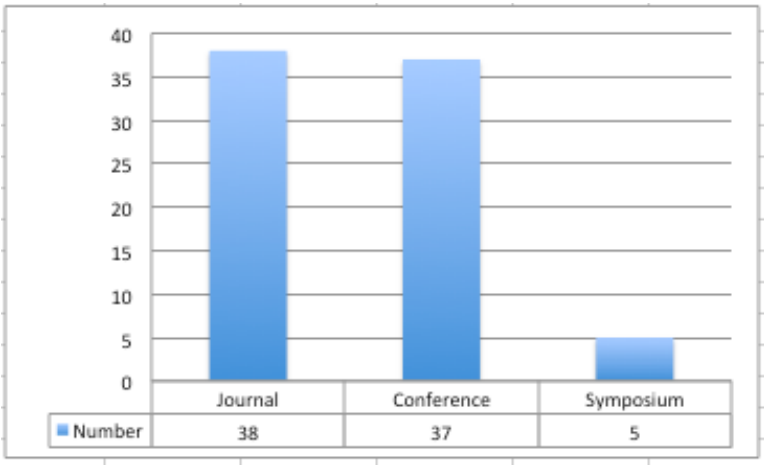


Figure 3.3: Numbers of publication source

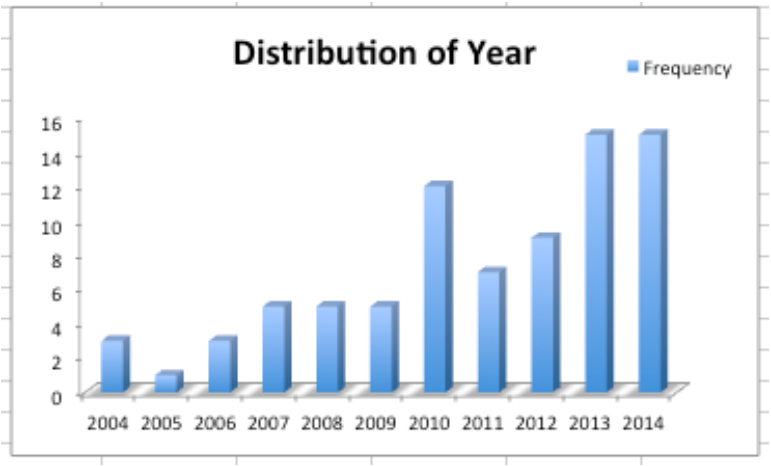


Figure 3.4: Numbers of published papers over 10 years

E-science [120], student performance [45], Information system [52, 125], Chlorine Processing system [74], transportation industry system [186], power system [190], cloud computing [11, 98, 111, 132] and mobile application [82]. The development of ISRA in these industries illustrates that securing information is becoming more and more important not only traditional industries but also other emerging domains such as mobile Applications and cloud computing. Additionally, risk assessment has played a vital role in securing their information and reducing the leakage risks in these domains.

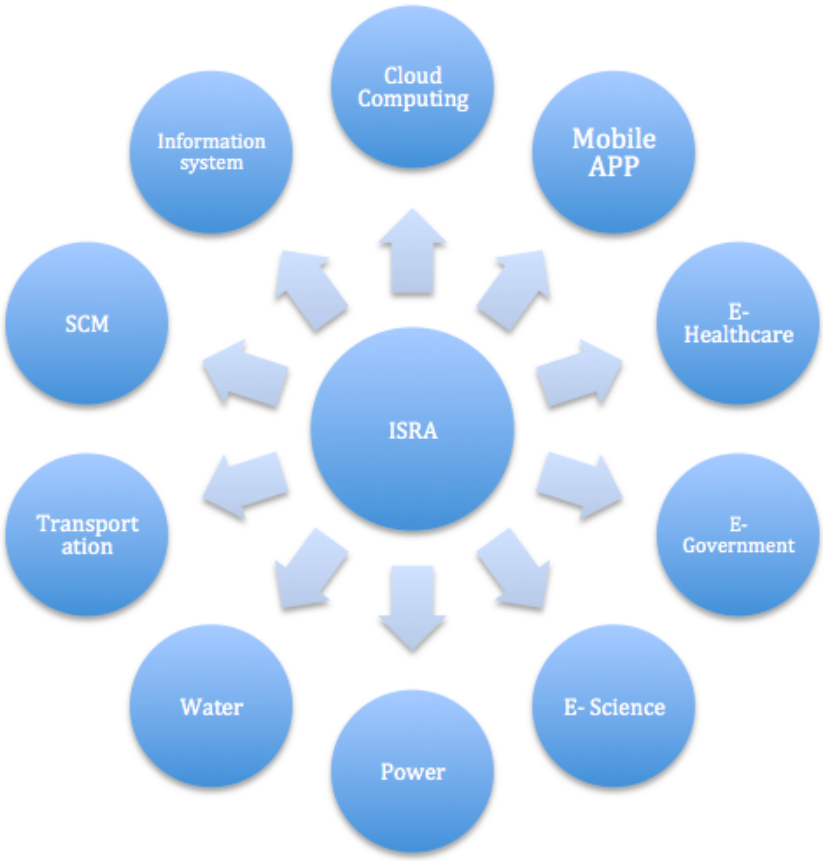


Figure 3.5: Application industries of ISRA

3.3.2 Classification Framework on ISRA

The overview shows that the definitions of risk analysis, risk assessment and risk evaluation are various in these papers. Sometimes the researchers do not apply the definitions accurately. We understand this problem due to the very much similar meaning if the authors do not follow some standards. For example, ISO 27995:2011 provides an easy-to-understand definition in the real practical ISRA. Nevertheless, some authors use risk analysis as a synonym to risk assessment in their research papers. Thus, it is necessary to distinguish the definitions about them when applying. Moreover, risk evaluation is about the selection of risk criteria to judge whether the risk is acceptable, rather than discussing the risk analysis methods.

Figure 3.6 shows the research framework of ISRA. There are four kinds of risk identification including asset, threat, vulnerability and existing control identification. Mainly, asset identification is more important in these four types. Other types of

identification are the basis on asset identification. Once assets are identified, we can analyse the threats, existing controls and vulnerability of them. So the researchers of this field focus on how to identify the asset easily and feasible.

Risk analysis has three types of methodologies as follows: quantitative, synthetical and qualitative. Now, a simple quantitative or qualitative risk analysis method is not suitable for the current environment, more and more researchers develop the hybrid models by a combination of quantitative and qualitative methods [99]. Most of these hybrid models are based on the analytic hierarchy process (AHP) and soft computing.

AHP is a decision-making model and made up of three steps. First, it organises a hierarchy of decision objectives or criteria identification. Second, it evaluates the differences in pairs among the relevant elements according to the hierarchy. Finally, it syntheses the compared results by a solution algorithm [149]. Overall, AHP will support the organisations to weight the risk factors [99]. Furthermore, AHP is widely applied in ISRA due to transferring the qualitative index into quantitative one [99].

Soft computing becomes a keystone of ISRA research [99]. It is a method to construct intelligent systems which "are supposed to possess hunmanlike expertise" to help make decisions in changing environments [81]. Soft computing contains neural networks, rough sets, grey sets, fuzzy systems/fuzzy set theory, generic algorithms, support vector machine, Bayesian classifier and Bayesian network [81, 99]. Thereinto, the fuzzy set theory is widely used in the improvement of risk analysis methods. In fact, fuzzy set is defined by Zadeh as "play an important role in human thinking, particularly in the domains of pattern recognition, communication of information, and abstraction" [196]. Moreover, fuzzy logic theory [3], which is an extension of the fuzzy set theory [182], is also the primary method in the hybrid models [99].

A classification framework is provided by reviewing research papers. Table 3.1 describes the categories and the corresponding papers. The framework helps researchers understand the state of art in the study of ISRA. There are seven types of current research directions in this classification: improvement and comparison of risk assessment guidelines, risk identification, improvement and comparison of risk analysis methods, case study and others.

We explain the content of each category as follows. Firstly, the kinds of 'framework-comparison and framework-improvement' discuss the papers which mention the entire stages of ISRA, the comparison between pros and cons, and the improvement for therein aspect. Secondly, the category of 'risk analysis-comparison' emphasises on comparing the risk analysis methods. Thirdly, this publication is passed to the type of 'risk

[3]Fuzzy logic provides a mathematical power for the emulation of the ligher order cognitive functions, the thought and perception [182]

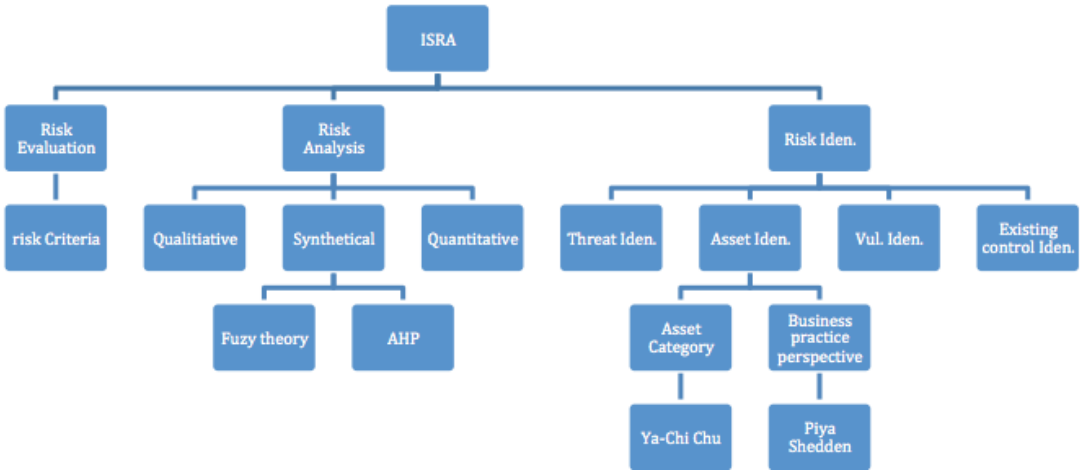


Figure 3.6: Research framework of ISRA

analysis-improvement' if the author proposes an improved method. Fourthly, a paper's priority is to introduce a case study of a particular subject or industry, and we assign it to the category of 'case study'. Finally, the type of 'others' is that some papers analyse ISRA in different systems or related to cost model.

3.4 Discussion

We will make a deeper discussion about the contents and contributions of the relevant studies in this session.

3.4.1 Risk Identification

Risk identification is "the process of finding, recognizing and describing risks" [8]. In the academic sector, researchers emphasis on how to identify the risks with more efficiency and accuracy. However, some of them ignore the importance of valuing these risks when studying this phase.

The earlier risk identification method is Hierarchical Holographic Modelling (HHM) [68]. Haimes initially proposed HHM in 1981, and then he applied HHM to risk identification in 1995 [68, 67]. HHM identifies the risks from eight main parts of the system including program consequences, management of change, system acquisition, temporal, modal, information management, functional and geographical [68]. However, HHM is appropriate for general risks and large-scale management systems. But HHM is more difficult to identify the enterprise and operation risks [169]. HHM is not mentioned very much by the current researchers, although it has detailed identification model.

Table 3.1: Classification framework of research types in ISRA

Research categories	List of Studies
Risk Identification	[37] [66] [89] [127] [154] [155]
Comparison of Risk Analysis	[48] [74] [121] [150]
Improvement of Risk Analysis	[17] [23] [24] [35] [36] [50] [52] [57] [76] [86] [89] [99] [100] [103] [107] [111] [113] [120] [132] [147] [160] [164] [167] [168] [180] [181] [185] [186] [190] [192] [198] [199]
Comparison of Framework	[95] [153]
Improvement of Framework	[11] [16] [18] [53] [55] [58] [59] [73] [82] [87] [94] [96] [102] [105] [108] [109] [118] [125] [138] [139] [148] [156] [157] [165] [177] [178] [187] [193] [194]
Case Study	[19] [39] [45] [191]
Others	[40] [56] [75] [174]

We can not find many relevant papers about HHM in the selected publications. So far, brainstorming and questionnaires are the general methods of risk identification and frequently applied by most organisations. Nevertheless, these general techniques are too objective and time-consuming for users [37].

To improve the efficiency and accuracy of risk identification methods, Shedden et al. propose a complete list to identify risks efficiently from a business practice perspective [155]. Chu et al. classify assets into five types such as hardware, software, information, people and services and present very detailed contents for each type [37]. The knowledge-based and genre-based (GBM-OA [4]) methods are also capable of identifying the risks efficiently [66, 127]. Guan et al. explain that knowledge base consists of basic rules and special rules, where basic rules are no effect on the external relationships, and special rules are organisation own provisions [66].

Genre base is an approach to introduce the application methods of producer or user information entities to obtain various vital organisation information [127]. OA is proper for small organizations to identify information assets by explicit steps [127].

In conclusion, researchers present all kinds of methods to identify the risks efficiently. However, existing approaches to risk identification cannot deal with some

[4]Genre-based method-OCTAVE Allegro

critical factors such as asset leakage [5], user-created assets and essential knowledge [155]. Furthermore, from the systematic review, we find that Shedden [155] is the principal author in the field of risk identification. Other authors' studies frequently cite her papers [154, 155]. Shedden also illustrates that technical infrastructure is the core concern from the standpoint of current risk identification [155]. Most of the risk identification approaches above are proposed from academic level, although Shedden et al. make some connection from an organisational perspective. We have to sort out the methods and apply them in the practical or regulatory ISRA. These ways should have their research values when they are used in the companies, not just stay in the research domain. Therefore, the future research direction on risk identification should focus on how to apply the methods in a real world and achieve their values in an organisation. In fact, the threat and vulnerability categories from ISO 27005:2011 or NIST SP800-30 are enough to identify the risks for individual institutions.

3.4.2 Risk Analysis

Risk analysis is "the process to comprehend the nature of risk and to determine the level of risk" [8]. It provides the decision-making basis for risk evaluation, and a magnitude of risk and expresses regarding the combination of consequences and likelihood [8]. In general, qualitative, quantitative and synthetic analysis are the three types of risk analysis approaches [132].

For each type, there are some typical approaches. For instance, "factor analysis, logical analysis, historical-comparative and Delphi method" [56] are the qualitative representative. "cluster analysis, time series model, regression model and decision tree method" [56] are on behalf of quantitative analysis. The typical synthetic methods contain "hierarchical analysis, probabilistic risk assessment and fuzzy comprehensive evaluation method" [56].

To some extent, these methodologies are not impeccable due to their respective nature. Qualitative methods are subjective and rely on the knowledge and experience of the evaluators. Quantitative ones depend on the quality of data [56, 107]. The synthetic ways diminish the subjective of qualitative methodology by using a mathematical model, or improve the accuracy of quantitative methods by adding the expert's knowledge. Therefore. The mainstream of risk analysis methods is developing the synthetic methods. The impact and likelihood are two critical indexes for risk score. Hence, improving risk analysis methods is mainly to obtain more accurate and efficient values of impact and likelihood. In the systematic review, there are 32 papers on the

[5] "Asset leakage is the product of both employee negligence and 'broken' business processes, reflecting on individuals performing workaround activities away from the formal view of the organisation" [155].

improvement of risk analysis methods and four papers about the comparison of them.

3.4.3 Risk Analysis-Comparison

Four papers mention the comparison of risk analysis tools in the systematic review. The contrast is about the disadvantages and advantages of quantitative or qualitative risk analysis methods. For instance, Lee compared the advantages and disadvantages of quantitative and qualitative methods from the view of economics [99]. He presents quantitative approach can make a cost-benefit analysis and obtain more accurate results, but it relies on the scale of measurement body [99]. A qualitative method is more challenging to do a cost-benefit analysis. Furthermore, Chien-Cheng Huang compares the five common methods of risk scenario analysis and points out the features and problems of every technique [74]. These risk scenario analysis methods include "Hazard and Operability Analysis (Haz-Op), Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Attack Tree Analysis (ATA)" [74, 161].

The classification research is various for the risk analysis methods. For instance, knowledge-based and model-based [56], software-based and paper-based methods [86], asset-based [23, 197], business process-based [89]. For example, ISRAM (Information Security Risk Analysis Method) [86] is a quantitative and paper-based method, which measures the complex information systems by independent surveys. Though ISRAM is easy to use due to no sophisticated mathematical tools, it depends on the quality of survey results and the knowledge of participants.

3.4.4 Risk Analysis-Improvement

In 32 papers of 'improvement' type, 12 papers are about the hybrid models. These hybrid models are mostly applied at least two of the following theories: AHP and soft computing, notably fuzzy set theory.

The reason of applying hybrid models in risk analysis methods is that they could overcome certain flaws and nature of qualitative and quantitative tools. Saaty presented the concept of AHP in the 1970s firstly and applied it to study the complicated problems [190]. AHP decomposes the complex issues into several sub-questions and analyses these sub-questions independently [190]. Additionally, AHP can obtain more correct data when used in quantitative methods. Most authors apply fuzzy theory to reduce the subjective of qualitative risk analysis methods [107]. For example, Chang and Lee [35] apply fuzzy expert systems to reduce the subjective of likelihood. Furthermore, risk scenario analysis methods are frequently used to improve the synthesis methodologies

[128]. Whatever risk scenarios, AHP, fuzzy sets or soft computing will become the future research directions of risk analysis methods [99].

To sum up, comparison and improvement are two primary parts of the current research directions of risk analysis methods. Figure 3.7 shows the detailed about these two pieces. The research trends of 'comparison' are the advantages and disadvantages of quantitative and qualitative. In the 'improvement' part, authors study a hybrid model of fuzzy systems [6] and AHP [107] in the future research of risk analysis.

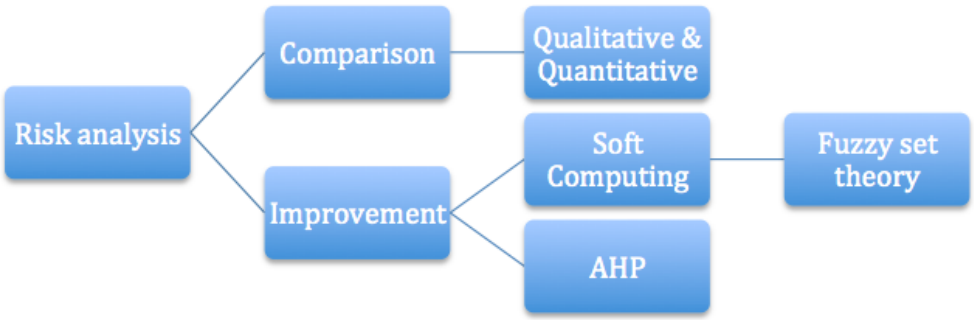


Figure 3.7: Current research direction of risk analysis

3.4.5 Framework-Comparison

Two papers compare the ISRA methods from the conceptual structure. Shamala et al. [153] discuss the well-documented approaches by a conceptual framework. The comparison assists organizations to choose the most suitable ISRA method. However, the comparison does not mention ISO 27005:2011 and the matched methodologies to the different organizations. Korman et al. also apply the conceptual framework to compare and analyse the ISRA methods [95]. In their analysis, more well-documented ISRA methods discuss the differences between the extent of input information and data collected by statistical tools. By contrast, Shamala et al. do not consider the scopes of input data for users [153].

3.4.6 Framework-Improvement

In the category of 'framework', most of the authors try to improve the whole process of ISRA by following different standards such as ISO 27005:2011 and NIST SP800-30. Some of them propose the improvement of the risk identification methods from the

[6] a component of soft computing [99]

standpoint of defined subjects. For instance, Albakri et al. present that it is more realistic and easier to identify risks from the views of cloud clients and cloud service providers in cloud computing [11]. Jing et al. [82] identify the risks from users' coarse expectations in mobile applications. Additionally, they use the relatively onefold risk analysis methods in their frameworks.

Generally speaking, the improvement of risk identification methods will provide some more detailed lists to identify the risks and assets from different users' views. But this kind of 'improvement' does not offer a new perspective to risk analysis. Most of the modified risk analysis methods make the calculations of risk level more objectively and efficiently to some extent, although they are relatively onefold. More and more subjects and industries assess the risks by the ISRA frameworks, especially in the field of healthcare and cloud computing. But the academic researchers are far not enough for the demand of two subjects. Researchers pay more attention to the areas and propose more practical risk analysis models for improving the whole ISRA process. Overall, the enrichment of the frameworks aims at a defined subject when compared with the process of ISO 27005:2011. These improvements propose more detailed steps to identify the risks from different views, calculate the values of risks by specific risk analysis methods, and set the criteria for accepting the risks.

3.4.7 Case Study

Four papers discuss ISRA from the view of 'case study'. ISRA had been applied in healthcare and student performance of learning course since 2004. Coleman [39] provides an excellent example of the applications of OCTAVE in different scale healthcare organisations. OCTAVE, a common and industry-recognised methodology, offers more freedom to consider organisations' unique situation in the process of risk assessment [39]. Nevertheless, Workshop [7] may increase the relative overhead in conducting these workshops [34] when identifying risks. The tool of Workshop is also too time-consuming for large-scale organisations. Additionally, the tool does not provide the detailed calculation method to risk score. Thus, we have no idea whether the Workshop is objective. Yeo et al. [191] discuss the decisive factors of an ISRA process, and examine them by a large university. However, this case study is not so powerfully reliable to their conclusions due to only investigating one case.

All the relevant papers on case studies, we know the authors apply ISRA in education and healthcare subjective in the early development stage of risk assessment of information security. However, in academia, the authors less refer to other types of organisations and give some detailed examples of practical ISRA. We can not say

[7] the tool to collect data in OCTAVE [128]

that ISRA is applied less for different kinds of institutions, "but fewer authors focus on studying the real case in real organisations" [128]. The authors would like to explore the ISRA methods from an academic level.

3.4.8 Others

The papers of 'others' conclude the discussions about the role of ISRA in different systems, the applications of the cost analysis and the future directions of ISRA development. These papers also provide some unique and rare research directions for studying ISRA. For example, it is worth to analyse ISRA from the economic views such as cost-benefit analysis and game theory. Furthermore, they discuss the ISRA impacts of facilitators in different systems.

3.4.9 Risk Evaluation

Risk evaluation is "the process of comparing the results of risk analysis with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable" [8]. The primary work for risk evaluation should be the ways of choosing risk criteria, and making the compared results more fair, suitable, efficiency and accuracy. As we know, risk criteria are "derived from standards, laws, policies and other requirements" [8]. Some papers mention risk evaluation but do not introduce a detailed way of selecting the risk criteria [128]. In a word, the study of this part is relatively rare, even has, it is known as risk analysis.

We have analysed all types of the classification framework and obtain the answers to the research questions. The analysis results demonstrate that cloud computing and healthcare will become the primary subjects in the future study. In reality, more and more researchers focus on the improvements to the existing risk analysis methods and frameworks. Thereinto, soft computing and hybrid models are primarily applied to improve risk analysis approaches. Risk evaluation is rarely paid attention to by the researchers. Therefore, for the part of risk evaluation, the selections of risk criteria may become a new and valued research in the field of ISRA. Additionally, the researchers would like to study the combinations between fuzzy theory and AHP. The hybrid models will build up the efficiency and accuracy of risk analysis methods.

3.5 Conclusion

The systematic review of ISRA examines the existing research papers and presents an unbiased result of the developing status. In a word, this chapter provides a classification

framework for research studies of past ten years (2004-2014). The classification aims to help researchers obtain a clear and unbiased picture of the terminology and development trends of ISRA in the academic sector.

The first part is to develop the methods of risk identification. The existing methodologies are hard to deal with asset leakage, user-created assets and critical knowledge [155]. The ISRA standards show that risk identification is the first and most vital step in the whole assessment progress. That is, it is imperative to develop the efficient and accurate methods in the practical ISRA for organisations. Now, some researchers not only study them from the standpoint of an academic but also examine the identification approaches about the actual values. For example, Shedden et al. support to identify the risks from the organisational standpoint [154]. Their study might become the further approach for risk identification.

Risk analysis, as the second part of the classification framework, consists of two subparts: comparison and improvement. The comparison mainly focuses on comparing the benefits and drawbacks of quantitative and qualitative risk analysis methods. Whereas, the 'improvement' is about how to obtain more objective and accurate risk scores by improving the calculation of likelihood and impact. The fuzzy theory is widely used to reduce the subjectivity of risk scores.

Researchers enrich the assessment framework to a defined subject. Furthermore, they design more detailed steps of the whole ISRA process, including risk identification from organisational views, the risk calculations by specific approaches and the selection of risk criteria. Moreover, the reviewed papers of case studies suggest that the application of the whole ISRA process in education and healthcare are too subject in the early development stage. In academia, researchers rarely refer to the other types of organisations We can not say that ISRA is applied less for different kinds of institutions, but fewer authors focus on studying the real case in companies. The authors would like to explore the ISRA methods from academia level. The part of Others concludes the discussion of the role of ISRA in different systems, the application of cost analysis and the future directions of ISRA development. The classification of others provides some unique and rare research directions for studying ISRA. For example, we can discuss the impact of other roles, not only facilitators [40], of ISRA in different information systems [128]. Furthermore, it is also desirable to pay attention to analyse ISRA from the economic view of cost-benefit analysis and game theory.

However, ISO 27005:2011 and the reviewed papers rarely mention the methods for collecting and managing the information (or data). And the lack of training data and real-world data has become an urgent research problem in information security risk assessment [18, 59]. Moreover, the reviewed studies on ISRA have not divided

information system into two group: open and closed systems and given the related the methods of risk assessment. Therefore, in the further study, we would like to examine whether we can propose a risk analysis model for ISRA with limited data.

Chapter 4

Time Pattern Analysis of Malware by Circular Statistics

Chapter 3 suggests that risk analysis is the research emphasis in the field of ISRA, and the improvement of risk analysis methods is the top priority. This thesis also tries to develop a new approach to assess the cyber threats like malware. The new approach will focus on the quantitative part of risk analysis. The distribution models of information security risks are pivotal for the quantitative risk analysis methods. However, to the best of our knowledge, finding the probability distribution of information security risks is still a challenge in current research. Most of quantitative risk analysis models assume that the attack attempts follow a Poisson Distribution, even if this assumption is not suitable in the real-world [70, 142]. Therefore, this chapter tries to apply the collected dataset to analyse the distribution of malware attacks by circular statistics.

Circular statistics present a new technique to analyse the time patterns of events in the field of cybersecurity. We apply this technique to examine incidents of malware infections detected by network monitoring. In particular, we are interested in the daily and weekly variations of these events.

Based on "live" data provided by Spamhaus, we examine the hypothesis that attacks on four countries are distributed uniformly over 24 hours. Specifically, we use Rayleigh and Watson tests [133]. While our results are mainly exploratory, we can demonstrate that the attacks are not uniformly distributed, nor do they follow a Poisson distribution as reported in other research. Our objective in this is to identify a distribution that can be used to establish risk metrics.

Moreover, our approach provides a visual overview of the time patterns' variation, indicating when attacks are most likely. This will assist decision makers in cybersecurity to allocate resources or estimate the cost of system monitoring during high-risk periods.

Our results also reveal that the time patterns are influenced by the total number of attacks. Networks subject to a large volume of attacks exhibit bimodality while one case, where attacks were at a relatively lower rate, showed a multimodal daily variation.

4.1 Introduction

Circular statistics have been applied to analyse time patterns in diverse areas such as public disorder, wind direction, and the turning patterns of elephant movement [33, 122, 133]. Brunsdon and Corcoran show how this technique may be applied to the time pattern analysis of certain types of public disorder and thus assist the police in prioritising resources and improving targeting [33]. Our aim is similar but within the field of network monitoring and cybersecurity.

To the best of our knowledge, circular statistics are rarely used in cybersecurity research. Analysis usually focuses on linear statistics applied to the distribution of malware over IP address space [140, 159]. Analysing time patterns events by circular statistics is a new approach, providing visual methods to identify the distribution of attacks over a fixed period.

In the following, we restrict our notion of an "attack" to an automated opportunistic attack on a network or host, and consider the distribution of such attacks over fixed time periods. Dedicated targeted attacks are beyond the scope of this work. A typical opportunistic attack is an infection by malware. In studies of malware, it is conventional to use standard histograms over the entire time course of data and view the distribution of attacks over long periods such as several months or years. By focusing on linear distributions over long time periods in their statistical analysis, most studies of malware do not consider the viewpoint of time-of-day or day-of-week relating to cyber risk.

In practice, our observations show that attack data appear to be non-uniformly distributed over 24-hour periods. For instance, the frequency of malware spreading with a sinkhole may seem to follow a Poisson distribution from 01:00 to 15:00 (the results come from section 4.3.2.1), but a different distribution outside these hours.

Maillart and Sornette consider a cyber risk of personal identity losses to follow a power-law tail distribution, which is related to the size of organisations [110]. But in their study, the exact time of identity theft is not considered for quantifying the distribution. We argue that certain types of attacks are more likely to occur at different times. Our goal in this work is to be able to characterise distributions of attacks on enterprise networks over fixed time periods. If we can do this, we will be in a better position to carry out a risk assessment for such networks. Current approaches to risk assessment either classify the likelihood of attack as, for example, low/medium/high;

or use probability figures estimated by experienced security professionals. Thus the ability to provide such estimates based on the identification of a known probability distribution will improve the overall risk assessment.

Moreover, by identifying distributions and visualising time patterns, we can help security managers to allocate and adjust monitoring resources and firewall and intrusion detection rules to target malware.

We will study the time patterns of events caused by malware and analyse the daily and weekly variation by applying circular statistical methods. Our approach is to describe the time variation patterns of malware events in a circle. We base our analysis on data provided by the Spamhaus Project [1]. Spamhaus has a long history of providing network monitoring and traffic analysis services and has a vast collection of data which is updated in real time. We used a dataset based on around 1000 users from commercial (business) organisations. The complete dataset was just over 1GB and contained approximately 9 million records, each one containing a source and destination IP address, time of observation, and type of traffic.

To narrow things down to a manageable size, we chose to focus on the Conficker malware and corresponding botnet traffic, and in particular traffic sending data to a sinkhole. Statistical analysis of Conficker was presented by Shin et al. [159], but they looked at the distribution over the IP address space and domain name by linear statistics and did not investigate the distribution of events around the clock.

