Development of premises security

Aleksi Sadeoja

2021 Laurea

Laurea University of Applied Sciences

Development of premises security

Aleksi Sadeoja

Security management

Bachelor's degree

June 2021

Laurea University of Applied Sciences **Abstract**
Security management
Bachelor's degree

Aleksi Sadeoja

Development of premises security

Year 2021 Number of pages 299

The purpose of this thesis was to produce a clear way for small and medium enterprises to develop premises security. A common tool that can be used by people who lack previous knowledge regarding premises security measures.

The thesis concentrates on developing a model for enhancing premises security. The goal is to educate the SME decision maker and to guide how to develop premises security by using a roadmap, to achieve the company desired level of security.

Method used in the thesis was selected as desk research, qualitative research was used in literature review. Literature is reviewed from various sources, including local authorities' guidelines. Major role in this research is document analysis, as various sources are gathered and combined to create a new model for developing premises security.

Main goals, purposes, and the need for research are presented in the first part of the thesis. The conclusions and the developed model are presented in the fourth phase of the thesis. At the end of this thesis, final conclusions and possible future considerations are reviewed.

Keywords: Auditing, premises security, risk management

Contents

1 Introduction

This thesis is a research on what it takes to improve premises security. A clear model is developed from existing models, to improve and simplify the process for private entities to use. As many published models lean heavily on governmental building security, these are quite restrictive and expensive to implement. This model can be suitable for small and medium enterprises (SME) as larger corporations usually have existing risk management policies and security department in their organizations. As SME's usually have fewer assets compared to larger corporations, a cost-effective model with clear instructions on how to develop premises security could be beneficial and attractive for SME's to introduce as part of their risk management program, and in case a SME does not have a risk management program, this model could give the SME eagerness to draft their business continuity plan and disaster recovery plan and increase their focus on risk management.

The purpose of this thesis is to solely focus on security related issues, such as breaching the perimeter. The completed result is planned to be used as a tool to develop premises security in small and medium enterprises, and further development of the topic can be used to form a basis for consultant work or establishing a company focused on premises security.

The development objective is to form a clear, easy to follow plan how to develop premises security for private entities, such as small and medium enterprises.

1.1 Need for research

The need for developing premises security became clear during the authors internship at unidentified company. The author was tasked to map security deficiencies at various sites. The company has evolved and expanded through the years, and the focus has been on production. Security measures had been neglected for prolonged time and a major security breach had occurred at one company location. This provoked the company management to focus to improve structural security company wide. Security has been improved since the incident, some deficiencies remained at time of the authors internship.

By having a clear development plan regarding premises security, the developed plan can be used at several locations with minor modifications, a cost-effective way to improve premises security.

Possible breaches may have the possibility to reach the news cycle, which would have negative effects on company image. Companies value their public image, as the key part of business is to sell products to consumers and companies, thus increasing the profits. Negative public image could interfere with company goals and lower expected profits.

Often it is in the best interest of the company to restrict access to their buildings, in some cases due to the legal requirements, keeping unwanted individuals of the property and critical areas is not just a company desire, but a legally binding cause. Security is an issue that is constantly evolving, and by having a clear, easily available tool for security professionals inside the company to use, the development of premises security can continue the cycle of development to infinity.

1.2 Reputation and financial impact

It is in best interest of a company to maintain the reputation of the company. Good reputation increases financial returns, helps the access to capital markets and attracts better employees. Good reputation also attracts paying customers (Bradford). Positive reputation also helps locating investors for the case company (Fasaei, et.al. 2018, 1). Studies suggest that enforcing proper security measures benefit the company's interests. Goel and Shawnky (2009) states that: "Security breaches can have a significant impact on the financial performance of firms". By reducing security breaches and investing in security, impact to company reputation and finances are decreased.

1.3 Limiting the research

As premises security is a wide topic with various sites, buildings, office spaces, security clearances etc. this thesis will mainly focus on general issues regarding companies and organizations premises security needs. Safety related issues are excluded from this thesis, even though these may overlap with security. Safety issues, such as fire safety, require a different kind of aspect and these issues can be identified during the auditing process once the developed model has been taken into action by a company. There are several legal requirements regarding safety issues of buildings, premises, occupational healthcare etc. of companies, due to that reason safety is excluded from this development model.

2 Theoretical background

In this section theoretical background for premises security is presented. In addition to premises security, the concept of risk, risk management, risk assessment techniques and required methods for developing premises security are introduced. This section forms a layout for the developed method for developing premises security.

2.1 Basics of premises security

Premises security constructs of several layers. Layers form situation where each layer protects the subsequent, the inner layer becoming the most protected one (Katakri, 2020). The United Nations have identified security layers in their manual “Security of UN Premises” (2017, 3) as following: “Components of the security system must be designed in sufficient number of layers to make it more difficult to defeat the whole system.” As premises security rely heavily on layers, the layers stand as first layer is the outer rim, outer rim structures from proper fences, motion detectors and video surveillance. Structural changes to the environment can also be done by constructing pathways, ditches, bodies of water etc. Adequate lightning at the protected area is extremely important in order to identify possible intruders. Electronic surveillance systems are helpful, but on sight security personnel must be present to operate these systems properly, and to respond possible security breaches promptly. Once the outer rim is protected, focus transfers to the actual buildings at the area. Building shells are protected by doors, adequate locking systems, access control, security cameras and alarm systems (Katakri, 2020, 27). Access to the roof must also be protected, preferably by surveillance cameras and lockable ladders or doors accessing the ladders and routes to the roof.

