FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Lauri Haverinen

IMPLEMENTATION OF INFORMATION SECURITY CONTROLS IN SMALL AND MEDIUM-SIZED BUSINESSES

Bachelor's Thesis
Degree Programme in Computer Science and Engineering
July 2019

Haverinen L. (2019) Implementation of information security controls in small and medium-sized businesses. University of Oulu, Degree Programme in Computer Science and Engineering. Bachelor's thesis, 43 p.

ABSTRACT

Information systems and networks play an important role in today's working environments. To keep offering their products and services, companies need to handle large amounts of data. Businesses need to be prepared to face criminals, who see this data as a high value target. While large enterprises can spend great amount of money for keeping their systems secure, SMEs are struggling with their limited resources. In this paper, a group of Finnish companies with 10-250 employees are surveyed to find out what information security controls they are using as defense measures against hostile actors. Although no alarming shortcomings are discovered, there is a lot of variation in what controls different companies are using.

Keywords: cyber security, monitoring, office network, staff awareness

Haverinen L. (2019) Tietoturvakontrollien toteutus pk-yrityksissä. Oulun yliopisto, tietotekniikan tutkinto-ohjelma. Kandidaatintyö, 43 s.

TIIVISTELMÄ

Tietojärjestelmät ja -verkot ovat tärkeä osa nykypäivän työympäristöjä. Jatkaakseen tuotteidensa ja palveluidensa tarjoamista yritysten on käsiteltävä suuret määrät dataa. Yritysten täytyy valmistautua kohtaamaan rikollisia, jotka näkevät tämän datan arvokkaana kohteena. Suuret yhtiöt voivat käyttää suuria summia järjestelmiensä suojaamiseen, kun taas pk-yritykset koettavat selviytyä rajallisten resurssiensa kanssa. Tässä tutkielmassa ryhmältä 10-250 henkeä työllistäviä suomalaisia yrityksiä selvitetään kyselyn avulla, mitä tietoturvakontrolleja niillä on käytössä järjestelmien suojaamiseen vihamieliseltä toiminnalta. Vaikka kyselyssä ei ilmene mitään hälyttäviä puutteita, kontrollien käytössä on eri yritysten osalta paljon vaihtelua.

Avainsanat: kyberturva, valvonta, yritysverkko, henkilöstön tietoisuus

TABLE OF CONTENTS

FOREWORD

The aim of this thesis is to find out what kind of information security policies and system security mechanisms do small and medium-sized businesses in Finland use in order to protect their data against criminals and other hostile actors. The subject originated from my personal interests.

I would like to thank my supervisor, professor Juha Röning, for giving me the opportunity to make my thesis for the research group OUSPG and Christian Wieser for helping me to get in contact with companies and guiding me through the whole research process.

Oulu, Finland July 1, 2019

Lauri Haverinen

ABBREVIATIONS

2FA	two-factor authentication
CEO	chief executive officer
CTI	cyber threat intelligence
CTO	chief technology officer
DMZ	demilitarized zone
DoS	denial-of-service
DDoS	distributed-denial-of-service
IaaS	infrastructure-as-a-service
IDS	intrusion detection system
IPS	intrusion prevention system
ISP	internet service provider
LAN	local area network
MFA	multi-factor authentication
NDA	non-disclosure agreement
OS	operating system
SME	small or medium-sized enterprise
SSO	single sign on
VPN	virtual private network
WLAN	wireless local area network

1. INTRODUCTION

Regardless of the line of business, information systems and networks are playing an important role in today's working environments[1]. In order to keep providing their services to customers, companies need to be able to handle large amounts of data[2]. This data may contain critical information about the company, its products, services and customers, and it is one of the most important assets businesses have. Because of its importance, the data is a high value target for cyber criminals. It is essential for companies to keep their data and systems secured against attackers, since incidents such as data breaches may end up costing businesses millions of dollars[3].

Since smaller businesses usually have fewer information and system security resources, criminals are increasingly targeting them[4]. There are numerous different threats that attackers create for companies, e.g. phishing, emails with malicious attachments, malware, denial-of-service attacks and data breaches[5]. One of the most popular attack types against SMEs (small and medium-sized enterprises) is spear-phishing, a phishing attack that targets specific individuals using previously collected information about them or their organization[6]. In 2014, 34% of spear-phishing attacks detected by a computer security company Symantec[7] were targeted at 45% of small businesses. Since then, criminals have changed their tactics to much more focused approach, and although larger percentage of attacks (43%) were aimed at small businesses in 2015, the proportion of companies affected was significantly smaller, only 3%.

In addition to the change of tactics in social engineering attacks, criminals are coming up with new and improved versions of old threats. The arrival of cryptocurrencies gave attackers new options to transfer money anonymously, which lead to the increase in ransomware attacks against SMEs. Ransomware is a malware that encrypts the files on the infected device and does not decrypt them until a ransom is paid[8]. This kind of attack may have a big impact especially on small businesses, since their limited resources can make the recovery process more difficult. Although the overall amount of ransomware infections decreased in 2018 by 20%, the amount of infections in businesses rose by 12%[9].

The aim for this study is to find out what kind of security controls, including organizational policies and technological mechanisms do small and medium-sized businesses currently use in order to protect their data and information systems against hostile actors. This is done with a questionnaire, which focuses on five categories; staff awareness, information security in daily working, network and system security, monitoring and system testing. A group of small and medium-sized companies are surveyed in order to gain understanding of the level of preparedness against cyber attacks and the current status of protection mechanisms in businesses. The gathered information can be used to find out how companies prioritize different aspects of information and system security and whether there are any noticeable shortcomings in the overall level of preparedness of the SMEs in Finland.

2. BACKGROUND

Since information systems are an important asset for companies[1], they need to be protected against criminals and malicious activity. According to earlier studies about information and system security situation in SMEs, most companies actively utilize some types controls in order to protect their data and information systems. These controls include information security policies, staff education and technological mechanisms such as antivirus softwares, firewalls and IDSs (intrusion detection systems). Every company implements their information systems differently, and although there are multiple information security guidelines and standards for businesses, e.g. ISO/IEC 27000 series information security management system standards[10], there is no one-size-fits-all technical solution that would suit every company. The level of utilization of information and system security controls differs between different companies, and there is a lot of variation on how companies prioritize the use of these measures[11].

2.1. Related work

Gupta and Hammond[12] published a study in 2005 about information security issues faced by SMEs. They surveyed 138 companies in Lynchburg, Virginia, USA, about their use of different technologies, information security policies, system security mechanisms and their level of concern for different information security threats and risks. Responding companies regarded viruses to be the most important concern while their least important concern was insider access abuse. Based on that, companies might be too optimistic in trusting their employees and do not necessarily see them as a threat, since in 2005 insider attacks were occurring as often as outside jobs[13]. Study concludes that SMEs often prioritize information security controls that are ineffective in their information system environments because they do not have enough resources and they may lack the experience from prior incidents.

In 2008, Merete Hagen, Alberchtsen and Hovden[14] surveyed 87 Norwegian companies and organizations about what organizational information security controls, e.g. policies, internal and external audits, risk analyses and staff education, they have implemented. Participants were also asked to evaluate their organization's information system security performance and how effective different security controls are. Although raising security awareness was thought to be the most effective way to improve company's information security preparedness, it was also the least implemented among the respondents. Organizations seemed to also be quite optimistic about their security performance, since more than half (52%) thought that their readiness was better than the average and only 3% replied that their performance was worse than the average. This kind of unsubstantiated optimism can lead to neglecting some important key aspects in company's information security[15].

Osborn[11] conducted a survey in 2015 about cyber security awareness, risks, budgets, requirements and implemented measures in SMEs and microenterprises in the UK. She received 33 responses from 19 different business sectors. The study

addresses several key issues that companies are facing concerning their cyber security, such as lack of time and awareness, limited financial resources and cyber security industry's focus on government and large enterprise level infrastructure. Some of the questions addressed a possibility of a cyber security standard becoming a requirement for companies. Because of their limited financial resources, large proportion of respondents thought that the implementation of such standard should cost no more than £500 if it should become a requirement. Their low cyber security budgets might also make the industry think that SMEs are a less appealing market than large enterprises with bigger budgets.