For the dataset selected, we test a uniformity hypothesis about the malware activity, and potential daily and weekly relationships. Rayleigh and Watson's tests are two common methods to examine the uniformity hypothesis in circular statistics [133]. These tests could help us identify time patterns of the Conficker attacks around the 24-hour clock. Furthermore, we use the Mardia-Watson-Wheeler test [133] to compare distributions of different types of malware.

In the following, we demonstrate the time variations in the malware attacks using three different types of graphs: ordinary histograms, rose diagrams and helix graphs. In addition to the above uniformity tests and visualisation, we analyse the Conficker daily and weekly cycles by country. We conclude our analysis by comparing the time patters between Conficker and the other kind of malware and test whether these patterns have a common distribution using the Mardia-Watson-Wheeler test. The combination of studies provides us with an overview of the time pattern variations under different conditions or sub-datasets.

[1] www.spamhaus.org

4.2 Dataset

The data we analyse is captured as IP packets enter and exit monitoring points (taps) on networks. The data recorded contains the source and destination IP address of the packet, the time recorded, and a diagnostic message identifying the type of malware that was observed. It also identifies the ASN (Autonomous System Number), domain name, and geographical region associated with the source IP address. An Autonomous System is "a connected group of one or more IP prefixes run by one or more network operators which has a single and clearly defined routing policy" [69]. We, therefore, have a set of records describing malware traffic as the enters and exits points on the networks under observation. Once infected, in general, a host will do some things:

1. It will propagate the virus to other hosts.
2. It will often communicate with a controller.
3. It will send data to a receiver, or sinkhole.

The diagnostic data from Spamhaus can determine if data is being sent to a sinkhole. We are therefore able to select records from this dataset for further analysis according to some different parameters. For example, we choose to investigate data from a bt.net domain and from geographical location, e.g. networks located in the UK or China. We also may select which specific virus, or botnet, to analyse and choose to focus on command and control data or data being sent to the sinkhole.

4.3 Circular statistics

Mardia states that circular statistics analyses distributions of random variables that are cyclic in nature [112]. Thus, regarding the time of an attack as a random variable, we map our original data covering several contiguous days to a 24-hour circle. The ensuing analysis will be different from that of the original data stretched along its entire time span. Special statistical tools have been developed to assist researchers with circular data analysis [133].

4.3.1 Circular Mean

To illustrate the importance of circular statistics, Brunsdon and Corcoran [33] provide an example to reveal the misuse of ordinary, or linear, statistics with cyclic data. For instance, four disorder incidents recorded at midnight times 23:30, 00:15, 00:30 and 00:45, then the mean value of these four times by the ordinary (arithmetic) averaging

provides a morning time of 06:15. Whereas the true (Fréchet [46]) average is 00:15. There are different ways to average circular data. One can argue that the most natural definition is the Fréchet mean [46] given by:

$$\bar{\theta}_F = \arg\inf_{\theta\in\mathbb{S}} \sum_{i=1}^{n} d^2(\theta_i, \theta) \tag{4.1}$$

where $\mathbb{S}$ is the unit circle ($\mathbb{S} \in \mathbb{R}^2$) and $d(\cdot,\cdot)$ is the arc length on it. But in practice one often uses an alternative definition [33]:

If

$$A = \sum_{i=1}^{n} \sin(\theta_i), B = \sum_{i=1}^{n} \cos(\theta_i) \tag{4.2}$$

then

$$\bar{\theta} = \begin{cases} \arctan(A/B) & \text{if } B \geq 0 \\ \arctan(A/B) + \pi & \text{if } B < 0 \end{cases}$$

where $\theta_1, \theta_2, \ldots, \theta_n$ are the n observations of circular data.

This definition can be considered an approximation to the Fréchet sample mean, and its version is implemented by R package 'Circular' [133].

4.3.2 Distribution Hypothesis Tests

Pewsey et al. proposed that the uniformity hypothesis is the most basic null hypothesis in circular statistics, and its rejection in favour of a generic alternative means that the data provide the evidence that circular distribution in question is non-uniform [133]. Disregarding, for the time being, the issue of periodicity, the theoretical assumption: (unordered) attacking attempts are distributed uniformly over a time interval $(a, b]$ of interest, suggests that (ordered) number of attacks follow a homogeneous Poisson process. Consequently, the number of attacks in a fixed time interval should have a Poisson distribution with parameter $\lambda(b - a)$, where $\lambda > 0$ and is known as rate or intensity of the Poisson process. This assumption may or may not hold in practice [70].

4.3.2.1 Tests for a Poisson process

We consider an example of malware received at a sinkhole in the domain bt.net over a period of 15 days. Thus, we find these BT data to be a random sample from a particular point process, and we test the null hypothesis that the process is Poisson.

Table 4.1: Chi-square goodness-of-fit tests reveal evidence (at 5% significance level) that malware received at the sinkhole in domain bt.net do not conform to the Poisson assumption. Y is "Yes"; N is "Not", and TNH is the total number of attacks in the given hour; λ is the estimated mean (and the variance) of the number of attacks in the given hour; df is the degree of freedom of the test. The results are based on the minimum chi-square estimates of λ.

Time slots	P-value	Poisson	TNH	λ	df
00:00-00:59	0.5778	Y	126	2.1359	5
01:00-01:59	0.4904	Y	63	1.0771	3
02:00-02:59	0.8509	Y	52	0.8830	2
03:00-03:59	0.2307	Y	42	0.7370	3
04:00-04:59	0.9593	Y	28	0.4812	1
05:00-05:59	0.8745	Y	31	0.5212	2
06:00-06:59	0.9134	Y	33	0.5542	2
07:00-07:59	0.8495	Y	55	0.9307	3
08:00-08:59	0.2407	Y	137	2.3353	5
09:00-09:59	0.4820	Y	178	3.0978	4
10:00-10:59	0.3918	Y	192	3.1835	7
11:00-11:59	0.2525	Y	219	3.8242	9
12:00-12:59	0.7202	Y	186	3.1350	6
13:00-13:59	0.5833	Y	201	3.5358	9
14:00-14:59	0.0781	Y	195	3.7625	10
15:00-15:59	0.6344	Y	190	3.2320	6
16:00-16:59	0.5061	Y	227	3.7705	8
17:00-17:59	0.0012	N	214	4.1493	11
18:00-18:59	0.4774	Y	198	3.3066	6
19:00-19:59	0.0013	N	230	4.6770	12
20:00-20:59	0.0272	N	261	4.8489	12
21:00-21:59	0.0906	Y	242	4.2135	9
22:00-22:59	0.0079	N	230	3.7304	7
23:00-23:59	0.0237	N	176	3.3006	9

Without assuming homogeneity of the process, we partition the day into 24-hour intervals and apply the standard Chi-square goodness-of-fit test to each of these 24 sub-samples, lumping all the days together. Thus, our null hypothesis is that the i-th sub-sample is a random sample from a Poisson distribution with an unspecified parameter λ_i, $i = 0, 1, \ldots, 23$. For example, we observe a total of 63 attacks during

01:00 – 01:59 and out of these 60 minutes, 18 minutes have no attacks, 25 minutes have one attack each, 14 minutes have two attacks each, 2 minutes have three attacks each, and only 1 minute has four attacks. Hence, we have five bins labelled by the number of attacks as 0, 1, 2, 3, 4 and more (accounting for the infinite tail of the Poisson distribution). We use the standard implementation of the goodness-of-fit test provided in R ('vcd' package [145]) with its default settings (minimum chi-square estimation of λ_i and the rule to have at least five expected counts disabled).

The results in Table 4.1 show only five hours with p-values below 5%, a common significance level. That is, unlike the other 19 sub-samples, these five sub-samples display significant evidence against the null hypothesis that the frequency of malware observed on bt.net follows a Poisson distribution.

Assuming further that the 24 sub-samples are independent and all the 24 null hypotheses hold true (i.e. the day process is Poisson with intensity varying from one hour to another but constant within each hour), we would expect only $0.05 \cdot 24 \approx 1$ of the 24 tests to reject its null hypothesis. Thus, aggregating these 24 tests into a single binomial test, we would obtain the overall p-value, i.e. the probability of rejecting five or more (at 5% significance level) out of the total of 24, of 0.006, which is very low. The sample subjected to these simple tests reveals strong overall evidence against the Poisson hypothesis, which is concentrated in the evening hours (5 pm and later). In our BT dataset, we record the attacks by minutes and merge 15-day data to do the Poisson distribution test. We find the 15-day graphs of λ from each day have various variations as shown in Figure 4.1.

All charts display the similar variations that morning have fewer attacks than afternoon and evening. Given these variations in the process intensity, it appears sensible to also examine the Poisson hypothesis for each hour of each day separately. However, if we were to apply the same Chi-square goodness of fit test within each such time interval, we would have too little data for the test to be meaningful. If we instead partitioned the data over longer intervals, then this could easily miss the distinct inhomogeneity feature of the process. Fortunately, some tests are specifically designed for situations when homogeneity of the Poisson process cannot be assumed [90]. Kim and Whitt [90] study several such tests based on an earlier work of Brown [32]. We also use one such test, referred to as 'Log Test' in the research of Kim and Whitt [90], which is based on pivotal quantities (4.3). Table 4.2 shows all test results of every hour of the acceptance or rejection of a Poisson process.

The first part of the idea is as before, i.e. to use a piece-wise approximation of the rate, or intensity, function $\lambda(t)$. But the main part of the idea is to convert the attack times into the transformed inter-arrival times (4.3), as those (under the null

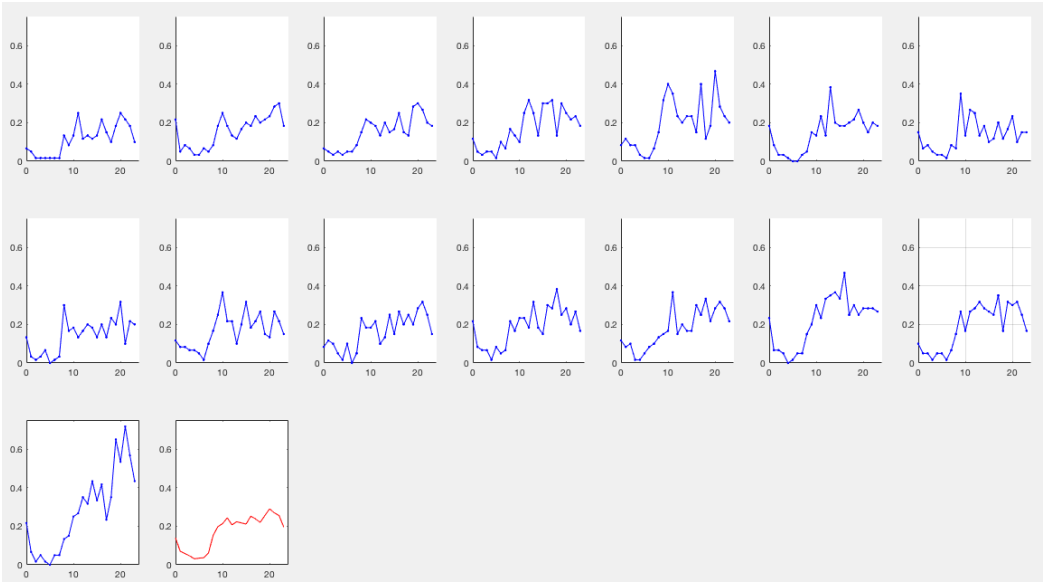


Figure 4.1: Lambda graphs (1-15 sub-graphs present the variation of λ in each day, the final sub-graph denotes the variation of the 15-day average λ), x-axis indicates the hours of a day (0-24) and y-axis presents the values of λ on each hour (0-1).

hypothesis) follow the exponential distribution with a constant mean (λ=1).

Brown et al. define log transformed inter-arrival times X_{ij} as follows [32]: $i = 1, ..., I$, $j = 1, ..., n_i$,

$$X_{ij} = -(n_i + 1 - j) log \left(\frac{T - T_{ij}}{T - T_{i,(j-1)}} \right), \tag{4.3}$$

where

$\boldsymbol{I}$**:** the total number of time intervals;

$\boldsymbol{n_i}$**:** the total number of attacks in the ith interval;

$\boldsymbol{T}$**:** the total time (minutes) of an interval (1 hour);

$\boldsymbol{T_{ij}}$**:** the jth ordered attack time in the ith interval so that $T_{i1} \leq ... \leq T_{i,n_i}$ and T_{i0} =0.

We transform the original data T_{ij} to X_{ij} and test the variables X_{ij} by the 'Log test' to examine whether X_{ij} are a sequence of independent and identically distributed exponential variables with mean 1 [32] such that

$$X_{ij} \sim Exp(1)$$

.

Table 4.2: Test results for a Poisson process. H1 (0:00-0:59) is the first hour of a day; d1 (7th Aug) is the first day of the tested datasets; A is "Accept" the Poisson hypothesis; R is "Reject"; T is the number of attacks in each hour or each day; "NA" means there is no attack in that hour; all tests are at 5% significance level.

Hour	d1	d2	d3	d4	d5	d6	d7	d8	d9	d10	d11	d12	d13	d14	d15	T
H1	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H2	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H3	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H4	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H5	A	A	A	A	A	A	A	A	A	A	R	A	NA	A	A	A
H6	A	A	A	A	A	NA	A	NA	A	A	A	A	R	A	NA	A
H7	A	A	A	A	R	NA	R	A	A	NA	A	A	R	A	A	A
H8	A	A	A	A	R	A	A	A	A	A	A	A	A	A	A	A
H9	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H10	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H11	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H12	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H13	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H14	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H15	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H16	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
H17	A	A	A	A	A	A	A	A	A	A	A	A	A	A	R	A
H18	A	A	A	A	A	A	A	A	A	A	R	A	R	A	A	R
H19	A	A	R	R	A	A	A	A	A	A	A	A	A	A	A	A
H20	A	A	A	A	A	A	A	A	R	A	A	A	A	R	A	R
H21	A	A	R	A	A	A	R	A	A	A	A	A	A	A	R	R
H22	A	A	R	A	A	A	A	A	A	A	R	A	A	A	R	A
H23	A	A	A	A	A	A	A	R	A	A	A	A	A	A	A	R
H24	A	A	A	R	A	A	R	A	R	A	A	A	A	A	A	R
T	A	R	R	R	R	A	R	R	R	R	R	R	R	A	R	R

Not only does this make goodness of fit tests such as the Kolmogorov-Smirmov one applicable within each short subinterval, but it also allows us to merge the transformed data from the individual intervals into larger samples to increase the test power.

Our results show that with small samples (individual one-hour intervals) the Poisson process hypothesis appears acceptable (see Table 4.2). However, when we start aggregating our data as described above, the large sample tests lead to rejection. An immediate interpretation is that this is due to the increase of the test power (although we do not specify the alternative hypothesis). We then do more experiments to examine this explanation. Thus, we test sub-samples of increasing size corresponding to the first k hours in a given day.

We then also randomly permute our transformed samples and aggregate those. Interestingly, the former experiment shows how the p-value tends to drop as the sample size increases. The result of the previous experiment supports our conjecture that the actual process is mildly non-Poisson, which was impossible to detect with small samples. The latter experiment shows that the p-value does not drop noticeably as the sample size increases, which suggests that unlike a Poisson process, our attack process may be violating the assumption of independence of inter-arrival times. This may be a sensible explanation as attacks indeed need not be statistically independent.

In the original dataset, we find that there is no attack at some hours. In that case, we consider them missing data and no p-value in these hours. Most p-values are higher than the 5% significance level. Therefore, we have no evidence against the Poisson process hypothesis.

4.3.2.2 Uniformity Hypothesis Tests

It may be interesting to experiment with other partitions as a way of assessing the robustness of the above results. In practice, most of the existing research of malware distributions do not consider the periodicity of the data over 24 hours. For instance, Ramachandran and Feamster illustrate that the vulnerable hosts across IP address space follow a uniform distribution in the assumptions of the worm propagation analysis [140]. But they do not mention the relationship between this uniform distribution and time periods. Therefore, we will apply two common circular tests, Rayleigh and Watson tests, to examine the uniformity hypothesis to the selected malware data [133]. Bogdan et al. [26] state that Rayleigh and Watson's tests are the classical methods for testing the uniformity hypothesis in circular statistics. We set the null hypotheses H_0 of the tests as

- H_0: the observations θ of attack times are uniformly distributed around the circle.

where decimals observations θ are converted from the original time. For example, 3:30 is converted to 3.5 by $3+\frac{30}{60}$. That is, we have an observation $\theta = \frac{7}{12} \times \frac{\pi}{2} = \frac{7\pi}{24}$ (indicates 3:30). Thus, if the p-value is less than the 5% significance level, we have significant evidence that the observations are not uniformly distributed around the circle.

4.3.2.3 Rayleigh test

The Rayleigh test is considered to be the most common test for uniformity hypothesis [27]. Given n observations of $\theta_1, ...\theta_n$ [47], calculate the test statistic R:

$$R = (V^2 + W^2)^{\frac{1}{2}} \tag{4.4}$$

and

$$V = \sum_{i=1}^{n} \cos\theta_i, W = \sum_{i=1}^{n} \sin\theta_i \tag{4.5}$$

where R is the length of the vector sum, V is the northerly component of the sum (southerly, if negative), and W is the easterly component. Thus, the p-value of the Rayleigh test is $e^{-R^2/n}$. If the p-value is less than given significant level (like 5%), then we have evidence against the uniformity hypothesis.

4.3.2.4 Watson test

Brunsdon and Corcoran [33] state that Watson test is another common method to the uniformity hypothesis. In later section, we will apply two tests to the samples of attack times. They demonstrate the differences between Rayleigh and Watson test in the uniformity hypothesis as follows [33]:

1. Rayleigh will focus on whether the observations θ are distributed uniformly around the circle;
2. Watson pays more attention on whether the observations θ have the same means around the circle.

4.3.3 Large-sample Mardia-Watson-Wheeler Test

Large-sample Mardia-Watson-Wheeler test is a method to test multiple independent samples for a common distribution [133]. The test statistic W_g is given by Pewsey et al. as follows [133]:

$$W_g = 2\sum_{k=1}^{g} \frac{C_k^2 + S_k^2}{n_k}, \tag{4.6}$$

where

$$C_k = \sum_{j=1}^{n_k} \cos(\frac{2\pi R_{kj}}{N}), S_k = \sum_{j=1}^{n_k} \sin(\frac{2\pi R_{kj}}{N}) \tag{4.7}$$

$\boldsymbol{R_{kj}}$ **:** the rank of the j^{th} element in the k^{th} sample;

$\boldsymbol{g}$**:** the number of independent samples;

$\boldsymbol{\theta}$ **:** the vector which is combined by the g sub-samples and ranked by an arbitrary zero direction;

$\boldsymbol{N}$**:** the total number of combined sample of θ;

$\boldsymbol{n_k}$ **:** the sub-sample of N with $N = \sum_{i=1}^{k} n_k$;

$2\pi R_{kj}/N$: the uniform scores of the data in θ.

4.4 Datasets and Geo-Location

4.4.1 Dataset Source

Spamhaus [2] provides the malware datasets which are observations from 1000 hosts on commercial (business) organisations between 8th August and 21st August 2016. The datasets include the following information.

IP address : The address of the host detected originating behaviour.

ASN : The autonomous system number of the IP address via routeviews at the time of file generation and less than 24 hours old.

Country : The Country code where the IP address is geo-located derived partly from private database and partly from RIRs.

Domain : The domain associated with the entity that owns the ASN and derived from private database.

Timestamps : Epoch time of last connection.

Diagnostic : An unformatted raw record as generated from the CBL engine.

4.4.2 Dataset Selection

This section will focus on the sinkhole class of diagnostic from 8th August 2016 to 21st August 2016. The top three countries, plus the UK, are chosen from the whole malware dataset, followed by the sinkhole(s) data, from the information of the diagnostic of these four countries. Then we select the top domain from the sinkhole datasets and the top three malware from the top domain. The flow chart of Figure 4.2 illustrates how we selected the datasets.

The top 3 countries are selected: India (IN), Vietnam (VN) and China (CN). The UK is ranked 36 and chosen into our datasets. IN, VN and CN have the same top 3 malware. Furthermore, Conficker is common malware in these four countries. The attack attempts of each country are described in Table 4.3.

[2] www.spamhaus.org

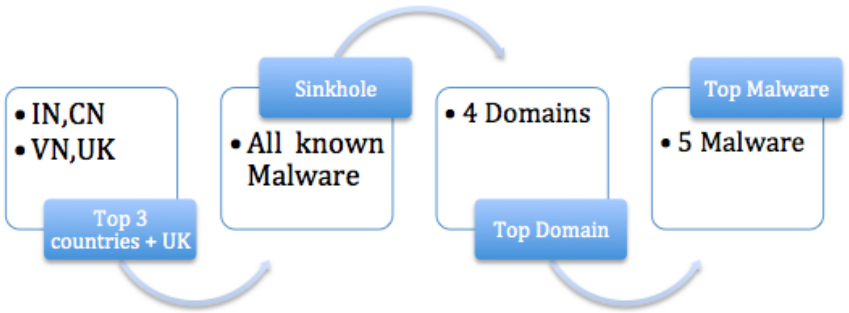


Figure 4.2: Flow chart for the selection of malware datasets

Table 4.3: The number of malware attacks in 4 countries (C.N. is the total attack number of a country; D.N. is the total attack number of top domain; S.M(w)/(t) is the second top malware :worm_dorkbot(w) and tinba(t).)

Country	C.N.	Domain	D.N.	Conficker	S.M(w)/(t)
IN	288779	sancharnet.in	213874(74%)	99821(47%)	110428(52%,w)
CN	302135	chinanet.cn.net	217047(72%)	20763(96%)9	7896(4%,w)
VN	135780	vnnic.net.vn	133097(98%)	82029(62%)	47652(36%,w)
UK	5894	opaltelecom.co.uk	3455(59%)	1352(39%)	1451(42%,t)

Table 4.3 shows that India has 288779 attacks and therein 74% are from the top domain of 'sancharnet.in'. 99821 are Conficker attacks in the top domain. There are 110428 worm attacks in the same domain. Conficker accounts for a larger proportion in the top domains of four countries (96% in 'chinanet.cn.net' and 62% in 'vnnic.net.vn').

4.5 Top Domain Analysis

Shin and Reddy state the importance of Conficker in their research and study the victim distribution patterns to provide better defence against this particular malware [159]. They also illustrate that the current analysis of Conficker has two classifications: binary behaviour and internet propagation pattern [159]. However, this section will apply circular statistics as a new technique to analyse the time patterns of Conficker attacks as follows:

- Daily cycles;
- Uniformity hypothesis tests for the daily cycles;
- Weekly circles

Table 4.4: Mean Times of Countries (Top domains in four countries; Mean time is computed in R 'circular' package [133])

Country	Domain	Mean time
IN	sancharnet.in	13:25
CN	chinanet.cn.net	13:06
VN	vnnic.net.vn	14:03
UK	opaltelecom.co.uk	14:12

4.5.1 Linear Histograms, Daily Cycles and Helix Graphs

This subsection will plot three different graphs including linear histograms, rose diagrams and helix graphs. The graphs describe 14-day data from different perspectives and reveal the time variations of malware attacks.

4.5.1.1 Linear Histograms

Usually, a linear histogram is a universal graph to describe the frequency distribution of attacks in cybersecurity. We draw the line plots for four countries by converting 14 days into 336 hours as Figure 4.3.

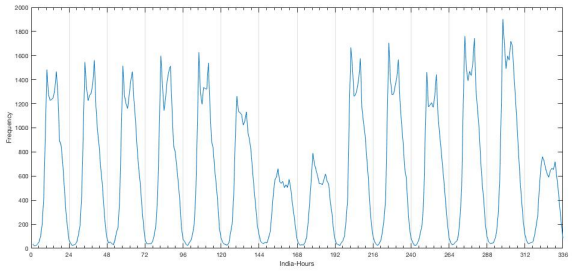
IN Figure 4.3a: The second Saturday (20th August) has the highest frequency; the first Sunday (14th August), the second Monday (15th August) and second Sunday (21 August) have the lower frequency of conficker attacks; it is worth to noting that 15th August is the Indian public holiday (Independence Day).

CN Figure 4.3b: There are roughly three peaks in each day; two higher peaks appear in the mid morning and mid afternoon; the first peak is generally higher than the second one; the attacks of malware in the working days are more than the weekend as a whole.

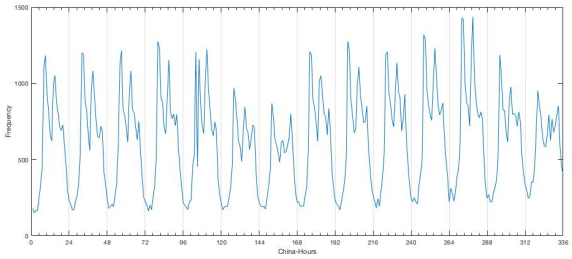
VN Figure 4.3c: The line histogram of Vietnam also has three peaks in each day; the second peak is generally higher than the other two ones; the attacks of malware at the weekend are less than the weekdays.

UK Figure 4.3d: The UK linear histogram shows the relatively irregular changes in the overall trend; it is multimodal variation in each day.

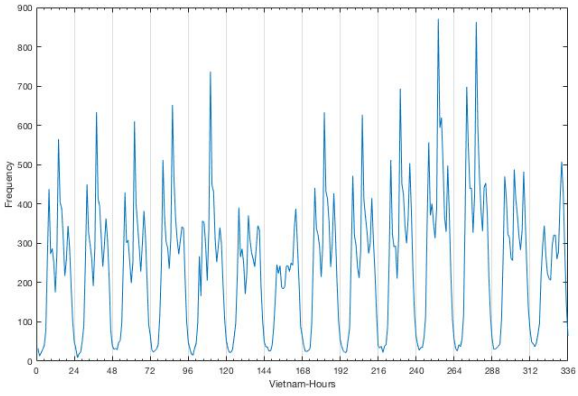
To sum up, the linear histograms show the frequency distribution of malware over hours. There are roughly two peak times in each day, one in the morning and the



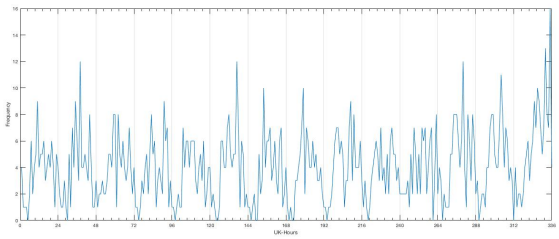
(a) IN



(b) CN



(c) VN



(d) UK

Figure 4.3: Linear histograms of four countries. (x-axis presents 0 to 336 hours and y-axis is the frequency of attacks in each hour.)

other in the afternoon. And then the frequency of Conficker attacks falls typically at noon and early overnight. Furthermore, it may reasonably infer that the attacks will occur less at Holiday and weekend. However, we still need more data to support this idea in future. However, these findings illustrate that the necessity of considering the relationships between working times and the frequency of attacks.

Although the linear histograms describe the frequency distribution over 336 hours, they do not illustrate the real relationship between the frequency of malware attacks and time-in-day. If the falling time point is consistent with some human-being living habits like mealtime, and the peak time points are located in the working time, we may infer reasonably the habit will affect the time behaviour of Conficker attacks. Therefore, we will apply a daily cycle model to demonstrate their relationships.

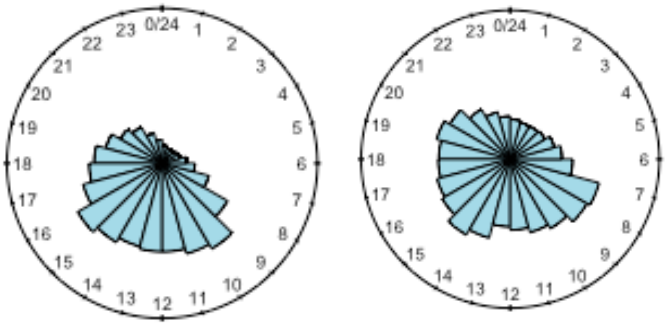
4.5.1.2 Daily Cycles

In the daily cycles, we aggregate the 2-week data into cycles and observe the active time periods in the 24-hour pattern. As we have mentioned above, the attack times are converted into decimals in modelling a daily cycle of Conficker.

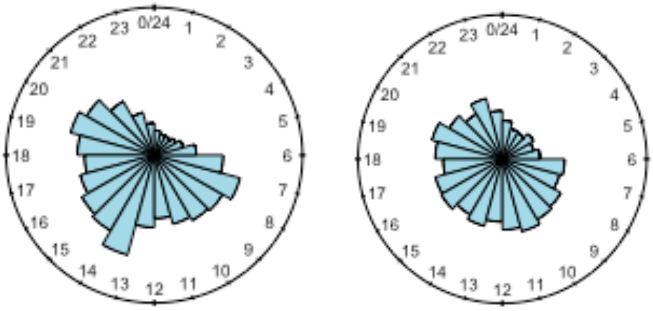
Four daily circles described in Figure 4.4 show that the same type of malware (Conficker) in different countries has different time patterns. Furthermore, the graphs also demonstrate the frequency of Conficker attacks is not evenly distributed around the circle. We observe four rose diagrams of attacks respectively and find their bimodality feature. For instance, the IN rose diagram illustrates that the frequency of Conficker attacks reaches a peak at around 15:30, falls off at approximately 2:00 and mountains at about 9:30 again. Table 4.5 summarises the frequency of Conficker attack in top domain and the active and quiet time. The usual peak hours for the Conficker are the working times in the morning and afternoon. The common quiet time is early overnight. Hence, the daily cycles show the features of bimodality and multimodality. In this case, we need to test the uniformity hypothesis of these four datasets to examine the characteristics in the later section.

