Security management during pandemic

Rami Achek

2021 Laurea

Laurea University of Applied Sciences

Security management during pandemic

Rami Achek

Safety, Security & Risk Management
Thesis
May, 2021

Laurea University of Applied Sciences
Safety, Security and Risk Management
Bachelor’s Degree

Rami Achek

Abstract

Security management during pandemic

Year	2021	Number of pages	36

The thesis focuses on answering research questions such as the effects of recent pandemics on security management. Security levels need to be held high even during and after a pandemic outbreak.

Thesis is structured so that it includes research data of how pandemic is affecting companies security departments in general and how it has affected the case company.

Research for pandemics is starting the in latest of 15000-era bringing around 700 years of researched data considering the influenzas, but most of the data irrelevant to the modern era of people mainly working remotely and the data has not much connection to security management.

For developing of security managers capability to succeed in pandemic a proper business continuity and crisis management plan need to be established as well as noticing that less occupied usage of premises changes the security of the premises by having decreased pair of eyes observing possible external forces.
This obligates security managers to maintain security levels by relying on technical surveillance while, also fire and water risks need to be considered even during low usage of premises.

Keywords: pandemic, premises, security management, business continuity, remote work

Laurea-ammattikorkeakoulu	**Tiivistelmä**

Turvallisuuden ja riskienhallinnan koulutusohjelma
Tradenomi (AMK)

Rami Achek

Pandemian vaikutukset turvallisuusjohtamiseen

Vuosi	2021	Sivumäärä	36

Opinnäytetyössä keskitytään vastaamaan tutkimuskysymyksiin, kuten lähihistorian eri pandemioiden vaikutukset turvallisuudenjohtamiseen, sillä turvallisuustasot on asetettava korkealle myös ennen pandemiaa, pandemian puhkeamisen aikana ja pandemian jälkeen.

Opinnäytetyö on rakenneltu niin, että se kuvaa jäsennettyä tietoa pandemian vaikutuksista turvallisuusjohtamiseen yrityksissä yleisesti, sekä myös kohdeyrityksessä. Eroavaisuuksia vertaillaan opinnäytetyön yhteenvedossa.

Tässä opinnäytetyössä on vastattu sivukysymyksiin siitä, miten pandemia vaikuttaa toimitilojen turvallisuuteen, etätyöhön ja miten toimistokulttuuri kehittyy pandemiasta. Tämän tutkielman tavoitteena ja tarkoituksena on kehittää turvallisuusalaa keskittyen pandemian aikana erilaisiin turvallisuuden hallinnan näkökohtiin. Tämä opinnäytetyö on tehty yhteistyössä nimettömänä pysyvän kohdeyrityksen.

Tutkimustausta pandemioille alkaa n. 15000-vuosituhannelta, mikä tuo n. 700 vuotta tutkittua tietoa ottaen huomioon erilaiset vaikutukset, mutta suurin osa tiedoista ei ole käyttökelpoista nykyajan aikakaudelle, jossa ihmiset työskentelevät päääsiassa etänä.
Käytettyihin tutkimusmenetelmiin kuuluvat dokumenttianalyysi ja osittain strukturoidut haastattelut.

Turvallisuuspäälliköiden kyvykkyyden kehittämiseksi pandemiasta onnistumiseksi on luotava asianmukainen liiketoiminnan jatkuvuuden, sekä kriisinhallintasuunnitelma. Huomioitavaa on, että tilojen vähenevä käyttö muuttaa tilojen turvallisuutta laskemalla kohteessa olevia silmäpareja mahdollisten ulkoisten tahojen varalta. Tämä edellyttää turvallisuudenjohtajat ylläpitämään turvallisuustasoja huomioimalla muun muassa teknistä valvontaan. Murto- ja datasuojan lisäksi myös, palo- ja vesiriskit on otettava huomioon pandemiassa.

Avainsanat: pandemia, toimitilat, turvallisuusjohtaminen, liiketoiminnan jatkuvuus, etätyö

Contents

1 Introduction 6
1.1 Limitations 6
1.2 Research aim 7
2 Theoretical framework 7
2.1 Security management 8
2.2 Pandemic 9
3 Development process 10
3.1 Document analysis 11
3.2 Semi-structured interviews 11
3.3 Research process 12
3.4 Ethics and reliability 13
3.5 Estimate of resources and costs 13
4 Results 14
4.1 Research data 14
4.2 Interviews 25
5 Conclusions 28
References 29
Figures 34
Tables 34
Appendices 35

1 Introduction

Todays security managers working field is complex by having many different evolving tasks to handle. Having a pandemic on top of that challenges security managers work even more. This thesis studies security management during pandemic to those of who are working in the field of security especially to deepen their knowledge of the affects of pandemic on security management.

Thesis is structured so that it includes research data of how pandemic is affecting companies security departments in general and how it has affected the case company and how do they compare.

Security is constantly developing and staying in touch with the development requires commitment and following the industry and its regulations regularly. Things such as physical and digital safety and security of company assets are the bread and butter of many security managers. Added to that risk management, business continuity, and information security with pandemics increases the required learning curve for security managers to thrive.

The thesis is made so that security professionals in future could utilize found research on new upcoming pandemics. Also, companies have realized that they may not need to pay for unnecessary space to keep their operations running because using remote work might be cheaper and safer in terms of keeping space between individuals.

