Making an information security plan

Henrik Miettinen 1702447

2021 Laurea

Laurea University of Applied Sciences

Making an information security plan

Henrik Miettinen
Security Management
Bachelor's Thesis
May 2021

Laurea University of Applied Sciences **Abstract**

Security Management

Degree in Security Management

Henrik Miettinen

Making an information security plan

Year 2021 Number of pages 29

The development objective of this thesis was to create a working, efficient and solid information security plan for a small-sized company. This thesis used qualitative and development methods, such as qualitative interview, literature reviewing as well as researching of the company premises and practices, as well as understanding and awareness of security culture to establish and create the information security plan. The information security plan will consist of a risk management table, as well as an information security-related auditing template, that may and should be used regularly even after the completion of this project, to ensure that the information security of the case company will remain stable and secure.

The overall outcome of the thesis was to strengthen the overall understanding of the importance of the information security within the company, as well as how to avoid jeopardizing it. The information security plan offers cost efficient and simple solutions to strengthen the overall risk assessment and information security awareness of employees within the company, as well as the employer's, from simple changes in attitude, behavior and habits to further raise awareness and to mitigate the likelihood of targeted attacks succeeding against the company and its employees, such as phishing attempts or malware attacks.

Keywords: Information security, Risk management, Auditing, security planning, corporate security

Contents

1 Introduction

In this development project, an information security plan has been developed for a small-sized company. Information security, and data protection in general, are ever-evolving fields of corporate security. With the constantly improving levels of technology. Especially in IT field, it is imperative for the companies to keep up with it, or they might fall behind, and become easy prey for cybercriminals, like hackers, malware developers and other such individuals. This of course, is not all that there is to information security.

Physical information must also be safeguarded, although these methods need not be updated as often, compared to the IT field, although chances to improve or update either should not be disregarded. The information security has many facets, and the companies and corporations must tackle nearly all of them in some shape or form. Some of the companies need to tackle this aspect more than others, depending on the size of the company, location, how much the company uses computers and digital information, as well as how they recruit and employ people. While the case company in this project is not the most advanced in IT field, it still has some elements to it, and thus, it must be taken to consideration as well, albeit not as much.

1.1 Case company

The case company was founded on a year 1985, and as its services, the company provides parts designing, assembly as well as mechanization of plastic parts. Their current business premises were constructed in year 2002, and the newest expansion was made in 2017. Their yearly turnover is around 900 000 euros, and the company has 10 employees. The case company has also now branched onto 3D printing.

The case company resides in the countryside of Mietoinen, within the municipality of Southern Finland. The premises of the company and its perimeters are surrounded by acres of untouched fields and forest, as well as some detached houses residing nearby, scattered about. The nearest town is approximately couple kilometers away, with the town lacking its own police department. Nearest police department is in Masku, which is over 20 kilometers apart from the premise and the facilities of the case company. There is very little traffic near the perimeters of the company due to how far out from the nearest town they are, but it comes with its own share of problems. Lack of lighting at the night, as well as relatively long, estimated time of arrival in cases of emergency, like burglary or fire hazards, gives the company a fair share of problems that they have to tackle with. Security guards and police might take too long to arrive on the scene if an intruder, such as burglar breaking into the buildings of the company, and with very few potential witnesses seeing what occurred, it

could definitely make the case company a prime target for vandals, thieves and burglars. This risk has been minimized with some alarms, such as motion detectors and glass break detectors, although the slow response time will still make this a sizable risk.

The company in question deals with light and heavy, computerized and automated machinery. The case company also deals with some IT-work, and they have a lot of documents that can be considered sensitive and essential, as they contain customer, employee and affiliate information and data. According to their CEO, the case company in question has not made any proper information security plan before this, having only barebones understanding of information security and how to protect data and information.

1.2 Development tasks

As such, coming up with a comprehensive and extensive information security plan would be a fundamental step in development in safeguarding the information and data that the company accumulates and deals with. In this project, I will be relying on materials and references that are already published and have been deemed as working ideas when it comes to information security to make a proper information security plan for the case company, as well as refer to any literature that feels relevant and proper to the matter at hand.

The end goal of my development project is to develop and reinforce the information security within the case company. Both of these are created based on what has been discovered. The objectives are as follows:

- To create a simple, but effective and efficient information security plan that consists or risk evaluation and treatment, along with how to prevent them, as well as what to do should the risk occur regardless.
- As an additional annex to information security plan, to create an information security audit template, which can be used to inspect the current status of the company regarding their information security, and spot any anomalies or faults. This would make it easier to fix these issues, rather than allowing them to fester and become worse.

1.3 Scopes and Limitations

The fundamental focus point of this project is to develop the information security of the case company, as well as make actual, physical and concrete policies and guidelines for them to follow and maintain, to avoid risks and dangers regarding information security, like data leaks and breaches, as well as loss of reputation or customers and their trust, should these risks happen. To that end, there will be a risk evaluation table, which can be used for easy referral what to do in information security situations, and how to treat and prevent such incidents

from happening. On top of that, there will also be a security information auditing template, which can, and should be used to regularly inspect and maintain the information security focal points, to ensure everything works as should be, and that there are no glaring gaps nor weaknesses for criminals to exploit, or dangerous accidents regarding information and data to occur.

As the company is relatively far out in the countryside in Mietoinen, and the company has a limited amount of IT work, despite their computerized machinery, there are some information security aspects that are not fully applicable to their situation. As such, there are many situations which has to be adapted to, and go along with their preferences, circumstances and limitations.

One such limitation was the difficulties to hand me any of their facilities blueprints or anything that gave me a good overview or visual representation where everything is. As such, some compromises had to be made, and conclusions had to be drawn what had been seen during premise inspection. There were a lot of questions the company couldn't really answer to me. Not because of confidentiality, but simply because the company did not know answers to questions, or recall properly.