The site security design guide (2007, 23) presents four layers of outer rim security zones before the building envelope. Physical vehicle restrains and fences are recommended to be implemented to the area as part of decorative architectural installments. Koski states that “for example a body of water flowing between buildings can be a landscaped driving barrier” (Aaltopro, 2018). By using landscaping methods to include security measures to protect an area or a building, WBDG states that “aesthetically pleasing approach can be achieved” (Whole Building Design Guide, 2016).

As security premises constructs from several layers, indoor security also has several sub layers, VAHTI presents color coded security areas. (VAHTI, 2013, 22). By construct office spaces usually have a lobby, restaurant or similar kind of environment which is considered in white color as public area. This area is not restricted by any means, other than usual office hours. Obviously, this does not apply to all installments, there are several locations where personnel are required to proceed through access control to enter the premises. First indoor layer of security is green zone or basic access, this area is usually allowed for all company personnel. This area does not contain any critical information, this is common office spaces, routes to more secure areas of the premises, social spaces etc. Security zones continue to yellow or heightened area. Yellow area requires additional structural changes, such as soundproofing of walls. The final stage is considered as blue zone, high level area. This is the most restricted area in this example. Picture 1 visualizes the security zones at office space.

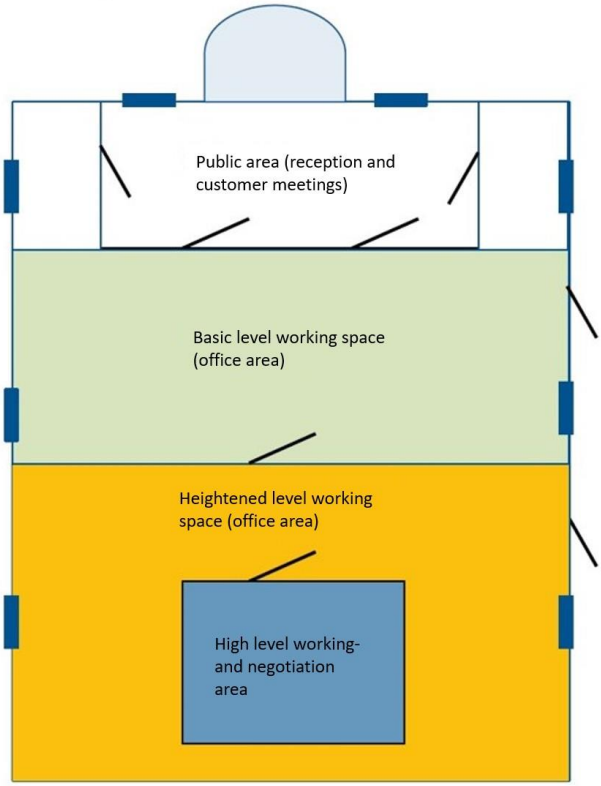

Figure 1: Security zones (VAHTI 2013, 22).

Security zones form a basis for premises security. Department of Prime Minister and Cabinet of New Zealand (2018) provides five zones in premises security. Based on literature, having security zones as a baseline for premises security is a common factor, and it is enforced in different continents as well.

2.1.1 Video surveillance

Video surveillance systems are video cameras covering certain area. Video surveillance systems can be implemented indoors and outdoors. Several laws are enforced regarding video surveillance, and video surveillance is also considered as personal data if the person can be identified from the footage (Tietosuojavaltuutetun toimisto, 2021).

Modern video surveillance cameras are IP cameras, digitalized video surveillance cameras, which work through local internet network. Modern IP cameras, depending on the device, have excellent video quality. IP cameras work with single PoE wire, or even wirelessly. Many sites still have older generation analog surveillance video cameras. These analog cameras lack

in video image quality, and usability since every camera requires power cable and coaxial cable (SFS-62676, 50). Video surveillance system can be implemented to other security systems, such as access control or alarm security system (SFS-62676, 57). As it comes to monitoring the surveillance feed, Chen (2018) states that “one security guard can only watch four monitors at the same time, and the concentration can last only for 10 minutes such that more than 50% of key information is lost.”. Modern surveillance systems offer detection for movement, which alerts the security guard to concentrate on video feed, which helps the security guard to identify possible intruder. Video analytic software can even track moving target automatically (Caputo, 2014, 285).

Video surveillance systems provide their users a possibility to detect an intruder by using the video surveillance. In case of a breach, the intruder may also be identified by using video surveillance system recordings. Camera surveillance systems can be used in real time, active picture monitoring or afterwards as passive analysis of video footage. (KATAKRI, 2020, 27). The video surveillance systems do also provide a deterring effect. According to Dongping, et. al. “surveillance cameras have a significant deterring effect on crime” (2021). By implementing camera surveillance systems, the company has the possibility to deter and detect intruders, and in case of a breach, have the possibility to investigate the intruder.

2.1.2 Access control

The main cause of access control system is access guidance and access limiting, which is targeted towards outsiders and the company’s own staff (Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät, 16). Most simple way access control can be executed is by having locked doors. Present days access control has developed to be quite electrical, electronic keys and electronic access systems are gaining popularity. These systems have a possibility to keep track of access times and who has been accessing the site. Restricting the access areas or expanding individual access rights are easy to change. KATAKRI lists methods which can be used in monitoring access to certain area as: “mechanical, electrical or electromechanical technical systems or other types of physical measures.” Access control can also be conducted by a person identifying personnel entering the restricted area.