Table 4.5: Peak and Fall times for conficker

Country	Frequency	Peak time	Fall time
IN	99821	9:30,15:30	2:00,13:30
CN	207639	7:30,14:30,19:30	2:00,12:30
VN	82029	7:30,13:30,19:30	2:00,11:30,17:30
UK	1352	10:30,19:30,22:30	2:00,12:30



(a) IN san.(99821,47%) (b) CN cnet.(207639,96%)



(c) VN vnc.(82029,62%)) (d) UK op.(1352,39%)

Figure 4.4: Rose diagrams of conficker attacks in the top domain (The top domains in four countries are respectively: sancharnet.in(san.), vnnic.net.vn(vnc.), chinanet.cn.net(cnet.), opaltelecom.co.uk(op.); the number of sub-caption shows the total attack times, followed by the percentages in their domains.)

4.5.1.3 Helix Graph

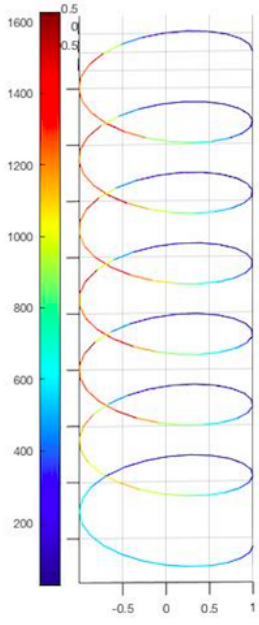
We have aggregated the 2-week data into the daily cycles. However, aggregating the data may miss some information such as the real peak times of Conficker attacks in each day. Therefore, we use a helix graph to describe the data by time-in-hour (168 hours for seven days, from 8th August to 14th August). The helix diagram provides a better view of the active time patterns of attacks. Figure 4.5 shows the four-helix graphs for India, China, Vietnam and UK. The gradual change of colour (the colour bar) of a helix graph suggests the range change of occurrence frequency of malware. There are seven cycles in a helix graph, and each cycle presents a day.

We observe the India helix (Figure 4.5a) that the dark blue appears at overnight in the parts of a cycle. That means, the Conficker is not active at overnight in this week. The colour of the cycles changes to light green, red and yellow from the mid-morning to afternoon. According to the gradual colour change, we can more intuitively observe the

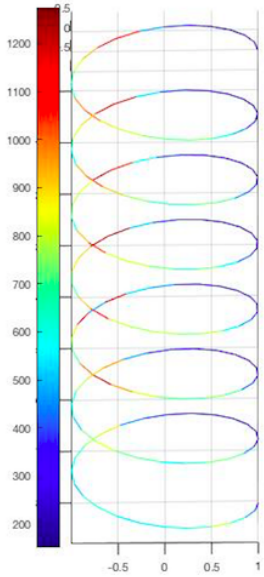
time variations of malware attacks in each day. In principle, the daily cycles and helix diagrams provide a new method to analyse the time patterns and the relationships with the frequency of malware attacks instead of linear statistics. Aggregating the data into circles helps us understand the active and quiet time of attacks.

4.5.2 Results of Uniformity Hypothesis Tests

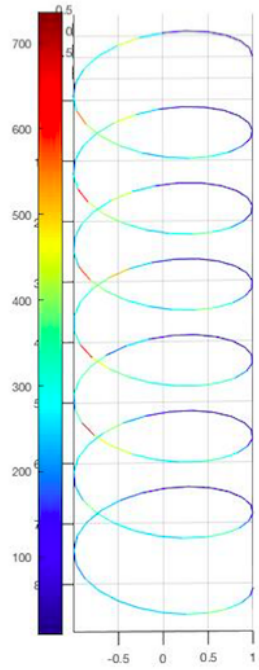
Although the daily cycles show the time-in-day attacks are not evenly distributed over 24 hours, we still need to use a statistical test to examine this finding. Thus, we implement two circular statistical methods: Rayleigh and Watson test to four countries' datasets in R's 'circular' package [133]. The results of two tests are p-value = 0 and p-value < 0.01 respectively for all datasets. Therefore, we have significant (at 1% significance level) evidence that the occurrence times of Conficker are not uniformly distributed around a 24-hour circle.



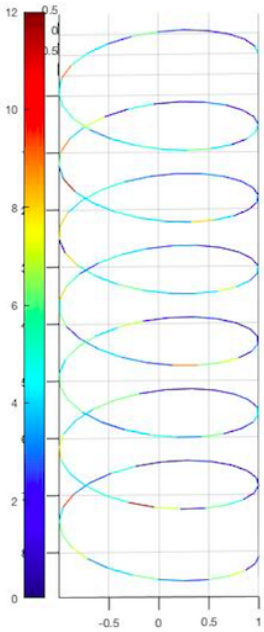
(a) IN



(b) CN



(c) VN



(d) UK

Figure 4.5: 7-day Helix graphs (Red indicates the highest frequency and blue presents the lowest one)

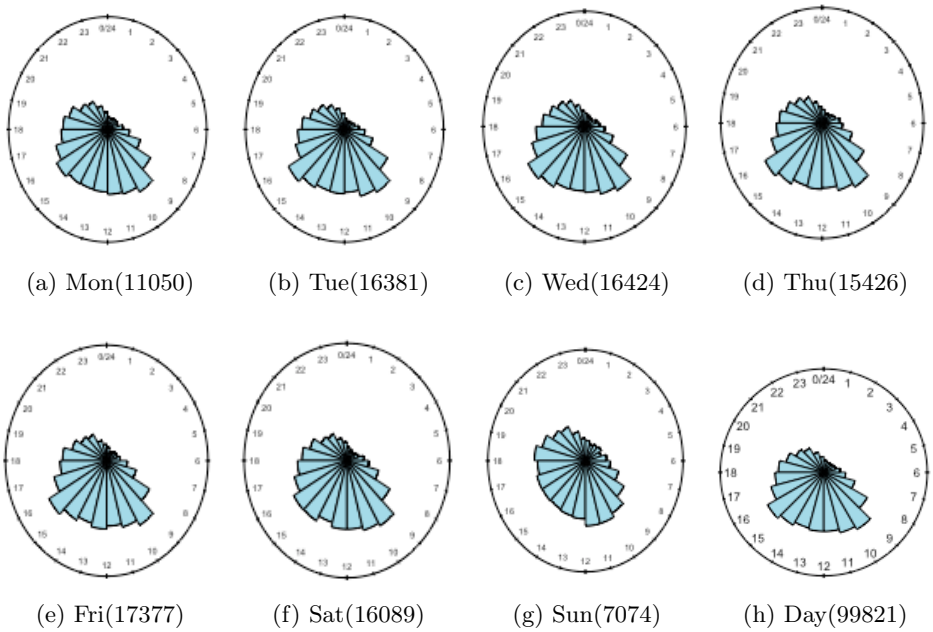
4.5.3 Weekly Circles

In this section, we calculate the circular mean for the time-in-week datasets and show the results in Table 4.6. Here, the mean time represents the average time that a Conficker attack is detected during a day. The mean times of India and China from Monday to Sunday are at around 13:00-14:00. For Vietnam, the mean times of a week are at approximately 14:00-15:30. 13:30-16:00 is the range of mean times for the UK. Moreover, Table 4.6 suggests that the mean times of Sunday are, in general, later than the other days in theses four countries. That is, the attack from Conficker will be detected at a later time on Sunday than the other days. Overall, the results of the Table 4.6 show the mean times of attacks for the top domain of four countries are between 13:00 and 14:00.

Table 4.6: Mean times of a week

Country	IN	CN	VN	UK
Monday	13:24	13:04	13:56	13:29
Tuesday	13:23	12:58	13:57	13:40
Wednesday	13:25	12:58	14:09	14:04
Thursday	13:22	13:00	13:49	14:23
Friday	13:23	12:59	13:36	13:44
Saturday	13:19	13:21	14:06	13:54
Sunday	13:55	13:43	15:29	15:56

The differences of mean times in each country help us to observe the daily distribution of each day and the changes of the attack frequency in 24 hours. We draw the rose diagrams to depict the variation of time-in-week datasets. The datasets include two weeks data collected from 8th to 21st August 2016. We check the India histograms for these 2-week data and find that the frequency of Conficker attacks of day-in-week has two peaks in Figure 4.3a. The linear histograms show that the data are not normalised.

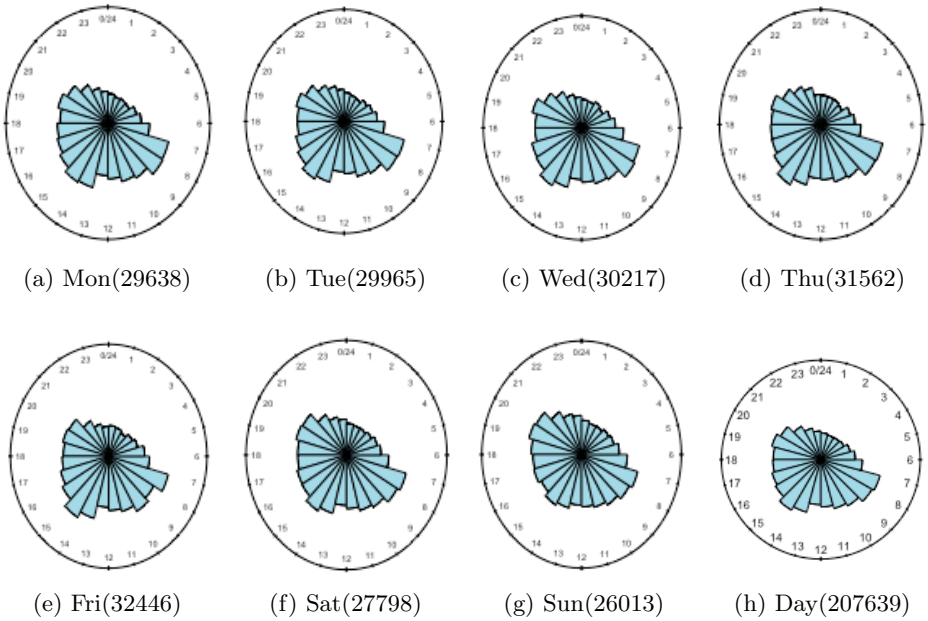


(a) Mon(11050) (b) Tue(16381) (c) Wed(16424) (d) Thu(15426)

(e) Fri(17377) (f) Sat(16089) (g) Sun(7074) (h) Day(99821)

Figure 4.6: IN Weekly Circles (Dataset of attacks in two weeks)

Figure 4.6 illustrates the time variations of time-in-week in India. The India rose diagrams from Monday to Saturday have the similar regulation distribution as the daily cycle. They peak at around 15:30, fall at about 2:00 and peak again at approximately 9:30. The Sunday rose diagram is different from the other days, it shows that the frequency of Conficker attacks mountain at around 11:30, and then keep a steady level until the next peaking time at about 18:30.



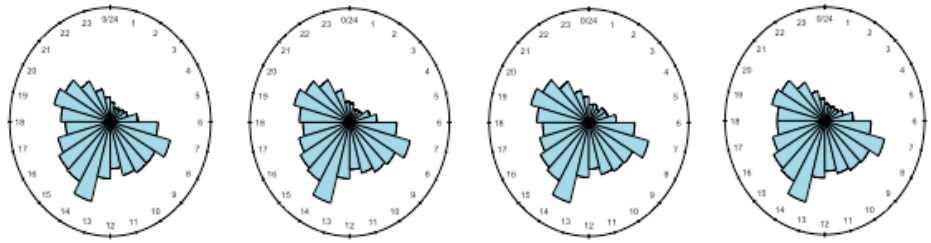
(a) Mon(29638) (b) Tue(29965) (c) Wed(30217) (d) Thu(31562)

(e) Fri(32446) (f) Sat(27798) (g) Sun(26013) (h) Day(207639)

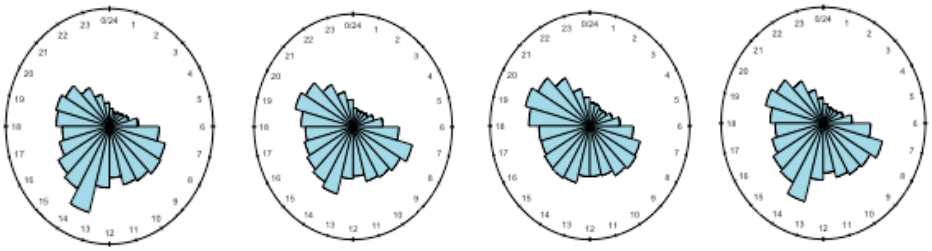
Figure 4.7: CN Weekly Circles

The China Conficker dataset is a large sample and has 207639 detected attacks. The rose diagrams of Monday to Sunday are similar to the daily circle. They have three peaks respectively are at around 7:30, 14:30 and 19:30, and the falling times at approximately 14:00 and 12:30. Overall, the China rose diagrams show a regular change in the time pattern variations of Conficker.

The VN weekly circles have a similar variation as India. From Monday to Saturday, the rose diagrams have a high similarity to the daily rose diagram with the same peak and falling times. Three peaks appear at around 7:30, 13:30 and 19:30, and 13:30 has the highest frequency. Nevertheless, the peak period of the Sunday rose diagram is 18:00-21:00. The incidence of Conficker occurring on Sunday afternoon is lower than the other days.

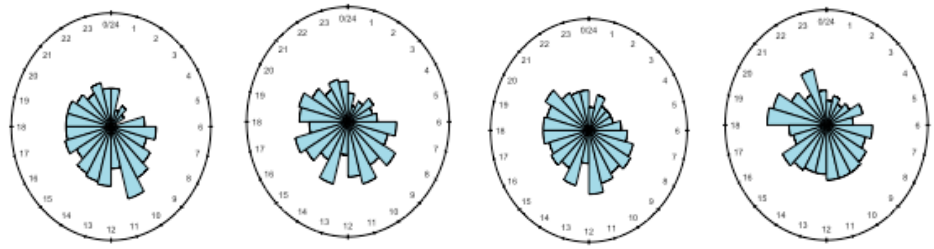


(a) Mon(11179) (b) Tue(11337) (c) Wed(11857) (d) Thu(13519)

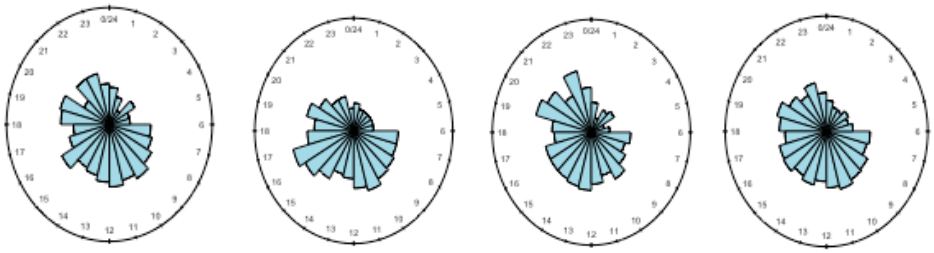


(e) Fri(13537) (f) Sat(10918) (g) Sun(9682) (h) Day(82029)

Figure 4.8: VN Weekly Circles



(a) Mon(176) (b) Tue(192) (c) Wed(184) (d) Thu(175)



(e) Fri(197) (f) Sat(200) (g) Sun(228) (h) Day(1352)

Figure 4.9: UK Weekly Circles

The UK has 1352 conficker attacks and its Figure 4.9 presents an irregular time pattern. The time pattern is very different from the other countries. The rose dia-

grams show the irregular peak and falling times. Therefore, we obtain the following information by observing all rose diagrams:

1. India and Vietnam have the similar patterns from Monday to Sunday. The frequency of Conficker attacks from Monday to Saturday has identical variations in the daily rose diagram. However, Sunday afternoon has different time variation.

2. All China cycles show the high similarity in the time variations.

3. The UK cycles have the irregular changing rules from Monday to Sunday and are different from its daily cycle.

4. The time pattern variations of Conficker illustrate that it is active during the working hours in working days plus Saturday. Figure 4.7 and 4.8 show the regular time variations like India rose diagrams. The rose diagrams of Monday, Tuesday, Wednesday, Thursday, Friday and Saturday in India, China and Vietnam are very similar to the corresponding daily circles. That means the attacks of Conficker in these days will become active from around 7:00, peak at about 13:30 or 14:00 and fall overnight.

5. The Sunday rose diagrams in India, China and Vietnam are different from the other circles. Firstly, the frequency of Conficker on Sunday is lower than the other six days. Secondly, the Sunday time patterns show that the incidence of Conficker will decrease at around 13:00 to 15:00.

To sum up, the occurrences of Conficker in the UK are in very small extent less frequent than India, China and Vietnam. We discuss the reasons for the users' habits of Microsoft Windows application in these countries. The Conficker working group illustrates the computers are infected by Conficker at around the world, particularly the developing world of Asia such as India [65]. The team infers reasonably the reason why densely located in the developing world that the computers universally install the pirated Windows operating system software without patching these systems [65]. Therefore, attackers prefer to attack individuals in these countries. The attacks also display more regular variation from Monday and Saturday as the related daily circles. The UK, with a low frequency of Conficker, has an irregular weekly time distribution.

The results of time-in-week analysis reveal that the total number of attacks affects the time patterns. Specifically, India, China, and Vietnam, which have noticeably larger numbers of attacks than the UK, exhibit bimodality in the daily distributions of the attack, and little day-to-day variation within the week. The UK instead shows a somewhat multimodal daily variation with irregular peaks and quiet times.

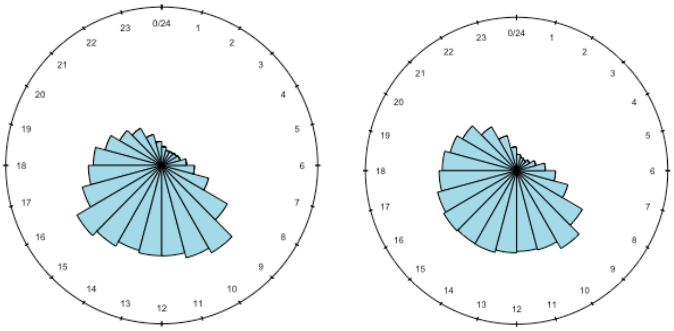
4.6 Comparisons

In this section, we focus on the time variations of different malware attacks in four countries. The two most frequent malware in each nation are compared, and the Mardia-Watson-Wheeler test (the test results are provided by the R 'circular' package [133]) is used to test whether these malware attacks have a common distribution.

We observe that Conficker and worm_dorkbot are the top two kinds of malware in India, China and Vietnam. In the UK, Conficker and tinba are the top two malware. All the observations of the malware are based on the top domain of each country.

4.6.1 Comparison in India

In India, 52% attacks are from worm_dorkbot and 47% are from Conficker. We observe from Figure 4.10 that the time variations of two m are very similar with no significant difference in the frequency of attacks. We apply the Mardia-Watson-Wheeler test to the relative attack samples and find the p-value is nearly 0. In this case, we have evidence against the null hypothesis that attacks from these two types of malware have a common distribution.

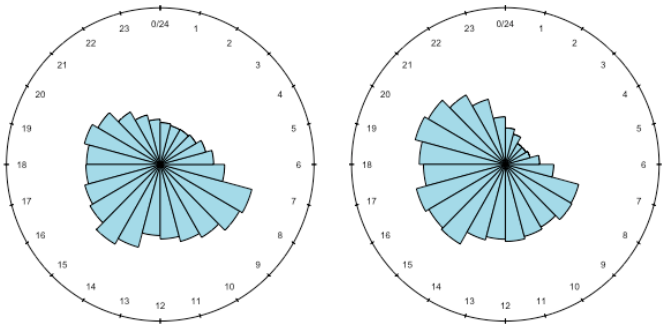


(a) Conficker(99821,47%) (b) Worm_dorkbot(110428,52%)

Figure 4.10: IN Daily Circles

4.6.2 Comparison in China

In China, 96% attacks are from the top malware Conficker and only 4% attacks from Worm_dorkbot. Figure 4.11 shows that the frequency of attacks from Conficker and Worm_dorkbot has similar time variations. The p-value of the Mardia-Watson-Wheeler test is nearly zero. Thus, we have significant evidence that the attacks from two kinds of malware do not have a common distribution.

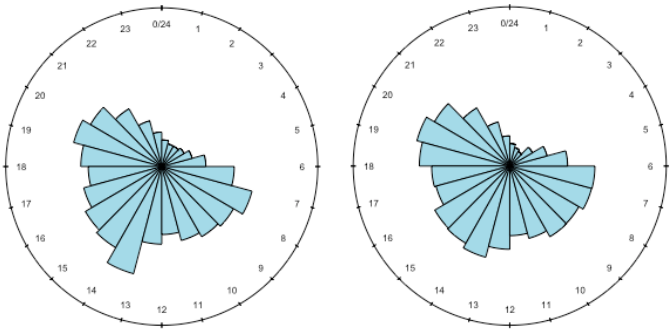


(a) Conficker(207639,96%) (b) Worm_dorkbot(7896,4%)

Figure 4.11: CN Daily Circles

4.6.3 Comparison in Vietnam

In domain vnnic.net.vn, 62% attacks are from Conficker and 36% attacks are from Worm_dorkbot. The time variations of the two categories of malware are very alike, although the number of attacks in each type of malware is slightly different as shown in Figure 4.12. The p-value of Mardia-Watson-Wheeler test is nearly zero. Thus, we have evidence against the common distribution hypothesis. In other words, the attacks from Conficker and Worm_dorkbot do not have a common distribution in domain vnnic.net.vn.



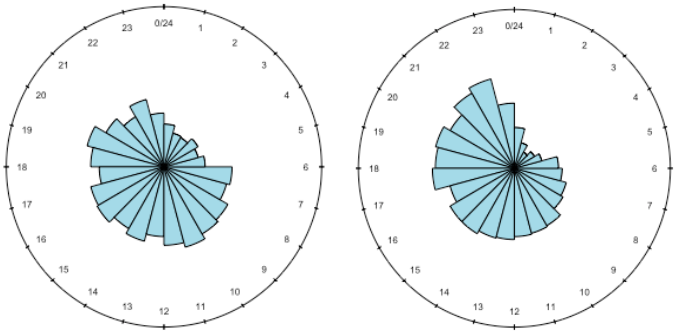
(a) Conficker(82029,62%) (b) Worm_dorkbot(47652,36%)

Figure 4.12: VN Dialy Circles

4.6.4 Comparison in the UK

Tinba is a trojan and the most prevalent malware in the domain opaltelecom.co.uk with 42% attacks. Conficker has 39% attacks in the same domain. The daily cycles of Conficker and tinba showed in Figure 4.13 are very different. We observe that

two cycles do not have common regular variations. The result of Mardia-Watson-Wheeler test shows that the p-value is nearly zero. That is, we have significant (at 1% significance level) evidence that two malware do no have a common distribution in domain opaltelecom.co.uk.



(a) Conficker(1352,39%) (b) Tinba(1451,42%)

Figure 4.13: UK Daily Circles

To sum up, Conficker and other malware in India, China, Vietnam and the United Kingdom do not have a common distribution regardless of the observation that the daily circle patterns of different malware. The test results of support this conclusion with very small p-values (like close to 0).

4.7 Conclusion

The objective of this work was to investigate the distribution of attacks on typical networks. By using circular statistics, we have found that the assumption of a Poisson distribution used by other researchers does not always hold. In addition, we have demonstrated circular statistics may be applied to analyse and visualise the time patterns of malware events. In particular, the daily, weekly cycles and helix diagrams provide a visualisation method. Thus we can monitor the malware behaviour and allocate resources to mitigate attacks more efficiently. The results of our analysis for four countries are also worth noting and are summarised as follows:

1. In India, China, and Vietnam, the active time periods for Conficker are approximately from 7:00 to 8:30, 13:00 to 15:00.

2. The frequency of Conficker attacks over these two weeks in the UK is lower than the other three countries.

3. The Rayleigh and Watson tests of uniformity illustrate that the active time of Conficker is not uniformly distributed around the 24-hour circle. Further, the results of time-in-week analysis reveal that the total number of attacks has an effect on the time patterns. Specifically, India, China, and Vietnam, which have noticeably larger numbers of attacks than the UK, exhibit bimodality in the daily distributions of the attack, and little day-to-day variation within the week. The UK shows a somewhat multimodal daily variation with irregular peaks and quiet times.

4. In the UK, the daily and weekly cycles show irregular time variations, but the cycles of India, China and Vietnam follow the similar and regular time pattern variations.

5. In India, China and Vietnam the Sunday cycles are different from the other weekdays. The occurrences of Conficker on Sunday afternoon is less than the same period in the other days.

6. The results of the large-sample Mardia-Watson-Wheeler test demonstrate that Conficker and the other malware do not have a common distribution, no matter the daily circles are alike or different, or the attacking frequency of malware is somewhat high or low.

We have demonstrated that the data strongly suggest non-uniform distributions of malware. In other words, the attack time of malware is not uniformly distributed over a 24-hour cycle. Malware will be active for some period and related to the human behaviours. We also illustrate that the malware time patterns of different countries have the common points such as peaking at mid morning and mid afternoon and falling at early overnight.

We believe that these findings will be helpful to improve the efficiency of detection systems. The analysis and visualisations could help decision makers in cybersecurity to efficiently allocate resources or estimate the cost of system monitoring in the different periods. And if malware activity is observed at an unusual time, security managers may then investigate further.

One possible limitation of this work is that we only use data in August. Thus we did not consider it would be useful to extend the analysis to monthly or quarterly patterns. But our goal was to examine the application of circular statistical analysis applied to incidents of malware attacks rather than looking at the distributions using linear statistics. Furthermore, in the future research, it is worth noting that closing the timeline into a circle results in having infinitely many uniform partitions (of a fixed

size, say, hourly). The new research directions will provide the possibility of assessing the robustness of various statistical tests to time translations.

However, we will keep tracking the time patterns of malware attacks by more real data. Having demonstrated that we can identify probability distributions for malware events, we are hoping to extend this work by investigating the likelihood of cyber attacks in general. If we can quantify this, it will allow us to make a better estimate of the risk an organisation faces regarding cyber attacks.

Chapter 5

VaR and Cyber Threats

Chapter 4 provided us with a deeper understanding of the distribution of attacks by specific types of malware. This knowledge is necessary if we are to apply VaR techniques to ISRA. Chapter 3 illustrates the advantages and disadvantages of existing quantitative risk analysis methods. In spite of models complexity, the quantitative approaches are more objective to assess the risks. Thus, the concept of VaR in ISRA is applied to reduce the complexity and make the quantitative models easy to understand. Moreover, different quantitative, qualitative or hybrid models require various information as the assessment dataset. For instance, Chang and Lee need the knowledge of the levels of threats and vulnerabilities, their corresponding values of C.I.A. [1] to assess the risk scores [35]. Khanmohammadi and Houmb consider the weight and effect of a vulnerability in the process-based risk analysis model [89]. Lo and Chen pay attention to the interrelations among security control areas in the hybrid model of risk analysis [107]. Therefore, when applying VaR as a risk analysis approach, we would like to focus on the distribution of malware attacks and use the relevant information as the input data in the VaR models.

Furthermore, some approaches divide the impacts of threats into three ranks including high, medium and low [8]. They also assign the scores to these three grades such as five representing high and one indicating week. But there is no single standard for setting these scores. For instance, we do not know the real difference between applying four and five as the score of high impact. The frequency is another essential factor in calculating the probability. It is hard to obtain the data of frequency for some threats such as insider threats.

The following sections examine the definition of a cyber threat and the evolution of VaR in ISRA. Assessing the losses of cyber threats is still a controversial topic in

[1] Confidentiality, Integrity, Availability

most of the risk analysis methods. Some authors propose to apply the VaR method as a solution. For example, Raugas et al. present a CyberVaR model to assess the losses of cyber threats [141]. The CyberVaR model estimates the threat levels from the theory of dynamic Bayesian network and attack tree. It also applies the Monte-Carlo Simulation to obtain the assessment results.

5.1 Cyber Threat

Organizations use risk assessment for making decisions of the investment in security and mitigating the risks by the results of risk assessments. There are various approaches of ISRA discussed in chapter 3. Fuzzy membership theories and Analytic Hierarchy Process (AHP) are two main types of risk analysis methods for quantifying or qualifying a variety of threats and vulnerabilities.

Nevertheless, these ISRA methods have their limitations due to the nature of information security risks. Information security risks are complicated and changeable in the different industries. Furthermore, the relevant standards and approaches are established for the general risks and not applied by the organisations effectively. Therefore, we argue to evaluate the information security risks by suitable methods for each type of threats. The data is collected from questionnaires and interviews. However, it is difficult to obtain the data of frequency of threat occurrence by the ways due to the nature of threats. Hence, it is hard to capture the likelihood of the risks due to the lack of frequency data in the traditional ISRA.

The systematic review of ISRA shows that most of the authors still improve the risk analysis methods to general information security risks [128]. In this instance, when such a method is used to a specific threat, it is hard to follow its calculation due to the specificity of the threat. For example, Denial of Services (DoS) of the cyber threats may cause severe impact in the energy-power industry. The leakage of the customer information by phishing will cause much severity of impact and financial losses in the banking industry. Moreover, the probability distributions of different cyber threats may not be the same due to their respectively unique propagation behaviours or the scope of networks [93]. Therefore, we will focus on the ISRA process of cyber threats.

ISO 27005 defines a threat as “a potential cause of an incident, that may result in harm to systems and organisation” [6]. Cyber threats are “potential cyber events that may cause unwanted outcomes, resulting in harm to a system or organisation” [179]. A cyber threat was one of the four highest risks in the national security strategy of the UK in 2010, and the most significant threat to the national security of the USA in 2013 [143]. With the innovation of internet banking technology, a cyber threat is becoming

more and more sophisticated and will continue to be the prime target in the following years [43]. However, Gilligan and Corporation find that low or very low sophisticated cyber attacks account for 75% in all threats [42].

Nowadays, banks much rely on the internet with the technological innovation and the broad application of web and mobile banking. In this case, cybersecurity becomes more and more important for banks. Cybersecurity is not only about information security technology but also from a business side. Thus, we have to consider the financial loss of a cyber attack and the cost of investing information security, not just study the technology of preventing all information security risks [20, 80].

5.1.1 Loss due to Cyber Threats

UK banks reported that the online banking losses were up to 59.7 million in 2009. Nelson states that the losses of the malware infection were about $120 million in the third quarter of 2009 for the online U.S. banking[2]. For companies, the loss of cybercrime may come from the theft of confidential business information for negotiations, stock market manipulation for price fluctuation, the financial crime like stealing money from the account and the interruptions of critical services [44]. Anderson et al. state that cybercrime has direct and indirect when considering its consequence [28]. They define the direct losses and indirect losses as follows.