2 Literature

To make an information security plan, understanding the basics is important, so that there are no outright flaws, nor breachable or exploitable gaps in it. To achieve this, the work will be referring and getting insight from several literature works that have been chosen at the task at hand, due to their relevancy. On top of that, though, there will also be some comparison and reflections related to the situations with the case company, and how they have handled these situations, or how these literature reviews can be used and implemented in order to make even better information security plan for the case company.

2.1 The basics of information security plan

To start with, there needs to be a cohesive and comprehensive understanding of information security plan and what information security is. According to Fruhlinger (2020), "information security is a set of practices intended to keep data secure from unauthorized access or alterations". From this definition of information security can be moved onto the definition of information security plan. According to Stealth Labs (2020), information security plan is a set of your information security policies, regulations, as well as standards of your company. Information security plan outlines the organization's sensitive information and the steps to be taken to secure that said information.

According to EzeCastle Integrations (2020) article regarding the creation of information security plan, the information security plan is the documentation of company plans and systems that are put in place to safeguard personal information, as well as any sensitive data the company may hold. The information security plan would then mitigate threats to the company, and protect its integrity, confidentiality as well as the availability of information.

When comparing to these two different sources, and what their understanding of information security plan exactly is, it does make sense. On top of that, according to Stealth Labs (2020) take on how to create a robust information security plan, they referred to this particular pattern, as seen in picture below.

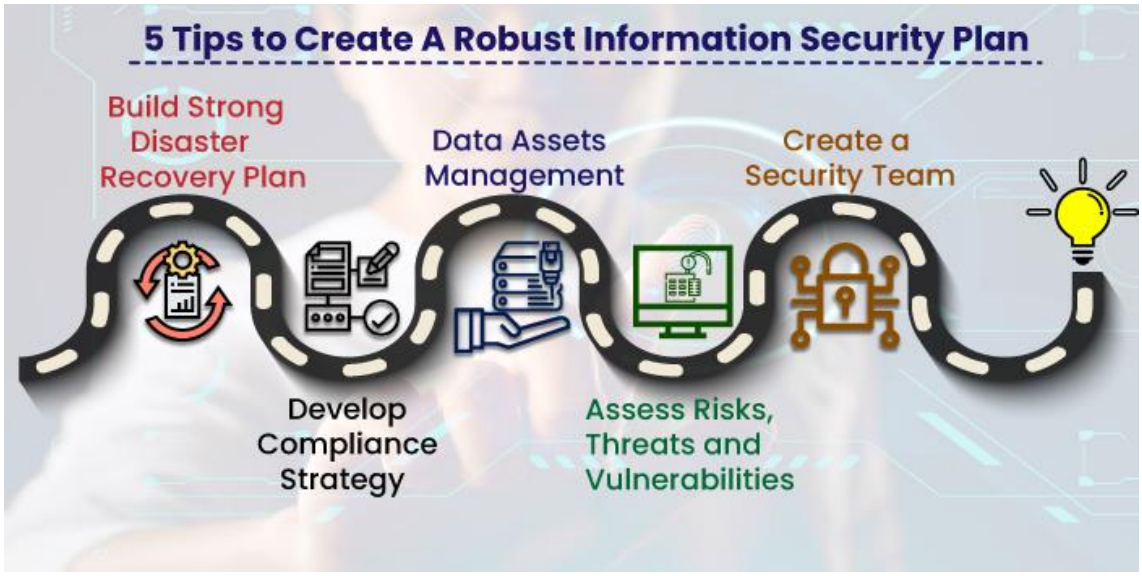

Figure 1: 5 Tips to Create a Robus Information Security Plan. Stealth Labs (2020)

While the case company do not need as extensive and thorough information security plan, it does still offer valuable insight what should be done. Having a recovery plan for the company in case of an information security disaster happening is paramount. It would reduce the time that the company operations and procedures need to recover back to full efficiency. And developing a good compliance strategy aids in that as well, not to mention having a proper management in handling data assets will reduce the risk of said disaster happening. Assessing risks and threats, as well as other vulnerabilities is important as well. Due to size of the company, however, assigning one or two members as data security team is sufficient in this case, rather than a whole team. Preferably at least one information security specialist or representative to handle and safeguard the company data.

There is also the matter of necessity for security management. Tipton and Krause (2006, 224) explain that “levels of risk are continuously changing, as every enterprise is a dynamic entity with controls being added and deleted, ports in the firewalls being opened, services and

systems being added, architectures being redeveloped, and acquired companies being added to the network. Additionally, vulnerabilities and threats, introduced external to the organization, will affect the level of risk of an organization and must be captured and measured". This gives further insight on the many facets of the security management, and thus, to extent, the need for information security management. The risks change and evolve as more features and systems are added to the company. As the field of expertise, services and variety of tools grow within the company, so do the many risks that entail those said areas. And as such, it is essential to maintain the information security management by updating it on a regular basis. As things currently stand, the case company will not likely change the core practices of their business processes, but this should be monitored and surveyed regardless of that.

This is further emphasized when using computers and collaborating with business partners. As Von Solms (1999, 51) observes,"as organizations link their computer networks to the Internet or to the IT networks of business partners, central control over their IT systems and users, thus information security, can be lost to a large extent". This would definitely apply to case company to an extent. By giving IT network access for example, transportation company that the case company might hire to transport goods, could very well endanger much of the information security of the case company, if it is not secured and monitored well. All the customer and employee information could very well be at risk.

Von Solms (1999, 51) further observes that "to ensure a secure IT environment, under these circumstances, it is required to have a secure IT community. A set of rules and regulations for all users will have to be introduced and some authority will have to see that all parties adhere to this". The case company would have to make sure that there are certain policies in place for anyone using and accessing the IT environment, and that someone would have to make sure those rules are being followed. An information security representative in the case company would be sufficient addition, to ensure that any usage and access to the IT network of the case company would be properly monitored and enforced. This would decrease the risks regarding misuse of the data, and the consequences that would follow right after.