Key control is important factor of access control, Finanssiala states that “In a company or in a community there has to be person responsible for locking, whose tasks include maintaining the guideline for users key guideline and their introduction” (2017). Keys that have been shared to personnel should be tracked and the keys should be kept as unidentifiable as possible, according to Fennelly (2012, 141) “precaution is to ensure that the lost key cannot be linked to the lock it operates.”

2.1.3 Security service provider

Security service provider is usually a private entity that providers security services for private people and companies. Security services include at site security guards, off site security guards and response, video surveillance, access control enforcement, security system maintenance etc. These are presented in law Private Security Services Act 1085/2015. Security service providers are licenced entities (section 6, section 68). For a person to act as a security guard, it requires a licence given by the police (section 25).

According to National emergency supply agency (2021) “Security guards also protect critical national emergency locations from nuclear power plants to local grocery stores”. As the quote states, security service providers are widely used in Finnish society. Lanne et.al. (2007, 22) states that in Finland majority of security service providers offer “guarding services, structural security products and electronic security systems”.

2.1.4 Structural security measures

Structural security measures are physical restraints which are built to fit a certain environment. Depending on the nature and desired security level of the protected area, by using structural measures such as bodies of water, vehicle traffic can be diverted, or even denied to certain location. Other landscaping measures such as rocks, cliffs etc. are available for designers to use as measures to protect the area. A common way to protect area or a building is to use fences, as this also have a symbolic impact of the area to be restricted. (The Site Security Design Guide, 2007, 41-58). Lighting is an important factor when designing structural security. Katakri states that the aim is to stop the intruder at the outer rim, proper lighting helps the security staff to notice the possible intruder (2020, 27).

Finanssiala has published a set of guides to design and implement structural security measures for companies to use. The guide provides instructions for wall materials, hinges, doors, floors, windows, etc. (Rakenteellinen murtosuojaus 3. 2017) The guide among Katakri provide the user several standards, such as locks standards, which are to be used in buildings. As these publications are free to use, these provide a cost-effective way for a company to examine the costs of upgrading structural security measures for their premises.

2.2 Social engineering

Social Engineer, LLC defines social engineering as “Any act that influences a person to take an action that may or may not be in their best interest” (Social-Engineer, 2021). Peltier states that “The goal of social engineers is to trick people into giving them what they want” (2006). Both have in common that social engineering is a way to gain something from another person.

In premises security social engineering may be used to gain access to restricted location. Social engineering may include targeting certain personnel of the company, by using skillful verbal language, target person of the social engineering may give access to an external identity with malicious intents. Personnel can be deceived at big locations where there are hundreds, or thousands of different employees to keep the door open for the next one. Social engineering may occur by someone exposing as authority, or by trying to develop a social relationship with the victim (Krombholz et.al 2015).

Physical restrains can be used to prevent external, unauthorized access to area. By requiring identification, use of access control at gates and doors effects of social engineering can be prevented. Hadnagy states that "Many of these attacks could have been avoided if people were educated…Sometimes just finding out how malicious people think and act can be an eye opener" (Hadnagy, 2010, 10) Educating employees of social engineering methods, how to identify them and to report these efforts to company lead can also have positive results on deflecting social engineering attempts. As these efforts are reported, the company lead can effectively inform the rest of the employee base to be aware of such actions.

2.3 Risk

The concept of risk has various angles. Hopkin has gathered risks in his book "Fundamentals of Risk management" from various sources. In his table, there are four different definitions of risk gathered from ISO guide 73, Institute of Risk management, Orange book from HM Treasury and from Institute of Internal Auditors. These all have common that risk includes something of uncertainty, probability, and outcome. Ostrom L. and Wilhelmsen C. define risk as "the probability of an unwanted event that results in negative consequences" (2019, 5). Probability aspect in defining risk is a common factor in these statements. Ostrom et. al. have also taken the approach of defining risk as something with negative outcome.

Leppänen, et.al. define risk as "Risk is an event or set of circumstances that have a positive or negative effect dependent on losses or hazards and possible profits in risk taking." Security related risks, such as breaches or break-ins are hardly positive risks, in cases like this, risks always have negative impact, which is also supported in Ostrom's et.al. statement of risk having negative consequences.

Defining a risk varies from the expected outcome. Financial risks may have positive outcome as profits may increase after taking a risk of investing to an asset. In security related risks, the possibility of having information stolen, or breaching secured facility may have negative outcomes as these can impact public image of the company as shown in section 1.2 of this thesis.

2.4 Risk management

Defining risk management is a wide topic. According to Pinto and Magpili (2016, 319) “applications of risk management have one common objective: To minimize loss associated with a system in case things go wrong.” Hillson states that “The risk management process aims to identify and assess risks in order to enable them to be understood clearly and managed effectively” (2003, 86).

As literature presents, there are a number of ways to approach risk management, by combining these together, we are able to understand process of risk management efficiently. David et. al. (2008, 25) presents a figure of risk management life cycle. Risk management is an ongoing process, which includes identifying risks, analysing risks, treating risks and monitoring risks. The cycle is never ending loop as risk management requires constant monitoring of risks. The figure 2 shows the life cycle of risk management.