Definition 5.1.1. *"Direct loss is the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime" [28].*

Definition 5.1.2. *"Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime" [28].*

Following the definitions, Anderson et al. also show the explicit examples in Figure 5.1 and Figure 5.2.

- Money withdrawn from victim accounts;
- Time and effort to reset account credentials (for banks and consumers);
- Distress suffered by victims;
- Secondary costs of overdrawn accounts: deferred purchases, inconvenience of not having access to money when needed;
- Lost attention and bandwidth caused by spam messages, even if they are not reacted to.

Figure 5.1: Examples of direct losses [28]

[2] http://www.computerworld.com/article/2520400/government-it/fdic--hackers-took-more-than--120m-in-three-months.html

- Loss of trust in online banking, leading to reduced revenues from electronic transaction fees, and higher costs for maintaining branch staff and cheque clearing facilities;
- Missed business opportunity for banks to communicate with their customers by email;
- Reduced uptake by citizens of electronic services as a result of lessened trust in online transactions;
- Efforts to clean-up PCs infected with malware for a spam sending botnet.

Figure 5.2: Examples of indirect losses [28]

Individual victims do not consider the problem of indirect losses [28]. In fact, it is an economic investment consideration to balance the attack losses and the defence costs in cybersecurity. Figure 5.3 illustrates the defence costs.

- Security products such as spam filters, antivirus, and browser extensions to protect users;
- Security services provided to individuals, such as training and awareness measures;
- Security services provided to industry, such as website take-down services;
- Fraud detection, tracking, and recuperation efforts;
- Law enforcement;
- The inconvenience of missing messages falsely classified as spam.

Figure 5.3: Examples of defence cost [28]

Annual Loss Expectancy (ALE) is an economic cost model to quantify cyber risks [30]. It is defined as "the total cost of an incident or Single Loss Expectancy (SLE), multiplied by the probability of the risk or the Annual Rate of Occurrence (ARO) occurring within that year" [30]. The ALE model provides a monetary number to present the probability and influence of cyber attacks to an organisation which will have the economic losses owing to these attacks [83]. However, ALE is a standard but not commonly used method to assess cyber risks due to the difficulties in measuring the cost and the likelihood of a cyber attack [83].

The quantitative economic analysis is an entirely reasonable way for the organization. However, the analysis is challenging in the field of cybersecurity due to the lack of relative data, such as the amount and influence of attacks [42]. Organizations do not report most cyber attacks [42]. The project of CCDCOE (Cooperative Cyber Defence Centre of Excellence) reports the problem of lacking the attack data [30]. However, most of the estimated losses of cybercrime are based on the incomplete data due to the lack of data [44].

There are many reasons to lead to the difficulty of data acquisition. For example, Moore suggests that the actual cost of cybercrime is difficult to estimate due to a

shortage of relevant information [119]. He also states that banks fear to reveal the fraud loss of online banking to terrify their customers, and companies don't like to show the cyber-espionage incidents to hit their reputation [119]. Moreover, Johnson highlights that it is challenging to estimate all the actual financial losses of cybercrime since its significant losses of intellectual property have immediate and long-term costs [83]. In fact, he demonstrates the reasons for this difficulty that there are no standardised cost measurement models, the standardised report protocol of security breaches [83]. In fact, business organisations are not reluctant to report all the security breach activities and the cybercrime [83]. In this case, there is no reliable empirical data on the losses of cyber threats or other attacks [83].

5.1.2 Network Externality

Most of the countries have not paid more attention to the calculation of cybercrime losses [44]. In reality, the national income levels have strong effects on the cybercrime losses [44]. The network externalities indicate that the protection of cybersecurity is not only your own business but also the social care. Moore explains that

Definition 5.1.3. *Network externality is " a larger network, or a community of software users, is more valuable to each of its members" [119].*

Network externalities are beneficial to explain the rise of the dominance of some popular computer applications such as the Windows operating systems, iTunes and Facebook. The phenomenon is "typical pattern of security flaws" [119] since it is difficult to develop a new application for an excessive secure operation system before dominating the market.

The attackers choosing a company as a victim consider the difficulty of hacking the networks and the attractiveness of a firm [44]. Thus, when we estimate the cyber risks, it is necessary to find the incentives of attackers and defenders. If the attackers can gain a higher return, they will do more. If the defenders underestimate the cyber risks, they will do less [44]. That means, the companies or individuals may underrate the risk and pay fewer attentions to the cybercrime losses and the cyber vulnerabilities [44].

Another reason for underestimating cyber risks for many companies is that they have no idea what is the extent of cybercrime losses and the amount of the acceptable losses [44]. The McAfee report presents a worry that whether companies can assess the risks accurately [44].

Therefore, we tries to find a relatively accurate model to assess the losses of cyber threats to companies. To make sure the accuracy, we only focus on the assessment of cyber threats, notably malware. We also measure the losses from the top organisation

level, not going into many details. The ISRA VaR model presents a possibility of constructing a new risk loss assessment method. In fact, the later Malware Value-at-Risk model only considers the direct loss for these computer users. Once their users will assess the direct losses by the value of inside data once malware attacks these networks, For example, the machine user of marketing department will estimate the losses of the customer information, which may be the most informative data, once malware infects their machines. Likewise, for the human administration officer, they have to evaluate the losses of the leakage of the staff data.

5.2 Value at Risk (VaR)

For the economic cyber risk models, the lack of data and the availability of data are the difficulties for estimating the losses of attacks [30]. In other words, the loss of malware infection is a complicated issue. We have to consider the scope of the networks, and the derivation of the business value in the estimation of malware loss [93]. Furthermore, there is a conflict between the types of losses and the idea of the VaR model. For instance, if we pay more attention to the details of direct and indirect losses of an organisation, and set up too more assumptions in the ISRA VaR model, this will limit the model availability. That means it is inconsistent with the construct of the ISRA VaR model, which as a quantitative risk analysis methods is to provide a unified model for organisations. To my knowledge, most quantitative methods are too complicated and limited for institutions. And the results of these methods cannot be compared among companies. Likewise, the qualitative risk analysis methods have the similar flaw except for the higher investigation costs in designing the survey and interviews. Therefore, so far, the ISRA VaR model provides a good idea of result unity.

In 1993, JPMorgan and G-30 presented the concept of Value-at-Risk (VaR) and took it as a market risk measurement. Until now, VaR has become a wide-used risk analysis model in the financial sector. We adopt an easy-understanding and well-accepted mathematical definition of Philippe Jorion [85].

Definition 2.1 (Value-at-Risk): Given a confidence level $\alpha \in (0, 1)$ and the loss L, and the probability that the loss L exceeds VaR is no larger than (1-α) such that

$$P(L > VaR) \leq 1 - \alpha.$$

In fact, Jorion describes VaR as "the worst loss over a target horizon" [85]. Let us denote L as the loss and $L = V_0 - V_T$, where V_0 is the value of an asset without an attack at time zero, and V_T is the value of an asset after a threat attack at time T. Hence, the probability of L exceeding the estimated the worst loss VaR will be less than (1-α).

Indeed, collecting a mass of data to determine distribution functions accurately may be difficult if the VaR method is applied for assessing information security risks [103]. Furthermore, VaR underestimates the risk of portfolios in financial risk assessment when the loss distribution of portfolios is fat-tailed and not normal [188]. Moreover, the calculation of VaR just considers the worst loss, not the average loss [80].

5.3 Evolution of VaR in ISRA

Nowadays, researchers pay more attention to the connection between financial risk model and ISRA methods. For instance, a financial risk model like VaR is used to assess cyber threats [141] or hedge risks [130].

Jaisingh and Rees initially used the application of VaR in measuring information security risks in 2001 [80]. They consider the logs of unauthorised external access and historical data as the input data of estimating the likelihood of threats [80]. However, in their VaR model, they just mention the concept of the worst loss of the input data of estimated impact without considering what the worst loss should include.

In 2004, Lenstra and Voss stated VaR was too difficult to apply in Enterprise risk assessment due to lack of historical data [103]. They also argued that VaR was too general and not applicable due to the difficulty of obtaining the input data [103].

Ozcelik and Rees suggested that VaR was a good quantitative method for ISRA to balance the risk and mitigation cost better in 2005 [126]. In 2009, Romanov and Okamoto illustrated VaR was an effective and object approach and applied annual loss expectancy as the input [146]. Romanov et al. further demonstrate the incident loss expressions in the VaR model in 2010. They depicted that the loss per incident contained the cost in man processing time, machine downtime, tangible and intangible asset damages [147].

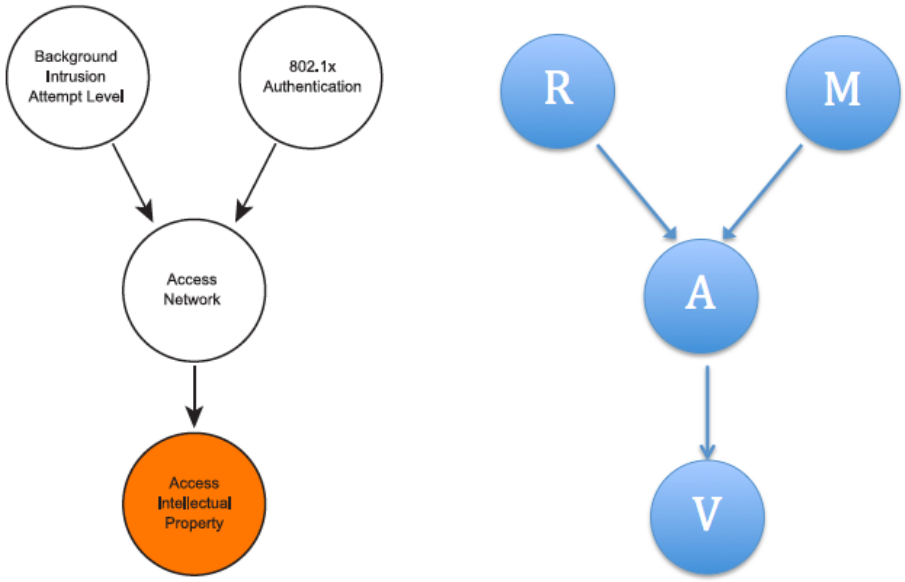
Raugas et al. initially proposed the concept of CyberVaR, which meant VaR was applied in assessing cyber threats in 2013 [141]. They solved the problem of lacking input data via the Monte Carlo simulation [141]. Beckstrom stated that the CyberVaR model provided a powerful framework for the risk estimation process [21] in 2014. The World Economic Forum stated that a Cyber VaR model was useful to "standardise and unify different factors that can quantify the cyber risk exposure" in 2015 [130]. At the same year, the CyberVaR model was applied to hedge cyber risks [130]. The Open Group promoted the application of CyberVaR models in 2016 [152]. Furthermore, so far, FAIR was the only international standard adopting CyberVaR for ISRA [152].

5.4 CyberVaR Model

This section will make a brief introduction to the CyberVaR model. It will not only present the concept of the model but also discuss the advantages and disadvantage including its assumptions. CyberVaR is a risk analysis method that uses a statistical probability to estimate the expected loss over a given period and confidence level [141]. The CyberVaR model solves the limitations of original VaR to some extent. It applied Monte Carlo simulation to obtain a sample loss distribution that is from conditional joint loss distributions. This model considers the losses where the successful attacks via passing the access nodes directly to the asset nodes [141]. Moreover, the CyberVaR model constructs a probability distribution to model the likelihood of loss at a given time horizon by a dynamic Bayesian network. Overall, the goals of a CyberVaR model are as follows. Firstly, the model could assess the loss amount of cyber threats over a given time horizon [21]. Secondly, the model has the business impact of the balancing decisions between protecting the organizations and running the business [152]. Thirdly, the model also analyse the relative economic costs at an organizational level [172]. Finally, the model provides the uniform and understandable financial terms [152].

5.4.1 Assumptions

The CyberVaR model starts at a simple case based on a Bayesian network [141]. A Bayesian Network is defined as "a directed acyclic graph in which each vertex v represents a random variable with probability distribution P_v, such that if v has parents $p_1, p_2, ..., p_n$, then P_v is conditioned on the p_i" [92]. Figure 5.4 shows the structure of a Bayesian network of the cyber threat, and presents a straightforward example including only one type of the cyber threat and only one security control measures [141].



(a) Model example [141] (b) Conversion chart

Figure 5.4: A simple example of a Bayesian network

Indeed, Raugas et al. consider each node in an attack tree as a random variable and describe each node by a probability distribution [141]. This probability distribution is based on the variables of the relative parent nodes if the nodes exist. According to Figure 5.4b, we demonstrate the initial assumptions of the CyberVaR model as follows.

1. **Probability of Risk nodes (R)** follows a Poisson distribution. There is a parent node for Risk nodes.

2. **Probability of Mitigation nodes (M)** follows a Bernoulli distribution with time-independent. The model supposes that the Bernoulli distribution with ξ given by some standards such IEEE 802.1X and CWEs such as $\xi = 0.71$ for the theft of credentials. The simple case (only one threat) of the model assumes that there is just one mitigation available in one network.

3. **Probability of Access nodes (A)** is conditional probability based on probabilities of R and M such that

$$A(d) = \begin{cases} 1 & \text{at least one successful attack on day d} \\ 0 & \text{no successful attack on day d} \end{cases}$$

4. **Probability of Asset nodes (V)** is also Conditional probability based on probability of A, Time-dependent; A given fixed loss rate r, initial loss values V(d) to

the threat, and set $V_i(d+1) = V_i(d) - l_{i_d}$ (but not mentioned these values are given by experts or historical data).

5. Only Mitigation nodes will access to Access nodes.
6. Only one Risk node will access to Access nodes ($R \longrightarrow$ A).
7. The number of parent nodes accessing to Access nodes is ≥ 0.
8. One or more than one Access nodes access to Asset nodes ($A \longrightarrow$ V).
9. A single Risk node (R) in a Bayesian network.
10. R and M are independent.
11. Loss distribution is not normal as Figure 5.5 shows.
12. Fix loss rate r is given by the initial condition.
13. Time period/resolution is Day.
14. Simulation sample sizes is 100.
15. The overall input is a set of attack tree instances.

5.4.2 CyberVaR Formula

Hence, the CyberVaR model computes the likelihood of a cyber threat by the following formula [141]:

$$P(B = b, \Xi = \xi, A = a, L = l) = P_B(b)P_\Xi(\xi)P(a|B = b, \Xi = \xi)P_L(l|A = a) \quad (5.1)$$

where

$\boldsymbol{n}$ **:** the number of attack attempts and n $\in [1, M]$;

$\boldsymbol{B}$ **:** random variable of a cyber threat;

$\boldsymbol{P_B(n, d)}$ **:** the frequency of threat;

$\boldsymbol{\Xi}$ **:** random variable of a risk mitigation;

$\boldsymbol{A}$ **:** a random variable of attack results;

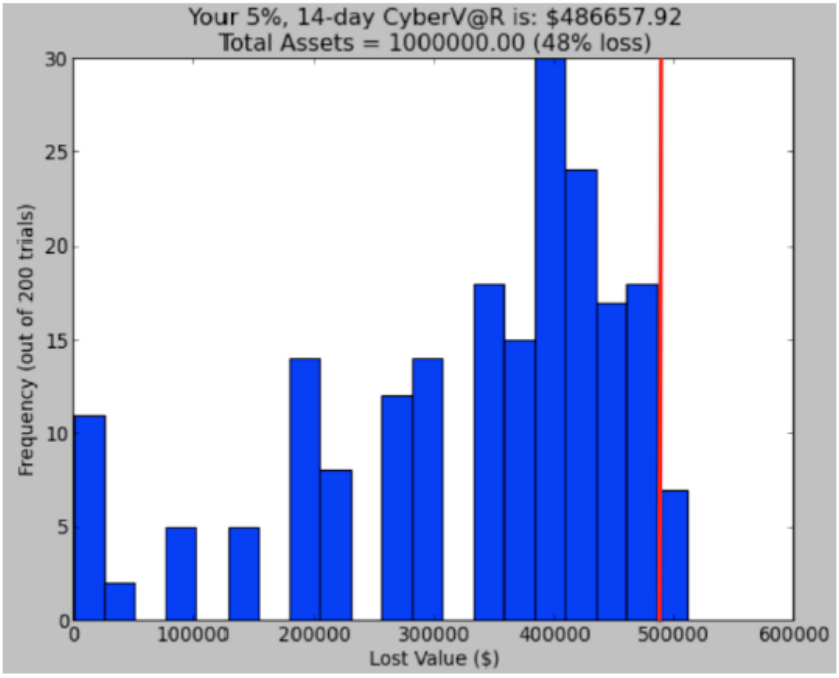


Figure 5.5: Loss distribution - computed by CyberVaR at 95 % confidence level [172]

***A(d)* :**

$$A(d) = \begin{cases} 1 & \text{at least one successful attack on day d} \\ 0 & \text{no successful attack on day d} \end{cases}$$

***L* :** random variable of the loss of attack to an asset;

***$P_I(i|J = j)$* :** probability of variable I taking value i given variable J taking value j.

A cyber attack is changeable as time goes on, thus the probability of loss distribution also changes with time. In this instance, CyberVaR also adds the time variable into the model. Furthermore, some standards list the efficacy values of specific risk mitigation which can replace the absent of information of efficacy of the risk mitigation technology in the model calculation. According to the formula of likelihood above and the added time variable and some certainty values, we can calculate the expected value of L on day d as follows:

$$E[L, d] = \sum_{n=1}^{n=M} \frac{\lambda_d^n}{n!} e^{-\lambda_d}(1 - (\xi)^n)\frac{1}{r}V(d). \tag{5.2}$$

The model sets up the simulation samples as S_i where i=1,..., K (Such as K=100). All the simulated loss values $V_i(d)$ are initialized to V(0). According to equation 5.1

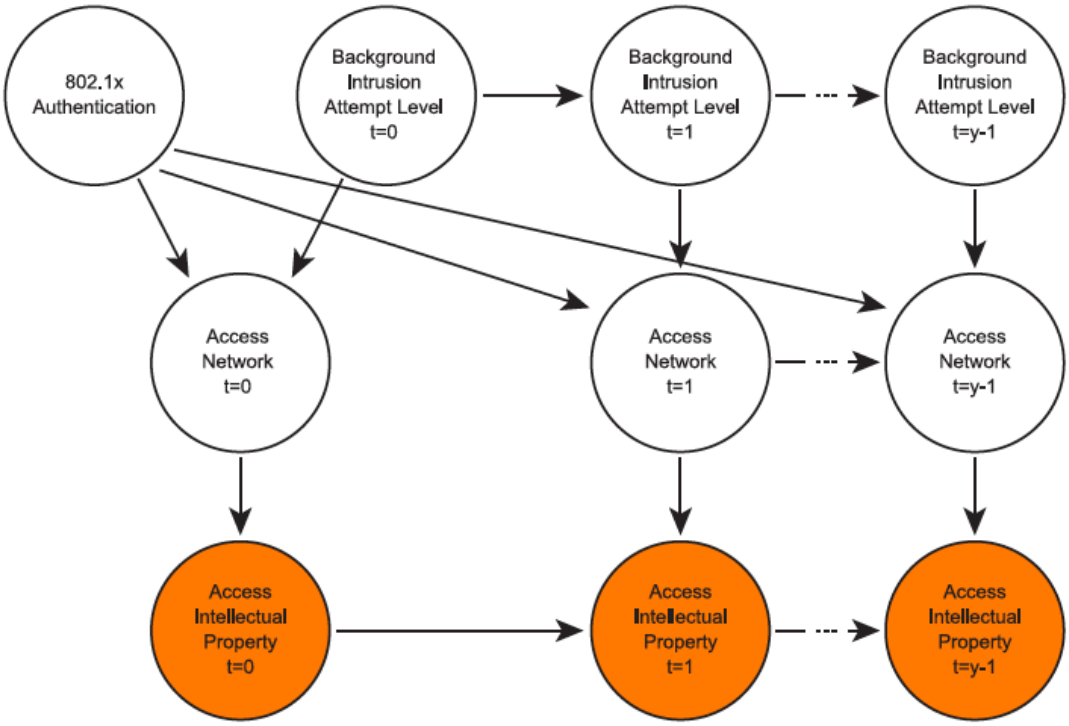


Figure 5.6: Two time-slice dynamic Bayesian network [141]

and equation 5.2, the total losses l_i are obtained by summing up all l_{i_d}. We will obtain the value of CyberVaR by ranking the total loss l_i in decreasing order and applying the equation $P(l_i \geq CyberVaR) \leq (1 - \alpha)$ to the ordered total loss.

Raugas et al. [141] propose CyberVaR is just consider one threat in the dynamic Bayesian networks over different segments of time. The model does not consider the multiple threats and their interrelations. In other words, the model still exist the following flaws. First, the CyberVaR model did not mention the correlations between threats. Second, a time period of the model needs to be discussed in future. For example, McQueen et al. [117] mentions eight hours (two non-professional attackers), 5.8 days for other situation, and 5.8 days + a function for the third situation). Moreover, the probability distribution of a threat node is not only Poisson distribution, may be others, such as Power law [110] or Weibull distribution [89].

It is a challenge but exciting research direction of applying VaR to assess the risk level of cyber threats, notably malware. Traditional cyber risk measure applies risk scores as the assessment standards, which did not connect to the economic view what do these risk scores mean for organisations. In other words, the scores may ignore the business impact. The application of VaR in cybersecurity overcomes this problem and

provider a monetary figure to decision makers of a company. However, the drawbacks of the CyberVaR model provide an opportunity for us to study the concrete and reasonable assumptions and the application scope of this model. The model limitations suggest the probability of assessing cyber threats from the other theory such as the portfolio VaR theory.

Chapter 6

Malware VaR-at-Risk (MVaR)

Johnson [83] states that an economic cost or loss model is essential for an organisation to assess the cyber threat and provide the evidence to make rational decisions about security investment. He further points out that the computer security effectiveness is hard to determine without such cost/loss models.

Chapter 5 has made a brief introduction to the original CyberVaR model established by Raugas et al. [141]. The model is a new and exciting idea for assessing the cyber threats. Based on the concept of their model, this chapter will construct a similar cyber VaR model by using the portfolio concept and focus on malware called malware VaR (MVaR) model. The MVaR model also tries to answer the research questions by making more explicit assumptions compared with the CyberVaR model. Hence, it will assess the losses of the cyberattacks on the company's computers by the portfolio VaR theory. Consequently, it is available to evaluate the worst losses when the company is considered as a portfolio and each machine as a stock.

We have discussed how time patterns of malware by circular statistics and revealed some interesting features of malware in chapter 4. For example, the malware attack is active during the working period on a day. Moore presents that the percentage of computers of malware infection increases to 25% or more [119]. The behaviours of malware usually are stealing a password, compromising online banking service, and planting a botnet to the infected machines [119]. Once the botnet is placed, infected computers will be controlled by the malware writers to send spam emails, launch DDoS, make phishing attacks, and commit the online-advertising fraud [119].

There are some usual methods to 'clean up' the malware. First of all, it is quite common to install the anti-virus software which can detect the malware. Second, Regularly update or patch the Windows systems. Third, malware identification and notification by third-party security firms. The third-party security teams will monitor

internet traffic and report the malicious activity to the related internet service providers [119]. However, the update of anti-virus software will be disabled by most of malware. Furthermore, the failing update of Window systems means the failure of detecting the malware [119]. Internet service providers will have two action opinions of finding malware: notify or quarantine consumers. But notification will be the first choice for these providers due to low costs [119].

Chapter 4 demonstrated that Conficker was the common malware in China, Vietnam, India and the UK according to the Spamhaus data of 2017. Thus, this chapter will make a brief introduction to the background of Conficker including the evolution, features and impacts, the theory of financial VaR, the new model MVaR.

6.1 Conficker

Conficker, as one type of malware, has become a severe cyber threat since released in 2008. The infected computers by Conficker become the propagation platforms of the malicious behaviours such as sending spam emails and stealing the user data. In fact, Conficker as a well-known and large-scale computer malware can self-propagate and infect the other computers via exploiting the vulnerabilities of the Window operating systems [163]. In this section, we will discuss the evolution, features, existing studies and impact of Conficker.

6.1.1 Evolution

According to ICANN security team report 2010 [134], Conficker was a worm discovered in October 2008 and quickly infected the home and company networks. The infection varied diffusely and spread over millions of personal computers. The Conficker infects the computer systems by sharing the network files, "mapped drives and removable media" [134]. Piscitello states Conficker malware cannot infect the machines alone, it has to be attached on an executable application to exploit the vulnerability of Windows operating system, and then the Conficker writer can make use of the vulnerability to execute the remote code on the Windows services [134]. The report further presents that Conficker attacks the networks by using the domain names rather than IP addresses. The Conficker common and control hosts are initially identified by sinkholing the domain registration to prevent the communication between the Conficker writer and infected machines. However, the Conficker writers create more variants, which can generate more domain names and distribute these titles widely, as against this first countermeasure.

How do the infected machine and Conficker malware writer connect each other?

In the early Conficker variant, once the machine is infected, the Conficker malware on that infected computer will run a new domain list. And the Conficker malware writers will generate the same domain list by the same algorithm, which is used in the infected machine, and register some of them. The registered domain names will be "assigned to Internet rendezvous logic points to be resolved to IP addresses by DNS resolvers" [134]. However, the Conficker variants have changed the methods as above to "a peer-to-peer network" [134]. That means the malware on the infected machines can make use of the botnets of other infected machines which have the same 'inject' code to share the files by "connecting to HTTP servers" [134]. In CERT-UK report 2015/2016, Conficker is still "the most prevalent malware" [134]. The report also mentions that many computers infected by Conficker will launch the attacks by network even not the victim of the attack and cause a vast cost [134]. The Conficker working group (CWG) keeps tracking the Conficker infection and find that the population are still large [134]. Moreover, ICANN report found that China, India and Vietnam were always in the top 5 list of the most infected countries in every quarter of 2009. In practice, this finding still exists in chapter 4. China, India and Vietnam are still the top 3 infected countries by Conficker.

There are primary variants of Conficker and shown in figure 6.1. The first Conficker named Win31/Conficker.A was discovered by Microsoft on 21 November 2008 and then the second variant of Conficker (Win32/Conficker.B) was reported to Microsoft on 29 December 2008 [88]. Conficker.A worm attempts to infect the unpatched Windows operating systems and then spread quickly by an Intranet to the other computers within an organisation [88].

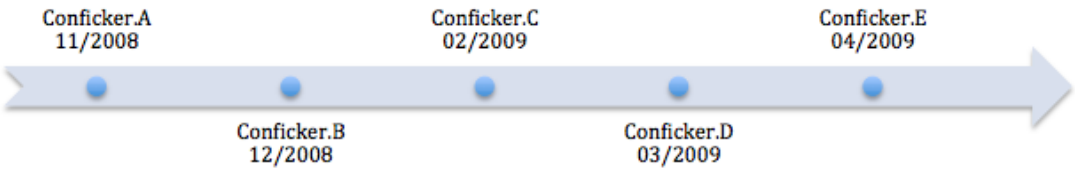


Figure 6.1: The historic time line of Conficker

6.1.2 Features

We summarise the features of Conficker as follows.

1. **Fast infection :** Kaska states the reason why Conficker can rapidly spread to the whole Intranet that it effectively and quickly release the malware to the relative exploited vulnerability in Windows [88].

2. **Unbalance distribution :** Irwin describes an example in his Conficker research that fewer data are observed from midnight to 5 am, but after the observe data increase quickly per hour after 5 am [77].

3. **Heavy dependency :** Conficker is a heavy dependency on the popularising rate of Windows systems; The Conficker working group illustrates the computers are infected by Conficker at around the world, particularly the developing world of Asia such as India [65]. The group infers the reason why heavily located in the developing world that the computers universally install the pirated Windows operating system software without patching these systems [65].

4. **Domain oriented :** Piscitello highlights that Conficker attacks networks via domain names rather than IP addresses [134].

6.1.3 Existing studies of Conficker Analysis

There are two directions for analysing Conficker: binary behaviour analysis and DNS sinkhole data analysis [158]. The study of binary behaviour focuses on revealing the domain generation algorithms [158]. DNS sinkhole data analysis would pay more attention to Conficker propagation patterns and the distribution over networks [158]. Shin and Gu provide an in-depth study of Conficker distribution over networks. They find the victims of Conficker do not follow a uniformity distribution over IP addresses space [158]. They found that the IP address ranges 109.*-125.* were vulnerable to Conficker attacks from 1 January 2010 to 8 January 2010 [158].

Based on their study of Conficker over IP address space, we also reviewed whether the ranges have changed or not so far. We collect the 14-day Conficker sinkhole data by an India domain 'san.*' which included 102833 unique IP addresses. Figure 6.2 shows the Conficker victim distribution over IP address spaces. We narrow down the ranges and find out the main prominent networks. Table 6.1 depicts the top 5 IP* networks. 117.* network accounts for 66.01% of all IP addresses and 59.* network accounts for 18.64%. That means a 117.* network is still in the ranges of 109.*-125.*, and 59.* network is a new one compared with Shin's research [158].

To sum up, the victims of Conficker over IP address space still do not follow a uniformity distribution in our research. However, there is a little bit change in the primary contributors of networks. The 59.* network range is a new one in our analysis.