2.2 The hazards in making a security plan

According to Woods (2019), over 90% of all cyber security breaches come as a result of human error, and "human error is the action of something that was not intended." Taking in account these human errors, such as insufficient training or orientation, negligence, laziness and indifference are some of the bigger mistakes in information security plan, and data protection in general. The plan is already going to fail if proper precautions are not taken to ensure that the plan and its policies are not enforced in any shape or form. Some employees might not take the new guidelines seriously, or they find it too much of a tedium or hassle to go

through, and thus, they might cut corners or outright just ignore the measures taken. In this way, they would knowingly or unwittingly set the company in danger. For example, there could be many mistakes when it comes to information security, which might cause more harm than good.

According to Von Solms, B. and Von Solms, R. (2004, 372), there are the 10 deadly sins of information security. The first one is not realizing that information security is a corporate governance responsibility.

The second sin is not realizing that information security is not a technical issue, but a business issue. The monetary loss and most importantly, the loss of the customers' and stakeholders trust in case of a major information security risk can be quite substantial setback to the company, not to mention in some cases, the risk can cripple and slow down the business practices and processes of the company as well.

The third sin is not realizing that the information security governance is a multi-dimensional discipline, mostly meaning that it is a complex matter, and there is not a single clear solution to all of its problems.

The fourth sin is not realizing that the information security plan must be based on identified risks. I agree with this one, too, since if the plan is based on assumed risks, without proper identification of those said risks, it would amount to nothing. Evaluating and identifying risks before basing your information security plan on them is important.

The fifth deadly sin is not realizing the important role of international best practices for information security management. It is essential to learn from the others all around the world who have done effective practices regarding information security. As such, it is important to seek counsel and advice from already well-established authors through their published literature, as well as from information security related organizations that have years, maybe even decades of knowledge and experience regarding this particular field.

The sixth sin is not realizing that a corporate information security policy is absolutely essential to the company. I agree that without proper, written policies, employees are not going to remember, much less follow said information security measures. Making them into actual corporate policies is important, as the literature suggests.

Seventh sin is not realizing that information security compliance enforcement and monitoring is absolutely essential. I would have to agree with that as well. Ensuring that everyone follows the policies set in place is important step as well. The employees who fail to follow the policies, whether wittingly and unwittingly endanger the information security within the

company, and thus, makes the case company more liable to the many risks that come with information security, such as not disposing the documents that are supposed to be disposed.

Eighth sin is not realizing that a proper information security governance structure, or in other words, organization, is absolutely essential as well. Leaving the information security governance structure into state of disarray and ambiguity can cause serious issues, both in implementing the information security policies, but also in order to enforce them. Granted, the case company is a small-sized company, so this sin does not apply quite as directly to them, but it is something to keep in mind as the organization grows, and need for more information security governance arises.

Ninth sin is not realizing the core importance of information security awareness amongst the users. Awareness is important, as it reduces chances of human error when it comes to information security, and proper vigilance and understanding of information security and its risks can prevent many dangerous situations that could potentially lead to loss in revenue within the company. It is very important that not just one or two employees, but all of them have at least basic understanding and awareness when it comes to information security.

Tenth and final sin is not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities. Leaving the information security managers with minimal tools or none at all can lead to information security plans and policies that are below the standard in quality, efficiency and in scope of application.

Reflecting on these aforementioned ten deadly sins, it does make sense that the greatest struggles and difficulties that come up with information security planning, is the fact that lot of its contents are not fully realized, or it is not taken seriously enough by the company or by its employees, or the one who writes the information security plan for the company. Thus, it is important to take note of these ten sins, and to make sure that they will not be repeated.

As mentioned before, it is a consistent trend that the information security is not taken too seriously and with proper regard, up until the point that something grievous regarding information security happens. According to Todd Fitzgerald (2011, 11), that more often than not, the need for information security just appears one day, usually as a result of an incident, such as public disclosure of information, or that new law or regulation comes in, and the company must realign itself to meet its requirements or demands.

Fitzgerald (2011, 11) also mentioned that what often follows is that someone will be assigned to resolve the said incident, and come up with what needs to be done in regards to the information security, and that someone often is associated with the IT side of things, due to the common conception that information security is seen similar to information technology.

Fitzgerald (2011,12) also mentions that more often than not, when requesting for more resources regarding the solution of the issue, the proposition is met with resistance. This is something that definitely must be taken to account for as well, and make the resource requestions and demands realistic, as well as be able to come up with a convincing reasoning for the top management to allow these solutions and information security related practices within the guidelines and protocols of the company.

CEO and the company want to naturally make more money and profit, so it stands to reason as to why they are often initially opposed in using resources on something that does not bring the company immediate wealth and profit. Thus, it is imperative to convince them as to why the solution at hand will save them a lot of money on the long run, whether avoiding incidents that are fatal or grievous to the business continuity and the safety of the employees and customers of the company.

According to Ben Griffin (2020), their 10 practical tips were as follows. I will point out only the most relevant ones, as there are many good tips, but not all of them directly apply or fit to the Company X's case.

The first one according to Ben Griffin (2020) is to write up a strategy. Rather than just vague ideas in the air in regards to the information security policies and procedures, there should be a more formal and concrete information security strategy, regardless of the size of the business. It should be as detailed and extensive as possible. And it is certainly something that has to be agreed upon. This reduces many of the rash and impulsive reactions that might make things worse than they already are, as the article points out.

The second tip according to Ben Griffin (2020) is the protection against malware. Having a proper firewall, as well as anti-virus and anti-spam protections in place is essential and imperative. Luckily, there are only two actual PCs in the company premises, so this particular aspect is easy, and relatively cheap to accomplish and maintain. As an annex, the tip number 6 is also directly linked to this one. Setting up automatic software updating to these said computers, as many of the cybercriminals tend to exploit more likely systems that are outdated and not up to par with current updates.