2.2. Past events

Multiple high-level information and cyber security incidents have been reported in Finland during the last few years. Waves of phishing and denial-of-service attacks that concern Finnish organizations have happened since the beginning of 2015, as can be seen in Figure 1. The data is collected from yearly reports published by FICORA (Finnish Communications Regulatory Authority) [16][17][18][19]. Although most of the large-scale attacks have not directly targeted SMEs, they show that the threat of becoming a victim of one exists. However, smaller-scale denial-of-service attacks are commonly found in Finland, and thousands of them are reported yearly to FICORA[20] in addition to other kinds of incidents.

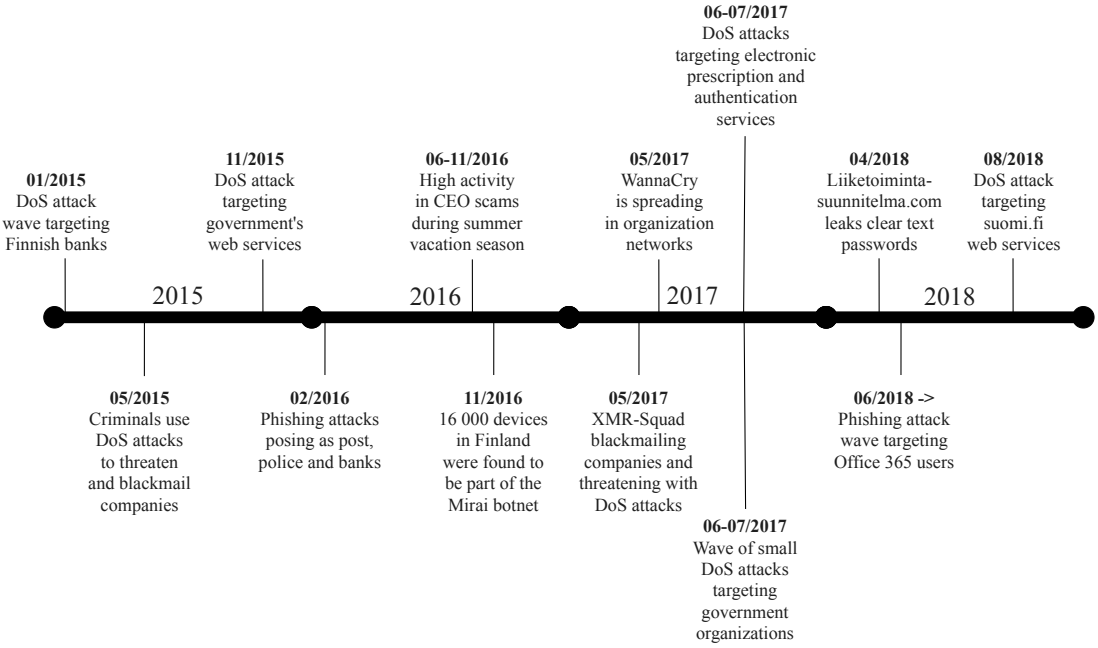

Figure 1. Cyber security incidents concerning Finnish organizations.

2.3. Information and system security threats

Helsinki Region Chamber of Commerce[5] collects data from Finnish companies about their views on different information and cyber security threats. Table 1 shows the most common threats among the respondents, their descriptions and the company asset that they are primarily targeting. Companies of all size find phishing and malware to be their greatest information security threats. Phishing attacks are often one of the first steps in a larger targeted attack, and they are also regularly used to distribute malware to victims.

Table 1. Common information security threats for Finnish companies

Threat	Description	Primary target
Phishing	Social engineering, attacker tries to collect information from employees by posing as someone else[21]	Employees and management
Malware	Software that is designed to cause harm to the user, often spread via email, e.g. worms and viruses	Workstations and mobile devices
Leakage of confidential company data	Adversarys get access to company's confidential data either deliberately or accidentally	Confidential company data
Insider threat	Employee or subcontractor who abuses their position in the organization[22]	Confidential company data
Denial-of-service attacks	Disrupting the use of assets, services or resources, typical attack is to overflood servers with requests[23]	Services used or developed by the company
Ransomware	Malware that encypts the filesystem and holds the data as hostage[8]	Workstations
Data breach	Confidential data, e.g. personal data and login details are stolen from the company	Company and customer data

Although leakage of confidential company data and insider threats are mentioned separately, there is little to none contrast between them. Both usually require actions performed by company's own staff either on purpose or accidentally and both of these threat types are targeting company data.

During the last few years, DoS (denial-of-service) attacks and especially DDoS (distributed-denial-of-service) attacks that utilize several sources have become a part of everyday life in Finland[19]. Although largest attacks have so far mostly targeted government services and banks, every company should be prepared to face them.

For smaller businesses, ransomware attacks can have severe consequences. Limited computer security resources can affect how a company is able to recover from such incidents. When a system gets infected with ransomware, it may be easier to get rid of the device instead of trying to restore it.

Data breaches are considered to be incidents where criminals get their hands to data they should not have access to by utilizing vulnerabilities in i.e. web services or network devices. Usually these kinds of incidents involve vulnerable, outdated services that reveal customer data to attackers.

2.3.1. Evolution of threat landscape

Since 2012, ENISA (European Union Agency for Network and Information Security)[24] has published a yearly report about information and cyber security threats. They collect CTI (cyber threat intelligence) from several sources all around the world, and their reports can be used to compare how the threat landscape against individuals and organizations has evolved year by year. Although threat types such as malware, web application attacks, denial-of-service and phishing have kept their places among the top threats for years, some new trends can also be seen from ENISA's[25] listings.

Money is one of the main motives for individual attackers and hostile actors. In 2018, attackers started to prefer cryptojacking instead of ransomware. Cryptojacking involves a malware that uses the processing power from its host system to mine cryptocurrencies. According to estimation by Check Point[26], criminals had profited over $2.5 billion in total during the first half of 2018 from these kinds of attacks, so it is very likely that attackers will continue to use them. Some criminals are also making profit by renting and leasing botnets to other parties, and since almost anyone has easy access to a botnet, criminals are able to make larger scale attacks more effortlessly.

For larger hostile parties, money is not however often the main motive. There can sometimes be even state-level actors with some political agenda. Depending on the country, SMEs can have a huge impact on its economy. Since state-level actors are playing larger role on the attacking side, governments should also be invested in the defense especially since the complexity of attacks has increased. Criminals who are targeting companies and organizations are using several attack vectors and combining technical and non-technical approaches. Attacks against information systems and networks are also becoming increasingly automated, which means that automated controls are also needed on the defending side.

3. INFORMATION SECURITY CONTROLS

The information and system security controls and mechanisms addressed in this paper are a collection taken from standards[10] and related studies[12][14][11]. Here these controls are divided into three groups; organizational, logical and physical controls.

3.1. Organizational

Organizational controls are measures that do not necessarily need any hardware or software implementation and they include risk assessment, increasing staff awareness, training and different written policies and protocols for employees and management. These policies are used to define roles and responsibilities, guidelines for different situations and how to work securely. Organizational controls are more abstract than logical and physical mechanisms and because of that they may be seen to be more difficult to implement correctly. However, without correct organizational controls, other mechanisms may become ineffective against the threats the company is facing.

Since information security incidents often include actions performed by the personnel[27], it is important that employees and management are aware of the threats[28]. This can be achieved by educating staff about different risks concerning information security, how to prevent any incidents and what to do in case of one. However, Merete Hagen, Albrechtsen and Hovden[14] suspect that awareness training is less used than other organizational controls because it might need more resources due to the fact that it needs to be repeated in order for the education to be effective. To make the process easier for companies, many organizations in the information security industry have started to offer cyber security training programs for companies to help them spread awareness.