6.1.4 Impact

According to McAfee report in 2017, the Conficker exploiting the vulnerabilities of Windows systems was on the list of top user malware. Once the Windows system

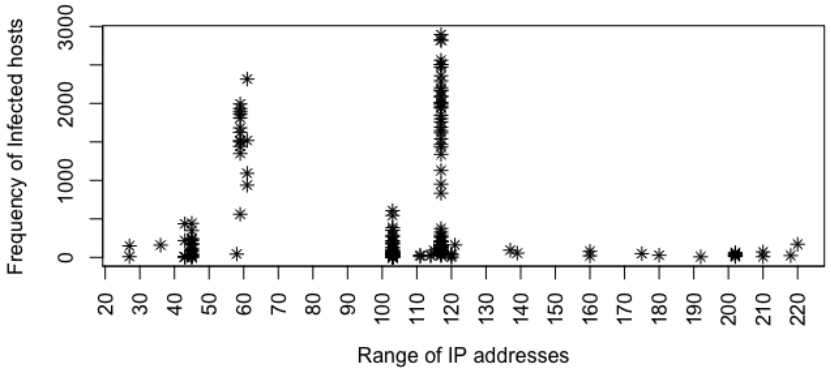


Figure 6.2: Conficker victim distribution over IP address space

Table 6.1: The frequency of top 5 IP addresses

IP*	Frequency	Percentage
117.*	67876	66.01%
59.*	19168	18.64%
61.*	5864	5.70%
103.*	5147	5.01%
45.*	2444	2.38%

is infected, some security services will be disabled such as the automatic updating and the defensive schemes. The Bitdefender organisation states that once defender systems corrupt, the infected computers will exploit a colossal security breach at any time [4]. Furthermore, Conficker attacks may cause network isolation such as DDoS by disrupting the connectivity of victim networks' bandwidths or overloading the resources of their computers systems [4].

The third impact of Conficker is to infect machines. Conficker usually is attached to a spam email and may be triggered by clicking the link to some malicious web pages for Frauds. These web pages may record your personal information including your passwords or bank accounts. The infected machines also may send or forward a mass of spam messages to the other computers.

6.2 Portfolio VaR

A portfolio VaR is "constructed from a combination of the risks of underlying securities" [85]. The individual securities' returns of a portfolio are assumed to follow a normal

distribution in the Delta-Normal model [85].

Before going to the introduction of the portfolio VaR, some basic definitions need to be clarified. In financial VaR, a return is "the change in the price divided by the original value" [183] and normally represents the rate of return in finance [85]. The volatility named as σ is a figure of "measures the standard deviation of the returns" [183] and it can be estimated by the daily, monthly or yearly historical data [135].

We take the following example to introduce the portfolio VaR and infer the formula. This example simply supposes that a portfolio P consists of N stocks with monetary position weight W_i, i=1, 2, ..., N. R_i is the return on stock i. The daily volatility $\sigma_{i,day}$ of the R_i is obtained by estimating the historical data. Then, the T-day volatility of return R_i on stock i is $\sigma_{i,T} = \sigma_{i,day} \times \sqrt{T}$.

The portfolio returns R_p on day T is defined as [85]:

$$R_{p,T} = \sum_{i=1}^{N} W_i R_{i,T} \tag{6.1}$$

Then we can derive the mean and variance of $R_{p,T}$, the mean [85] is

$$\mu_p = E(R_{p,T}) = \sum_{i=1}^{N} W_i E(R_{i,T}) = \sum_{i=1}^{N} W_i \mu_{i,T} \tag{6.2}$$

Where $\mu_{i,T}$ is the mean of the stock return on day T.

The variance $\sigma^2_{p,T}$ of $R_{p,T}$ on day T is written as [85]

$$\sigma^2_{p,T} = V(R_{p,T}) = V(\sum_{i=1}^{N} W_i R_{i,T}) = \sum_{i=1}^{N} W_i^2 \sigma^2_{i,T} + 2 \sum_{i=1}^{N} \sum_{j=1, j\neq i}^{N} \rho_{i,j} W_i \sigma_{i,T} W_j \sigma_{j,T} \tag{6.3}$$

where $\rho_{i,j}$ is the correlation coefficient of price changes between two stocks.

If the return $R_{i,T}$ of the stock prices over T day is assumed to distribute normally with mean 0 and variance $\sigma^2_{i,T}$ and written as $R_{i,T} \sim \mathcal{N}(0, \sigma^2_{i,T})$[85]. In this case, the return $R_{p,T}$ of the portfolio P also follows a normal distribution with $R_{p,T} \sim N(0, \sigma^2_{p,T})$ [85]. Based on the distribution assumption of $R_{p,T}$, and supposing $R_{p,T}$ as the loss L, then the VaR can be inferred at the confidence level α such that

$$P(R_{p,T} > VaR) = P(L > VaR) = \frac{1}{\sigma_{p,T}\sqrt{2\pi}} \int_{x=VaR}^{\infty} e^{-\frac{x^2}{2\sigma_{p,T}}} dx = 1 - \alpha \tag{6.4}$$

The standard normal distribution table lookup shows that $N(-2.33) = 0.01$, at the

confidence level 99%, the T-day VaR is 2.33 $\times\sigma_{p,T}$.

Under the assumption that the portfolio return follows a normal distribution, Jorion summarises the portfolio VaR on day T as [85]:

$$VaR_p = c \times \sigma_{p,T} \times P_0 \tag{6.5}$$

where c is the standard normal deviation under the confidence level α, σ_p is the standard deviation of the portfolio return, P_0 is the initial value of the portfolio and $P_0 = R_{p,o} = \sum_{i=1}^{N} W_i R_{i,0}$.

Overall, there are several crucial factors including the daily volatilities of stock prices' returns, the correction coefficient, the time horizon T in the portfolio VaR. Furthermore, we find that $VaR_T = VaR_{day} \times \sqrt{T}$ under the assumption of the normal distribution of the portfolio return or stock returns. However, we have to consider the case that the assumption of normal distribution of returns or losses in cybersecurity is reasonable or not. If not, how can we carry out the cyber VaR by the theory of portfolio VaR? The following section will try to answer this question by an MVaR model.

6.3 MVaR model

This section presents a VaR model of cyber threats as MVaR. The MVaR model is constructed by an analogy analysis with a portfolio VaR. It supposes each available computer (laptop and desktop) of a company as a stock and the company as a portfolio which consists of all these machines. The data values held on by the computers compose the value of a company portfolio. As we know, the stock prices will fluctuate when the financial risks occur. Likewise, the data value of a computer will change when it is under cyber attacks.

The reason why we take a computer as the valued item in the MVaR model. First, a machine is easy to assess its data value compared with an asset. The value of an asset will vary differently for the different user. However, a computer is valued by its user. The held data is evaluated as the value of a machine. Second, a machine is the primary and direct target of a cyber attack, and the change of its value will reflect upon mainly in the working time. That is, the staffs turn on the attacked computer when they do the routine job. In this case, the loss occurs when a computer has been successfully attacked during the working time. Third, the attack on a network often occurs in the working time which finds in the last chapter. Compared with a stock, the stock price will change during the market opening period when the share suffers from some financial risks.

In the MVaR model, a firm is regarded as a portfolio. The company has intangible

and tangible assets. In finance, the values of intangible and tangible assets are reflected in the stock price of a company. However, the MVaR model does not consider the value of intangible assets, and it only assess the losses of the data held on the computers which are attacked by malware.

6.3.1 Model Assumptions

The assumptions of the MVaR model are as follows.

***P*:** the portfolio value, here a company is regarded as a portfolio and P consists of only the data values of the computers. Some constraints of P are presented:

1. Information stored on any computer throughout the company;
2. Computer: the available device to store the data in an organisation;
3. Intangibles of a company are out of the model consideration; The model takes the concepts of a portfolio and stocks as an example to represent the idea of P;
4. The market trade of the stolen information is also out of the model consideration; A computer suffers from a loss with a successful malware attack;
5. The model only consider data leakages as the results of malware attacks, not data corruption or tampering with data.

***N*:** the number of computers in a company. We assume each staff only has one machine when he works in the company.

***T*:** time horizon. The loss of a company portfolio changes over T days.

***t*:** any given day and $1 \leq t \leq T$.

***$x_i(t)$*:** the random variable of attack attempts to computer i on day t with $x_i(t) = 0, 1, 2, ..., \infty$. $x_i(t)$ is assumed to follow a Poisson distribution with parameter $\lambda_i(t)$ [141]. The probability of random variable $x_i(t)$ is [71]

$$p(x_i(t)) = \frac{\lambda_i(t)^{x_i(t)}}{x_i(t)} e^{-\lambda_i(t)} \tag{6.6}$$

where $\lambda > 0$. The mean and variance of $x_i(t)$ are given by [71]

$$E(x_i(t)) = \lambda_i(t), V(x_i(t)) = \lambda_i(t). \tag{6.7}$$

Hence, if $x_1 \sim Po(\lambda_1)$ on day t, and $x_2 \sim Po(\lambda_2)$ on day t, then $x_1 + x_2 \sim Po(\lambda_1 + \lambda_2)$ on day t.

k: the type of malware attacks. In this model, we consider the Conficker attack.

a_k: the successful rate of k, $0 \leq a_k \leq 1$.

m_k: the mitigation rate of k and $0 \leq m_k \leq 1$; the value of m_k can be obtained by some standard such as IEEE 802.1x standard [141]; hence, the MVaR model supposes $a_k = 1 - m_k$.

l_k: the fixed loss rate of cyber attack k and given by the assumption, and the concept of l_k is cited from the CyberVaR model [141] and $0 \leq l_k \leq 1$.

v_i: the initial data value of a computer i. It depends on the stored information in the computer i. In other words, each v_i is determined by each unique computer user.

In the computers of different departments, it is reasonable to assume that they are unlikely to store the same data. For instance, the stored data of human resource computers will focus on the salary and performances of the whole company staff. However, the computers of the marketing department will pay more attention to the client information. The data values held on computers have different weights in the company. Once machines are attacked, the losses will be various. The model considers stealing data as the attack results. The data corruption or tampering is out of the model consideration.

$l_i(t)$: the daily loss caused by a computer i at a given day t such that

$$l_i(t) = x_i(t) a_k l_k v_i \tag{6.8}$$

$L_i(T)$: the total loss of computer i over T days and $L_i(T) = \sum_{t=1}^{T} l_i(t)$

L_P : the total loss of the N-computer portfolio over T days and $L_P = \sum_{i=1}^{N} L_i(T)$.

On the basis of assumptions above, we posit a very simple case to illustrate the MVaR model. There is only one computer which attacked by one attack type k in a company portfolio. Suppose the fixed loss rate $l_k = 1\%$ of the data value when a machine is attacked successfully, the successful rate of attack k $a_k = 10\%$ and the original data value held on the computer is $v_1 = £1000$. Now, we set on day 1, the related probabilities of attack attempts x_1 and the losses $l_1(1) = x_1(1) a_k l_k v_1$ are listed in Table 6.2.

Hence, on day 1, the portfolio loss $L_P = l_1(1)$ and VaR at the 95% confidence level

Table 6.2: The one-computer example of MVaR where $x_1^s(1)$ indicates the successful number of attack attempts under the given a_k, $l_1(1)$ is the attack loss caused by the computer 1 on day 1 .

Only one computer in the company portfolio							
parameters	value1	value2	value3	value4	value5	value6	...
$p(x_1(1))$	50%	25%	12%	8%	5%	0%	...
$x_1(1)$	0	1	2	3	4	5	...
$x_1^s(1)$	0	a_k	$2a_k$	$3a_k$	$4a_k$	$5a_k$	...
$l_1(1)$	0	$a_k l_k v_1$	$2a_k l_k v_1$	$3a_k l_k v_1$	$4a_k l_k v_1$	$5a_k l_k v_1$	...

such that

$$\begin{aligned} & p(L_P < VaR_1) = 95\% \\ & \Rightarrow p(x_1 < \frac{VaR_1}{a_k l_k v_1}) = 95\% \\ & \Rightarrow p(x_1 \geq \frac{VaR_1}{a_k l_k v_1}) = 5\% \\ & \Rightarrow p(x_1 = 4) = 5\% \\ & \Rightarrow VaR_1 = 4a_k l_k v_1 = 4 \times 10\% \times 1\% \times 1000 = £4 \end{aligned} \tag{6.9}$$

Therefore, for the one-computer portfolio, $VaR_1 = £4$ means there is only 5% probability that the loss exceeds $£4$.

Let us consider a more complex example. There are only two machines in the company and one type of attack k. Suppose the original computer values are $v_1 = 1000$ and $v_2 = 2000$, $l_k = 1\%$ and $a_k = 10\%$, at T=1, all the corresponding factors are showed are listed in Table 6.3.

Table 6.3: Two-computer example of MVaR

Only one computer in the company portfolio							
parameters	value1	value2	value3	value4	value5	value6	...
$p(x_1(1))$	50%	25%	12%	8%	5%	0%	...
$x_1(1)$	0	1	2	3	4	5	...
$x_1^s(1)$	0	a_k	$2a_k$	$3a_k$	$4a_k$	$5a_k$	...
$l_1(1)$	0	$a_k l_k v_1$	$2a_k l_k v_1$	$3a_k l_k v_1$	$4a_k l_k v_1$	$5a_k l_k v_1$	...
$p(x_2(1))$	50%	25%	20%	5%	0%	0%	...
$l_2(1)$	0	$a_k l_k v_2$	$2a_k l_k v_2$	$3a_k l_k v_2$	$4a_k l_k v_2$	$5a_k l_k v_2$	...

Hence, the portfolio loss on day 1 $L_2(1) = l_1(1) + l_2(1) = x_1(1)a_k l_k v_1 + x_2(1)a_k l_k v_2$ As we assumed, the $x_1(1) \sim Po(\lambda_1(1))$ and $x_2(1) \sim Po(\lambda_2(1))$, then $L_2(1) \sim Po(\lambda_1(1)R_1 + \lambda_2(1)R_2)$. That is, the total loss of a 2-computer portfolio L_P over 1 day is equal to

$L_2(1)$. Hence, at the 95% confidence level, $p(L_P < VaR_2) = 95\%$, where $L_P \sim Po(\lambda_1(1)R_1 + \lambda_2(1)R_2)$. We apply R-programme to computer VaR_2.

Therefore, the total loss of a computer i over T days $L_i(T) = \sum_{t=1}^{T} l_i(t)$ follows a Possion distribution such that

$$L_i(T) \sim Po(\sum_{t=1}^{T} \lambda_i(t)R_i) \tag{6.10}$$

Hence, the total loss of a N-computer company portfolio over T days $L_P = \sum_{i=1}^{N} L_i(T)$ follows a Poisson distribution such that

$$L_P \sim Po(\sum_{i=1}^{N}\sum_{t=1}^{T} \lambda_i(t)R_i) \tag{6.11}$$

According to the additivity property of a Poisson distribution, L_P is given by the Poisson assumption of attack attempts. However, if the attack attempts follow another distribution which hasn't the additivity property, we have to find alternative way to calculate the total loss L_P of an N-computer portfolio over T days. In this case, when the computer number N is large enough, then L_P can be obtained by Central Limit Theorem (CLT).

6.3.2 Central Limit Theorem for L_P

The classical central limit theorem requires that the random variables are independent identical distributed [25]. However, for a sequence of independent but not identical distributed random variables, we can apply the Lindeberg CLT [106]. Suppose that $\{L_i(T), L_i(T), ..., L_N(T)\}$ is a sequence of independent random variables with finite mean $E(L_i(T)) = \mu_i$ and finite positive variance $V(L_i(T)) = \sigma_i^2 < \infty$ for i=1,2,...,N. Let

$$\begin{aligned} Y_i &= L_i(T) - \mu_i \\ Y_N &= \sum_{i=1}^{N}(Y_i) \\ S_N^2 &= \sum_{i=1}^{N}\sigma_i^2 \end{aligned} \tag{6.12}$$

then the distribution of $\frac{Y_N}{S_N}$ is approximately N(0,1) as N goes to infinity such that

$$\frac{Y_N}{S_N} \xrightarrow{\text{condition}} N(0,1). \tag{6.13}$$

There are two classical conditions. One is Lindeberg condition [195]:

$$\text{if every } \epsilon > 0, \frac{1}{S_N^2} \sum_{t=1}^{T} E(Y_N^2 I | Y_N \geq \epsilon S_N) \to 0 \text{ as } N \to \infty. \tag{6.14}$$

Another one is Lyapunov condition [25]:

$$\text{for some } \delta > 0, \lim_{N \to \infty} \frac{1}{S_N^{2+\delta}} \sum_{i=1}^{N} \left[|Y_i|^{2+\delta} \right] = 0. \tag{6.15}$$

Thus, suppose the loss sequence $L_1, L_2, ..., L_N$ satisfies the Lindeberg/Lyapunov CLT, then, at 95% confidence level then, N(-1.65) = 1-0.95=0.05,

$$\begin{aligned} & p(\frac{Y_N}{S_N} > 1.65) = \frac{1}{2\pi} \int_{x=1.65}^{x=\infty} e^{-\frac{x^2}{2}} dx = 0.05 \\ & \Rightarrow p(\sum_{i=1}^{N} L_i(T) > 1.65 S_N + \sum_{i=1}^{N} \mu_i) = 0.05 \\ & \Rightarrow MVaR_{0.95} = 1.65 S_N + \sum_{i=1}^{N} \mu_i. \end{aligned} \tag{6.16}$$

Therefore, suppose c is the constant and $N(-c) = 1 - \alpha$ under the standard normal distribution, then

$$MVaR_\alpha = c \times S_N + \sum_{i=1}^{N} \mu_i \tag{6.17}$$

6.3.3 MVaR model

The MVaR model can be expressed by two ways:

1. if $x_i(t) \sim Po(\lambda_i(t))$ and $L_P = \sum_{i=1}^{N} \sum_{t=1}^{T} x_i(t) R_i$, then for a N-computer portfolio, $MVaR_\alpha = f(\lambda, \alpha)$ where $\lambda = \sum_{i=1}^{N} \sum_{t=1}^{T} \lambda_i(t) R_i$ and where $R_i = a_k l_k v_i$.

2. if $x_i(t)$ follows a non-Poisson distribution, the T-day loss caused by a machine i $L_i(T)$ with finite mean μ_i and variance σ_i^2, then $MVaR_\alpha = c \times S_N + \sum_{i=1}^{N} \mu_i$ where $S_N = \sqrt{\sum_{i=1}^{N} \sigma_i^2}$.

Nevertheless, Hogg et al. present that if a random variable $X \sim Po(\lambda)$ where λ is sufficiently large, then $\frac{X-\lambda}{\sqrt{\lambda}} \sim N(0,1)$ [71]. In this case, the first expression of the MVaR model can be merged into the second expression. We describe the whole process of the model by Figure 6.3.

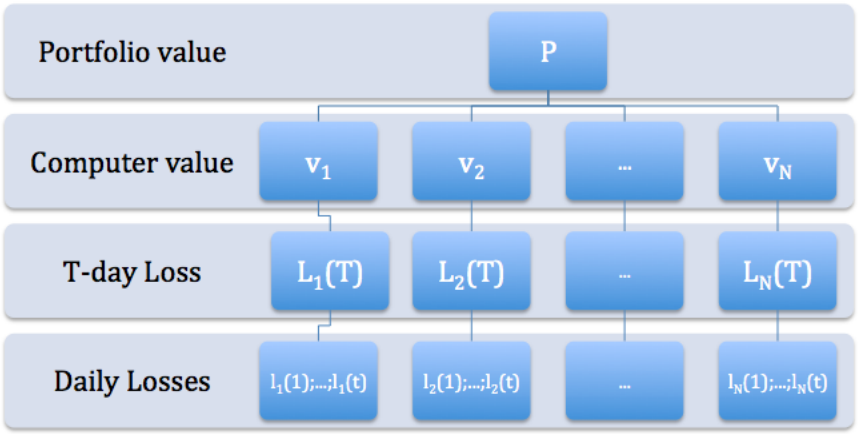


Figure 6.3: The process of the MVaR model

6.4 Simulation Process

This section will discuss the different cases of the MVaR model and show the related simulation results. The Poisson distributions of the attack attempts are independent and identically distributed (IID) or not.

1. Identical Case: $x_i(t) \sim Po(\lambda)$, all attempts follow the same Poisson distribution with parameter λ.

2. Non-Identical Case: $x_i(t) \sim Po(\lambda_i(t))$, each $\lambda_i(t)$ is generated randomly and not all the same.

   For these two cases, the simulation process sets up the other constraints:

   (a) $\boldsymbol{k}$ presents the Conficker attack;
   (b) $\boldsymbol{a_k = 0.5}$ is cited from the CyberVaR model [141];
   (c) $\boldsymbol{l_k = 0.1}$;
   (d) $\boldsymbol{T = 10}$;
   (e) $\boldsymbol{N = 1 \text{ to } 100}$;
   (f) $\boldsymbol{v_i}$ is generated from a uniform distribution between £10000 and £50000.

Based these constraints, we start to implement the simulation process by 'R'. There are several reasons for using R. First, R is free software for everyone and available for most systems like Mac and Windows. Second, R is "the world's most popular language for developing statistical software" [114]. Moreover, R is a programming language, and many people contribute the great packages of analysis. These packages make statistical analysis smoother and easier for users.

6.4.1 Identical Case

For the identical case, we will simulate a value of λ and take it as the sample parameter to all Possion distribution. That means in the identical case, the Poisson distributions of Conficker attacks in every day and every machine are independent and identically distributed. In such conditions the simulation process will run firstly a 2-computer company portfolio, and followed by a 100-machine example. The constant case generates only one random variable λ such that $x_i(t) \sim Po(\lambda)$. Hence, $L_P \sim Po(\lambda T \sum_{i=1}^{N} R_i)$.

```
T <- 10
N <- 2
ak <- 0.5
lk <- 0.1
value_c <- sample(10000:50000, N, replace=TRUE)    ### v_i
value_c
[1] 26164 15762
R_c <- value_c * ak * lk      ### R_i
R_c
[1] 1308.2  788.1
lambda_c <-  sample(1:10, 1, replace=TRUE) %>% rep(T*N)
lambda_c
 [1] 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
    10
attack_c <- sapply(lambda_c, function(x) rpois(1,x)) %>%
   matrix(.,N,T)
attack_c  ### x_i(t)
     [,1] [,2] [,3] [,4] [,5] [,6] [,7] [,8] [,9] [,10]
[1,]   12   10   10    8    5   14    9    8    5    10
[2,]   10   11   12    6   15    7    8   12   13     6
loss_c <- apply(attack_c * R_c,1,sum)      ### L_i(T)
loss_c
[1] 119046.2  78810.0
lambda_matrix_c <- lambda_c %>% matrix(.,N,T)
big_lambda_c <- R_c %*% lambda_matrix_c %>% sum
qpois(0.95, big_lambda_c)
[1] 210383
sigma_c <- sqrt(big_lambda_c)
qnorm(0.95, big_lambda_c, sigma_c)
```

```
[1] 210383.1
```

The simulation results show if a generated $\lambda_c = 10$, two computer values $v_1 = 26164$ and $v_2 = 15762$, then the loss for computer 1 over 10 days is $L_1(10) = £119046.2$ and $L_2(10) = £78810.0$. Hence, the total loss of the company portfolio over 10 days will not exceed £210383 under 95% confidence level when two computers are attacked by conficker malware. That is, $MVaR_{0.95} = £210383$.

If we keep $N = 100$, $\lambda = 10$, then the simulation results are $MVaR_{0.95} = £14816375$.

```
N = 100
lambda_c = 10
....
qpois(0.95, big_lambda_c)
[1] 14816375
sigma_c <- sqrt(big_lambda_c)
qnorm(0.95, big_lambda_c, sigma_c)
[1] 14816375
```

6.4.2 Non-Identical Case

In the non-identical case, the parameter $\lambda_i(t)$ is a generated integer. Every computer in every day will be attacked by a non-identical Poisson distribution. Likewise the identical case, the simulation process starts with 2-computer portfolio in R as follows.

```
T <- 10
N <- 2
ak <- 0.5
lk <- 0.1
value <- sample(10000:50000, N, replace=TRUE)    ### v_i
value
[1] 21197 18576
R <- value * ak * lk    ### R_i
R
[1] 1059.85  928.80
lambda <- sapply(runif(N*T)*10,function(x) ceiling(x))  ## $\
    lambda_i(t)$
lambda
[1]  5  9  8  9  4 10  1  9  2  7  3  6  5 10  7  8  3  7  1
    6
```

```
attack <- sapply(lambda, function(x) rpois(1,x)) %>% matrix(.,
    N,T)
attack ### x_i(t)
      [,1] [,2] [,3] [,4] [,5] [,6] [,7] [,8] [,9] [,10]
[1,]    8   11    4    0    2    5    3    9    2     0
[2,]   11    7    8   16    4    7   16   10    9     6
loss <- apply(attack * R,1,sum)        ### L_i(T)
loss
[1] 46633.4 87307.2
lambda_matrix <- lambda %>% matrix(.,N,T)
big_lambda <- R %*% lambda_matrix %>% sum
qpois(0.95, big_lambda)
[1] 117130
sigma <- sqrt(big_lambda)
qnorm(0.95, big_lambda, sigma)
[1] 117128.5
```

The simulation result shows $MVaR_{0.95} = £117130$ and there is 95% probability that the total loss will not exceed £117130 for a 2-computer company, which attacked by Conficker malware. Moreover, we find the CLT results of the MVaR model are very approximately to the Poisson case. Thus, the results of simulation verify that we can use the CLT approach of the MVaR model to the Possion distribution. If we extend the number of computers to 100, the simulation results are as follows.

```
T <- 10
N <- 100
ak <- 0.5
lk <- 0.1
value <- sample(10000:50000, N, replace=TRUE)    ## v_i
R <- value * ak * lk
lambda <- sapply(runif(N*T)*10,function(x) ceiling(x))  ## $\
    lambda_i(t)$
attack <- sapply(lambda, function(x) rpois(1,x)) %>% matrix(.,
    N,T) ## x_i(t)
loss <- apply(attack * R,1,sum)        ## T-day Losses of each
    machine

lambda_matrix <- lambda %>% matrix(.,N,T)
```

```
big_lambda <- R %*% lambda_matrix %>% sum
qpois(0.95, big_lambda)   # => 8488400

sigma <- sqrt(big_lambda)
qnorm(0.95, big_lambda, sigma) # => 8488400
```

Visibly, for a 100-computer portfolio, the Poisson and Normal expressions have the same value $MVaR_{0.95} = £8488400$. We run the program above again and find that two expressions of the MVaR model will obtain the same MVaR value when the number of computers is large enough and at 95% confidence level. If we change the confidence level from 95% to 99%, then implement the program, the results reveal that they still keep the same values of MVaR.

Overall, the simulation processes of two cases illustrate that the Poisson and Normal expressions will produce the similar, even same MVaR values at the same confidence level like 95% or 99%. The number of computers will have a slight effect on the simulation results. The larger number of machines will have a higher probability to obtain the same MVaR value in both cases.

6.5 Model Limitations

The MVaR model tries to use the theory of portfolio VaR to assess the losses of stealing data. Furthermore, the model operates the simulation to show some reasonable results under the limited assumptions. However, we know the assumptions of the model still imply certain limitations such as determination of data values on machines and the other distribution of attack attempts. We will discuss these limitations in the following.

6.5.1 Data Value of Machine

The MVaR model does not provide the reasonable approaches to determine the data values of machines. We suppose that the data values could be determined by the computer users and run a simple simulation process, but not a mathematical model. Nevertheless, the data partition of a company's database and the malware cross infection on machines could affect the data values.

6.5.1.1 Data Partition

In the MVaR model, we assume that data values of machines could be assessed by the computer users. However, if we take data partition of a company's database into account, data values could depend on the entitlements of accessing data of internal

users (staff). Data consumers in a company will be allocated a registration account to download the relevant documents to their computers. In this case, data consumers will share a part of data due to their access entitlements of a company database. The MVaR model did not consider two extreme cases of data partition when determining data values.

- **Case 1:** each computer has distinct data. A company's database could be partitioned into N parts and store in N machines. The loss occurs once the data of a machine is stolen via malware attacks. Data values has no any correlation among N machines for the data leakage of any computer. That is data leakage of the first machine does not affect the data value of the second computer. For example, for a staff from marketing sale department, if his computer is attacked successfully via malware and the data of his clients is stolen, there is no effect for the other computers' data values. In this instance, the risks could decrease via more dispersive machines.

- **Case 2:** every computer stores the same data. If a machine is attacked successfully and data is stolen, then the other computers will suffer the same losses which will be vast. In other words, there is a perfect correlation among data values for data leakage. The leakage of client data may cause the data useless and no value for this part of data. The data value of each machine may minus the value of leaked data.

In short, we have to discuss the applications and results of the MVaR model in these two cases for further study. The study also could examine the relationship between data partition and risk diversification.

6.5.1.2 Correlation Coefficient

In the financial market, the risks generally can be traded off by a portfolio. All share prices in a portfolio will not go up or down at the same time due to the different correlation coefficient. The correlation coefficient $\rho(-1 < \rho < 1)$ in finance represents the interaction relationship of the changes of stock prices. The MVaR expressions did not think about the impact of correlation coefficient to data values. It is worth to note the data value fluctuation when importing correlation coefficient in the model. We have the following discussion about this factor.

We could suppose that the attacked machine may infect the other computers at a certain probability named ρ. Figure 6.4 depicts ρ as the relationship among machines. If the machines belong to the same department, then we may suppose they share the same ρ.

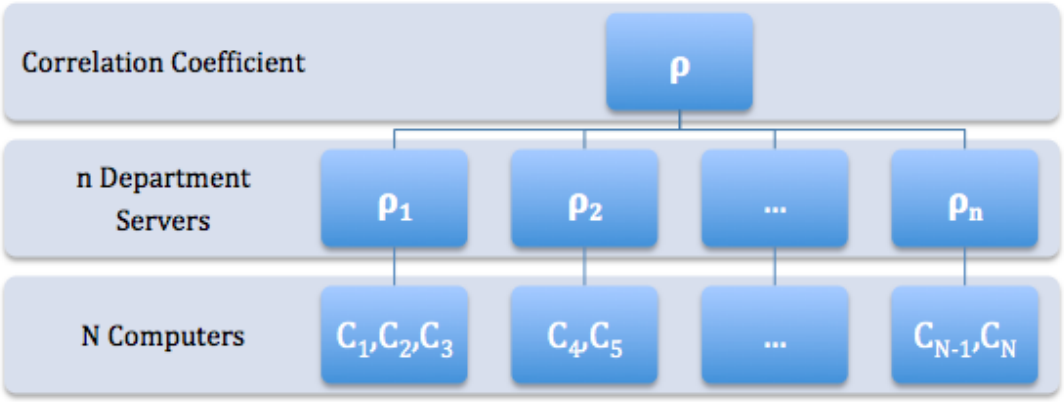


Figure 6.4: Correlation Coefficient among computers

Furthermore, we describe the infecting factor between the computer as $\rho_{i,j}$. $\rho_{i,j}$ is an infection probability of malware from computer i to j. The MVaR model supposes that a computer suffers a loss and reduces its data value when it is attacked successfully by malware. We have the following discussions about the meaning of $\rho_{i,j}$ if it is applied at the MVaR model.