The tip number eight According to Ben Griffin (2020) is to dispose data properly. Leaving the information unattended and undisposed creates major information security risks. Shredding documents that are supposed to be disposed of is essential, as is deleting and wiping out any unneeded data packages from flash drives, hard drives and from folders. Just leaving the data to sit on computers or on top of the cabinets within the company premises is very risky, and it makes a very enticing target for criminals to exploit. And worst of all, the forgotten, undisposed data is something that the company might not even realize is missing for a good while, which makes the situation all the more worse.

Tips number seven and ten, according to Ben Griffin (2020) are as follows. Conducting background checks on new employees, as well as educating the employees regarding security policies. While the case company is not likely to be a target for industrial espionage or organized crime, it should still be essential to do a brief checkup on the new employees, mostly regarding their past, or whether or not they have criminal record, and just what kind of person the new employee is. The article also points out to be mindful of changes in the existing employee's behavior and personality, which could be an indicator of large number of issues, not just information security issues. On top of this, educating these employees immediately on what the information security policies are is also essential. They immediately know what they can or cannot talk about, which makes things easier for all the parties involved.

2.3 Risk identification and evaluation

Risk assessment and management is also an important part of security plan, and in this case, making an information security risk management for the information security plan. As stated in previous segment when it came to the fourth Deadly Sin, which was that information security plan must be based on identified risks, not on assumed or imagined risks. As for how to identify risks, according to ClearRisk's (2021) article regarding 8 Ways to Identify Risks in Your Organization, "is to break down the bigger picture and begin with a high-level analysis. It is important to realize what are the most obvious things that go wrong in the company. Asking the important questions is also helpful. Some examples the article gave were whether all employees are properly trained, or whether or not the processes are fully safe". If those questions cannot be answered in satisfied manner, then according to the article, it represents a risk that needs to be better managed.

The article also encourages the risk identifier to be pessimistic, imagining what is the worst that could happen to the organization. It is essential to avoid overconfidence and think that something will not or cannot happen. While pessimism is not ideal way to run a company, it is certainly helpful in identifying risks.

After the risks have been identified, they should be evaluated. According to Silverbulletrisk's (2018) blog How to Evaluate Risks in Your Company, risk evaluation is a process used to compare the estimated risk the given risk criteria to determine the significance of the risk.

2.4 Information Security Auditing

On top of risk assessment and management, a proper information security audit would complement the information security plan sufficiently. To summarize what data and information auditing is, according to Martin Doyle's (2017) article, "data audit refers to the auditing of data to assess its quality or utility for specific purpose". As to why it is important,

according to the same article, it reduces errors, especially the human errors, with the average company losing 12% of its revenue as a direct result. While it is likely not as high a revenue loss on the current case company, it is still something to consider.

It is also a developmental suggestion from the results of this thesis that there should be an internal auditor who conducts the security audits to the company once the information security plan, and the audit template are in place. According to DNSstuff (2020) article regarding What Is an IT Security Audit, for smaller companies, the role of an internal auditor can be filled by a senior-level IT manager. They would be responsible for building audit reports for CEO, for example. In regards to the case company, one could imagine someone a bit less experienced could work as well just fine.

As for when it comes to making the information security effective and functional. According to Atymtayeva, Bortsova, Inoue and Kozhakhmet (2012, 238), the information security audit is often conducted in these steps. First step is scoping and pre-audit survey, to determine the focal areas, and to establish auditing objectives. The second one is planning and preparing, to create a working checklist and plan. Third step is fieldwork, to gather evidence via interviewing, reviewing documents and data, as well as observe the processes in action. Fourth step is to analyze, to sort out and to review all of the gathered evidence, and how it all relates to the objectives. And fifth step is reporting, which consists of going through all the previous steps, and finally compose a report.

Further according to Atymtaeva, Bortsova, Inoue and Kozhakhmet (2012, 238), all of these stages are typically accompanied with massive amounts of information, and it needs to be organized and analyzed. In the case of this company, however, this was not as severe case, but the need to organize, compose and analyze the data is still relevant and very much necessary.

There are also other things that must be takin into consideration when making an audit plan. According to Resolver (2021), there are inherent internal risks that need to be accounted for. One such example that the article gives is the changes in operating systems as well as in policies, as well as development and launch of new products and services. Company X has quite recently branched out into the 3D printing as its new service. While it is not something that changes the grand scheme of information security plan that much, it also needs to be taken into consideration.

Computer usage is one important focal point of the information security audit as well, since much of the information within the case company is stored electronically. According to Suduc, Bîzoi and Filip (2010, 45), “the aim of security in the user access control area is to optimize the productive computer time, mitigate de risk of error and fraud, eliminate unauthorized access and secure confidentiality of information”. As the situation currently is

in the case company, the lack of security and awareness in their user access control area is lacking. The situation creates opportunistic scenarios for anyone visiting or intruding on the premises of the company. Investing some more to the secure user access control area would mitigate the risk of the computers being misused and abused, or that the data stored within them would be stolen or leaked.

2.5 Finnish Legislation

On top of everything else, there is one last thing that must be truly taken into consideration as well so that the information security plan is as legitimate and reliable as possible. And that is so that it is in accordance and in line with Finnish legislations, regulations and laws, to make sure that the information security plan, as well as the company practices regarding information security do not break laws or regulations of any kind. Even if the information security plan is protecting the data and flow of information flawlessly within the company, it is detrimental and defeats the whole purpose if it breaks the legislations surrounding data protection.

While there are not many Acts that touches too heavily on the subject of the information security planning, there are still some, and they are quite important in order to understand the legal boundaries and limits what can be done in order to bolster the safeguarding of data, documents and information within the company. Not only that, but discover new tools or methods as which to use to reinforce the information security of the company in general.