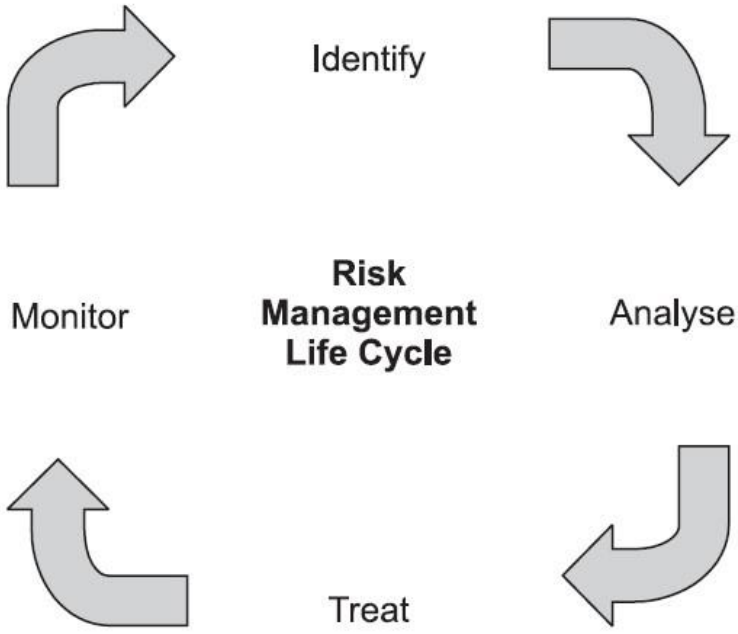

Figure 2: Risk management life cycle (David, et. al. 2008)

Risk management and risk assessment are linked together. According to Calder (2008, 97), risk management plans can be divided to four phases:

1. Eliminate risks.
2. Reduce those that cannot be eliminated to acceptable levels.
3. Live with the risks.

4. Transfer the risks by means of insurance.

Calders risk management plan falls fittingly to the figure “risk management life cycle”, phases analyse, treat and monitor can be converted to sections 1, 2 and 3. Calder jumps into analyzing and treating risks, he does not mention identifying risks at all. Like defining risk, risk management also varies depending on the sources.

2.5 Risk assessment

Assessing the risks is important to risk management. Risks are determined by a number to track the significance of the risk. Valuables for the number are e.g., frequency of the risk, severity of the risk, impact of the risk. Bradford states that risk assessment is “Where risk is identified, measured and assessed, and reputation is analyzed against corporate goals.”

Giving the encountered risks a number on significance can be difficult. Heerkens (2006, 262) states that “we ‘make up’ numbers – they’re called estimates” in risk assessment. The risks assessment is evaluation, the auditor is in a place where they do not have perfect information regarding the risks.

To be able to evaluate the risks efficiently and clearly, a risk matrix is a tool to evaluate risks. Ministry of Finance has developed a risk matrix tool, which will be used in this thesis. Risk management tool helps to assess the severity and the impact of the risks that can be identified. Risk matrix tool is used to support findings of security audit and interviews.

Table 1 presents the risk matrix. Probability of the risk is given a grade of 1-4, which is found on the left side of the matrix. Impact of the risk is given the same value of 1-4 at the lower section of the matrix. The colors, green, yellow, orange, and red help the reader to identify the probability, impact, and severity of the risk. By using the presented risk matrix tool, the risks identified will have risk value. Risk value is calculated by taking the probability value e.g., 2 and multiplying the impact value e.g., 3 together and receiving risk value of 6. Final risk values are the following:

- Value 1 is regarded as minor or no risk.
- Value 2 is regarded as moderate risk.
- Value 3 is regarded as significant risk.
- Value 4 is regarded as unbearable risk.

Table 2 explains the number and color value of the assessed risks in case of probability. Table 3 explains the number and color value of the assessed risks in case of impact.

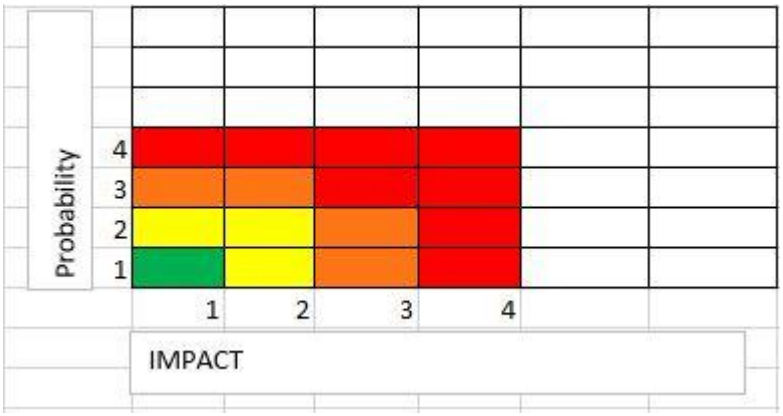

Table 1: Risk matrix

Probability values	
4	Almost certain
3	Probable
2	Possible
1	Unlikely

Table 2: Probability values

Impact values	
4	Critical
3	Significant
2	Moderate
1	Minimal / No effect

Table 3: Impact values

2.6 Interviews

Part of the data gathering is done by interviewing key personnel at the case company. As this tool focuses on limited security concern, only a few selected personnel are recommended to be chosen to be interviewed. Main goal is to gather crucial and accurate information regarding physical security measures and deficiencies at the company. Semi structured interviews should be chosen, as the plan is to conduct the interviews as a discussion with a question framework. This way the researcher can gather information which would not be accounted in structured interviews, where a predefined set of questions would steer the interview.