Information security policies are the defining guidelines on how employees should consider the information security in daily working. They describe restrictions in how to use devices or software, handle and recognise sensitive or confidential data and how different information security roles and responsibilities are distributed.

In many companies, employees must sign NDAs (non-disclosure agreements) in the beginning of their employment. They are used to make sure that employees are obligated to keep any confidential company information to themselves even after the end of their contract. They are often used in large enterprises, but many SMEs utilize them also.

3.2. Logical

Logical controls are hardware and software based measures, such as anti-malware programs, firewalls, IDSs (intrusion detection systems), IPSs (intrusion prevention systems) and honeypots. They are essentially the mechanisms that are used to protect information systems and networks. Like physical mechanisms, logical

controls are not as abstract as organizational measures and they can be easily presented for example in a network topology. For easier visualisation, the network topology shown in Figure 2 is used as an example of a small company network with in-house servers.

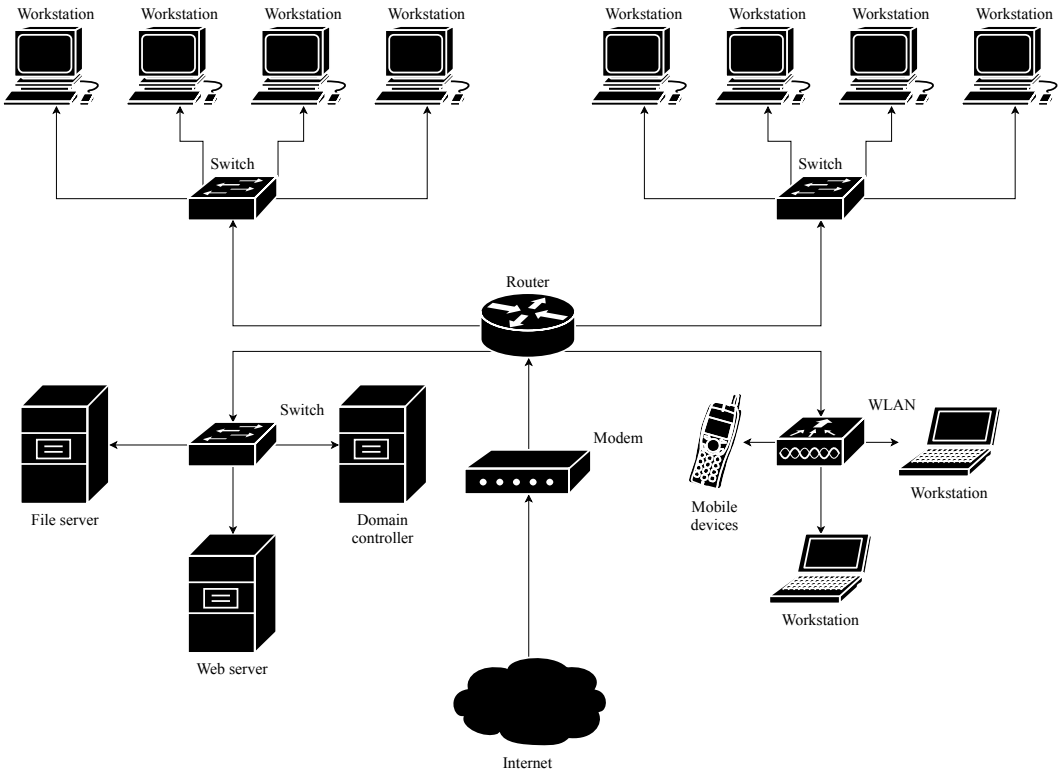

Figure 2. A typical network of a small company with in-house servers.

Firewalls are used to control and restrict the network traffic. A set of predetermined rules are used to define what type of traffic will be blocked and what can be passed through. Software firewalls are used to between computer and a network where they filter the incoming and outgoing network packets on the host computer and most modern operating system include integrated software firewall components, e.g. Windows Firewall and iptables. Hardware firewalls usually control the traffic between two separate networks and they are placed on the edge of a trusted network in the DMZ (demilitarized zone) as Figure 3 shows.

Intrusion detection and prevention systems are used to find suspicious events in the system or in network traffic in real time. The main difference between these two systems is that IDS is a passive and it only requires a read-only access to the network traffic or system logs. IPS needs a full read/write access to be able to control the system or the network traffic if a malicious event is discovered. There are two main types of intrusion detection systems; HIDS (host-based intrusion detection system) and NIDS (network-based intrusion detection system). HIDS is a software that is running on a host computer and it analyses the audit logs of the operating system to discover malicious events in the system or on its network interfaces[29]. NIDS is a system that consists of management server

and a monitoring component that reads the network traffic data from the firewall's interface and alerts the management system when an intrusion attempt is discovered[30]. A typical network-based intrusion detection system is placed in the network topology shown in Figure 3.

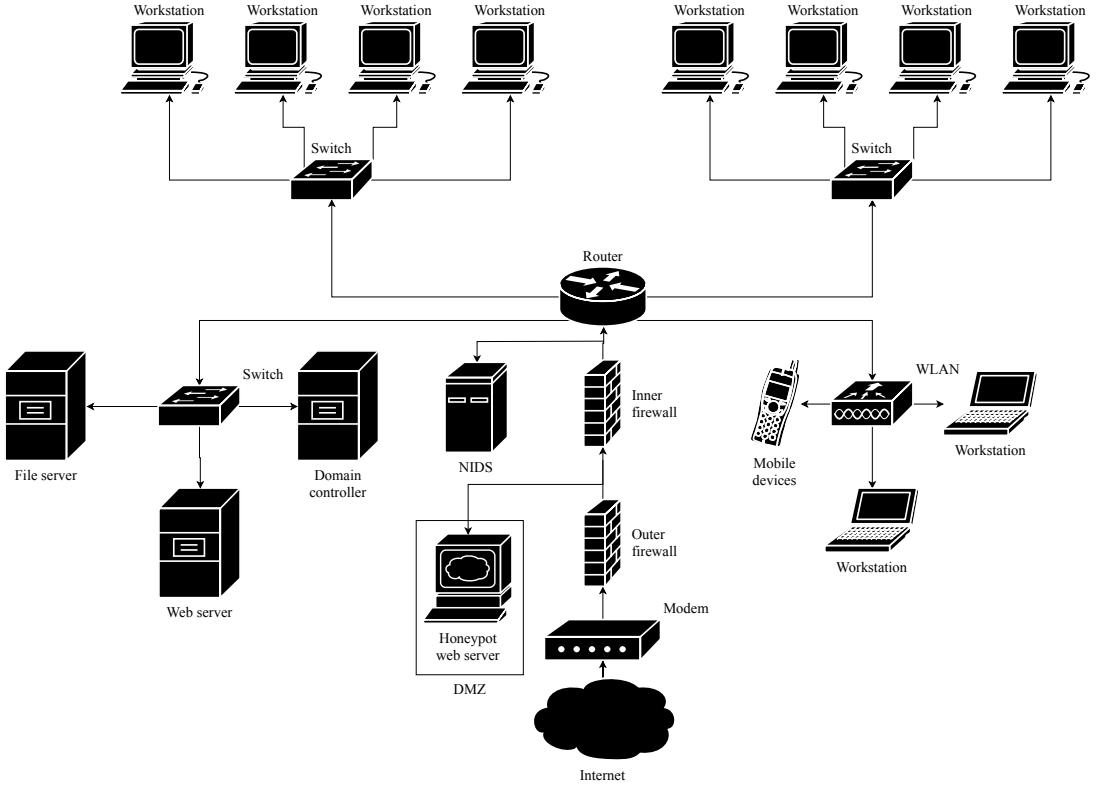

Figure 3. A small company network with firewalls, DMZ, honeypot and IDS.