2.5.1 Personal Data Act

One such relevant Act is the Personal Data Act 523/1999. According to the section 1, which is the Objectives, the objectives of the Act in question are to implement, in the processing of personal data, the protection of private life, and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice. This fits into the task at hand quite adeptly, given how the data that the company handles is personal data of its employees and customers, and as such, the Act is strictly in line with the purpose of the information security plan. In the next section, which is the scope of application, the Act goes into further detail as to what this applies to. First segment, according to the Personal Data Act, Section 2, Scope of Application, the provisions of this Act apply to the processing of personal data, unless otherwise provided elsewhere in the law. The act does make a distinction on the third segment of this Section 2 that the Act does not apply to the processing of personal data by a private person for purely personal purposes. But since the information security plan in question does not deal with just one private individual, it is largely not relevant to the case at hand.

The Personal Data Act handles in section 3 all the definitions of the terms, but those can be put aside for now, and move on to the Chapter 2 which is the General Rules on the Processing of Personal Data. According the Section 5, Duty of Care, the controller shall process the personal data lawfully and carefully in compliance with good processing practices. And anyone else acting on the behalf of the said controller is subject to this same duty of care. In essence, anyone that the controller of the personal data assigns to do their job for them holds the same responsibilities. The aforementioned good processing practices are then explained a bit further on section 6, which defines the purpose of the processing. In short, it must be appropriate and justified to process the said data.

The real important part comes in the Chapter 7, the Data Security and storage of personal data. According to Section 32, Data Security, the controller needs to carry out the technical and organizational measures for security personal data against unauthorized access, as well as against accidental or unlawful destruction, manipulation, disclosure and transfer of such unlawful processes. The very things that the information security plan is trying to safeguard the company from. The Section 33 handles the secrecy obligation, regarding the revelation of confidential data.

2.5.2 Act on the Protection of Privacy in Electronic Communications

Another relevant Act on the matter is the Act on the Protection of Privacy in Electronic Communications 516/2004. As the company in question communicates a lot through the electronic means, such as phones and emails, it stands to reason that this particular Act is well-justified to be quite relevant to the case at hand. According to the Act's Chapter 1 Section 1, Objectives, the goal of the act is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications. The objectives of this Act line up well with the purpose and the objective of the information security plan.

The Chapter 2 Section 4 handles the confidentiality of messages, identification and location data. In the segment one, the Act states that all messages, identification data as well as location data are confidential unless this Act or another Act provides otherwise. This part in particular makes it clear that even when in order to bolster the information security of the company, the employees' messages and data are confidential and shouldn't be exposed or disclosed in any shape or form.

According to the Chapter 11 Section 41, which is the Coercive measures, states that anyone that violates this Act or provisions issued under it, despite being requested to do so, and failure to rectify the actions within reasonable time period, the Finnish Communications Regulatory Authority may order the rectification of errors or neglections. The said organization or the Data Protection Ombudsman may impose a fine or a threat of having the

Act done at the defaulter's expense as sanctions to support the obligation. In regards to the severe violations, it may end up in the termination of violator's business. Partially or fully. While there is little doubt that situations will ever escalate to those degrees in the case company, it is still regardless important to pay heed to such possibilities, so as to not violate the Act or any provisions that are under of the said Act.

2.5.3 Act on International Information Security Obligations

Third relevant Act is the Act on International Information Security Obligations 588/2004. As the name suggests, it deals heavily in information security, especially its obligations. National Security Authority, or NSA, for example, works in accordance with the Act in question. The Act is only in Finnish language, for those who wish to read it. According to the Section 1, the scope of application, this Act provides measures for public authorities in order to implement internal information security obligations.

In the Section 10, Safety requirements related to the premises, protected information material shall be stored in premises where the protection of documents and other such materials and the information contained within can be ensured. In other words, to make sure that the documents and other sources of sensitive information are kept in locked and secured places, and that the access to these said documents and premises is restricted quite heavily.

3 Methods

The focus will mainly be on the methods and the methodology used in this particular thesis. Since this is a development project, the will be focus on the qualitative interview over the quantitative interview. Because the company is quite small to begin with, quantitative interview wouldn't work as well. Based on the results of these methods, a risk management table, as well as information security related auditing table will be created.

3.1 Interview with the CEO

To start with, I needed to know more about the state of the company, and its current understanding and measures regarding information security in general. After conversing with the CEO of the case company via emails, a meeting was arranged, to which had been prepared for by coming up with most essential questions that were relevant to information security. During this meeting, the CEO of the case company was the sole interviewee. Unfortunately, there was no possibility to interview anyone else due to the busy and hectic schedule the company had at the time. The pandemic also affected to this in some extent. The full transcription can be found in at the end of the work.

One of these interview questions was that does the case company have someone in charge of information security, or security in general. To which the answer was that the case company has never had anyone representing the security in any actual form.

The next question conducted to the CEO was regarding their management of information and data assets like the physical data, such as documents. The interview question was whether or not the company stores physical data in locked or restricted room, and the answer was that they do have the data and the documents stored in specific room. The CEO and their secretary have access to the said room.

The follow-up question was regarding locked doors and rooms. According to the CEO, the last one leaving usually locks the doors of the company buildings. Otherwise, they keep most doors unlocked through the whole day, which could be confirmed after inspecting the premises. It is a very risky habit. Forgetting to lock the doors, for example, is a rather realistic risk in this scenario. The premises would be unlocked all night, and anyone who happens by might manage to get in, and do some major damage to the company assets or get access to their data. Investing into automated locking system is another recommendation on the matter.

The next question was whether or not the company has conducted any education or instructions when it comes to information security, such as confidentiality and managing sensitive information in general. The answer that was given indicated that the company has not conducted anything of the sort.

It was also asked that whether or not the devices and computers within the case company have an adequate protection against computer viruses. The CEO did say that they had anti-virus program installed into the computers, but when asked with a follow-up question regarding the frequent updating of the said programs, the CEO admitted that they usually postpone the update notifications and pay very little attention to keep the said software up to date.

3.2 Premise Inspection and Studying

After the interview, it was necessary to also thoroughly inspect the place, to identify any immediate threats and risks regarding the information security. The unlocked doors were certainly an issue that could perceived to be a considerable risk. Almost anyone could get in and get nearly anywhere in the building, like the secretary's and CEO's offices, even when they were not present in those rooms.