The interviewees can be security management personnel, as they have the most information regarding the security at the company and the obstacles in developing security any further. The interviews support the auditing process and the research to define the gaps in premises security. Interviewing daily users at the site can be beneficial, as they use the property continuously. They may identify common problems, which cannot be seen from management perspective. An issue of this kind could be for example a door that does not close properly during winter months, something that a daily user would notice. Daily users can also identify user errors in security systems, or gaps in security systems. These issues might be for example malfunctioning surveillance camera. The interview should focus on past incidents, how the incidents occurred and does the interviewee have a plan how to prevent such incidents occurring in future.

2.7 Auditing

Security structures from several layers. A way to test these layers is done by auditing. Several auditing tools, such as Katakri, includes physical security and IT security. Finnish National Security Authority (NSA) has published information security auditing tool Katakri for authorities to use. This tool is designed for authorities, but it serves private companies interests as well. Katakri is free to use and available publicly and it forms a great basis for companies to use as auditing material. Ease of access and the fact that the tool is free makes it extremely attractive and beneficial tool to use.

Using Katakri as auditing tool is unnecessary heavy for multiple organizations. By constructing auditing tool suitable for private entities, the process becomes more user friendly and lowers the threshold to start penetration testing and auditing. ISO 31000 offers risk management and risk assessment guidelines which are helpful in determining values of risks found in auditing. By simplifying auditing process, auditing becomes more cost- and time effective. Section F of KATAKRI involves physical security. As Katakri is designed for governmental use, it focuses on securing classified information. Sections of physical security tool can be used for private entities, such as F-03, F-05.2, F-05.4, and F-05.6 (Katakri, 26-39).

2.8 Roadmap

A way to present the results is to use a roadmap for developing security from the current point to desired level. By using a roadmap, the security related risks can be presented as they are today, what steps need to be taken now and near future to achieve desired level of security.

A roadmap gives the reader the ability to identify what it takes to develop premises security. The roadmap presents the current situation, the time when the research takes place. Following the next steps to be taken, review of the research results. After reviewing the results, taking actions, and allocation of resources take place. Final stage of the roadmap is the preferred premises security status that has been achieved. As the roadmap is to be presented in a circular generic model, the roadmap is not to be tied to one project, as the idea is that the development for premises security is continuous effort.

3 Methods and methodology

Research requires methods to be selected. As this thesis focuses on development project, qualitative research was chosen as main method. Literature from precisely selected sources help to narrow the amount of information required in this thesis. The project is a desk top literature review.

3.1 Qualitative research

Qualitative research is described by Babchuk as “umbrella term used to designate a family of approaches that emphasise inductive reasoning, collecting data in natural settings and understanding participants’ point of view” (Babchuk, 2019). In qualitative methods interviews can be used to collect data. Questions are formed in a way where interviewee does not have exact answer choices, rather than interviewees are expected to construe answers independently (Vilpas).

As this thesis focuses on certain area of security, qualitative methods were selected as research method. Interviews are conducted as semi structured for selected personnel of the case company. By selecting individuals for interviews, a detailed and extensive image of the security level, future considerations and previous obstacles were identified.

4 Model for developing premises security

As a result, a model for developing premises security was formed. The model is presented in this section, at the end a roadmap steers the progress of achieving a desired level of premises security. Key part of visualizing of the process is introduced in section 4.1. The following sections 4.2 presents the roadmap for the company to use. Sections 4.3 and 4.4 form a crucial part of the development work, as auditing and risk assessment are designed to find key risks regarding premises security, to locate possible gaps in security and to focus on issues which need to be revised. Interview model is presented in section 2.6 in this paper.

The model presents the reader how these methods should be conducted and how these could be developed further to minimize the risks and effects in cost effective way. In case results emerge as incomplete, the cycle of risk management, and cycle of development of premises security can be restarted.

4.1 Methods combined

To visualize the development work, the Figure 3 shows the reader how the model for developing of premises security is to be executed. In the center of the picture lies the ultimate task of developing premises security, in order to develop premises security, the person responsible of the development work has to find out the status of premises security. On the outer rim there are four smaller bubbles: audit, interviews, risk assessment and results. These all four methods support each other in the research of developing premises security.

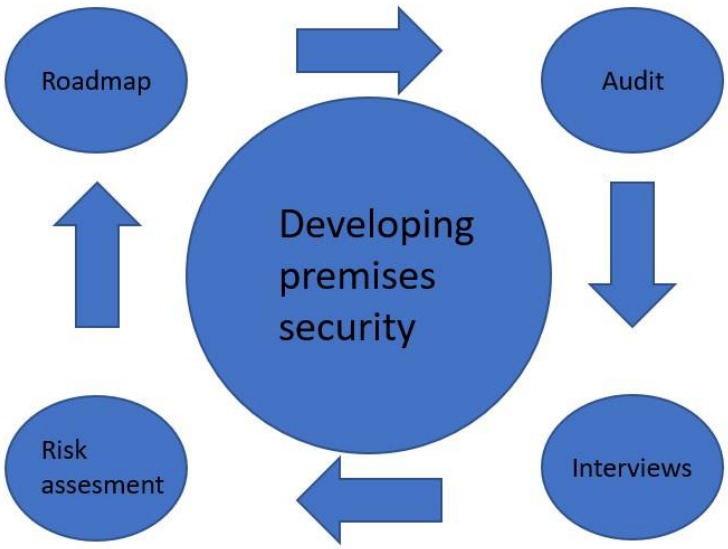

Figure 3 : Methods combined

As the figure 3 presents the development work for premises security is ongoing process. The four phases of the figure 3 are presented in detail, how these parts should be conducted as someone who is responsible for the company's premises security.