In addition to using different intrusion detection and prevention controls, some companies use honeypots. They are programs, systems or even networks that do not have any production value for the organization and their only purpose is to attract attackers to interact with them[22]. Honeypots are used for a wide variety of things, e.g. gathering information and slowing down attacks, and they are one of the most cost-effective security controls to implement. The network topology in Figure 3 shows a honeypot web server placed in the DMZ.

Anti-malware software is a program running on the host device that can monitor the use of network interfaces, scan file system and downloaded files and alert the user if any malicious files are found. Most anti-malware solutions use signature-based methods for detecting malicious software, so they might not be very effective against previously unknown malware.

3.3. Physical

One of the key aspects in information system security is physical security. Physical security controls are the mechanisms that are used to restrict and monitor

the access to hardware or certain areas. These include for example surveillance cameras and access control systems. These controls are important especially for those companies that have in-house servers, since nobody should be able to access them without permission.

4. INFORMATION AND SYSTEM SECURITY SURVEY

Since all of the previous studies with similar subject have used questionnaires in order to collect data from businesses, it was an obvious choice for the research method for this paper as well. In total, 145 companies were invited to participate in the survey and 26 responses were received. The questions were divided into 5 categories and the main focus of the questionnaire was in the use of organizational and logical controls. First set of questions focuses on staff awareness, training and information security responsibilities in the company. Second part includes questions about daily working protocols, such as remote work possibility and policies concerning the use of personal accounts. Third part focuses on the network infrastructure and logical controls that are being used. Fourth part focuses on monitoring systems and employees, and the fifth part consists of questions about testing and auditing of company's information systems.

4.1. Participant requirements

Companies that were invited to participate were working on software industry, financial services or marketing. Although information systems and networks are widely used in many different business sectors, these three sectors were chosen because it is a necessity for them to use IT systems to provide their services to customers. There were two additional requirements for participating companies:

- Company had to be either Finnish or have its head office in Finland.
- Company had to have 10-250 employees to qualify as an SME.

4.2. Surveying process

The research process began by creating the information sheet shown in Appendix 1 and the questionnaire shown in Appendix 2. The main focus for the survey was decided to be in the organizational and logical information security controls. Next step was to collect a list of Finnish small and medium-sized companies to contact by using business directories provided by BusinessOulu, Fonecta and Helsinki Region Chamber of Commerce. The initial list consisted of 50 companies that filled the previously mentioned requirements.

Surveying started with telephone interviews. After noticing how much time it would take to contact each company one by one, it was decided that email would be a better approach as it made possible to contact all companies simultaneously. Email that included information about the study and a link to a web survey created with Webropol was sent to the rest of the companies on the initial list, but this resulted in only one additional response. A phone call was used as a reminder for contacted companies to encourage them to participate, but as the response rate stayed at around 10%, another 50 companies were invited to participate.

Because of the low response rate of the web survey, additional 45 companies were contacted over the phone. They were asked whether they would like to participate in the study, and if they accepted the invitation, the link to the survey was sent to them. Most of the responses were received using this approach giving the study its final response rate of 17.9%, which is similar as in studies conducted by Gupta and Hammond[12] and Merete Hagen, Alberchtsen and Hovden[14]. A more detailed view on the timeline of how the responses were received is shown in Table 4.

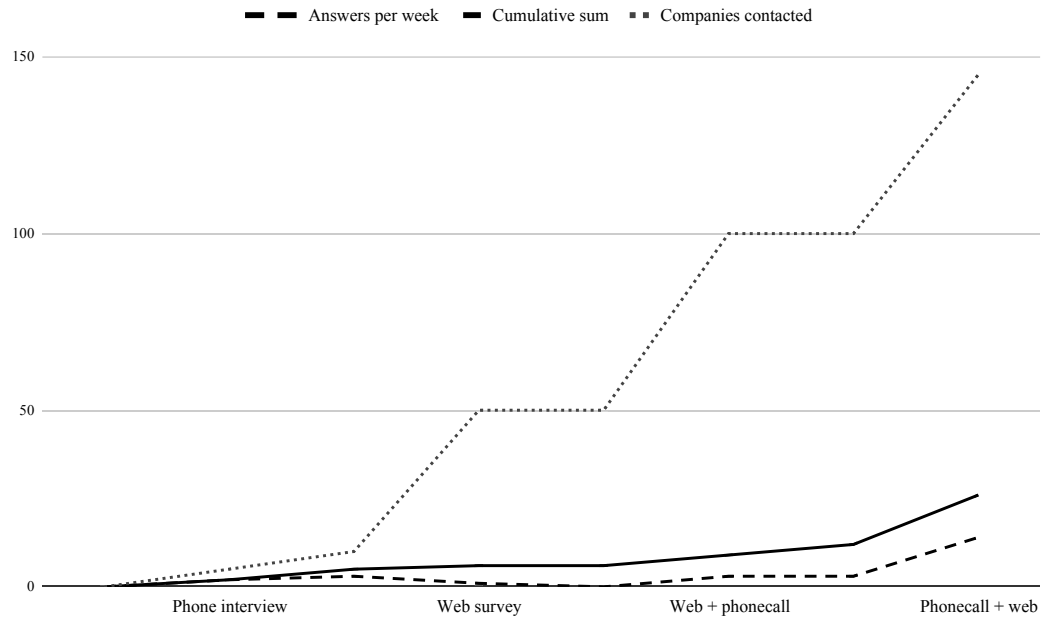

Figure 4. Timeline of response activity.

5. SURVEY RESULTS AND DISCUSSION

In total, the survey had 48 questions that were divided into five categories. Most of the answers given by the respondents are presented and discussed here, and the summary of results can be seen in Tables 2 to 10. The summary of all the answers can be found in Appendix 3. Although most of the responses were received from the web questionnaire, some interviews were also made over the phone.

During the phone interviews, it became clear that many companies prefer not to disclose a lot of details about their information and system security controls and especially the hardware and software products used by the respondents often seemed to be something that they would rather keep as a secret. Most participants did not mind telling about them either. The results show a lot of variation on However, it may not be the case since the results show so much variation among answers.

5.1. Current status

As attacks against organizations' systems and networks have become more common, use of defense mechanisms has also increased. Survey results show that none of the participants entirely neglected their company's information security and every company had implemented at least some of the security controls presented in the questionnaire.

5.1.1. Responsibility, policies and awareness

The first part of the survey was about information security policies, staff awareness and responsibility distribution. As can be seen in the summary of answers in Table 2, 73% of the responding companies had one or more people designated to be responsible for the company's information and system security. However, phone interviews revealed that the responsible party was sometimes the CEO or the CTO of the company. Although it is important that the top management is aware and involved in the decisions made about the information security, taking care of it entirely might need more attention that the CEO is able to give.

Information security policies are the main guidelines for employees on how to work securely. As can be seen in Table 2, only 58% of the respondents did have an information security policy approved by the top management fully in place. 34% answered that they had it partially in place and only 8% were lacking it entirely. Out of the companies that at least partially had said policy in place, 58% also told that they review it regularly. Employees were relatively informed about their company's policies, since only 4% of respondents that had some information security policy told that their staff was unaware of it. 64% of companies gave their employees additional training about information security in daily working and 65% also provided their staff basic training about the use of their company's information systems. It is important that employees know how to correctly use company's systems in order to prevent incidents caused by accidental misuse, but

Table 2. Summary of answers for staff awareness and policies

Question	Yes	Partly	No
Does the company have one or more person designated as responsible for information and system security?	19 (73%)	-	7 (27%)
Does the company have information security policies approved by the top management?	15 (58%)	9 (34%)	2 (8%)
Is the staff fully aware of company's information security policies?	15 (63%)	8 (33%)	1 (4%)
Has every employee committed to comply with company's information security policies?	19 (79%)	4 (17%)	1 (4%)
Are information security policies being reviewed regularly?	14 (58%)	6 (25%)	4 (17%)
Does staff receive basic training on how to use company's information systems before using them?	17 (65%)	-	9 (35%)
Does staff receive training in information security in daily working?	16 (64%)	-	9 (36%)

since most of the respondents were software companies, the staff should already have prior knowledge about working with information systems in general.