After carefully documenting up what was perceived to be the largest and most considerable risks, as well as other noteworthy circumstances, these would later be used as a basis to

make the information security plan, tailored to their needs. There would also be a necessity to make a comprehensive risk assessment and risk evaluation table. It would contain the risks relevant to the company, the causes to the said risks and their consequences, as well as how to try and prevent the risks and how to treat and deal with said risks if they end up occurring regardless.

4 Results

In this chapter, the results of the methods used in this thesis have resulted in a risk management table, as well as information security audit table. All the literature groundwork that had been done beforehand. With all the basics covered, with greater understanding of Finnish Legislation, risk management and auditing, particularly regarding information security.

There was an intention of having an actual information security workshop in the premises of the company, but due to the worsening situation of COVID-19 pandemic, we came to conclusion that it was best to postpone it for now, and instead focus on the information security plan itself.

The result of the work is the information security risk management table, as well as information security auditing table, that the company, and the future information security representative should use in order to ensure and maintain the safety of the company data.

4.1 Information Security Risk Management

As previously stated in the goals of the thesis, there is definitely a necessity to make a comprehensive risk assessment and risk evaluation table to the information security plan. It would give the company a good insight and notion what are the biggest risks and dangers for them to watch out for when continuing their business practices. The risk table that has been made contains the following columns that has been perceived to be the most important ones.

The first column contains the name of the risks relevant to the company. Short and simplistic, but descriptive enough to make sure that the risk is not too vague or hard to grasp as a concept. This column explains what the risk is.

The second column would be the causes and reasons to the said risks and their consequences. Knowing how they happen most often and most likely is already considerable progress, and a step in improving the company practices and overall vigilance.

The third column contains the consequences of the said risk if it happens. These consequences may appear cynical, but as it was mentioned in the literature chapter, it is better to be overly cynical than overly optimistic when it comes to risk management. And it gives the company a good incentive to do everything in their power to prevent such scenarios from happening.

The fourth column is prevention. It offers advice as to how to prevent and mitigate the chances of the said risk, and subsequently, the consequences of the said risk from happening. That said, the risks are rarely completely removed, and those that can be are very specific and situational. Risks can be mitigated, and their chances of happening decreased, but seldom do they ever have zero percent chance of happening.

The fifth column is the treatments. Should the risk happen regardless, the company would then roughly know how to act during an incident, instead of being completely paralyzed, or doing impulsive, unwise and rash decisions under pressure and distress, which could potentially lead into even worse consequences.

Below is an example of the said risk assessment and risk evaluation table, with six biggest risks that I found relevant to the circumstances of the case company. They will be explained bit by bit as to why these six particular risks to represent the risk management table in the case company, and how are they related to the case company specifically, and what causes these said risks, how the likelihood of these risks could be mitigated from happening in the first place, as well as how to act during these said incidents, should they occur regardless of the prevention measures.

Information Security risk	**Causes to risk**	**Consequences of the risk**	**Prevention**	**Treatments**
Classified documents end up being missing/stolen	Carelessness, unrestricted access to the documents	Data leaks, flow of information is jammed, loss of reputation.	Documents are stored as well as carried only those entrusted. Storing and locking them up in secured containers and rooms.	In the case the documents aren't found or recovered, call the police, as well as informing those that are relevant to the said, missing data.

Confidentiality obligation broken by employee	Carelessness, breaking obligation with malignant intentions	Information leakage, loss of reputation, rival organizations get edge in business.	Edification on importance of confidentiality, choosing better places to hold confidential conversations.	Trying to mitigate reputation damage, like transparency, apology, refunds and gifts.
Organization's computer(s) get infected with malware, viruses, ransomware	Careless behavior on computer, opening random links in email	Organization's data gets leaked in the internet or in the hands of creators of virus. Extortions.	Stricter internet use policy inside the organization. Cybercrime education.	Not much can be done in regards at this point. Paying up in extortion is probably only way to hopefully get data back.
Communications are down / Flow of information is broken	Outages, blackouts, device errors, internet problems	Business activities slow down or halt entirely. The risk of miscommunication or errors grows exponentially.	Stable network, making backup plans, like alternative ways of communication (Phone calls, fax, physical meeting)	Using the aforementioned, alternative ways of communication, as well as making the calls and efforts to re-establish or repair the main way of communication.
Someone has accessed company IT network / computer and tampered with the information stored within.	Not logging off from the computer when it is not in use, poor password policy.	Potential data leakage, ransoming of the information, loss of reputation, safety of customers and employees jeopardized.	Logging off from the computer when not in use. Making sure that the passwords are secured and concealed.	Calling the authorities, making sure that the access to the IT network and the computers are restricted to prevent further damage from spreading.

The abuse of privilege, such as administration rights or access to the information.	Personal gains, disgruntled employee, greed, careless background checks.	The misused data causing damage to the company reputation, business processes halting, employees and customers endangered.	Making sure that only the trustworthy employees or contractors have access to the information or rights, as well as making background checks, such as seeing whether or not the person has criminal background.	Calling the authorities, making sure that the person in question won't have access to the said information and privileges again. Transparency with those affected by the misuse and abuse of the information.

Since the case company works a lot with classified documents, and they do not have any strict or coherent policies in place where and how to store them, this risk felt rather notable as of right now And on top of that, the company premises are for the most part all unlocked and unrestricted, meaning that anyone with even slightly malicious or ill intents could walk in and do as they please. With the loud machinery thundering all around company premises, it is not unthinkable possibility of someone managing to slip in, take something, with none being the wiser.

Then, the confidentiality risk. The employees might accidentally slip out something confidential information to someone that is not supposed to know that. From what had been gathered from the interview with CEO, it came to the attention that the company does not either really tell the employees what they should or should not say. Granted, the workers do not often come in direct contact with the customers. Only CEO and the secretary, most likely, but that does not prevent them from accidentally overhearing something, and not considering it could be potentially sensitive information. And some consideration must be taken as well when it comes to potentially disgruntled employees who might wish to cause harm to the company out of spite, or put them into unfavorable light.