4.2 Roadmap

When the company or organization starts the development of premises security, a roadmap is a beneficial tool to schedule and follow the progression of the development. The roadmap is presented as a circle, with four (4) main phases. Each phase includes two (2) sub phases, the roadmap is presented in circle form, as the purpose is to have constantly ongoing process.

The roadmap works as an example of the process of developing premises security. This can be used to have a framework of the process, and the roadmap can be altered to fit the company in question to meet their processes. Sections of the roadmap can also be divided to subsections to expand the processes.

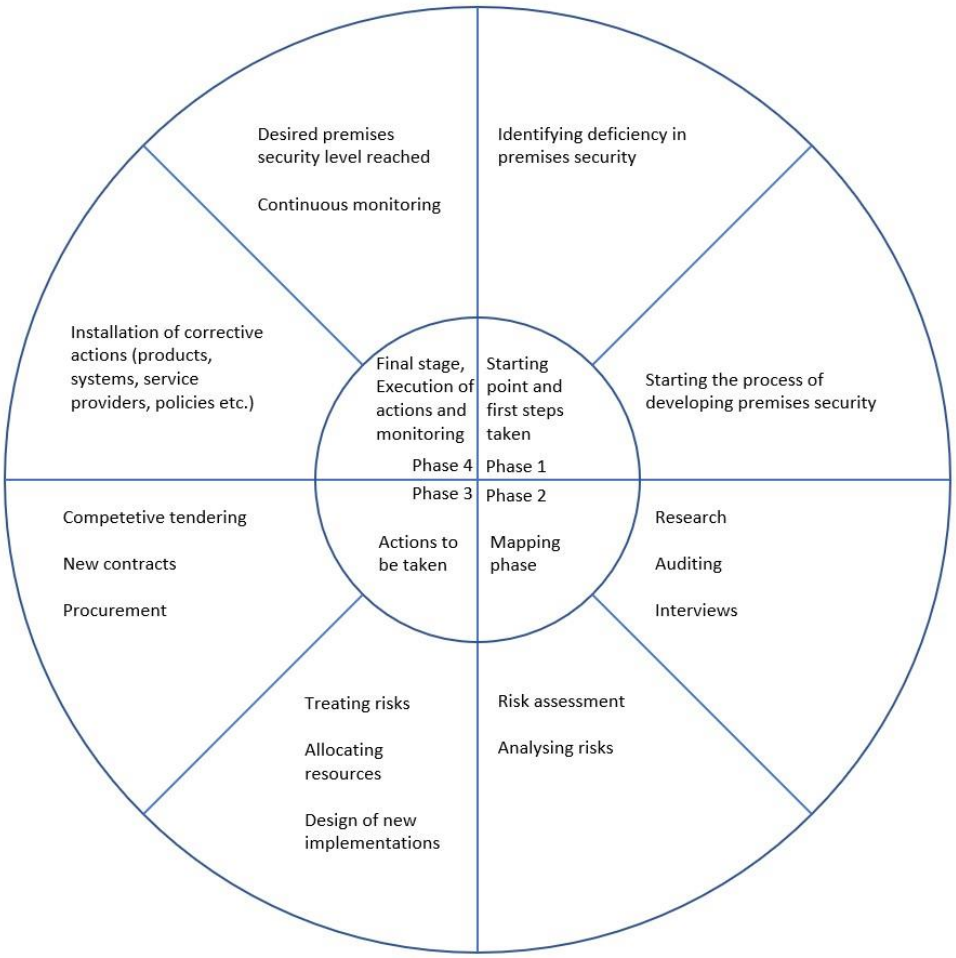

Figure 4: Roadmap

The roadmap is intended to work by using the methods presented in this phase of the thesis. Auditing, risk assessment and risk management are key factors of this roadmap. The roadmap follows the cycle of risk management, as can be seen at phase 4 of the roadmap, continuous monitoring is the final phase, due to the fact that risk management is continuous process. The roadmap guides the whole process, and in case some section or phase come true as incomplete, the company can return to that section and restart the phase.

4.3 Auditing

Auditing process starts by determining the assets the company needs to protect. Once the assets to be protected have been identified, the company has to evaluate their premises security status. To evaluate their status, to protect their assets, an auditing process of the premises security should be started. A framework for processes to be evaluated can be structured from section 2.1 of this paper.

Premises security auditing requires the auditor to walk around the premises to determine the status of the location and to identify the gaps in premises security. The auditor should have a predetermined list made of the desired level of security. The auditor can follow the list and inspect the premises security measures if they follow the predetermined list. This means the auditor has to evaluate are the security layers effective, inspect the level of camera surveillance, the possible gaps in camera surveillance, locking systems, alarm systems etc. During the auditing process the auditor marks the results to the list, the results can identify the premises security measures as adequate and / or locate deficiencies in some locations. In case there are gaps and / or proper security measures are identified, both are marked down as inspected during the auditing process.

Once the auditing process has been completed, careful examination of results is expected. Auditing may find crucial security concerns at the audited location, which may require immediate actions to be taken to treat the possible risks discovered. As part of the risk assessment, the identified risks during the audit process are recommended to be placed in a table where the risk is identified, the reason for the risk is presented, and if possible, mitigation actions or actions to remove risks are presented. Table 4 below with example risks is an illustration of such process.

Risk	Reason for risk	Actions to be taken
Master key has disappeared.	Neglected key control.	New locks to be installed, key control policy to be drawn and executed.
Unaccompanied guest at the premises.	Guest policy is inadequate.	Update of guest policy and informing the staff.