5.1.2. Information security in daily working

Out of the 92% of respondents that told that their employees had their own accounts for at least some of the company's systems, about half (54%) responded that employees were required to use only them while working as is shown in the summary of answers in Table 3. In case of an information security incident, having personal accounts may make it easier to pinpoint any individual employees associated with it. If staff is using accounts that only they have access to, the company might want to be sure that the authentication is secure. About a third (35%) of the companies responded that they did not verify the security of the passwords created by the employees. Among the companies that at least partially made sure that employees were using passwords that comply with the password complexity requirement set by the company, minimum length and the use of upper and lower case characters were the most commonly used as is shown in Table 4.

In addition to password complexity validation, some respondents also utilised MFA (multi-factor authentication) and SSO (single sign on) solutions. MFA and its most common type 2FA (two-factor authentication) use multiple authentication methods, both hardware and software-based in addition or in place of a traditional password-based approach. SSO solutions provide the ability to login to multiple accounts with only one authentication.

Table 3. Summary of answers for information security in daily working

Question	Yes	Partly	No
Does every employee have their own logins for all ICT systems?	17 (65%)	7 (27%)	2 (8%)
Are employees using only their personal logins when working?	13 (54%)	11 (46%)	0 (0%)
Is the creation of secure passwords verified?	10 (38%)	7 (27%)	9 (35%)
Is it possible for employees to work remotely?	24 (92%)	2 (8%)	0 (0%)
Does the company provide a VPN connection for connecting to company network remotely?	17 (65%)	-	9 (35%)
Is the necessary data being backed up regularly?	25 (96%)	-	1 (4%)

Table 4. Password requirements for employee accounts (n=17)

Requirement	n	% of companies
Change interval	7	41.18
Minimum length	12	70.59
Must have upper and lowercase characters	12	70.59
Must have numbers	10	58.82
Must have special characters	9	52.94

Although 92% of the companies responded that their employees could work remotely and the rest told that it was partially possible, only third of them (65%) offered their staff a VPN connection to the company network. If an employee works remotely and needs to transfer sensitive data, e.g. customer information or internal documents, third parties such as ISPs (internet service providers) and public WiFi hotspot owners are able to monitor the traffic. VPN could be used to offer a more secure, encrypted network traffic between office and remote work place.

In case of an incident that leads to a loss of data, it is important that backups are up to date. Taking frequent backups was a commonly used measure among respondents, since 96% told that the necessary data is being backed up regularly.

5.1.3. System security

65% of the respondents had in-house servers as is shown in Table 5. These companies were often using multiple servers for different tasks, and the most commonly used operating systems were UNIX/Linux-based. The server OS distribution is

shown in Table 6. 59% of the companies had servers with UNIX/Linux based operating systems, 47% had some version of Windows running on at least some of their servers and 18% had servers that were running macOS. 62% of the respondents with in-house servers also told that they were using some anti-malware software on their in-house servers.

Table 5. Summary of answers for system security

Question	Yes	Partly	No
Does the company use in-house servers?	17 (65%)	-	9 (35%)
Is some antivirus software being used on the servers?	10 (62%)	-	6 (38%)
Does the company use cloud servers?	20 (83%)	-	4 (17%)
Is some antivirus software being used on staff computers?	18 (69%)	-	8 (31%)
Is the company network separated from the public internet with a hardware firewall?	22 (85%)	1 (4%)	3 (11%)
Do company devices use software firewalls?	15 (60%)	2 (8%)	8 (32%)
Is it possible to connect to the company network wirelessly?	26 (100%)	-	0 (0%)
Are software and operating system updates being automated?	10 (38%)	15 (58%)	1 (4%)
Are software and operating system updates being tested before distribution to company systems?	1 (4%)	17 (68%)	7 (28%)
Is the company network divided into separate segments based on different tasks?	11 (44%)	-	14 (56%)
Are software updates distributed to different network segments simultaneously?	6 (55%)	-	5 (45%)

Table 6. Operating systems on in-house servers (n=17)

OS	n	% of companies
UNIX/Linux	10	58.82
Windows	8	47.06
macOS	3	17.65

Cloud servers were more commonly used than in-house servers (83%). Some companies did not want to disclose their service providers, but according on the received answers that are shown in Table 7, SMEs do not centralise their cloud on

any single cloud provider's platform and many companies replied that they were using multiple providers. Although large enterprises' platforms e.g. Amazon AWS, Google Cloud and Microsoft Azure were commonly used, many smaller Finnish providers were also mentioned in the responses.

Table 7. Use of different cloud service providers (n=20)

Cloud provider	n	% of companies
Amazon AWS	5	25
Google Cloud	6	30
IBM Cloud	0	0
Oracle Cloud	1	5
Microsoft Azure	6	30
Other or confidential	11	55

The workstation OS distribution shown in Table 8 shows that responding companies used a wide variety of different operating systems on their workstations. The two most commonly used operating systems were Windows (77%) and macOS (62%). About a third of the companies (35%) replied that they had workstations that were running some Linux distribution and 12% had computers that were running Chrome OS. Although Windows has been traditionally seen as the OS that the most of the malware is targeted to, based on the fact that 69% of the companies told that they were using some anti-malware software on their workstations, it can be concluded that some of the respondents that had Windows workstations do not use antivirus on them. Since 31% of the respondents did not use antivirus on their workstations, companies might believe that using Linux-based operating system or macOS might keep them entirely safe from malware. However, that is not the case since multiple different malware have been discovered that are targeted to devices running on Linux[31] or macOS[32].

Table 8. Workstation OS distribution (n=26)

OS	n	% of companies
Chrome OS	3	11.54
Linux	9	34.61
macOS	16	61.54
Windows	20	76.92
Other	2	7.69

89% of the companies responded that they use hardware firewall to at least partially separate their company's network from the public internet, and 68% replied that software firewalls are used on company devices. Although some of the companies did not want to tell whether their network was divided into separate segments, 44% of the respondents answered that they had. Businesses

can divide their networks into subnets in order to control who inside the company has access to certain data.

96% of the companies at least partially automated their software and operating system updates, and out of those respondents, 92% told that it takes one week or less to distribute the updates to company devices. 28% of the respondents did not test any updates before installing them and only 4% said that they did. About half of the companies that had separated their network into different segments distributed the updates simultaneously to all devices in different subnets.

5.1.4. Monitoring

The answers shown in Table 9 are for the fourth part of the survey that had questions about monitoring network traffic and usage of devices and software. It is important for the business to know what is happening in order to discover any suspicious events that might occur. In addition to finding acts committed by unauthorised third parties, different monitoring tools can be used to discover or even prevent information security violations that are committed by employees[33].

While 38% of the respondents did not allow staff to use any unauthorised external storage devices and 12% only partially forbade it, 69% of the companies at least partially prohibited the use of unauthorised software. Hardware and software products that come from an unknown origin can create risks for company's information security. Around half of the companies did not monitor the use of external devices (56%) or the software (52%) and although 58% of the companies had blocked the installation of unauthorised programs, 81% did not use mechanisms to prevent the use of external devices and 19% answered that they only partially did. Some of the companies did not want to share any information about whether they were using an IDS to monitor their network or not, and among those who answered the question only 12% were using one.

5.1.5. System testing

The last part of the questionnaire was about testing of the company information systems. As can be seen in Table 10, 56% of the respondents at least partially commissioned penetration testing on their networks and information systems. In 36% of these companies, the testing was done on regular basis and most of the companies (72%) hired an outside contractor for it. In half (50%) of the companies that tested their systems, the same tester was used every time. Although 48% of the respondents did at least partially audit their systems based on some certain criteria, only 4% had been granted some information or cyber security certificate.