And since the company also works moderate amount with computers, a risk of malware, virus or other malevolent programs is more than feasible risk. Given how passive the attitude

towards the dangers of cybercrime and malware was, it stands to reason that the risk for a computer-related information security issues is relatively substantial.

And as the fourth risk, there is the matter of communications being brought down, either by a natural occurrence like blizzards, storms or blackouts in general. Given the location of the case company, it is feasible to consider there to be blackouts during harsh seasons and storms. The fixing of lights, electricity, internet connection and phonelines might take a while, considering the premise is located in relatively secluded place.

Fifth risk covers the more direct issues and dangers with the computer usage. Based on the earlier impressions of the computer policy the company has, it is clear that those who use the said devices are used to not logging off when leaving the devices unattended. As such, anyone who manages to sneak in to one of the offices unnoticed, can access the computer with full administration rights. All the information that is stored in the computer would be exposed. This could lead to information theft or misuse of said information and data.

Sixth risk is the danger of an employee or contractor abusing their rights and privileges to access data or use their administrative rights to do harm to the case company, whether out of personal grudges against the company, or to use these rights to personal gains. New employees and contract workers should be monitored properly, to make sure that the risk wouldn't happen. If it does happen regardless, swift actions need to be taken, such as calling the police, making sure that the said person does not have access to the features and rights again. To mitigate the chance of this happening, it is also crucial to do more thorough background checks on the new employees, and make sure that the company collaborates with contract workers that are confirmed to be trustworthy and have immaculate background.

4.2 Information Security Auditing

While the risk management table is a good addition to the information security plan, the thesis had another particular addition to it. Information security auditing template. The template is naturally based on the risk management table, and tailored so that it could be used to monitor regularly the current situation and state of the measures put in place.

This auditing process would be the responsibility of whoever the CEO assigns as the information security representative. My suggestion was the secretary, if the company is not interested in hiring someone to exclusively fill in that spot as well. My suggestion for how often the information security auditing should be done is preferably once in half a year, but more often than that is also recommended. And of course, keeping a vigil eye on everyday happenings daily is important as well.

As such, I made the case company a simple, but effective information security audit tool, that is specifically designed and tailored to their needs and circumstances. Here is the auditing template. This particular example I had filled out myself, when I gave the auditing template a test run while back. Each segment will be properly explained as to why the particular scenario is important to the overall auditing plan.

No.	Evaluation question	Working as intended	Partially working as intended	Not working as intended	Additional statements and descriptions of the situation
1.	Is the virus protection on the computers and devices sufficient and often updated?	X			
2.	Are the rooms with sensitive data, information and documents properly secured and restricted?		X		The rooms were open, but the said drawers that contained the documents were locked.
3.	When not in use, are the computers properly being logged out of from?			X	The computers were on the desktop state, meaning anyone could have used them.
4.	Are all the documents, flash drives and other similar objects properly stored where they belong?	X			
5.	Are the unnecessary, expired documents containing sensitive data properly disposed of? (Shredder, security container...)		X		Some documents were left beside the shredder, yet to be shredded.
6.	Are all the suspicious activity (phishing emails, suspicious individuals and phone calls within the company's premises) properly discussed and dealt with?		X		It's not being exactly talked about, but the employees are at least aware of being wary of suspicious emails and calls.

Figure 2: Audit Template for Company X. Made by me. 2020

Section 1. The most important parts of the auditing is to make sure that the computers and other devices are always safeguarded, with their protective programs always at their prime. For the current processes within the company, the antivirus were sufficient, even if they had to be updated after notifying them about its importance.

Section 2. The unrestricted access to sensitive data rooms that contain the documents was open, but fortunately, the drawers in which the said documents were in had been locked. Still, it is something worth mentioning about, given how, as previously discussed, the premises are often filled with sounds of loud machinery and working, thus masking any quieter noises completely. If given enough opportunities, someone might be able to break through the locked drawers to get access into their contents. This same logic applies to the doors as well, but with added layer of protection that the hypothetical intruder must go through, the chances of them being caught in action rises exponentially, and thus, the incentive for them to go through the act will decrease, as the risk of getting caught grows.

Section 3. Another computer-related issue that is easy enough to rectify, if taken seriously. The computers within the company during the audition trial run were logged into their admin accounts. Meaning that just about anyone could have used those said computers, perused and perhaps even stolen data out of it without much effort.

Section 4. As with the section 1, the situation was quite similar, although it felt just slightly different from it to have a section dedicated fully to making sure that the sensitive information is really storage in secure containers and places. This includes any laptops, documents, flash drives and discs. The papers and the drives were stored properly, behind a locked door, as the CEO had explained to me, and even showed me briefly.

Section 5. Disposing of unnecessary and unneeded documents is also an important part of information security procedures. Shredding them or disposing them to the appropriate containers is quite essential as well. As the trial audit was conducted, there were some papers beside the shredder. The CEO explained that they were going to be disposed today. While the objective was partially completed, it still contains a risk of someone swiping some of those papers with them if they are not shredded immediately.

Section 6. The employees do not particularly have work computers in the premises, with the exception of the CEO and the secretary, but the company in question does not exactly communicate any strings of suspicious emails or phone calls either. This one might be an odd one to audit, but it feels still necessary to monitor any possible, targeted phishing attempts at the company or its employees.

Letting the employees and especially the ones using computers know of attempted scams and phishing attempts is important for everyone to maintain vigilance. If there are no recent, suspicious activity or it has been properly conveyed forward, this section in particular can be considered as working as intended.

5 Conclusion

The objective of this particular thesis was to develop and make a working and fitting information security plan for the case company. Granted, there were several complications and difficulties regarding the development project. The foremost difficulty was the lack of blueprints or anything other concrete documents or depictions that would have made the visualization easier.