1. $\boldsymbol{\rho_{i,j} = -1}$ shows a perfect negative correlation. Computer i fails to infect computer j and computer j enhances its defence system. In this case, computer j will remain its value v_j.

2. $\boldsymbol{-1 < \rho_{i,j} < 0}$ denotes the values of two machines go up or down in opposite direction. At the same server, computer i attacked by malware will provide the useful information to computer j to help defend against the same malware. The value of computer i will go down named loss I, and no loss for computer j.

3. $\boldsymbol{\rho_{i,j} = 0}$ suggests no relationship between two computers. Computer i is not infected by computer j. Thus, v_j is not affected by the attacks of computer i.

4. $\boldsymbol{0 < \rho_{i,j} < 1}$ means the values of two machines go up or down in the same direction. Computer i is infected by a malware attack, then computer j has the probability $\rho_{i,j}$ to be infected by computer i. In this case, $\rho_{i,j}$ will lead to the loss of v_j.

5. $\boldsymbol{\rho_{i,j} = 1}$ shows a perfect positive correlation (rare in the share market, but may usual in cybersecurity). That means the computer i 100% infects the computer j and leads to the values of two computers go down. In this instance, we could measure the losses of two machines once the computer i is attacked successfully.

All the discussions above about ρ have to be verified by the further study. Overall, for a new MVaR mdoel, it is an interesting challenge to import ρ into the model expressions. The involvement of ρ could make more sense to the explanation of reducing the risks via the portfolio VaR theory.

6.5.2 Probability Distribution of Malware Attacks

The model supposes the malware attacks follow a Poisson distribution with a parameter λ, although we discuss the identical and non-identical cases of the parameter λ. The model did not consider the possibility of the other distributions like a power law.

We prove that the existence of a power law distribution for some malware attacks and show in appendix D. However, due to the nature of a power law distribution, we could not apply the results in the model. The power distribution could not provide the sequential attack attempts for assessing the loss. For example, for the dataset of the first day, the top 3 attack attempts on a day in a power law distribution are 2, 1 and 3. That is 2 is the most frequently attacked times. For the dataset of the second day, the top 3 attack attempts in a power law distribution are 0, 2 and 1. In this instance, we could not fold the dataset to calculate the MVaR value, and could not state that at 95% confidence level, the attack attempts and the corresponding total loss will not exceed over a specific number.

Thus, although we examine some datasets of attack attempts which follow a power law distribution, we still apply the assumption of a Poisson distribution rather than a power law in the MVaR model.

6.6 Summary

The most important reason for applying the concept of the financial VaR to cybersecurity is a cyber VaR model provides a monetary figure which is easy to understand the consequences of cyber attacks for the managers or leaders of a company. For instance, the worst losses it will cause the single cyber threat. Based on the losses, the managers or leaders can decide whether increasing the security investment such as buying a new cyber insurance or improving the defence systems.

The CyberVaR model [141] pays more attention to analyse the VaR from the traditional cyber security standpoint of Dynamic Bayesian Networks and attack trees. The MVaR model prefers to discuss the VaR from a portfolio standpoint, which assumes a computer as a stock and a company as a portfolio. However, the common issue of two cybersecurity VaR models is applying the Monte-Carlo simulation method to carry out the VaR on the lack of historical data. Typically, it is hard to assess the loss of cyber

attacks on a company or an organisation.

The MVaR model provides a new idea to measure the losses and make it more countable in the real scenario, although it still has its limitations under the limited assumptions. In practice, a computer is a direct target for the cyber attacks, and it is feasible to value the data in a network. But in the MVaR model, we only simply assume that data values could be determined by users, and simulated them by a uniform distribution. The impacts of data partition and correlation coefficient to data values are not the application in the current MVaR model. The influence is worth noting in the further study of the model. Furthermore, determining the data values of computers allows us to arrange the defence source in a more suitable strategy. For instance, the machines of finance department will focus on the payment login more frequently than the other units. Thus, we may allocate more ID defence sources or strength the ID anti-phishing system to the computers of this department.

The further benefit of the MVaR model is to provide a more clear concept of what kinds of historical data is valuable to collect for assessing the cyber threats. For a computer in a company it is easier to observe the number of attacks x on a day or 10 days. The observed data is helpful to evaluate the worst loss of specific attack type to a company. The third advantage is feasible to apply the method when the distribution of attack attempts changes. For instance, if the distribution of attack attempts is not a Poisson, we still can use the MVaR model to assess the worst loss of a company portfolio by the CLT. However, the power law distribution is out of the model consideration due to its nature. The power distribution could not provide the sequential attack attempts for assessing the loss in the MVaR model. Therefore, the MVaR model still applies the assumption of a Poisson distribution rather than a power law distribution.

The MVaR model is based on data leakage. If we concern about an attacker tampering with data then the model will be different. Because the attacker might only need to tamper with data on a single computer succeed in his attack. For example, the company under attack might release a faulty/buggy application which could lead to financial loss; or the bug might allow the attacker to gain access to data at a later date. But either way, we might need to think carefully about a new model. Overall, studying the methods of solving the limitations is essential to improve the availability of the model in a real scenario.

Chapter 7

Conclusion

Information security is a vital topic in the current information age. Many theories and approaches are applied to secure information for individuals and organisations. To the best of our knowledge, they are two directions for these methods: first, avoiding the information security risks by access control or other ID-based technologies; second, assessing and managing the risks by some frameworks of related standards. This thesis pays attention to the second aspect. Information security management standards are essential to information security. As we know, it is challenging for any cryptographic technology or IT product to guarantee 100% security of the information. However, the standards enable a provision of a complete framework for securing the data at an appropriate level. Furthermore, most of these rules are internationally accepted and beneficial for organisations to apply for their products. The thesis primarily discusses the evolutions of ISO 27000 family and Common Criteria (CC). ISO 27000 family are well-known international standards for managing information security risks. CC is used to evaluate the risks of IT products. These guidelines are helpful for organisations to obtain global certification on their information systems. Nevertheless, today's standards are based on ideas going back to the 70s and are difficult to apply to things like cloud and BYOD. Moreover, the scopes of these standards are too generic and not unified due to the nature of institutions in different countries.

This thesis further discusses the standards for information security risk assessment (ISRA). ISRA is the core part of the whole process of information security management. Risk assessment is applied in many industries and subjects including finance, power system and public health. Risk assessment in information security has a particular role in most industries. In practice, enterprises cannot exist without information in the information age. That means they have to keep the information safety. ISRA provides a complete framework to identify information security risks and implement the security

controls by related standards.

We examine four commonly and widely used ISRA standards: OCTAVE, FAIR, ISO 27005 and NIST SP800-30. ISRA has a different process in these four frameworks. Thus, we compare and discuss their contents, advantages and disadvantages. They are useful to guide the organisations from different emphasises. For example, FAIR pays more attention to the calculation methods of risk analysis, while ISO 27005 prefers to provide a complete framework for risk assessment. The ISO 27005 framework is prevalent in the world because it is easy to follow with explicit definitions such as information security risks, risk analysis and risk evaluation. Another favourite reason is that ISO 27005 has the support of the ISO 27000 family.

However, the first drawback for these ISRA guidelines is that they are difficult to run in shorter or daily ISRA. Their assessment processes cost a lot of time for organising experts' interviews and questionnaires. The second flaw in most ISRA standards is that they are too generic to all information security risks. Therefore, this thesis tries to solve this problem by the application of a financial risk model to a particular type of information security risks such as cyber threats.

The classical financial risk model named value-at-risk (VaR) and was first applied at ISRA in 2001 by Jaisingh and Rees [80] and improved to a complete model CyberVaR by Raugas et al. in 2013 [141]. The CyberVaR model analyses the cyber threats by the theory of Dynamic Bayesian Network (DBN). However, this model can't be used to compare different companies due to varying values of the same asset. For example, personal information may have higher sensitivity for a bank and consequently assigned a higher value compared with that of, perhaps, a supermarket. Based on this reason, we propose another improved ISRA VaR model called MVaR. MVaR starts the analysis from the standpoint of the portfolio VaR theory. The portfolio VaR is constructed from a combination of the risks of underlying securities [85].

From the time patter analysis of malware by circular statistics, we find that the attacks of malware are active during the day working time but becomes quiet during the night. This finding makes sense to the human behaviour. The successful attacks will result in the loss of the direct target like computers. That means the data losses of computers will fluctuate with the malware attacks. Likewise, the financial risks will affect the stock prices. Thus, the machines and the data held on them are the underlying securities and a company consisting of all computers is the portfolio in the MVaR model. Overall, the MVaR model assesses the worst case loss of computers in a company portfolio due to the risk of malware.

7.1 Main Contributions

The thesis makes three contributions as follows: a systematic review of ISRA, a time pattern analysis of malware by circular analysis and an improved ISRA VaR model named MVaR.

By the method of systematic review, we examine the existing research papers of ISRA and provides a classification framework to position current study directions between 2004 and 2014. The frame shows the study focus on each process of ISRA. For example, current approaches to risk identification are hard to deal with asset leakage, user-created assets and critical knowledge well [155]. The comparisons of risk analysis methods primarily pay attention on the quantitative and qualitative method, and their benefits and drawbacks. These methods are discussed and improved to obtain more objective risk scores. In practice, fuzzy theory is a widely used method to reduce the subjectivity of the estimates. In a word, the systematic review presents an unbiased view of current research activities to study ISRA.

Despite existing all kinds of malware studies, it is the first time to apply circular statistics to analyse the incidents of malware infections. Our analysis provides a visual overview of the time patterns' variation, indicating when attacks are most likely. Moreover, results reveal that the total number of malware attacks influence the time patterns. For example, machines subject to vast attacks show bimodality in the daily variation, while they subject to comparatively few attacks will exhibit multimodality. All the findings of the analysis assist decision makers in cybersecurity to allocate resources or estimate the cost of system monitoring during high-risk periods.

The MVaR model is built on the systematic review of ISRA and the time patterns analysis of malware detection. It assesses the risk levels of malware attacks from the standpoint of the portfolio VaR theory. The most important reason for applying the concept of financial VaR to ISRA is that the ISRA VaR model provides a monetary figure which makes it easier for managers to understand the consequences of cyber attacks. Thus, managers have a basis for making decisions whether to increase their security investments such as buying cyber insurance or improving the defence systems.

7.2 Future Works

The MVaR model tries to use the theory of portfolio VaR to assess the worst losses of stealing data via malware. It operates the simulation to show some reasonable results under the limited assumptions. However, the assumptions of the model still imply certain limitations such as determination of data values on machines and the other

distribution of attack attempts.

The MVaR model does not provide the reasonable approaches to determine the data values of machines. The model assumes that data values could be determined by the computer users, and runs a simple simulation process rather than a mathematical model. Nevertheless, the data partition of a company's database and the malware cross infection on machines could affect the data values. Thus, it is worth considering a more scientific method to assess the value of v_i. A possible approach is that we separate the data value of a machine into department data value. If machine stores or accesses to the related department data, then the associated department value will be added to v_i. For instance, a machine i only store the information of human resource and marketing departments, then v_i is the sum of these two department values. But beyond that, the future study could concern the impact of correlation coefficient to data values. The involvement of data partition and correlation coefficient of machine infection may make more sense to the explanation of reducing the risks via the portfolio VaR theory. Overall, studying the methods of solving the limitations is essential to improve the availability of the model in the future study.

Having discussed the independence case of malware attacks to each machine in the MVaR model, it is worth noting the dependent condition to some networks. At a conditional constraint, the MVaR maybe possible to be carried out by the dependent Central Limit Theorems [115]. Additionally, more types of malware might be interested in examining in this model. We only apply the Conficker attack rate as a case study in the simulation process. We could study differences for the model application in different malware types such as Tinba.

The MVaR model is based on data leakage. If we concern about an attacker tampering with or corrupting data, then the model will be different. The attacker might only need to tamper with data on a single computer and succeed in his attack. For example, the company under attack might release a faulty/buggy application which could lead to financial loss; or the bug might allow the attacker to gain access to data at a later date. But either way, we might need to think carefully about a new model. Overall, studying the methods of solving the limitations is essential to improve the availability of the model in a real scenario.

VaR as a classical financial risk model, VaR has itself limitations such as lacking the feature of sub-additivity of a coherent risk measure [1] [85]. Therefore, we could discuss the application of another financial risk model named Expected Shortfall (ES) to assess cyber threats.

[1] Appendix C introduces a coherent risk measure and Expected Shortfall

Bibliography

[1] IBM Data Security Support Programs,USA. 1984. 22

[2] *OECD Recommendation, Guidelines and Eexplanatory Memorandum for the Security of Information Systems*. OECD Publishing, 1992. 33, 34

[3] BS7799 (Code of Practice for Information Security Management, Department of Trade and Industry). *British Standard Institute, London, UK*, 1995. 23

[4] Kalculator: Bits key risk measurment tool for information security operational risks. *BITS*, 2004. 100

[5] ISO 27001:2005 (Information technology – Security techniques – Information Security Management Systems – Requirements). *International Organization for Standardization*, 2005. 16, 38

[6] ISO 27005:2008 (Information technology-Security techniques-Information Security Risk Management). *International Organization for Standardization*, 2008. 25, 27, 28, 84

[7] ISO Guide 73:2009. *Risk management: Vocabulary*, 2009. 28

[8] ISO 27005:2011 (Information technology-Security techniques-Information Security Risk Management). *International Organization for Standardization*, 2011. 28, 30, 38, 45, 47, 51, 83

[9] NIST Special Publication 800-39: Managing Information Security Risk, Organization, Mission and Information System Review. 2011. 29, 31

[10] H. J. Adèr and G. J. Mellenbergh. *Advising on research methods: A consultant's companion*. Johannes van Kessel Publishing., 2008. 39

[11] S. H. Albakri, B. Shanmugam, G. N. Samy, N. B. Idris, and A. Ahmed. Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, 2014. 42, 46, 50

[12] J. P. Anderson. Computer security technology planning study. volume 2. Technical report, Anderson (James P) and Co Fort Washington PA, 1972. 25, 26

[13] G. Antoniou, M. C. Saravanou, and V. Stavrou. An overview of risk assessment methods. 35

[14] P. Artzner. Application of coherent risk measures to capital requirements in insurance. *North American Actuarial Journal*, 3(2):11–25, 1999. 146, 148

[15] P. Artzner, F. Delbaen, J.-M. Eber, and D. Heath. Coherent measures of risk. *Mathematical finance*, 9(3):203–228, 1999. 147, 148

[16] A. Asosheh, B. Dehmoubed, and A. Khani. A new quantitative approach for information security risk assessment. In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 222–227. IEEE, 2009. 46

[17] G. A. Awad, E. I. Sultan, N. Ahmad, N. Ithnan, and A. Beg. Multi-objectives model to process security risk assessment based on ahp-pso. *Modern Applied Science*, 5(3):246, 2011. 46

[18] W. H. Baker, L. P. Rees, and P. S. Tippett. Necessary measures: metric-driven information security risk assessment and decision making. *Communications of the ACM*, 50(10):101–106, 2007. 33, 34, 46, 52

[19] M. Bava, D. Cacciari, E. Sossa, D. Zotti, and R. Zangrando. Information security risk assessment in healthcare: The experience of an italian paediatric hospital. In *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on*, pages 321–326. IEEE, 2009. 46

[20] BBA. The cyber threat to banking - a global industry challenge. 2014. 85

[21] R. Beckstrom. Cybervar: Quantifying the risk of loss from cyber attacks, 2014. 89, 90

[22] A. Behnia, R. A. Rashid, and J. A. Chaudhry. A survey of information security risk analysis methods. *SmartCR*, 2(1):79–94, 2012. 8, 35, 36, 37

[23] J. Bhattacharjee, A. Sengupta, and C. Mazumdar. A formal methodology for enterprise information security risk assessment. In *Risks and Security of Internet and Systems (CRiSIS), 2013 International Conference on*, pages 1–9. IEEE, 2013. 46, 48

[24] D. Bhilare, A. Ramani, and S. Tanwani. Information security risk assessment and pointed reporting: Scalable approach. In *Computer Engineering and Technology, 2009. ICCET'09. International Conference on*, volume 1, pages 365–370. IEEE, 2009. 46

[25] P. Billingsley. *Probability and Measure*. John Wiley & Sons, Inc., 1995. 106, 107

[26] M. Bogdan, K. Bogdan, and A. Futschik. A data driven smooth test for circular uniformity. *Annals of the institute of statistical mathematics*, 54(1):29–44, 2002. 63

[27] M. Bogdan, K. Bogdan, and A. Futschik. A data driven smooth test for circular uniformity. *ACM Trans. Program. Lang. Syst.*, 54(1):29–44, March 2002. 63

[28] R. Böhme. *The economics of information security and privacy*. Springer, 2013. 9, 85, 86

[29] J. Boltz. *Informational Security Risk Assessment: Practices of Leading Organizations*. DIANE Publishing, 1999. 14, 21, 28, 35

[30] P. Brangetto and M. Aubyn. Economic aspects of national cyber security strategies. *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex*, 1:9–16, 2015. 86, 88

[31] J. S. Broderick. Isms, security standards and security regulations. *information security technical report*, 11(1):26–31, 2006. 23

[32] L. Brown, N. Gans, A. Mandelbaum, A. Sakov, H. Shen, S. Zeltyn, and L. Zhao. Statistical analysis of a telephone call center: A queueing-science perspective. *Journal of the American statistical association*, 100(469):36–50, March 2005. 60, 61

[33] C. Brunsdon and J. Corcoran. Using circular statistics to analyse time patterns in crime incidence. *Computers, Environment and Urban Systems*, 30(3):300–319, May 2006. 55, 57, 58, 64

[34] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson. Introducing octave allegro: Improving the information security risk assessment process. Technical report, DTIC Document, 2007. 50

[35] L. Chang and Z. Lee. Applying fuzzy expert system to information security risk assessment-a case study on an attendance system. In *Fuzzy Theory and Its*

Applications (iFUZZY), 2013 International Conference on, pages 346–351. IEEE, 2013. 15, 46, 48, 83

[36] G. Chen and D. Zhao. Model of information security risk assessment based on improved wavelet neural network. *Journal of Networks*, 8(9):2093–2100, 2013. 46

[37] Y. Chu, Y. Wei, and W. Chang. A risk recommendation approach for information security risk assessment. In *Network Operations and Management Symposium (APNOMS), 2013 15th Asia-Pacific*, pages 1–3. IEEE, 2013. 46

[38] A. Clauset, C. R. Shalizi, and M. E. Newman. Power-law distributions in empirical data. *SIAM review*, 51(4):661–703, 2009. 149, 150, 151, 152, 153

[39] J. Coleman. Assessing information security risk in healthcare organizations of different scale. In *International Congress Series*, volume 1268, pages 125–130. Elsevier, 2004. 46, 50

[40] L. Coles-Kemp and R. E. Overill. On the role of the facilitator in information security risk assessment. *Journal in Computer Virology*, 3(2):143–148, 2007. 16, 46, 52

[41] L. Coles-Kemp and M. Theoharidou. Insider threat and information security management. In *Insider threats in cyber security*, pages 45–71. Springer, 2010. 23

[42] A. C. Committee. The economics of cybersecurity: A practical framework for cybersecurity investment. 2013. 85, 86

[43] CSBS. Cybersecurity101: A resource guide for bank executives. 2015. 85

[44] CSIS. Net losses: Estimating the global cost of cybercrime. June 2014. 85, 86, 87

[45] M. J. Dark. Assessing student performance outcomes in an information security risk assessment, service learning course. In *Proceedings of the 5th conference on Information technology education*, pages 73–78. ACM, 2004. 42, 46

[46] I. L. Dryden, A. Koloydenko, and D. Zhou. Non-euclidean statistics for covariance matrices, with applications to diffusion tensor imaging. *The Annals of Applied Statistics*, 3(3):1102–1123, March 2009. 58

[47] D. Durand and J. A. Greenwood. Modifications of the rayleigh test for uniformity in analysis of two-dimensional orientation data. *The Journal of Geology*, 66(3):229–238, May 1958. 63

[48] P. Ebenezer. Taxonomy of security risk assessment approaches for researchers. In *CASoN Computational Aspects of Social Networks (4th)*, pages 257 – 262. IEEE, 2012. 34, 46

[49] EPPI. http://eppi.ioe.ac.uk/cms/. 39

[50] Z. F. Eren-Dogu and C. C. Celikoglu. Information security risk assessment: Bayesian prioritization for ahp group decision making. *International Journal of Innovative Computing, Information and Control*, 8:8001–8018, 2012. 46

[51] K. J. Farn, S. K. Lin, and A. R. W. Fung. A study on information security management system evaluation - assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6):501–513, 2004. 24

[52] N. Feng and M. Li. An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, 11(7):4332–4340, 2011. 42, 46

[53] N. Feng, J. Xie, and P. Chang. An intelligent system to assessing information systems security risks in electronic business. In *Information Science and Engineering (ISISE), 2012 International Symposium on*, pages 303–306. IEEE, 2012. 46

[54] T. Finne. Information systems risk management: key concepts and business processes. *Computers & Security*, 19(3):234–242, 2000. 34

[55] F. Foroughi. Information security risk assessment by using bayesian learning technique. In *Proceedings of the World Congress on Engineering*, volume 1, page 133. Citeseer, 2008. 46

[56] S. Fu and Y. Xiao. Strengthening the research for information security risk assessment. In *International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering*, volume 9, pages 386–392, 2012. 46, 47, 48

[57] S. Fu and H. Zhou. The information security risk assessment based on ahp and fuzzy comprehensive evaluation. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pages 124–128. IEEE, 2011. 46

[58] Y. Fu, Y. Qin, and X. Wu. A method of information security risk assessment using fuzzy number operations. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, pages 1–4. IEEE, 2008. 46

[59] G. Gao, X. Li, B. Zhang, and W. Xiao. Information security risk assessment based on information measure and fuzzy clustering. *Journal of Software*, 6(11):2159–2166, 2011. 34, 46, 52

[60] C. S. Gillespie. The powerlaw package: Comparing distributions. 151, 153

[61] C. S. Gillespie. Fitting heavy tailed distributions: the powerlaw package. 2014. 9, 152, 153

[62] C. S. Gillespie. The powerlaw package: Examples. 2016. 9, 150, 151, 153, 154

[63] C. S. Gillespie. Analysis of heavy tailed distributions:the powerlaw package. 2017. 10, 160

[64] M. L. Goldstein, S. A. Morris, and G. G. Yen. Problems with fitting to the power-law distribution. *The European Physical Journal B-Condensed Matter and Complex Systems*, 41(2):255–258, 2004. 149, 150, 151

[65] C. W. Group. Conficker working group: Lessons learned. *Conficker-Working-Group-Lessons-Learned-17-June-2010-final. pdf, published Jan*, 2011. 77, 99

[66] J. GUAN, M. LEI, X. ZHU, and J. LIU. Knowledge-based information security risk assessment method. *The Journal of China Universities of Posts and Telecommunications*, 20:60–63, 2013. 46

[67] Y. Y. Haimes. Hierarchical holographic modeling. *Systems, Man and Cybernetics, IEEE Transactions on*, 11(9):606–617, 1981. 45

[68] Y. Y. Haimes, J. Lambert, D. Li, R. Schooff, and V. Tulsiani. Hierarchical holographic modeling for risk identification in complex systems. In *Systems, Man and Cybernetics, 1995. Intelligent Systems for the 21st Century., IEEE International Conference on*, volume 2, pages 1027–1032. IEEE, 1995. 45

[69] J. Hawkinson and T. Bates. Guidelines for creation, selection, and registration of an autonomous system (as). 1996. 57

[70] N. Heard. *Modelling dependencies in internet traffic data.* 54, 58

[71] R. V. Hogg, E. Tanis, and D. Zimmerman. *Probability and statistical inference.* Pearson Higher Ed, 2014. 103, 107

[72] K. Höne and J. H. P. Eloff. Information security policy - what do international information security standards say? *Computers & Security*, 21(5):402–409, 2002. 22

[73] Z. Hou. Application of gb/t20984 in electric power information security risk assessment. In *Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on*, volume 1, pages 616–619. IEEE, 2010. 46

[74] C. Huang, K. Farn, and F. Y. Lin. A study on implementations of information security risk assessment: Application to chlorine processing system of water treatment. *IJ Network Security*, 16(4):377–384, 2014. 8, 23, 25, 42, 46, 48

[75] S. Huang, C. Lin, and N. Chiu. Fuzzy decision tree approach for embedding risk assessment information into software cost estimation model. *Journal of Information Science and Engineering*, 22(2):297–313, 2006. 46

[76] Y. Imamverdiyev. An application of extreme value theory to e-government information security risk assessment. In *AICT, International Conference on Application of Information and Communication Technologies*, pages 1 – 4. IEEE, 2013. 46

[77] B. Irwin. A source analysis of the conficker outbreak from a network telescope. *SAIEE Africa Research Journal*, 104(2):38, 2013. 99

[78] ISO27K. http://www.iso27001security.com/html/timeline.html. 8, 24

[79] ITSEC. Information technology security evaluation criteria (ITSEC): Preliminary harmonised criteria. Document COM(90) 314, Version 1.2, 1991. 22

[80] J. Jaisingh and J. Rees. Value at risk: A methodology for information security risk assessment. In *Proceedings of the INFORMS Conference on Information Systems and Technology*, pages 3–4, 2001. 17, 85, 89, 118, 148

[81] J. R. Jang, C. Sun, and E. Mizutani. Neuro-fuzzy and soft computing: a computational approach to learning and machine intelligence. 1997. 44

[82] Y. Jing, G. Ahn, Z. Zhao, and H. Hu. Towards automated risk assessment and mitigation of mobile application. 41, 42, 46, 50

[83] T. A. Johnson. *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. CRC Press, 2015. 86, 87, 96

[84] J. Jones. An introduction to factor analysis of information risk (fair). *Risk Management Insight LLC*, 2005. 29, 32

[85] P. Jorion. *Value at risk: the new benchmark for managing financial risk*, volume 3. McGraw-Hill New York, 2007. 17, 88, 100, 101, 102, 118, 120, 148

[86] B. Karabacak and I. Sogukpinar. Isram: information security risk analysis method. *Computers & Security*, 24(2):147–159, 2005. 46, 48

[87] B. Karabey and N. Baykal. Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities. *Int. Arab J. Inf. Technol.*, 10(3):297–304, 2013. 46

[88] K. Kaska. Conficker: Considerations in law and legal policy. 2012. 98

[89] K. Khanmohammadi and S. H. Houmb. Business process-based information security risk assessment. In *Network and System Security (NSS), 2010 4th International Conference on*, pages 199–206. IEEE, 2010. 15, 46, 48, 83, 94

[90] S.-H. Kim and W. Whitt. Choosing arrival process models for service systems: Tests of a nonhomogeneous poisson process. *Naval Research Logistics (NRL)*, 61(1):66–90, January 2014. 60

[91] B. A. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. 2007. 39

[92] D. Koller and N. Friedman. *Probabilistic graphical models: principles and techniques*. MIT press, 2009. 90

[93] S. Kondakci. A concise cost analysis of internet malware. *computers & security*, 28(7):648–659, 2009. 84, 88

[94] S. Kondakci. A causal model for information security risk assessment. In *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, pages 143–148. IEEE, 2010. 46

[95] M. Korman, T. Sommestad, J. Hallberg, J. Bengtsson, and M. Ekstedt. Overview of enterprise information needs in information security risk assessment. In *Enterprise Distributed Object Computing Conference (EDOC), 2014 IEEE 18th International*, pages 42–51. IEEE, 2014. 46, 49

[96] L. K. H. Lai and K. S. Chin. Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security. *Industrial Engineeering & Management Systems*, 13(1):87–100, 2014. 46

[97] W. Lai. Fitting power law distributions to data, 2016. 149, 151

[98] R. Latif, H. Abbas, S. Assar, and Q. Ali. Cloud computing risk assessment: A systematic literature review. In *Future Information Technology*, pages 285–295. Springer, 2014. 42

[99] M. Lee. Information security risk analysis methods and research trends: Ahp and fuzzy comprehensive method. *International Journal of Computer Science*, 2014. 16, 44, 46, 48, 49

[100] Z. Lee and L. Chang. Apply fuzzy decision tree to information security risk assessment. *International Journal of Fuzzy Systems*, 16(2):265–269, 2014. 46

[101] M. Leitner and S. Rinderle-Ma. A systematic review on security in process-aware information systems–constitution, challenges, and future directions. *Information and Software Technology*, 56(3):273–293, 2014. 8, 39, 40

[102] S. R. Lenkala, S. Shetty, and K. Xiong. Security risk assessment of cloud carrier. In *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on*, pages 442–449. IEEE, 2013. 46

[103] A. Lenstra and T. Voss. Information security risk assessment, aggregation, and mitigation. In *Information Security and Privacy*, pages 391–401. Springer, 2004. 46, 89

[104] W. Li. *Risk assessment of power systems: models, methods, and applications*. John Wiley & Sons, 2014. 28

[105] W. Lijian, W. Bin, and P. Yongjun. Research the information security risk assessment technique based on bayesian network. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, volume 3, pages V3–600. IEEE, 2010. 46

[106] J. W. Lindeberg. Eine neue herleitung des exponentialgesetzes in der wahrscheinlichkeitsrechnung. *Mathematische Zeitschrift*, 15(1):211–225, 1922. 106

[107] C. Lo and W. Chen. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, 39(1):247–257, 2012. 15, 46, 47, 48, 49, 83

[108] D. Lopez, O. Pastor, and L. J. G. Villalba. Data model extension for security event notification with dynamic risk assessment purpose. *Science China Information Sciences*, 56(11):1–9, 2013. 46