5.2. Room for improvement

Although every responding company were somehow taking notice of their information and system security, there is a lot of variation in the level of preparedness

Table 9. Monitoring

Question	Yes	Partly	No
Does the company prohibit the use of unauthorised external storage devices?	10 (38%)	3 (12%)	13 (50%)
Is the use of external storage devices being monitored?	3 (12%)	8 (32%)	14 (56%)
Has the company blocked the use of external storage devices?	0 (0%)	5 (19%)	21 (81%)
Does the company prohibit the use of unauthorised software?	12 (46%)	6 (23%)	8 (31%)
Is the installation of unauthorised software being monitored?	5 (20%)	7 (28%)	13 (52%)
Has the company blocked the installation of unauthorised software?	6 (23%)	5 (19%)	15 (58%)
Is the company network being monitored with some IDS?	3 (12%)	-	21 (88%)

Table 10. System testing

Question	Yes	Partly	No
Does the company commission penetration testing on its networks and information systems?	5 (20%)	9 (36%)	11 (44%)
Does the testing happen regularly?	5 (36%)	7 (50%)	2 (14%)
Does the company hire outside contractor to do the testing?	10 (72%)	2 (14%)	2 (14%)
Is the same tester being used every time?	3 (21%)	4 (29%)	7 (50%)
Are the company information systems being audited based on some certain criteria?	5 (20%)	7 (28%)	13 (52%)
Has the company been granted some security certificate?	1 (4%)	-	25 (96%)

in different companies. The results are not showing any significantly alarming shortcomings among the respondents, but there is definitely room for improvement in the use of some controls.

Although organizational controls were widely implemented among survey participants, over third of the companies did not educate their staff about information security. The same effect can be seen in the study by Merete Hagen, Albrechtsen and Hovden[14]. Although staff awareness is thought to be important, staff awareness training is the least implemented of the organizational controls.

31% of the companies answered that they were not using any antivirus software on employees' workstations and phone interviews revealed that it is a common belief that there is no malware that could affect non-Windows OS. Multiple types of malware however exist for also macOS[32] and Linux-based operating systems[31], so the threat of infection exists on every platform and it should be taken into account regardless of the operating system used.

The use of external storage devices was not prohibited, monitored or blocked in over half of the businesses as is shown in Table 9. Since criminals can use USB storage devices and other peripherals as an attack vector[34], this seems concerning. If devices are acquired from an unreliable source or they are also being used in other, less controlled environments, there is a higher risk for infected or malicious devices to end up in the work environment. Another common issue is that users could be plugging in random USB flash drives that they have found. Although it may seem unlikely that someone would plug in a device with entirely unknown origins, Tischer et al.[35] proved that it does happen. A company policy that restricts the use of unknown external devices could be used to prevent incidents from happening.

Although majority of the companies did commission some kind of testing on their devices and networks and almost half also audited their systems, only 4% of the respondents had received some system security certificate. This could be due to the company not passing the criteria used by the tester or because the tester might not have the authority to grant certifications. Finnish information security industry has many different companies and organisations that offer information system testing services, but all of them are not certified by any authority behind standards. Acquiring some globally recognised information security certification such as ISO 27001[36] is a good way to be assured that the company is dealing with its information and system security properly.

6. CONCLUSION

The aim of this study was to find out what information system security controls Finnish SMEs use in order to protect their systems and data against criminals and other hostile parties. 26 companies were surveyed either over the phone or by using a web questionnaire about what controls have they implemented in their organisation.

Information security policies are widely implemented in Finnish SMEs, but depending on a company the staff education leaves something to be desired. Phishing attacks are one of the most common information security incidents faced by SMEs, so awareness training could be an efficient way to improve organization's information security.

Although in-house servers are commonly used, cloud-based solutions are also increasing their popularity. Using cloud services, SMEs can transfer some of the technical security responsibility to service providers. Different IaaS (infrastructure-as-a-service) solutions are popular especially among small businesses who have limited information and system security resources.

The majority of the respondents commission security testing on their systems and networks, but acquiring security certificates is quite uncommon. This may be due to the additional cost that comes with certification process.

SMEs are generally aware that they need to be prepared against criminal activity in their information systems. According to the survey results, all responding companies utilise some sort of information security policies, controls and mechanisms in their systems and networks. None of the respondents are entirely neglecting the information security aspect, but there is a lot of variation in what controls are used in different companies.

7. REFERENCES

[1] Smith J. (1999) Information Technology in the Small Business: Establishing the Basis for a Management Information System. Journal of Small Business and Enterprise Development 4, pp. 326–340.

[2] Solita (2017), Thinktank: The data revolution and business. URL: https://hub.solita.fi/think-tank-data-revolution-and-business.

[3] Ponemon Institute (2018), 2018 cost of a data breach study: Global overview. URL: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

[4] Hiscox (2018), 2018 hiscox cyber readiness report. URL: https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf.

[5] Helsinki Region Chamber of Commerce (2016), Yrityksiin kohdistuvat kyberuhat 2016. URL: https://issuu.com/kauppakamari/docs/yrityksiin_kohdistuvat_kyberuhat_20.

[6] Hong J. (2012) The state of phishing attacks. Commun. ACM 55, pp. 74–81.

[7] Symantec (2016), Internet security threat report. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[8] Richardson R. & North M.M. (2017) Ransomware: Evolution, mitigation and prevention. International Management Review 13, p. 10.

[9] Symantec (2019), Internet security threat report. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[10] ISO Central Secretary (2016) Information technology – security techniques – information security management systems – overview and vocabulary. Standard ISO/IEC 27000:2016, International Organization for Standardization, Geneva, CH. URL: https://www.iso.org/standard/66435.html.

[11] Osborn E. (2015) Business versus technology: Sources of the perceived lack of cyber security in SMEs. Tech. rep., University of Oxford, Centre for Doctoral Training in Cyber Security.

[12] Gupta A. & Hammond R. (1999) Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination. Information Management & Computer Security 4, pp. 297–310.

[13] Gordon L.A., Loeb M.P., Lucyshyn W. & Richardson R. (2005) 2005 csi/fbi computer crime and security survey. Computer Security Journal 21, p. 1.

[14] Merete Hagen J., Albrechtsen E. & Hovden J. (2008) Implementation and effectiveness of organizational information security measures. Information Management & Computer Security 16, pp. 377–397.

[15] Rhee H.S., Ryu Y.U. & Kim C.T. (2012) Unrealistic optimism on information security management. Computers & Security 31, pp. 221–232.

[16] Finnish Communications Regulatory Authority (2016), Kyberturvallisuuskeskuksen vuosiraportti 2015. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberturvallisuuskeskuksen_vuosiraportti_2015.pdf.

[17] Finnish Communications Regulatory Authority (2017), Tietoturvan vuosi 2016. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf.

[18] Finnish Communications Regulatory Authority (2018), Tietoturvan vuosi 2017. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan-vuosi-2017.pdf.

[19] Finnish Communications Regulatory Authority (2019), Tietoturvan vuosi 2018. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf.

[20] Finnish Communications Regulatory Authority (2018), #kybersää helmikuu 2018. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybersaa_2018_02.pdf.

[21] Jagatic T.N., Johnson N.A., Jakobsson M. & Menczer F. (2007) Social phishing. Communications of the ACM 50, pp. 94–100.

[22] Spitzner L. (2003) Honeypots: Catching the insider threat. In: 19th Annual Computer Security Applications Conference, 2003. Proceedings., IEEE, pp. 170–179.

[23] Douligeris C. & Mitrokotsa A. (2004) Ddos attacks and defense mechanisms: classification and state-of-the-art. Computer Networks 44, pp. 643–666.

[24] European Union Agency for Network and Information Security (2012), Enisa threat landscape report 2012. URL: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape.

[25] European Union Agency for Network and Information Security (2018), Enisa threat landscape report 2018. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[26] Check Point Software Technologies LTD (2018), Cyber attack trends 2018 mid-year report. URL: https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf.

[27] Helsinki Region Chamber of Commerce (2017), Yritysten rikosturvallisuus 2017. URL: https://kauppakamari.fi/wp-content/uploads/2017/10/yritysten-rikosturvallisuus-2017web.pdf.