Table 4: Identified risks

4.4 Risk assessment results

Part of the auditing process is to identify risks concerning premises security. The risks can be identified during the auditing process, where the company has determined their assets to be protected. As presented in section 2.5 in this paper, risk assessment is “making up” numbers and estimating the severity of the risk. As the company has assets to protect, the severity of the risk has to be determined by evaluating the effect of loss of the asset. For example, if an intruder is able to breach the premises by using a lost master key and to steal a prototype of a product, the loss of the master key would have a high-risk impact value. If the master key is stored in a safe, which can be accessed by only a one person, the possibility and probability of losing the master key is low, hence the risk probability value would be unlikely.

Identified risks can assessed as presented in this paper at section 2.4. Once risks have been valued, the identified risks are recommended to be placed in a table, for example the kind as table 1 presents. Risks have been given a probability value, and impact value. For reader to visualize the impression of the numeral value, colors have been introduced to help the reader to notice the severity of the identified risk.

Risk	Risk probability value	Risk impact value	Risk value
Example risk 1	2	3	5 (unbearable)
Example risk 2	2	1	3 (significant)
Example risk 3	1	1	2 (moderate)

Table 5: Risk values

Once the risks have been assessed by using the presented table 5, the risk management procedure can begin, this is explained in section 2.4 of this paper. Risks should be treated accordingly once they are discovered. For a company, it can be beneficial to sort the risk values from highest to lowest, in a way that the company has the ability to focus on high level risks first.

4.5 Reaching the desired level of premises security

Once the risk management procedure has been completed, the company can design and install the corrective actions. In this phase the company can use a security service provides as a consultant to acquire proper security related products to treat the gaps found in the risk assessment phase. The company can use the presented roadmap in figure 4 to help to visualize the timeline for corrective actions. As there are a wide variety of security service providers, the company developing their premises security have a possibility to tender out the procurements.

The presented roadmap is in a circle form, as stated, the cycle of risk management and developing premises security never stops. The company should revise the premises security and risk management periodically as part of their risk management program. In case security related issues take place before the revision date is set, the development cycle for premises security can be started instantly.

5 Conclusions

As the thesis shows, there are multiple factors to take account when developing premises security. The development project was conducted to develop a premises security auditing model for companies to use. This model can be used by private entities which have a desire to improve their premises security. Clear, easily available, and affordable method was developed as a result. Best practices were chosen from governmental issued security tools and stripped down to be suitable for private entities, which hardly have classified information such as governmental stakeholders may have. As classified information requires strong methods for premises security, the cost of these measures can be unbearable for small and medium enterprises. This model gives the SME decision maker the ability to pick and choose the best methods gathered from high security level guides, to increase their premises security in a cost-effective way.

Developing premises security starts by identifying deficiencies in the premises security. This does not require a company to have a security professional, as the need for development can be identified by anyone. The process of developing premises security can be started by the company lead, in case the company does not have sufficient knowledge of security, external consults and service providers can be commissioned to the process. This thesis and the developed result share the reader the ability to develop premises security even without previous knowledge of premises security.

As the literature presents, there are a number of ways to provide measures for premises security. There is no one clear way on how premises security should be carried out. Similarities were found, the basis for developing premises security is for the company to evaluate their risks and to determine a level of premises security most suitable for their needs. Security development is an issue where resources and financial assets can be designated neverendingly, without it being necessary.

A research turned out to be successful, a clear model for developing premises security was achieved for private entities, companies, and organizations to use. The guides and the sources for premises security turned out to be quite similar, some overlapping’s were found in sources from different continents. This shows that the model presented in this thesis can be used all over the world. As this development project focused on premises security, safety issues were ignored. Although, this same roadmap and method can be used to develop safety issues with some changes. This will require further research, as there are some legal requirements to the evacuation policies and emergency plans of buildings. Same risk management method, auditing and roadmap can also be used to enhance occupational safety.

References

Printed

Alexander, David. Finch, Amanda. Sutton, David. Taylor, Andy. 2008. Information Security Management Principles.

Bradford. 2016. Taking the risk out of risk management: Holistic approach to enterprise risk management. Strategic Direction.

Calder, Alan. 2008. Corporate Governance: A Practical Guide to the Legal Frameworks and International Codes of Practice Chapter 12: Risk management. London: Kogan Page Ltd.

Caputo, Anthony C. 2014. Digital Video Surveillance and Security.

Dongping Long, Lin Liu, Mingen Xu, Jiaxin Feng, Jianguo Chen, Li He. 2021. Ambient population and surveillance cameras: The guardianship role in street robbers' crime location choice.

Fennelly, Lawrence J. 2012. Effective Physical Security.

Hadnagy, Christopher. 2010. Social Engineering: The Art of Human Hacking.

Heerkens, G. 2006. 11 - Risk Management, Decision-Making, and Business, The McGraw-Hill Companies, Inc., The Professional Book Group, New York.

Hillson, D. 2003. "Using a risk breakdown structure in project management", Journal of Facilities Management, vol. 2, no. 1.

Hopkin, Paul. 2018. Fundamentals of Risk Management: Understanding, Evaluating and Implementing effective risk management.

Kansallinen turvallisuusviranomainen. Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille.

Leppälä, J. Murtonen, M. and Kauranen, I. 2012. Farm Risk Map: A contextual tool for risk identification and sustainable management on farms.

Ostrom, Lee. Wilhelmsen, Cheryl. 2019. Risk Assessment: Tools, Techniques, and Their Applications. John Wiley & Sons.

Peltier, T.R., 2006. Social Engineering: Concepts and Solutions. Information Systems Security.