[109] W. Ma. Study on architecture-oriented information security risk assessment model. In *Computational Collective Intelligence. Technologies and Applications*, pages 218–226. Springer, 2010. 46

[110] T. Maillart and D. Sornette. Heavy-tailed distribution of cyber-risks. *The European Physical Journal B*, 75(3):357–364, April 2010. 55, 94

[111] O. Makarevich, I. Mashkina, and A. Sentsova. The method of the information security risk assessment in cloud computing systems. In *Proceedings of the 6th International Conference on Security of Information and Networks*, pages 446–447. ACM, 2013. 42, 46

[112] K. V. Mardia. Statistics of directional data. *Journal of the Royal Statistical Society. Series B (Methodological)*, 37(3):349–393, March 1975. 57

[113] J. Markovic-Petrovic and M. Stojanovic. An improved risk assessment method for scada information security. *Elektronika ir Elektrotechnika*, 20(7):69–72, 2014. 46

[114] N. Matloff. *The art of R programming: A tour of statistical software design*. No Starch Press, 2011. 108

[115] D. L. McLeish. Dependent central limit theorems and invariance principles. *the Annals of Probability*, pages 620–628, 1974. 120

[116] A. J. McNeil, R. Frey, and P. Embrechts. *Quantitative risk management: Concepts, techniques and tools*. Princeton university press, 2005. 9, 146, 147, 148

[117] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Time-to-compromise model for cyber risk reduction estimation. In *Quality of Protection*, pages 49–64. Springer, 2006. 94

[118] S. C. Misra, V. Kumar, and U. Kumar. A strategic modeling technique for information security risk assessment. *Information management & computer security*, 15(1):64–77, 2007. 46

[119] T. Moore. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3):103–117, 2010. 87, 96, 97

[120] E. Mouw, G. van't Noordende, B. Louter, and S. D. Olabarriaga. A model-based information security risk assessment method for science gateways. In *IWSG*, 2013. 42, 46

[121] A. Munteanu. Information security risk assessment: The qualitative versus quantitative dilemma. In *Managing Information in the Digital Economy: Issues &*

Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, pages 227–232, 2006. 46

[122] R. M. Mutwiri, H. Mwambi, and R. Slotow. Approaches for testing uniformity hypothesis in angular data of mega-herbivores. *International Journal of Science and Research*, 5(3):1202–1207, March 2016. 55

[123] NIST. Nist800-30 revision 1: Guide for conducting risk assessments. 2012. 38

[124] R. Nuzzo. Statistical errors. *Nature*, 506(7487):150, 2014. 151

[125] H. Očevčić, K. Nenadić, and K. Šolić. Decision support based on the risk assessment of information systems and bayesian learning. *Tehnički vjesnik*, 21(3):539–544, 2014. 42, 46

[126] Y. Ozcelik and J. Rees. A new approach for information security risk assessment: Value at risk. 2005. 89

[127] A. M. Padyab, T. Paivarinta, and D. Harnesk. Genre-based assessment of information and knowledge security risks. In *System Sciences (HICSS), 2014 4th Hawaii International Conference on*, pages 3442–3451. IEEE, 2014. 46

[128] L. Pan and A. Tomlinson. A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*, 6(2):270–281, 2016. 16, 30, 35, 38, 49, 50, 51, 52, 84

[129] L. Pan, A. Tomlinson, and A. A. Koloydenko. Time pattern analysis of malware by circular statistics. In *Proceedings of the Symposium on Architectures for Networking and Communications Systems*, pages 119–130. IEEE Press, 2017. 17

[130] P. Pandey and E. A. Snekkenes. A performance assessment metric for information security financial instruments. In *Information Society (i-Society), 2015 International Conference on*, pages 138–145. IEEE, 2015. 89

[131] S. Pavilion and M. Way. Cochrane methods. 2012. 38, 39

[132] L. Peiyu and L. Dong. The new risk assessment model for information system in cloud computing environment. *Procedia Engineering*, 15:3200–3204, 2011. 42, 46, 47

[133] A. Pewsey, M. Neuhäuser, and G. D. Ruxton. *Circular statistics in R*. Oxford University Press, 2013. 11, 54, 55, 56, 57, 58, 63, 64, 67, 71, 78

[134] D. Piscitello. Conficker summary and review. *ICANN, May*, 7, 2010. 97, 98, 99

[135] J. M. Poterba and L. H. Summers. The persistence of volatility and stock market fluctuations, 1984. 101

[136] P. G. Prassinos, J. W. Lyver, and C. T. Bui. Risk assessment overview. In *ASME 2011 International Mechanical Engineering Congress and Exposition*, pages 673–677. American Society of Mechanical Engineers, 2011. 14, 28

[137] PWC. A practical guide to risk assessment–how a principle–based risk assessment enables organizations tp take the right risk, 2008. 28

[138] Y. Qing, Z. Changhong, W. Xiaoping, and Z. Dingjun. Information security risk assessment based on ahp/dst. In *Management and Service Science, 2009. MASS'09. International Conference on*, pages 1–4. IEEE, 2009. 46

[139] P. Ralston, J. Graham, and J. Hieb. Cyber security risk assessment for scada and dcs networks. *ISA transactions*, 46(4):583–594, 2007. 46

[140] A. Ramachandran and N. Feamster. Understanding the network-level behavior of spammers. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 291–302. ACM, 2006. 55, 63

[141] M. Raugas, J. Ulrich, R. Faux, S. Finkelstein, and C. Cabot. Cyberv@r. 2013. 9, 17, 84, 89, 90, 91, 92, 94, 96, 103, 104, 108, 115, 118, 148

[142] M. V. Raugas and J. L. Ulrich. Assessment of cyber threats, January 2017. US Patent 9,537,884. 54

[143] L. Research. Cyberrisk in banking. 2013. 84

[144] P. Rezakhani. A review of fuzzy risk assessment models for construction projects. *Slovak Journal of Civil Engineering*, 20(3):35–40, 2012. 143

[145] V. Ricci. Fitting distributions with r. *Contributed Documentation available on CRAN*, 96, February 2005. 60

[146] A. Romanov and E. Okamoto. A quantitative approach to assess information security related risks. In *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on*, pages 117–122. IEEE, 2009. 89

[147] A. Romanov, H. Tsubaki, and E. Okamoto. An approach to perform quantitative information security risk assessment in it landscapes. *Information and Media Technologies*, 5(4):1361–1374, 2010. 46, 89

[148] A. Roy, A. Gupta, and S. Deshmukh. Information security risk assessment in scm. In *Industrial Engineering and Engineering Management (IEEM), 2013 IEEE International Conference on*, pages 1002–1006. IEEE, 2013. 41, 46

[149] T. L. Saaty. What is the analytic hierarchy process? In *Mathematical models for decision support*, pages 109–121. Springer, 1988. 16, 44

[150] M. Sajko, N. Hadjina, and D. Pesut. Multi-criteria model for evaluation of information security risk assessment methods and tools. In *MIPRO, 2010 Proceedings of the 33rd International Convention*, pages 1215–1220. IEEE, 2010. 46

[151] M. S. Saleh and A. Alfantookh. A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9(2):107–118, 2011. 38

[152] N. Sanna. What is a cyber value-at-risk model?, 2016. 89, 90

[153] P. Shamala, R. Ahmad, and M. Yusoff. A conceptual framework of info structure for information security risk assessment (isra). *Journal of Information Security and Applications*, 18(1):45–52, 2013. 30, 46, 49

[154] P. Shedden, R. Scheepers, W. Smith, and A. Ahmad. Incorporating a knowledge perspective into security risk assessments. *Vine*, 41(2):152–166, 2011. 46, 47, 52

[155] P. Shedden, W. Smith, and A. Ahmad. Information security risk assessment: towards a business practice perspective. 2010. 46, 47, 52, 119

[156] J. Shi. Security risk assessment about enterprise networks on the base of simulated attacks. *Procedia Engineering*, 24:272–277, 2011. 46

[157] Y. Shi and Q. Wen. A value based security risk assessment method. In *Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on*, pages 49–51. IEEE, 2012. 46

[158] S. Shin and G. Gu. Conficker and beyond: a large-scale empirical study. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 151–160. ACM, 2010. 99

[159] S. Shin, G. Gu, N. Reddy, and C. P. Lee. A large-scale empirical study of conficker. *IEEE Transactions on Information Forensics and Security*, 7(2):676–690, 2012. 55, 56, 66

[160] M. Shing and C. Shing. Information security risk assessment using markov models. In *2010 Third International Symposium on Electronic Commerce and Security*, pages 403–406, 2010. 46

[161] K. M. Silvianita and F. Kurian. Critical review of a risk assessment method and its applications. In *International Conference on Financial Management and Economics*, volume 11, pages 83–87, 2011. 48

[162] M. Siponen and R. Willison. Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270, 2009. 23, 26

[163] V. Subrahmanian, M. Ovelgönne, T. Dumitras, and B. A. Prakash. Types of malware and malware distribution strategies. In *The Global Cyber-Vulnerability Report*, pages 33–46. Springer, 2015. 97

[164] Z. Sun, J. Chi, and Y. Liu. Research on information security risk assessment based on fault tree. In *Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on*, volume 2, pages 457–459. IEEE, 2012. 46

[165] P. Szwed and P. Skrzyński. A new lightweight method for security risk assessment based on fuzzy cognitive maps. *International Journal of Applied Mathematics and Computer Science*, 24(1):213–225, 2014. 46

[166] M. Talabis and J. Martin. *Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis*. Newnes, 2012. 29, 34, 35, 142, 143, 144

[167] Y. Tang, L. Wang, L. Yang, and X. Wang. Information security risk assessment method based on cloud model. 2014. 46

[168] H. Tao, C. Liang, W. Chi, and H. Qun. The research of information security risk assessment method based on fault tree. In *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*, pages 370–375. IEEE, 2010. 46

[169] J. S. Ting, A. H. Tsang, and S. Kwok. Hybrid risk management methodology: A case study. *International Journal of Engineering Business Management*, 1(1):25–32, 2009. 45

[170] A. Tomlinson. Iy2840:computer and network security. Technical report, Royal Holloway, University of London, 2016. 25, 26

[171] R. I. Tricker. The management of organizational knowledge. *Information Systems Research, Sage*, 1992. 33, 34

[172] J. Ulrich. CyberV@R: A Model to Compute Dollar Value at Risk of Loss to Cyber Attack, 2013. 9, 90, 93

[173] R. Von Solms and J. Van Niekerk. From information security to cyber security. *computers & security*, 38:97–102, 2013. 22

[174] Y. Wang and W. Xiang. Role of information security risk assessment in establishing electronic archives safeguard systems. In *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on*, pages 1320–1325. IEEE, 2008. 46

[175] W. H. Ware. Security and privacy in computer systems. In *Proceedings of the April 18-20, 1967, spring joint computer conference*, pages 279–282. ACM, 1967. 25

[176] W. H. Ware. Security Controls for Computer Systems:Report of Defense Science Board Task Force on Computer Security, 2013. 25, 26

[177] D. Wawrzyniak. Information security risk assessment–the development of the standard approaches. 46

[178] D. Wawrzyniak. Information security risk assessment model for risk management. In *Trust and Privacy in Digital Business*, pages 21–30. Springer, 2006. 46

[179] WEF. Partnering for cyber resilience: Risk and responsibility in a hyperconnected world-principles and guidelines. *World Economic Forum,Tech. Rep.270912*, 2012. 84

[180] G. Wei, X. Xhang, X. Zhang, and Z. Huang. Research on e-government information security risk assessment-based on fuzzy ahp and artificial neural network model. In *Networking and Distributed Computing (ICNDC), 2010 First International Conference on*, pages 218–221. IEEE, 2010. 41, 46

[181] J. Wei, B. Lin, and M. Loho-Noya. Development of an e-healthcare information security risk assessment method. *Journal of Database Management (JDM)*, 24(1):36–57, 2013. 41, 46

[182] N. Werro. *Fuzzy classification of online customers*. Springer, 2015. 44

[183] P. Wilmott, S. Howison, and J. Dewynne. *The mathematics of financial derivatives: a student introduction*. Cambridge University Press, 1995. 101

[184] D. A. Wilson. Managing knowledge. *Butterworth Heinemann, Great Britain*, 1996. 34

[185] K. Wu and S. Ye. An information security threat assessment model based on bayesian network and owa operator. *Appl. Math*, 8(2):833–838, 2014. 46

[186] Z. Xiangmo, D. Ming, R. Shuai, L. Luyao, and D. Zongtao. Risk assessment model of information security for transportation industry system based on risk matrix. *Applied Mathematics & Information Sciences*, 8(3), 2014. 42, 46

[187] Z. Xinlan, H. Zhifang, W. Guangfu, and Z. Xin. Information security risk assessment methodology research: Group decision making and analytic hierarchy process. In *Software Engineering (WCSE), 2010 Second World Congress on*, volume 2, pages 157–160. IEEE, 2010. 46

[188] Y. Yamai and T. Yoshiba. Comparative analyses of expected shortfall and value-at-risk (2): expected utility maximization and tail risk. In *MONETARY AND ECONOMIC STUDIES/APRIL 2002*. Citeseer, 2002. 89, 146

[189] Y. Yamai and T. Yoshiba. Value-at-risk versus expected shortfall: A practical perspective. *Journal of Banking & Finance*, 29(4):997–1015, 2005. 146, 147

[190] Y. Ye, W. Lin, S. Deng, and T. Zhang. A practical solution to the information security risk evaluation problems in power systems. In *2014 International Conference on Future Computer and Communication Engineering (ICFCCE 2014)*. Atlantis Press, 2014. 42, 46, 48, 143

[191] A. C. Yeo, M. M. Rahim, and L. Miri. Understanding factors affecting success of information security risk assessment: The case of an australian higher educational institution. *PACIS 2007 Proceedings*, page 74, 2007. 46, 50

[192] X. Yin, Y. Fang, and Y. Liu. Real-time risk assessment of network security based on attack graphs. In *2013 International Conference on Information Science and Computer Applications (ISCA 2013)*. Atlantis Press, 2013. 46

[193] C. Ying. Information security risk assessment model of it outsourcing managed service. In *Management of e-Commerce and e-Government (ICMeCG), 2012 International Conference on*, pages 116–121. IEEE, 2012. 46

[194] Q. Yong, X. Long, and L. Qianmu. Information security risk assessment method based on coras frame. In *Computer Science and Software Engineering, 2008 International Conference on*, volume 3, pages 571–574. IEEE, 2008. 46

[195] S. L. Zabell. Alan turing and the central limit theorem. *The American Mathematical Monthly*, 102(6):483–494, 1995. 107

[196] L. A. Zadeh. Information and control. *Fuzzy sets*, 8(3):338–353, 1965. 44

[197] Y. Zhiwei and J. Zhongyuan. A survey on the evolution of risk evaluation for information systems security. *Energy Procedia*, 17:1288–1294, 2012. 48

[198] L. Zhou and Y. Zhou. Gray relational analysis based method for information security risk assessment. In *Computer Science & Education (ICCSE), 2012 7th International Conference on*, pages 1086–1089. IEEE, 2012. 46

[199] Y. Zhuang, X. Li, B. Xu, and B. Zhou. Information security risk assessment based on artificial immune danger theory. In *Computing in the Global Information Technology, 2009. ICCGI'09. Fourth International Multi-Conference on*, pages 169–174. IEEE, 2009. 46

Appendix A

Programming for circular statistics

A.1 R programme of Dataset extraction

```
data <- fread("/Users/pxai013/Desktop/lp/data.txt")
mw <- as.data.frame(data)

top10 <- sort(table(mw$Country),decreasing = T)[1:3]
mw_10 <- mw[mw$Country %in% names(top10),]
mw_10 <- mw_10[mw_10$Domain != "D?",]

freq <- aggregate(IP ~ Country+Domain,data= mw_10,length)
sorted <- freq %>%
  arrange(Country, -IP) %>%
  group_by(Country) %>%
  mutate(rank=row_number()) %>%
  .[.$rank<=2,!colnames(.) %in% c("IP","rank")]

mw_10 <- merge(mw_10,sorted,by=c("Country","Domain"))
mw_10 <- mw_10[grep("_s_", mw_10$Diagnostic),]
mw_10$date <- as.POSIXlt(as.numeric(mw_10$time),origin = "
    1970-01-01",tz="GMT")
mw_10 <- mw_10[mw_10$date >= "2016-08-07" & mw_10$date <= "
    2016-08-23",]
```

```
summary_number <- aggregate(IP ~ Country+Domain,data= mw_10,
    length) %>% as.data.frame
mw_10<- mw_10[,!colnames(mw_10) %in% c("State","Subflow","flow
    ")]
uu<-mw_10$Diagnostic %>% str_split_fixed(.," ",5)
mw_10$botnet <- uu[,4]

botnet_summary <- aggregate(IP ~ Country+Domain+botnet,data=
    mw_10,length) %>%
   arrange(Country,Domain, -IP) %>%
   group_by(Country,Domain) %>%
   mutate(rank=row_number()) %>%
   .[.$rank<=3,!colnames(.) %in% c("IP","rank")]

#write.csv(botnet_summary,"summary.csv")

mw_10 <- merge(mw_10,botnet_summary,by=c("Country","Domain","
    botnet"))

mw_10$dd <- str_sub(mw_10$date, -11, -10) %>% as.numeric
mw_10$hh <- str_sub(mw_10$date, -8, -7) %>% as.numeric
mw_10$mm <- str_sub(mw_10$date, -5, -4) %>% as.numeric
mw_10$ss <- str_sub(mw_10$date, -2, -1) %>% as.numeric
mw_10$new_time <- mw_10$hh + (mw_10$mm/60)
#write.csv(mw_10,"mw_10.csv")
mw_10 <- mw_10[mw_10$dd <= 21,]
mw_10 <- mw_10[mw_10$dd >= 7,]

country_name <- mw_10$Country %>% unique %>% as.data.frame
names(country_name) <- "country"

for (i in 1:nrow(country_name)){
   cou <- country_name[i,1]
   subdata <- mw_10[mw_10$Country == cou,]
   write.csv(subdata,paste(cou,".csv",sep=""))
}
```

A.2 Poisson Test via Matlab

```
function [pvals,chi2stat,lambdas,totals,df]=poitestmatlab(x)

[M,N]=size(x);
pvals=zeros(N,1);
df=pvals;

chi2stat=pvals;
lambdas=mean(x);
%totals=sum(x);
totals=M*ones(N,1);
for n=1:N
    table=tabulate(x(:,n));
    obs=(0:table(end,1))';
    counts=zeros(size(obs));
    counts(table(:,1)+1)=table(:,2);
    efs=poisspdf(obs,lambdas(n))*totals(n);
    MaxN=length(efs);
    %idx=find(efs<5);
    %if ~isempty(idx),
        %disregard low counts in the head of the list
     %   if idx(1)==1, idx(1)=[]; end;
     %   if ~isempty(idx),
          %efs(idx(end))=totals(n)*(1-poisscdf(idx(end)-2,
              lambdas(n)));
          %efs((idx(end)+1):end)=[];
          %counts(idx(end))=sum(counts(idx(end):end));
          %counts((idx(end)+1):end)=[];
          efs(MaxN)=totals(n)*(1-poisscdf(MaxN-2,lambdas(n)))
              ;
          %efs((idx(end)+1):end)=[];
          %counts(idx(end))=sum(counts(idx(end):end));
          %counts((idx(end)+1):end)=[];
           df(n)=MaxN-2;

    chi2stat(n)=sum(((counts-efs).^2)./efs);
```

```
    pvals(n)=1-chi2cdf(chi2stat(n),df(n));
    end;
end
```

A.3 Helix plots via Matlab

```
t = linspace(0,14*pi,7*24);
x = 20*t; y = cos(t); z = sin(t);

%# plot 3D line
plot3(x,y,z)
axis tight, grid on, view(35,40)

cc = [cn_7days1]
h = surface([x(:), x(:)], [y(:), y(:)], [z(:), z(:)], ...
    [cc(:), cc(:)], 'EdgeColor','flat', 'FaceColor','none');
colormap( gray(numel(t)) )
colorbar
```

Appendix B

Data Management and ISRA

This chapter describes the structure of data management as data collection, data analysis and data verification. Each part of data management respectively corresponds to the process of ISRA as Figure B.1. For instance, data collection corresponds to risk identification. The selection of data depends on the identified risks. Realistically, we can not identify all the risks due to the human resources and time. Thus, we need to assess the most critical risks. Data analysis could determine the risk levels and may provide the risk scores by collected data. Data Verification checks the risk scores that whether they are unusual by the nature of system and risk criteria.

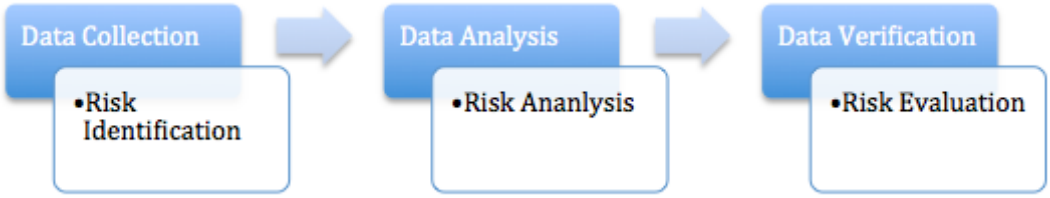


Figure B.1: Process of Data Management

B.1 Data Collection

Data collection is not only the first step of ISRA but also the most critical part of identifying risks. It most likely decides the success of the other stages of ISRA [166]. Furthermore, we can improve the accuracy and efficiency of data collection by identifying the risks from a business practice perspective [166]. Figure B.2 demonstrates that the first step of data collection is to interview the sponsors for achieving the assessment goals. According to the targets, we conduct the project team of implementing ISRA.

Information Security Officer, SSA (Senior Security Analyst) and JSA (Junior Security Analyst) are the crucial members of such team [166]. The second step is to identify the information security risks by some structure techniques such as AHP (analytic hierarchy process). AHP can obtain more correct data by decomposing the complex problems into several sub-questions and analyse these sub-questions independently [190].

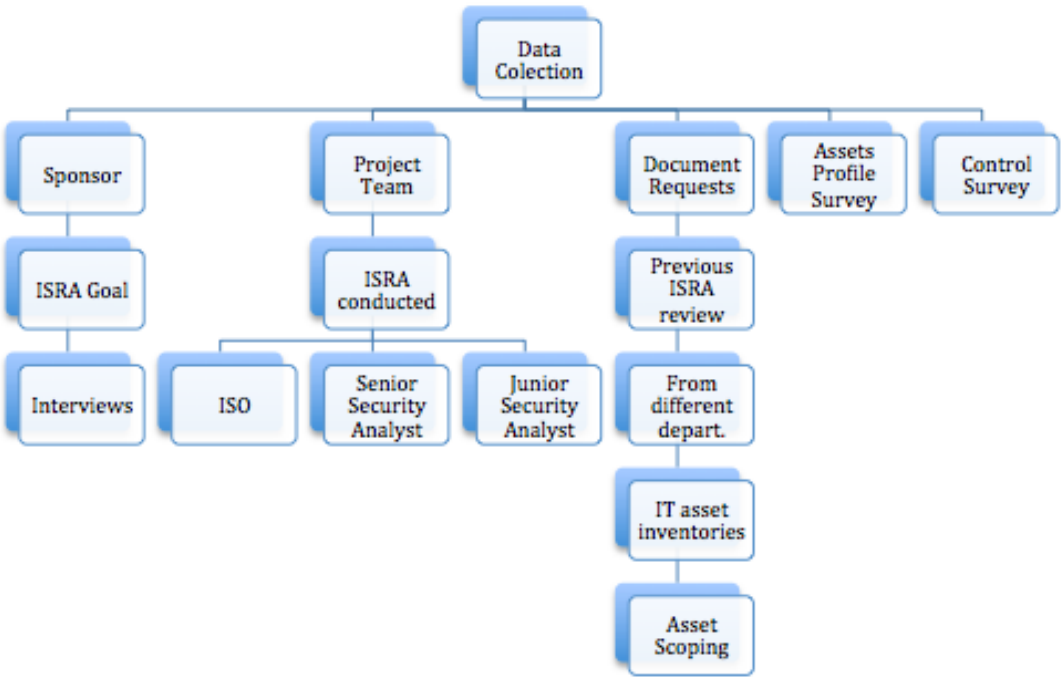


Figure B.2: Process of Data Collection

B.2 Data Analysis

Data analysis will obtain the likelihood and impact of the collected data. In a practical application, organisations apply the simple formulas to calculate the risk levels. But these simple equations can not present more accurate results due to the subjectivity of data or biased sampling. Specific models are introduced into the organisations to mitigate the subjectivity or biased estimator. For instance, researchers apply the fuzzy theory to determine the risk levels and incorporate uncertainties [144]. In the practical ISRA, most methods of risk analysis just stay on the academic level, other than real applications in organisations. Therefore, we have to find a bridge to connect the theoretical, analytical methods and the practical use of the data analysis. Talabis and Martin state that likelihood can be easily achieved by exposure, frequency and

reverse control [166]. In fact, the impact of risks is determined by taking the maximum values of confidentiality, integrity and availability. Hence, the risk scores are equal to likelihood times impact.

B.3 Data Verification

For the phase of data verification, we check the risk scores of different information systems whether they have outliers. If there are outliers, we could examine the reasons why the outliers appear and whether they are reasonable. If they are not rational, we have to track back to the original database and find out the reasons. For instance, the wrong typed data in the worksheets. In this case, we just merely retype the right data. Secondly, the assessors assess threats or vulnerabilities inaccurately.

B.4 An Automated Method of Data Management

We have introduced some existing automated tools of standards in Figure 2.8 and Figure 2.9. However, these tools have not considered the attributes of organisations such as IT, finance and education. Generally speaking, different characteristics have different types of assets, threats and vulnerabilities. Thus, we suggest designing a system which takes organisation attributes into account. Considering all types of organisations is unlikely. In the circumstances, the first step could be the approach of choosing the types of companies in such system. The second phase is to determine the contents of the system. In future research, the detailed structure of an automated system presented in Figure B.3, could contain the pull-down menus of organisation types, sizes, the categories of input data, the selections of risk analysis methods, the formats of data output, the criteria of data verification and an ISRA report.

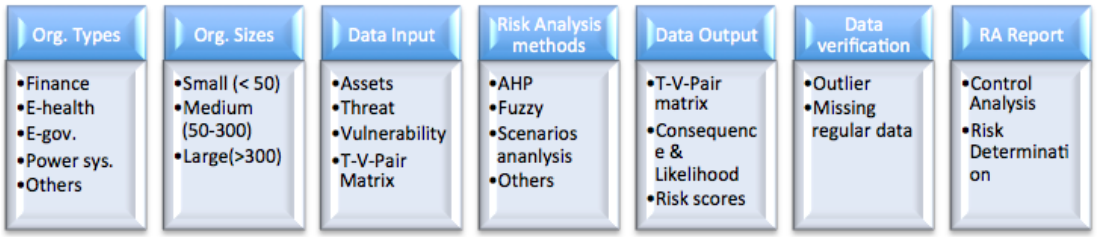


Figure B.3: Data management systems for a practical ISRA

A requirement for the system is to update the risks quickly and frequently. Additionally, it is necessary to have a questionnaire to investigate the feasibility of the

system such as the price and the target enterprises. It is also possible to require the system to alter the wrong risk scores easily. For instance, once wrong typing or inaccurate assessment of a particular threat-vulnerability matrix, the system managers can modify the responding data, and amend the related risk scores by the correct data. We have to alter all associated worksheets one by one and recalculate all data.

In a real scenario, many companies use worksheets or spreadsheets as the data containers of ISRA. These sheets can temporarily satisfy only once per ISRA. But it is not convenient to compare with the previous ISRA results or the data of another same type of organisations. The data in these spreadsheets may be different classification, if we want to compare the ISRA data of different years or various organisations, we have to spend more time to sort out the data and obtain the results. Additionally, it is difficult to monitor the changes in new risks.

All the discussions mentioned above about a new automated tool or method of ISRA imply that this is a possible direction in the future research, although we do not further study this issue in this thesis. A new tool needs to invest more resource in the system construction such as a well-structured IT team.

Appendix C

Expected Shortfall

To overcome the limitations of VaR, in 1997, Artzner et al. proposed the concept of expected shortfall (ES) as another risk measure model [14]. ES is "the conditional expectation of loss for losses beyond the VaR level" [189]. ES considers the problem of "tail risk" of loss distribution and satisfies the property of sub-additive of a coherent risk measure [189].

C.1 Expected Shortfall

This section will make a brief introduction about the definition and features of Expected Shortfall. We also discuss the advantages and disadvantages between ES and VaR.

Definition 2.2 (Expected Shortfall): Given X $\in L$ is the portfolio return with loss function L and the confidence level $\alpha \in (0, 1)$, expected shortfall is the expectation loss which L exceeds VaR [116]:

$$ES_\alpha(L) = E[L|L \geq VaR_\alpha(X)].$$

The mathematical definition depicts that ES considers the loss of a threat event as a distribution, preferably is a numerical expression in the calculation formula. The tail risk has no role in VaR and ES if the loss distribution is normal [188]. Otherwise, VaR is affected by the tail risk due to the underlying the asset prices in finance [188]. In the financial risk assessment, Yamai and Yoshiba present that ES "is a better risk measure than VaR regarding tail risk" [189]. McNeil [116] shows the difference between VaR and ES in Figure C.1.