[28] Furnell S. & Clarke N. (2012) Power to the people? the evolving recognition of human aspects of security. computers & security 31, pp. 983–988.

[29] Mukherjee B., Heberlein L.T. & Levitt K.N. (1994) Network intrusion detection. IEEE network 8, pp. 26–41.

[30] Conrad E., Misenar S. & Feldman J. (2012) CISSP study guide. Newnes.

[31] Koch M. (2015), An introduction to linux-based malware. URL: https://www.sans.org/reading-room/whitepapers/malicious/introduction-linux-based-malware-36097.

[32] Checkpoint, macOS malware encyclopedia. https://macos.checkpoint.com/. Accessed: 2019-06-04.

[33] Boss S.R., Kirsch L.J., Angermeier I., shingler R.A. & Boss R.W. (2009) If someone is watching, I'll do what I'm asked:mandatoriness, control, and informationsecurity. European Journal of Information Systems 2, pp. 151–164.

[34] Nissim N., Yahalom R. & Elovici Y. (2017) Usb-based attacks. Computers & Security 70, pp. 675–688.

[35] Tischer M., Durumeric Z., Foster S., Duan S., Mori A., Bursztein E. & Bailey M. (2016) Users really do plug in usb drives they find. In: 2016 IEEE Symposium on Security and Privacy (SP), IEEE, pp. 306–319.

[36] ISO Central Secretary (2013) Information technology – security techniques – information security management systems – requirements. Standard ISO/IEC 27001:2013, International Organization for Standardization, Geneva, CH.

8. APPENDICES

Appendix 1	Information sheet about the questionnaire
Appendix 2	Information and system security questionnaire
Appendix 3	Summary of answers for the questionnaire

Information and system security survey for small and medium-sized businesses

About this survey

This survey is made by Lauri Haverinen in University of Oulu as a part of Bachelor's Thesis about the implementation of information and system security controls in small and medium-sized businesses. In order to handle collected data ethically and in conformance to regulation, all participants are informed about the use of their data. You will keep a copy of this survey. If anything remains unclear you may contact me with the contact details provided at the end of this page.

What is the purpose of this research?

The purpose of this research is to find out what kind of security controls, mechanisms and policies are being used in small and medium-sized businesses in Finland in order to protect their data and ICT systems against hostile actors. We require general information about participating companies' security policies and implemented security controls and mechanisms. Publicly available data will be also used.

Why have I been invited to take part?

You have been invited to participate because your company fits the participant requirements for this study.

Do I have to participate?

You do not have to participate. If you want more information about this survey before participating you may contact me at any time. You can leave the study anytime without repercussions.

Do I have to reveal company confidential information?

You should not release any company confidential information to us. While the data we gather is usually neither confidential nor personal, it may occur that such may be revealed during this research.

What happens to any personal data I provide?

The definition of personal data is taken from the GDPR Article 4 (https://eur-lex.europa.eu/eli/reg/2016/679/oj):

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

After the information is gathered, it will be anonymized. This means any personal data will be removed and replaced with a random data string. We only collect, process and store anonymized data within the project. The data you have provided will not be forwarded outside this project!

What will happen to the results of this research?

The results of this research will help to understand the current status of information and system security policies and mechanisms of Finnish businesses. A summary of this survey may be published as a part of Bachelor's Thesis in the University of Oulu.

Who should I contact for further information?

If you have any questions or require more information, please contact me

Lauri Haverinen
University of Oulu

Information and system security survey

1. Staff awareness and security policies

1. Does the company have one or more person designated as responsible for information and system security?
□ Yes. □ No.

2. Does the company have information security policies approved by top management?
□ Yes. □ Partly. □ No.

If yes or partly

2.1. Is staff fully aware of company's information security policies?
□ Yes. □ Partly. □ No.

2.2. Has every employee committed to comply with company's information security policies?
□ Yes. □ Partly. □ No.

2.3. Are information security policies being reviewed regularly?
□ Yes. □ Partly. □ No.

3. Does staff receive basic training on how to use company's information systems before using them?
□ Yes. □ No.

4. Does staff receive training in information security in daily working?
□ Yes. □ No.

2. Information security in daily work

5. Does every employee have their own logins for all ICT systems?
□ Yes. □ Partly. □ No.

If yes or partly

5.1. Are employees using only their personal logins when working?
□ Yes. □ Partly. □ No.

6. Is the creation of secure passwords being verified?
□ Yes. □ Partly. □ No.

If yes or partly

6.1. What are the minimum requirements for passwords?
□ Change interval.
□ Minimum length.
□ Must have upper and lower case characters.
□ Must have numbers.
□ Must have special characters.
□ Other, what?

_____

7. Is it possible for employees to work remotely?
□ Yes. □ Partly. □ No.

If yes or partly

7.1. Does the company provide a VPN connection for connecting to company network remotely?
□ Yes. □ No.

8. Is necessary data being backed up regularly?
□ Yes. □ No.

3. System security

9. Does the company use in-house servers?
□ Yes. □ No.

If yes

9.1. What operating system are the servers using?
□ Windows
□ UNIX/Linux.
□ Other, what?
_____

9.2. Is some antivirus software being used on the servers?
□ Yes. □ No.

If yes

9.2.1. What antivirus software is used on the servers?
□ Avast.
□ Bitdefender.
□ ESET.
□ F-Secure.
□ Malwarebytes.
□ McAfee.
□ Kaspersky.
□ Other, what?
_____

10. Does the company use cloud servers?
□ Yes. □ No.

If yes

10.1. What service providers are used?
□ Amazon AWS.
□ Google Cloud.
□ IBM Cloud.
□ Oracle Cloud.
□ Microsoft Azure.
□ Other, what?
_____

11. What operating systems are staff computers using?
□ Chrome OS.
□ Linux.
□ macOS.
□ Windows.
□ Muu, mikä?
_____

12. Is some antivirus software being used on staff computers?
□ Yes. □ No.

If yes

12.1. What antivirus software is used on staff computers?
□ Avast.
□ Bitdefender.
□ ESET.
□ F-Secure.
□ Malwarebytes.
□ McAfee.
□ Symantec Norton.
□ Kaspersky.
□ Windows Defender.
□ Other, what?
_____

13. Is the company network separated from the public internet with a hardware firewall?
□ Yes. □ Partly. □ No.

14. Do company devices use software firewalls?
□ Yes. □ Partly. □ No.

If yes or partly

14.1. What software firewalls are being used?
□ Checkpoint.
□ Cisco.
□ Comodo.
□ Juniper.
□ Other, what?
_____

15. Is it possible to connect to the company network wirelessly?
□ Yes. □ No.

16. What percentage of the services and software that are used in the company are cloud-based?
□ 0-25 %. □ 26-50 %. □ 51-75 %. □ 76-100 %.

17. Are software and operating system updates being automated?
□ Yes. □ Partly. □ No.

If yes or partly

17.1. How long will it take for a software update to be installed on company devices after its release?
□ 24 hours. □ Week. □ Month.
□ More than month.

18. Are software and operating system updates being tested before distribution to company systems?
☐ Yes. ☐ Partly. ☐ No.