Pinto, C.A. & Magpili, L.M. 2016, "Risk Management" in 2nd edition; Engineering Management Handbook, 2nd edition, Huntsville, American Society for Engineering Management (ASEM), Huntsville.

Suomen toimitila- ja rakennuttajaliitto RAKLI ry. 2004. Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät.

Valtionhallinnon tietoturvallisuuden johtoryhmä. Toimitilojen tietoturvaohje VAHTI. 2013.

SFS-EN 62676-1-1 Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-1: Järjestelmävaatimukset. Yleiset vaatimukset.

Electronic

Babchuk, W. 2019. Fundamentals of qualitative analysis in family medicine. Us national library of Medicine National Institutes of Health. Accessed 10.4.2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6910734/

Chen, Ying-Jen. 2018. Particle-Filter-Based Intelligent Video Surveillance System. Accessed 1.6.2021. https://www.intechopen.com/books/intelligent-video-surveillance/particle-filter-based-intelligent-video-surveillance-system

Department of Prime Minister and Cabinet. 2018. Security Zones. Accessed 9.5.2021. https://www.protectivesecurity.govt.nz/physical-security/lifecycle/design/apply-good-practices/security/

Fasaei H, Tempelaar M, Jansen J. 2018. Firm reputation and investment decisions: The contingency role of securities analysts' recommendations. Elsevier. Accessed 3.4.2021. https://www.sciencedirect.com/science/article/pii/S0024630117303230?casa_token=o9Z50yJjdYsAAAAA:4DKslaHc_7GTrvLEKsF9lUHIe4H5wCE-Lq11jxKWNveGU3UcGhby3t1v6c5t1SrqTjISmM995LU

Finanssiala. 2017. Rakenteellinen murtosuojausohje 2. Accessed 26.5.2021 https://www.finanssiala.fi/wp-content/uploads/2017/12/Rakenteellinen20murtosuojaus20II.pdf

Finanssiala. 2017. Rakenteellinen murtosuojaus 3. Accessed 26.5.2021. https://www.finanssiala.fi/wp-content/uploads/2017/12/Rakenteellinen20murtosuojaus20III.pdf

Goel S, Shawky H. 2009. Estimating market impact after security breach. Elsevier. Accessed 3.4.2021.
https://www.sciencedirect.com/science/article/pii/S0378720609000895?casa_token=9tX2s3RMoj0AAAAA:YLiIQkVij9uqfGOcMbTFzfMyJD2xZkJMSJEqznd5xqHeW5C96o2-2XGclKfBkTznm9o1gX9I1uw

Kangas, Arto. VM 22/2017 Ohje riskienhallintaan Riskiarviotyökalu – käyttö-ja täyttöohje. Ministry of Finance. Accessed 10.4.2021.
https://vm.fi/documents/10623/1898625/Riskiarviointi+ohje/fe847307-0fc9-4389-bc0c-f003a98c150f

Koski, Samu. 2018. Tilaturvallisuus on tasapainoilua. Aaltopro. Accessed 26.5.2021.
https://www.aaltopro.fi/aalto-leaders-insight/2018/tilaturvallisuus-on-tasapainoilua

Krombholz K, Hobel H, Huber M, Weippl E. 2015. Advanced social engineering attacks. Elsevier. Accessed 3.4.2021.
https://www.sciencedirect.com/science/article/pii/S2214212614001343?casa_token=DgigERXJV4MAAAAA:GBU9ShXndkD4owo-ra0kDh8kGkLGOr6rB8mfE7FAj0AsuAXUAbDL67TnVNLj28zU9vhW3L7E07Y

Lanne, Marinka. Kupi, Eija. 2007. Miten hahmottaa security-alaa? Teoreettinen malli Suomen security-liiketoiminta-alueista. Accessed 1.6.2021.
https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2007/T2388.pdf

National Emergency Supply agency. 2021. Vartiointiala lujilla pandemia-aikaan. Accessed 26.5.2021.
https://www.varmuudenvuoksi.fi/aihe/artikkeli/543/vartiointiala_lujilla_pandemia-aikaan

Rajamäki J, Rajamäki M. National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process. European Conference on Information Warfare and Security. Accessed 3.4.2021.
https://search-proquest-com.nelli.laurea.fi/conference-papers-proceedings/national-security-auditing-criteria-katakri/docview/1400694884/se-2?accountid=12003.

Tietosuojavaltuutetun toimisto. Usein kysyttyä kameravalvonnasta. Accessed 25.4.2021.
https://tietosuoja.fi/usein-kysyttya-kameravalvonta

UNSMS Security Policy Manual – Security of UN Premises. 2017. Accessed 27.5.2021.
https://policy.un.org/sites/policy.un.org/files/files/documents/2020/Oct/spm_-_chapter_iv_-_section_e_-_security_of_un_premises_1.pdf

U.S. General Services Administration Public Buildings Service. The Site Security Design Duide. 2007. Accessed 25.4.2021. https://www.wbdg.org/FFC/GSA/site_security_dg.pdf

Vilpas, P. Ohjeita kvantitatiiviseen tutkimukseen Osa 1. Metropolia. Accessed 10.4.2021. https://docplayer.fi/503447-Ohjeita-kvantitatiiviseen-tutkimukseen.html

Whole Building Design Guide. 2016. Landscape Architecture And The Site Security Design Process. Accessed 26.5.2021. https://www.wbdg.org/resources/landscape-architecture-and-site-security-design-process

Figures

Tables