According to the CEO, they had none available to give for the project. Secondly, the company is not that large nor is it situated in middle of a city or town, so not all of the conventional and usual practices worked with one hundred percent proficiency. Some of the methods had to be adapted and altered to fit into the current case at hand. And with the current situation with the COVID-19 pandemic going on, there were many more difficulties at accomplishing the task overall, such as the unavailability of some of the key employees like the secretary of the company to interview, who was at the time working from home.

The case company in question has been satisfied and interested in implementing the information security planning and its tool to their company processes and practices, since it offered them solutions with minimal monetary losses, with the potential exception being a new, possible employee who will take it on themselves to enforce and make sure that the information security within the company is properly maintained and handled, and the quality of that newly added information security policy will not deteriorate or decrease.

In future, the risk table and auditing templates could very well be expanded upon further, especially if the case company branches out to new activities, as they more recently did with starting 3D printing as part of their business processes. And if they open up a new branch, located somewhere else, and the situation in that particular, new premise elsewhere is completely different. While a complete overhaul of the information security plan is quite unlikely, it would no doubt contain some changes, alterations or perhaps some more additions or removal of parts and segments.

To finalize, the case company will no doubt see steady improvement in their data protection, as well as in keeping their company secrets, employee and customer information secured and safeguarded, should they properly follow the information security plan, as well as maintain that state by auditing regularly, and not become complacent.

References

Printed

Atymtayeva, L. B., Bortsova, G. K., Inoue, A., & Kozhakhmet, K. T. 2012. Methodology and ontology of expert system for information security audit. In The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems, 238-243. Almaty: IEEE.

Fitzgerald, T. 2016. Information security governance simplified: from the boardroom to the keyboard. Boca Raton: CRC Press.

Suduc, A. M., Bîzoi, M., & Filip, F. G. 2010. Audit for information systems security. Informatica Economica, vol. 14(1). Romania: Valahia University of Targoviste.

Tipton, H. F., & Krause, M. (eds.). 2006. Information Security Management Handbook, Volume 3 (Vol. 3). 5th Edition. Boca Raton: Auerbach Publications.

Tsiakis, T., & Stephanides, G. 2005. The economic approach of information security. Computers & security, 24(2). Greece: Elsevier.

Von Solms, B., & Von Solms, R. 2004. The 10 deadly sins of information security management. Computers & security, 23(5). South Africa: Elsevier.

Von Solms, R. 1999. Information security management: why standards are important. Information Management & Computer Security 7/1. South Africa: Elsevier.

Electronic

Ben Griffin. 2018.10 Practical Tips for Keeping Your Business Data Secure. Published by Ben Griffin. Accessed 09.01.2021. https://www.comparethecloud.net/articles/10-practical-tips-for-keeping-your-business-data-secure/

DNSstuff. 2020. What Is an IT Security Audit. Accessed 17.2.2021 https://www.dnsstuff.com/it-security-audit

EzeCastle Integration. 2020. 9 Steps to Create Information Security Plan. Published by Eze Castle Integration. Accessed 8.11.2020. https://www.eci.com/blog/16023-9-steps-to-create-information-security-plan.html

Emma Woods. 2019. The Role of Human Error in Successful Cyber Security Breaches. Accessed 18.3.2021. https://medium.com/@emma.woods/the-role-of-human-error-in-successful-cyber-security-breaches-c6c4e5077233

Josh Fruhlinger. 2020. What is information security? Definition, principles, and jobs. Accessed 30.5.2021. https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

Stealth Labs. 2020. How to Create an Information Security Program Plan. Accessed 1.3.2021. https://www.stealthlabs.com/blog/how-to-create-an-information-security-program-plan/

Rebecca Webb. 2021. 8 Ways to Identify Risks in Your Organization. Accessed 17.2.2021. https://www.clearrisk.com/risk-management-blog/6-ways-to-identify-risk-0-0

Silverbulletrisk. 2018. How to Evaluate Risks in Your Company. Accessed 17.2.2021. https://silverbulletrisk.com/blog-how-to-evaluate-risks-in-your-company/

Martin Doyle. 2017. Do You Need to Audit Your Data. Accessed 17.2.2021. https://tdan.com/do-you-need-to-audit-your-data/22306#

Wade Brylow. 2020. Five Elements of an Effective Audit Planning Process. Published by Wade Brylow. Accessed 18.2.2021. https://misti.com/internal-audit-insights/five-elements-of-effective-audit-planning

Resolver. 2021. Best Practices for Building an Audit Plan. Accessed 19.2.2021. https://www.resolver.com/blog/best-practices-for-building-an-audit-plan/

Katakri. 2015. Information Security Audit Tool for Authorities. Pages 53. Accessed 8.11.2020. https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Finland. 1999. Personal Data Act 523/1999. Accessed 05.03.2021. https://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf

Finland. 2004. Act on the Protection of Privacy in Electronic Communications 516/2004. Accessed 5.3.2021. https://finlex.fi/en/laki/kaannokset/2004/en20040516_20110365.pdf

Finland. 2004. Act on International Information Security Obligations 588/2004. Accessed 6.3.2021. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Figures

Appendices

Appendix 1: Interview Questions

Questions for CEO of the case Company

- Do you have someone in the company that represents and is responsible of security? = “No, we do not right now.”
- Are the documents and other data stored in a restricted room? = “Well, the documents and flash drives are stored in a locked drawer, but the room is pretty much always open.”
- Who has access to the said drawers? = Me and the secretary.
- Has the company had any information security education prior to this? = “No, not really. It has not felt relevant to us.”
- Are the devices in the company sufficiently protected, such as antivirus on the computers? = “Yes, our computers do have antivirus programs installed on them.”
- Has there been any major incidents related to information security before? = “Well, there was one time when we lost some pretty important papers. Turns out they were simply misplaced, so we did dodge a bullet on that one.”