19. Is the company network divided into separate segments based on different tasks?
☐ Yes. ☐ No.

If yes

19.1. Are software updates distributed to different network segments simultaneously?
☐ Yes. ☐ No.

4. Monitoring

20. Does the company prohibit the use of unauthorized external storage devices?
☐ Yes. ☐ Partly. ☐ No.

21. Is the use of external storage devices being monitored?
☐ Yes. ☐ Partly. ☐ No.

22. Has the company blocked the use of external storage devices?
☐ Yes. ☐ Partly. ☐ No.

23. Does the company prohibit the use of unauthorized software?
☐ Yes. ☐ Partly. ☐ No.

24. Is the installation of unauthorized software being monitored?
☐ Yes. ☐ Partly. ☐ No.

25. Has the company blocked the installation of unauthorized software?
☐ Yes. ☐ Partly. ☐ No.

26. Is the company network being monitored with some IDS (intrusion detection system)?
☐ Yes. ☐ No.

If yes

26.1. What IDS is being used?
☐ Bro.
☐ Snort.
☐ Suricata.
☐ Other, what?
_____

5. System testing

27. Does the company commission penetration testing on it's networks and information systems?
☐ Yes. ☐ Partly. ☐ No.

If yes or partly

27.1. Does the testing happen regularly?
☐ Yes. ☐ Partly. ☐ No.

27.2. Does the company hire outside contractor to do the testing?
☐ Yes. ☐ Partly. ☐ No.

27.3. Is the same tester being used every time?
☐ Yes. ☐ Partly. ☐ No.

28. Are the company information systems being audited based on some certain criteria?
☐ Yes. ☐ Partly. ☐ No.

29. Has the company been granted some security certificate?
☐ Yes. ☐ No.

If yes

29.1. What security certificate(s) have been granted to the company?
☐ ISO/IEC 27001 certificate.
☐ FINCSC Finnish Cyber Security
Certificate.
☐ Other, what?
_____

Information and system security survey answers

1. Answers for staff awareness and security policies

Question	Yes	Partly	No
1. Does the company have one or more person designated as responsible for information and system security? (n=26)	19 (73%)	-	7 (27%)
2. Does the company have information security policies approved by the top management? (n=26)	15 (58%)	9 (34%)	2 (8%)
2.1. Is the staff fully aware of company's information security policies? (n=24)	15 (63%)	8 (33%)	1 (4%)
2.2. Has every employee committed to comply with company's information security policies? (n=24)	19 (79%)	4 (17%)	1 (4%)
2.3. Are information security policies being reviewed regularly? (n=24)	14 (58%)	6 (25%)	4 (17%)
3. Does staff receive basic training on how to use company's information systems before using them? (n=26)	17 (65%)	-	9 (35%)
4. Does staff receive training in information security in daily working? (n=25)	16 (64%)	-	9 (36%)

2. Answers for information security in daily working

Question	Yes	Partly	No
5. Does every employee have their own logins for all ICT systems? (n=26)	17 (65%)	7 (27%)	2 (8%)
5.1. Are employees using only their personal logins when working? (n=24)	13 (54%)	11 (46%)	0 (0%)
6. Is the creation of secure passwords verified? (n=26)	10 (38%)	7 (27%)	9 (35%)
7. Is it possible for employees to work remotely? (n=26)	24 (92%)	2 (8%)	0 (0%)
7.1. Does the company provide a VPN connection for connecting to company network remotely? (n=26)	17 (65%)	-	9 (35%)
8. Is the necessary data being backed up regularly? (n=26)	25 (96%)	-	1 (4%)

6.1. What requirements do passwords have? (n=17)	n	% of companies
Change interval	7	41.18
Minimum length	12	70.59
Must have upper and lowercase characters	12	70.59
Must have numbers	10	58.82
Must have special characters	9	52.94

3. Answers for system security

Question	Yes	Partly	No
9. Does the company use in-house servers? (n=26)	17 (65%)	-	9 (35%)
9.2. Is some antivirus software being used on the servers? (n=16)	10 (62%)	-	6 (38%)
10. Does the company use cloud servers? (n=24)	20 (83%)	-	4 (17%)
12. Is some antivirus software being used on staff computers? (n=26)	18 (69%)	-	8 (31%)
13. Is the company network separated from the public internet with a hardware firewall? (n=26)	22 (85%)	1 (4%)	3 (11%)
14. Do company devices use software firewalls? (n=25)	15 (60%)	2 (8%)	8 (32%)
15. Is it possible to connect to the company network wirelessly? (n=26)	26 (100%)	-	0 (0%)
17. Are software and operating system updates being automated? (n=26)	10 (38%)	15 (58%)	1 (4%)
18. Are software and operating system updates being tested before distribution to company systems? (n=25)	1 (4%)	17 (68%)	7 (28%)
19. Is the company network divided into separate segments based on different tasks? (n=25)	11 (44%)	-	14 (56%)
19.1. Are software updates distributed to different network segments simultaneously? (n=11)	6 (55%)	-	5 (45%)

9.1. What operating system are the servers using? (n=17)	n	% of companies
UNIX/Linux	10	58.82
Windows	8	47.06
macOS	3	17.65

9.2.1. What antivirus software is used on the servers? (n=10)	n	% of companies
Avast	2	20
Bitdefender	0	0
ESET	1	10
F-Secure	4	40
Malwarebytes	0	0
McAfee	1	10
Kaspersky	0	0
Other	2	20

10.1. What service providers are used? (n=20)	n	% of companies
Amazon AWS	5	25
Google Cloud	6	30
IBM Cloud	0	0
Oracle Cloud	1	5
Microsoft Azure	6	30
Other or confidential	11	55

11. What operating systems are staff computers using? (n=26)	n	% of companies
Chrome OS	3	11.54
Linux	9	34.61
macOS	16	61.54
Windows	20	76.92
Other	2	7.69

12.1. What antivirus software is used on staff computers? (n=16)	n	% of companies
Avast	4	25
Bitdefender	0	0
ESET	1	6.25
F-Secure	7	43.75
Malwarebytes	0	0
McAfee	2	12.5
Symantec Norton	0	0
Kaspersky	0	0
Windows Defender	5	31.25
Other	1	6.25

14.1. What software firewalls are being used? (n=13)	n	% of companies
Check Point	0	0
Cisco	1	7.69
Comodo	0	0
Juniper	2	15.38
Other	10	76.92

16. What percentage of the services and software that are used in the company are cloud-based? (n=26)	n	% of companies
0-25%	4	15.38
26-50%	9	34.62
51-75%	3	11.54
76-100%	10	38.46

17.1. How long will it take for a software update to be installed on company devices after it's release? (n=24)	n	% of companies
24 hours	3	12.5
Week	19	79.16
Month	1	4.17
More than a month	1	4.17

4. Answers for monitoring

Question	Yes	Partly	No
20. Does the company prohibit the use of unauthorised external storage devices? (n=26)	10 (38%)	3 (12%)	13 (50%)
21. Is the use of external storage devices being monitored? (n=25)	3 (12%)	8 (32%)	14 (56%)
22. Has the company blocked the use of external storage devices? (n=26)	0 (0%)	5 (19%)	21 (81%)
23. Does the company prohibit the use of unauthorised software? (n=26)	12 (46%)	6 (23%)	8 (31%)
24. Is the installation of unauthorised software being monitored? (n=25)	5 (20%)	7 (28%)	13 (52%)
25. Has the company blocked the installation of unauthorised software? (n=26)	6 (23%)	5 (19%)	15 (58%)
26. Is the company network being monitored with some IDS? (n=24)	3 (12%)	-	21 (88%)

26.1. What IDS is being used? (n=1)	n	% of companies
Bro	0	0
Snort	0	0
Suricata	0	0
Other	1	100.00

5. Answers for system testing

Question	Yes	Partly	No
27. Does the company commission penetration testing on it's networks and information systems? (n=25)	5 (20%)	9 (36%)	11 (44%)
27.1. Does the testing happen regularly? (n=14)	5 (36%)	7 (50%)	2 (14%)
27.2. Does the company hire outside contractor to do the testing? (n=14)	10 (72%)	2 (14%)	2 (14%)
27.3. Is the same tester being used every time? (n=14)	3 (21%)	4 (29%)	7 (50%)
28. Are the company information systems being audited based on some certain criteria? (n=25)	5 (20%)	7 (28%)	13 (52%)
29. Has the company been granted some security certificate? (n=26)	1 (4%)	-	25 (96%)

29.1. What security certificate(s) have been granted to the company? (n=1)	n	% of companies
ISO/IEC 27001 certificate	0	0
FINCSC Finnish Cyber ecurity Certificate	0	0
Other	1	100.00