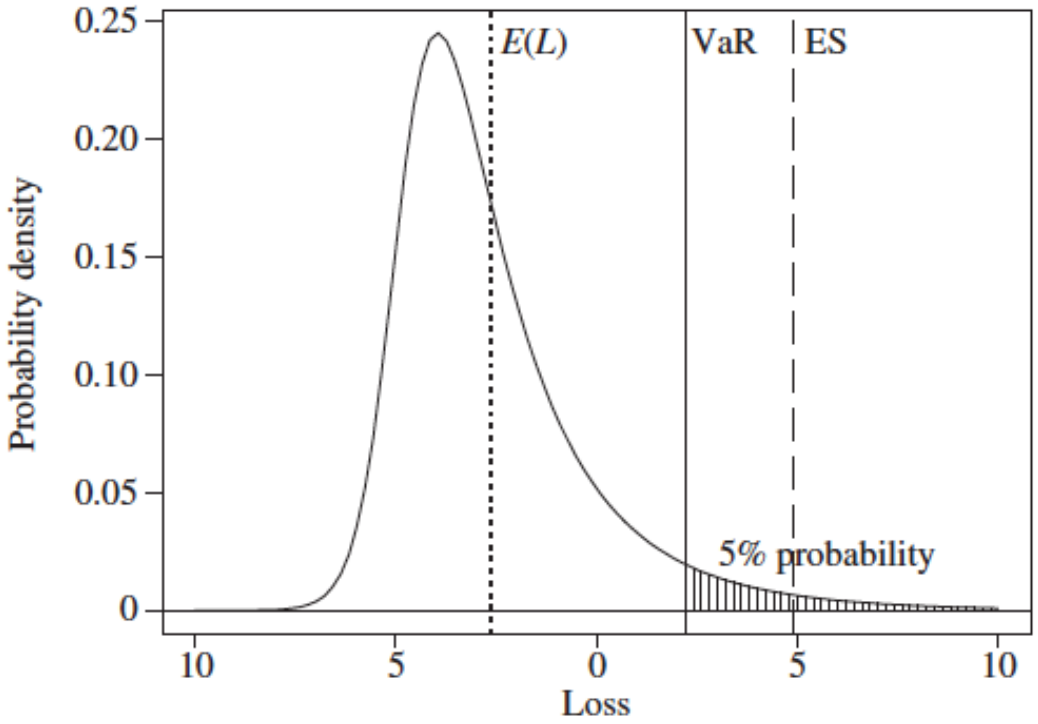


Figure C.1: The diagram of VaR and ES [116] . A vertical line denotes a loss distribution with 95% VaR; a dotted line denotes the mean loss E(L); a dashed line denotes a loss distribution with 95% ES.

However, when the underlying distribution is fat-tailed, the estimation errors of ES are much higher than those of VaR. To reduce estimation error, sometimes it is essential to increase the sample size of the simulation. That means ES is most costly when it most needs to be free from tail risk under the fat-tailed distribution [189]. These findings imply that the use of a single risk measure should not dominate financial risk management. Each risk measure offers its advantages and disadvantages. Complementing VaR with ES represents an efficient way to provide more comprehensive risk monitoring [189].

C.2 Coherent Risk Measure

This section will introduce the concept of coherent risk measure. According to Artzner et al., a coherent risk measure should satisfy "the four axioms of translation invariance, subadditivity, positive homogeneity, and monotonicity" [15]. They also claim that any reasonable risk measure, which can manage risks effectively, should satisfy these four

properties of a coherent risk measure [14]. We describe the four axioms as follows [15]:

- Translation invariance: $X \in S, a \in R \implies \rho(X \pm a) = \rho(X) \pm a$;

  This axiom means that any risk X belonging to the set of all risk S, for any given real number a, the value of $\rho(X + a)$ just merely increases by a to the initial amount of $\rho(X)$.

- Positive homogeneity: $b \geq 0, X \in S \implies \rho(bX) = b\rho(X)$; under the information security circumstance, b can be considered as the weight of an individual risk;

- Monotonicity: $X, Y \in S$ with $Y \geq X \implies \rho(Y) \leq \rho(X)$;

- Sub-additivity: $X, Y \in S,\ X + Y \in S \implies \rho(X + Y) \leq \rho(X) + \rho(Y)$, This property implies that "a merger does not create extra risk [15]." When counting the merger risks of (X+Y) by a risk measure ρ and ρ is subadditive; then we can obtain a feasible guarantee that the risk of (X+Y) does not exceed the sum risks of $\rho(X) + \rho(Y)$ [15].

where ρ is a risk measure; X or Y is a random variable denoted a risk; S is the set of all risks; a is a real number; R is the set of all real numbers.

Jorion illustrates that VaR has itself limitations such as lacking the feature of sub-additivity of a coherent risk measure [85]. McNeil et al. suggest that requiring sub-additivity may lead to some harmful side effects for VaR [116]. On the one hand, the risks are hard to be decentralised via VaR. Because it is not sure that aggregating the values of VaRs of different individual risk will obtain a boundary value for the total risks [116]. On the other hand, the VaR of combined portfolios in financial risk assessment may not be produced using summing the VaRs of individual portfolios. Artzner et al. mention that VaR neglects the losses beyond the VaR level called the problem of "tail risk" [15].

Although VaR has its limitations when applied in measuring information security risks, VaR still has an excellent theoretical basis compared with most of the qualitative methods of ISRA [80]. Moreover, VaR is a useful quantitative tool for assessing risks for an information security expert [80]. Hence, VaR is still adopted to evaluate the cyber threats of information security and denoted a new model called CyberVaR [141].

Appendix D

Power Law Test of Conficker Datasets

Lai presents that "power law distribution are usually used to model data whose frequency fof an event varies a power of some attribute of that event" [97]. Goldstein et al. in 2004 stated that a power-law distribution existed in many situations such as "the world wide web, metabolic networks, and internet router connections [64]. However, it can be wrong that these phenomena often fit to a power-law distribution by some "simple graphical methods [64]. In this case, they try to solve this problem by using a "KS-type goodness-of-fit test for the power-law distribution hypothesis [97]. Clauset et al. propose a method combining maximum-likelihood estimated and Kolmogorov-Smirnov (KS) goodness-of-fit tests to quantify the empirical data on the behaviour of a power-law distribution [38]. Therefore, this section will introduce mathematical definitions of a discrete power-law distribution and the KS goodness-of-fit tests, followed by fitting the power-law distribution to the datasets.

D.1 Power Law Definition

Definition D.1.1. *Clauset et al. [38] define the discrete power-law distribution over an integer variable x by*

$$p(x) = \frac{x^{-\alpha}}{\zeta(\alpha, x_{min})} = Cx^{-\alpha} \tag{D.1}$$

Where

- **x** is observed data and a positive integer (e.g. number of links per network node [64]);
- α is the power-law exponent;

- **p(x)**is the probability of the observed value x;
- $\zeta(\alpha, \mathbf{x_{min}}) = \sum_{\infty}^{\mathbf{n=0}} (\mathbf{n} + \mathbf{x_{min}})^{-\alpha}$ is the generalized zeta function, and is the number of x_i with i=1,2,...,n;
- $\mathbf{C} = \frac{\mathbf{1}}{\zeta(\alpha, \mathbf{x_{min}})}$ and C is the normalization constants;
- **observed data** are independent. The assumption of independent data is required in later KS goodness-of-fit test for the power-law hypothesis.

Definition D.1.2. *Log-likelihood function is given by [38]:*

$$\mathcal{L} = \ln \prod_{i=1}^{n} \frac{x_i^{-\alpha}}{\zeta(\alpha, x_{min})} = -n \ln \zeta(\alpha, x_{min}) - \alpha \sum_{i=1}^{n} \ln x_i. \tag{D.2}$$

Setting $\frac{\partial \mathcal{L}}{\partial \alpha} = 0$, then

$$\frac{-n}{\zeta(\alpha, x_{min})} \frac{\partial}{\partial \alpha} \zeta(\alpha, x_{min}) - \sum_{i=1}^{n} \ln x_i = 0. \tag{D.3}$$

where x_i, i=1,...,n. Thus, the MLE $\hat{\alpha}$ for the scaling parameter is the solution of

$$\frac{\zeta'(\hat{\alpha}, x_{min})}{\zeta(\hat{\alpha}, x_{min})} = -\frac{1}{n} \sum_{i=1}^{n} \ln x_i \tag{D.4}$$

Finally, when $x_{min} \geq 6$, then $\hat{\alpha}$ is estimated by the following equation

$$\hat{\alpha} \simeq 1 + n[\sum_{i=1}^{n} \ln \frac{x_i}{x_{min} - \frac{1}{2}}]^{-1} \tag{D.5}$$

In fact, the MLE can provide more accurate and robust estimates for fitting to the power law distribution [64].

D.2 Hypothesis Test

In this section, we test whether the selected Conficker datasets follow a power law distribution. Gillespie introduces two methods to do the test including a bootstrap function and the model comparison between a power-law and another model [62].

D.2.1 Bootstrap function

Gillespie states that fitting a power-law distribution is feasible for "any dataset" [62]. The null hypothesis test is that the observed data follows a power law distribution.

Clauset et al. propose that a bootstrapping program is an appropriate approach of goodness-of-fit test for testing this hypothesis [38]. A p-value is used to quantify the "plausibility of the hypothesis" [124], and if the p-value is greater than the given significance level, then we have no evidence again the power-law hypothesis. Goldstein et al. state that good-of-fit test is a quantitative measure to access "how well data approximates a power-law distribution and this quantitative measure can identify some possible events which may have the feature of power-law distribution" [64].

In the test, there is a uncertainty problem when estimating some parameters. Gillespie illustrates that the bootstrap function in the R "poweRlaw" package could deal with the problem of parameter uncertainty [62]. Furthermore, the bootstrap function also is used to "any distribution object" [62]. Lai states that the KS test is used to see whether the observed data are from the same power-law distribution with the generated data which have the estimated parameters α and x_{min} [97].

Definition D.2.1. *Clauset et al. state that KS statistic D is to calculate "the maximum distance between the CDFs of the data and the fitted model" [38]:*

$$D = \max_{x \geq x_{min}} |S(x) - P(x)|, \tag{D.6}$$

Where

$\boldsymbol{S(x)}$ is the CDF of the observed data with value at least x_{min};

$\boldsymbol{P(x)}$ is the CDF of the power-law model that best fits the data in the region $x \geq x_{min}$;

Data are independent, if data are dependent, there is a lower rejection rate for the KS test than expected;

$\boldsymbol{\hat{x_{min}}}$ is the value of x_{imin} that minimizes D.

In the KS test, we can decide whether the observations follow the power-law distribution under the given significance level by p-value. That means if the p-value is greater than the significance level, we have the no evidence against the power-law hypothesis. The KS test is implemented by R "poweRlaw" package [60]. The details of bootstrapping program are based on the theory of Clauset et al. [38] and showed in Figure D.1.

1: Calculate point estimates for $x_{\min}$ and the scaling parameter α.
2: Calculate the Kolmogorov-Smirnov statistic, KS_d, for the original data set.
3: Set n_1 equal to the number of values below $x_{\min}$.
4: Set $n_2 = n - n_1$ and $P = 0$.
5: **for** `i` in `1:B`:
6: Simulate n_1 values from a uniform distribution: $U(1, x_{\min})$ and n_2 values from a power law distribution (with parameter α).
7: Calculate the associated Kolmogorov-Smirnov statistic, KS_{sim}.
8: If $KS_d > KS_{sim}$, then $P = P + 1$.
9: **end for**
10: $P = P/B$.

Figure D.1: Bootstrapping program of the power-law hypothesis [61]

The null hypothesis is:

- H_0: dataset follows a power-law distribution.

In this case, if the result shows p-value $>$ 0.05 (significance level), we have no evidence against the power-law hypothesis H_0. However, it is worth to note that obtaining a large p-value does not mean that it is definitely correct for fitting a power-law distribution to the data. Clauset et al. illustrate that maybe another model fits to the data better "over the range of x observed" [38]. Furthermore, we have to pay more attends when you sample sizes n is small but with large p-values [38].

D.2.2 Model Comparison

The ami of model comparison is to find out which distribution can fit to the data better between a power-law distribution and the alternative one [38]. Clauset et al. demonstrate that the power-law distribution is normally tested in the goodness-of-fit test. When passing the test, it is possible to think about whether there is a alternative distribution may fit to the data better than the power-law model [38]. Clauset et al. further suggest that the likelihood ratio test is better than the KS test in the model comparison [38] due to the easy implement. They illustrate the likelihood ration test is to computer the likelihood of the data under two competing distributions. The one with the higher likelihood is then the better fit [38]. The mathematical definition of likelihood ratio tests is given by [38]:

Definition D.2.2. *Likelihood Ratio Tests:* $p_1(x)$ *and* $p_2(x)$ *present the PDFs of two*

distributions and the respective likelihoods for a given data set are

$$L_1 = \prod_{i=1}^{n} p_1(x_i), L_2 = \prod_{i=1}^{n} p_2(xi), \tag{D.7}$$

and the likelihood ratio is

$$R = \frac{L_1}{L_2} = \prod_{i-1}^{n} \frac{p_1(x_i)}{p_2(x_i)} \tag{D.8}$$

Change R to the log-likelihood ratio $\mathcal{R}$ is

$$\mathcal{R} = \sum_{i=1}^{n} [\ln p_1(x_i) - \ln p_2(x_i)] = \sum_{i=1}^{n} [l_i^{(1)} - l_i^{(2)}] \tag{D.9}$$

where $l_i^{(j)} = \ln p_j(x_i)$ are the log-likelihood for x_i within distribution j.

In the "poweRlaw" package for the model comparison, it uses the log-likelihood ratio $\mathcal{R}$ as the Vuong's test statistic [62]. The positive or negative results of the equation D.9 indicate which distribution is better fit [38]. However, this is not definitely correct due to the subjectivity of log-likelihood ratio [38].

The second method is to test the data between a power law distribution and the other distribution. Gillespie presents that this approach applies the likelihood ratio test under the same minimum x-value [61]. The assumed null hypothesis is [60]:

- H_0: Two tested distributions can not fit the true distribution .

D.3 Process with R language

As we mentioned above, there are two methods for testing the power-law hypothesis. Thus, Gillespie also provides two types of R program via "poweRlaw" package to calculate the p-value. This subsection will describe the steps how to fit a discrete power law to the observed data by R "poweRlaw" package provided [62]. The first type of programming details are shown in Figure D.2:

The program "$m_p l$setXmin" provide sthe values of estimate parameters α, x_{min} and the KS statistics. The bootstrap function examines all x_{min} values and reduces the searching area for large x_{min} values [62]. Furthermore, the Kolmogorov-Smirnov (KS) test is helpful for the good-of-fit test in the bootstrap function. By bootstrap function, we can obtain the p-value to adjudge the hypothesis. If the p-value is greater than the given significance level, then we have no evidence against the power-law hypothesis.

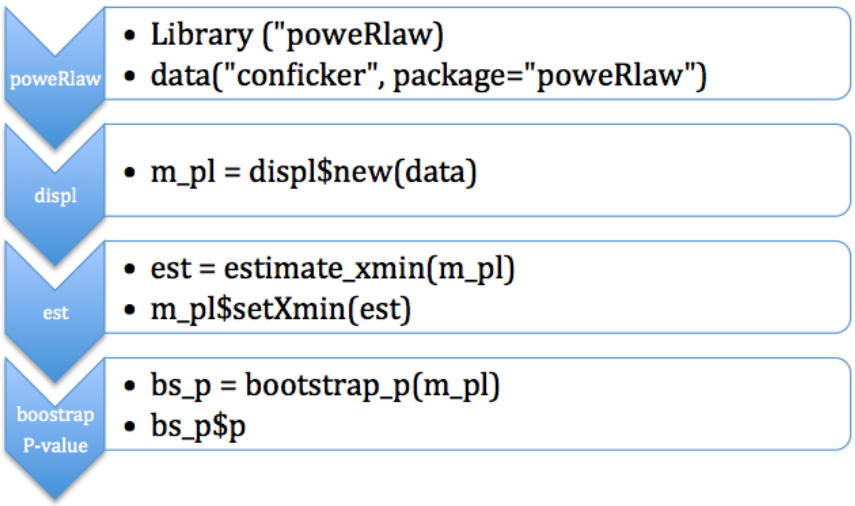


Figure D.2: Fitting a power law to discrete data [62], the displ is a constructor for discrete power law, est presents to estimate the lower threshold, $m_p l$setXmin is to "update the power-law object" [62].

The second programming of model comparison is described by the following Figure D.3:(we take a power-law and log-normal as two candidate distributions)

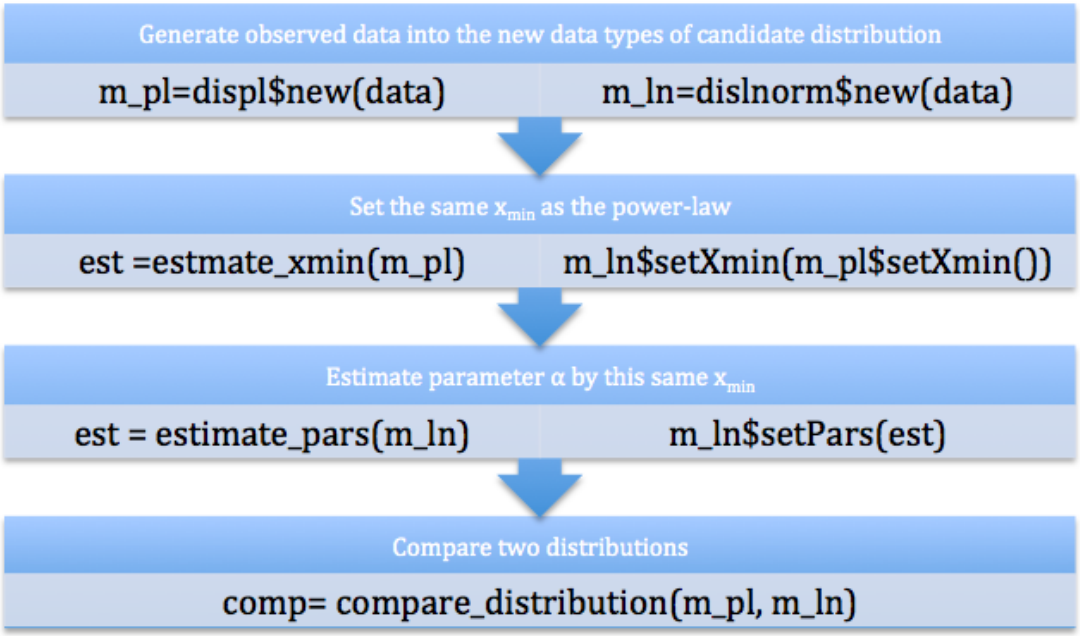


Figure D.3: Process of distribution comparisons by R "poweRlaw" package

D.3.1 R Programming

We run the R programming to extract the dataset and estimate the relative parameters of a power law distribution.

```
indata <- fread("/Users/pxai013/Desktop/lp/Powerlaw\ test-R/IN
    /in8-21power.csv")
data_day <- indata %>% filter(day == 8)    ## select 8 Aug data
     from the original

## count the mins frequency of unique attacks
day <- data_day %>%
          group_by(day) %>%
          summarise(count = n()) %>%
          nrow

dist <- data_day %>%                          # the outcome of
    frequency
          group_by(day,hour,min) %>%
          summarise(count = n()) %>%
          group_by(count) %>%
          summarise(distribution = n()) %>%
          rbind(c(0,day*24*60-sum(.$distribution))) %>%
          arrange(count)

data <- sort(dist$distribution, decreasing = TRUE)
attack <- sort(dist$count,decreasing = FALSE)
xmins <- unique(data) # search over all unique values of data
dat <- numeric(length(xmins))
z <- sort(data)

for (i in 1:length(xmins)){
  xmin = xmins[i] # choose next xmin candidate
  z1 = z[z>=xmin] # truncate data below this xmin value
  n = length(z1)
  a = 1+ n*(sum(log(z1/(xmin-0.5))))^(-1) # estimate alpha
      using direct MLE
```

```
  cx = (n:1)/n # construct the empirical CDF
  cf = (z1/(xmin-0.5))^(-a+1) # construct the fitted
      theoretical CDF cf = (z1/(xmin-0.5))^(-a+1)  cf = (z1/
      xmin)^(-a+1)
  dat[i] = max(abs(cf-cx)) }    # compute the KS statistic

D = min(dat[dat>0],na.rm=TRUE) # find smallest D value KS
    statistics value
xmin = xmins[which(dat==D)] # find corresponding xmin value
z = data[data>=xmin]
z = sort(z)
n = length(z)
alpha = 1 + n*(sum(log(z/(xmin-0.5))))^(-1) # get
    corresponding alpha estimate

# computer the constant C
for (i in 0:6)
{
  x[i] = (i+xmin)^(-alpha)
}
sum(x)

C=1/sum(x)

for (x in z)
p = c*z^(-2.9)    ## Prob of x
```

The following R program is to fit a discrete power law distribution via a continuous approximation.

```
plm.fit.discrete.approx <- function(data, xmin = 64, alpha.
    starting = 2.86) {
  N <- length(data)
  x <- sum(log(data / (xmin - 0.5)))
  alpha <- 1 + N / x

  sigma <- (alpha - 1) / sqrt(N)
```

```
  list(alpha = alpha, sigma = sigma, N = N, xmin=xmin, xmin.
      estimated=F)
}
```

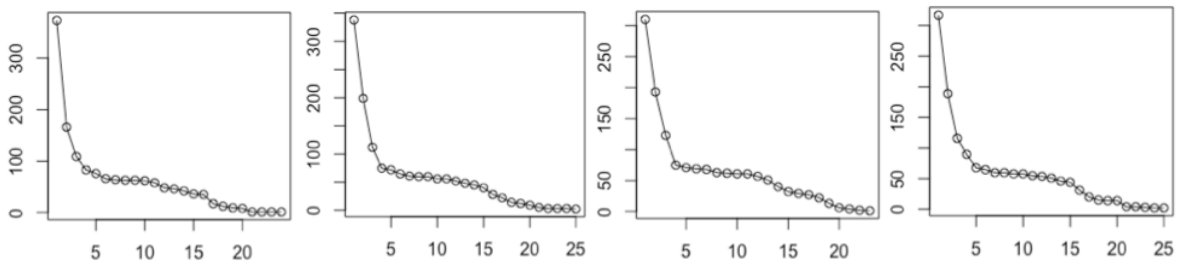
D.4 India Conficker dataset-powerlawe test

We take India as an example and extract the Conficker dataset from 8th August to 21st August 2016. We sum the attacks by minutes as Figure D.4. Then, we would like to fit the dataset to a discrete power law distribution. If the dataset can be fitted, we could conclude that the distribution of Conficker attacks is a discrete power law with the estimated parameter and x_{min}.

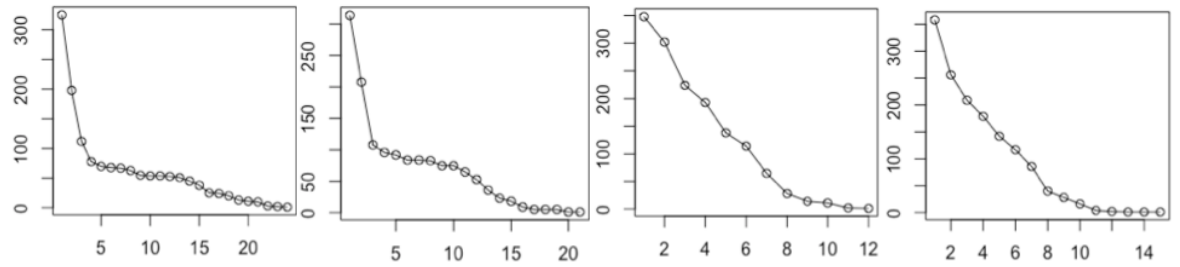
x_i	14ds	d8	d9	d10	d11	d12	d13	d14	d15	d16	d17	d18	d19	d20	d21
x_1	4541	373	338	310	317	325	314	348	358	317	306	298	307	295	335
x_2	2954	166	199	193	189	198	208	302	256	173	204	215	181	183	287
x_3	1834	109	112	123	116	112	108	224	209	101	97	139	103	107	188
x_4	1470	83	75	75	90	78	96	193	179	97	87	75	81	84	166
x_5	1131	76	72	71	68	70	92	138	142	66	64	71	63	68	151
x_6	1016	66	65	69	65	68	84	114	117	65	64	67	57	67	118
x_7	867	64	61	68	60	67	84	65	86	65	58	66	54	58	79
x_8	752	63	60	63	60	63	83	28	40	63	56	63	54	56	41
x_9	714	63	60	62	58	55	75	14	28	59	55	63	52	55	34
x_{10}	702	62	56	61	58	54	75	11	16	57	54	61	50	51	20
x_{11}	690	58	56	61	55	54	65	2	4	51	54	61	49	49	10
x_{12}	626	48	52	57	54	53	53	1	2	49	53	57	47	46	8
x_{13}	569	46	48	51	51	51	36		1	48	48	51	46	45	3
x_{14}	523	42	45	40	46	45	23		1	47	48	46	45	44	
x_{15}	435	36	40	32	44	38	18		1	47	43	30	44	39	
x_{16}	346	35	28	29	31	25	9			38	39	23	43	37	
x_{17}	261	17	22	27	20	24	5			26	27	21	39	33	
x_{18}	229	12	14	22	15	20	5			25	24	10	34	30	
x_{19}	162	9	12	13	14	13	5			14	21	9	25	24	
x_{20}	127	8	9	6	14	11	1			10	17	5	18	22	
x_{21}	73	1	5	4	4	10	1			9	4	5	15	11	
x_{22}	47	1	3	2	4	3				7	4	2	12	11	
x_{23}	30	1	3	1	3	2				2	4	1	6	8	
x_{24}	27	1	3		2	1				1	4	1	4	8	
x_{25}	16		2		2					1	1		4	4	
x_{26}	9									1	1		4	3	
x_{27}	3									1	1		1	2	
x_{28}	2										1		1		
x_{29}	2										1		1		
x_{30}	1														
x_{31}	1														

Figure D.4: Observed data for each day and 14days (14ds)

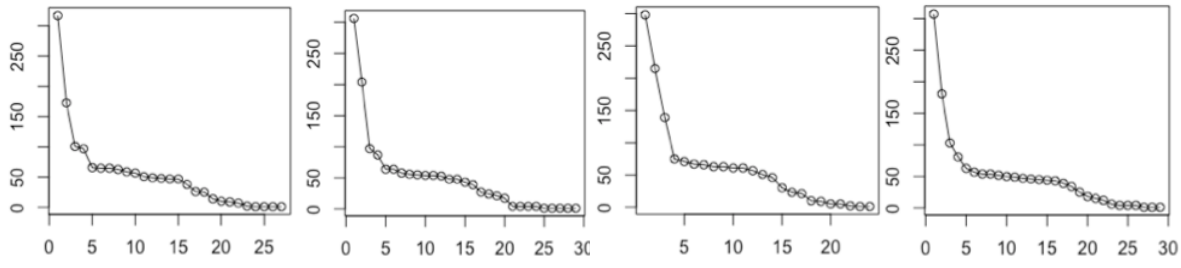
Figure D.4 shows the $x_i s$ in each day from 8th August to 21st August and the total days. $x_i s$ present the minute frequency of unique attacks. For example, x_1 is the most frequency minutes of attack attempts and there are 373 minutes on 8th August. We sort out data by decreasing order and find that the sample sizes of each day are different. Figure D.5 shows the all days' plots and the total days' plot. Based on these plots, the curve shapes follow a power law distribution under some estimated parameters. However, we have to test whether the data fit to a power law by statistical approaches. We applied a KS goodness-of-fit test to the same datasets.



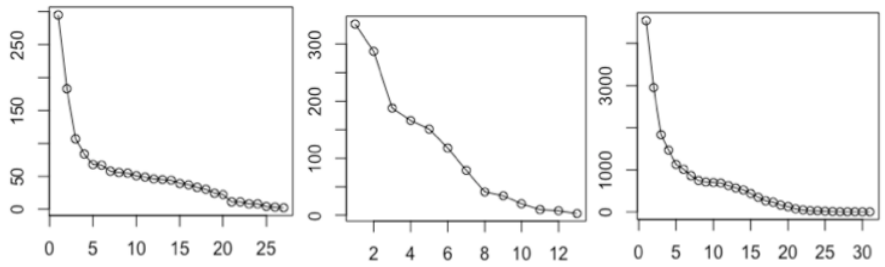
(a) d8 Mon (b) d9 Tue (c) d10 Wed (d) d11 Thu



(e) d12 Fri (f) d13 Sat (g) d14 Sun (h) d15 Mon



(i) d16 Tue (j) d17 Wed (k) d18 Thu (l) d19 Fri



(m) d20 Sat (n) d21 Sun (o) 14days

Figure D.5: Plots of Day 8-21 and total days data :x-axis presents the number of attacks, y-axis is the frequency of minutes of attacks

date	D	x_{min}	alpha	ntail	p-value (bootstrap)	n
14ds	0.11	569	2.52	13	0.91	31
8	0.17	66	2.68	6	0.72	24
9	0.16	45	2.88	14	0.41	25
10	0.21	51	3.06	13	0.14	23
11	0.16	44	2.9	15	0.42	25
12	0.14	45	2.86	14	0.65	24
13	0.18	65	3.15	11	0.43	21
14	0.26	114	2.71	6	0.28	12
15	0.22	142	3.33	5	0.63	15
16	0.18	47	3.24	15	0.14	27
17	0.18	43	2.95	15	0.18	29
18	0.19	46	2.79	14	0.17	24
19	0.15	39	3	17	0.19	29
20	0.12	44	3.02	14	0.7	27
21	0.22	118	3	6	0.5	13

Figure D.6: The results of a Power law test for the India Conficker dataset (from 8th August to 21st August 2016): ntail is the number of $x_i \geq x_{min}$ [63] and n is the number of data points.

Based on the given nine datasets, we follow the process provided by Figure D.2 and apply the bootstrap function to obtain the p-values. Figure D.6 shows the test results including the KS test statistic D, the lower threshold x_{min}, the scaling parameter α, the sample sizes n and p-values. If we set the significance level is 5% and compare it with all the p-values. We find that all p-values are greater than the significance level. That means we have no evidence against the power law hypothesis. In other words, the minutes of unique attacks in each day or total days follow the power law distribution.

However, it is worth noting that the p-value of day 14 is really higher than the other days. The sample size of day 14 of this data set is 31, which is not a large sample. For the high p-value with relative small sample ($n < 50$), we have to consider whether we can trust the test results. Maybe there is another distribution fitting the 14-day data better. Therefore, it is better to do the distribution comparison between a power-law and another alternative distribution in future.