The security of the companys devices, including laptops and cellphones, will have different threats compared to working at the off time of pandemics at the office. Thesis will also compare data acquired by document analysis and data acquired by semi-structured interview to see how modern big company whitstands during pandemic.

1.1 Limitations

Limitations to this thesis are that the subject is relatively newish on the recent historical scale, considering Covid-19 has had the most significant impact on our society and it not even ended yet at the time of writing this thesis. Of course, viruses and pandemics have been before in human history many times, but Covid-19 is the master of its kind because it affects modern civilized human society that lives in the informative globe which has access to almost any data at any time. (How Covid-19 is affecting societies and economies 2020).

Professional lab data on Covid-19 is yet not out there on a large scale at the time of writing this thesis. Even though the Covid-19 pandemic is affecting everywhere, and there is online availability everywhere globally, most of the data published is about how to protect ones health, what are the daily amount of people infected and number of deaths. Finding valuable qualitative data on this subject will have challenges because of the recent pandemics new nature. Although Ebola and Covid-19 are currently ongoing the pandemics before these are not so relevant considering how our society is different from example 1968-69 H3N2 influenza that started in China and spread globally into a pandemic. Research background for influenzas is starting around the 15000-era bringing around 700 years of researched data considering the pandemics. This data is mostly unsuitable for today, because of the nature of new ways of working and development of most current office environment job-positions. (Linnanmäki n.d.)

Disclaimer could be pointed out that this thesis is written physically in Finland to and will have some perspective towards the Finnish security field. Limitations can arise such as not having access to other countries physical data bases such as libraries, because of the ongoing pandemic. Also, timewise not all physical data can be gathered by single person for this thesis, but the most suitable ones will be.

The research problem may not be accurately expressed at the beginning of the research, but the research problem becomes clear throughout the research. (Aaltola, Laajalahti & Valli 2018).

1.2 Research aim

The key concepts of this thesis is to develop security management during pandemic. Questions related to the research goal of the thesis such as how does the pandemic affect premises and remote working security will also be answered. Similarly, how will the office working culture develop from pandemic and how the movement of company employees impact security managers daily working environments.

Data on pandemics affecting security management is low so this thesis focuses on researching existing data about pandemic and security management and combining them reasonably so that security field professionals could emerge better from pandemic.

2 Theoretical framework

Wrought research on the topic of this thesis discovered that there is not that much of a data available that is directly suitable for security managers and their work during pandemics before Covid-19 happened. There are studies of the impact of security management on business, but not that much on pandemics related to security management until recent events (AlgoSec survey 2013).

Pandemics internationally on large scale have been on history, but not so much on this level during digitalized civilization, which means the ways we live now is different than earlier so pandemic hits our societies on a new way. This increases the restriction of usable data on this thesis. Most of the theoretical data is researchable online through e-books, studies, theses, but some classified data about the topic might be unavailable or behind an unreasonable paywall.

At the time of writing the theoretical framework not even the commonly known website Wikipedia has mentioned the word pandemic or Covid-19 under the title of security management (Wikipedia 2021). Knowing that the page is not reliable at all, it is still disturbing that those words did not even show during background research.

2.1 Security management

Security management is systematical and result oriented activity, which seeks to purposefully prevent damages and to minimize the impact of damages. Company management can affect the organizations way of operating on safer way by committing on a visible way to it. For managing of security, the company management can determent: tasks, jurisdictions, develop clear instructions and rules with the employees. Development tasks are done in a timely manner and with efficiency. Activities are monitored and results are followed regularly. The staff is motivated on regular basis to work safely. Security managements basic purpose is that the safety and security in company is perceived as important and that it affect everyone. (Korhonen, Moisio & Tuominen 2003).

Occupational safety law: (738/2002) goal is to improve the working environment and conditions of staff members for the ability of working in safety. The function of the law is to prevent accidents in work, occupational diseases and other work or working environment caused physical or mental health disadvantages (1§). Legislation requires that occupational safety is taken into account on every activity and on all levels of hierarchy. Legislation states that the employer has an obligation to take care that the workplace is safe and healthy (8§). The obligation corresponds to standard of the principle of continuous improvement. (Korhonen et al. 2003).

The definition of security management is extensive because the title security manager keeps inside many different tasks handed to the job. These security management tasks vary from each other hugely depending on the size of the company, industry, and the distribution of other security-related roles on the company. The title tends keeps inside at least one of the three following aspects: security, safety, or risk management. Other aspects that could be used within the title are occupational safety, supervising, business continuity, access control, camera surveillance, security alarm systems, cybersecurity, network security, brand, training, asset management, audition, security walks, specific recruiting, inspections, budget, policies, data gathering, compliance, events, environmental and related. (Resources workable security manager description n.d).

Todays requirement for new security managers tends to require at least Bachelors or Associates Degree in security management, criminal justice, public administration, or related education. Some industries or positions may require a background based on engineering giving the challenges that are in the position. Significant colleagues for a security manager usually are the information, cyber, risk, financial, and networks managers/leaders. Good character traits for the positions keep inside having good communication skills, having a good and broad knowledge of security environments and hazards, being polite, interpersonal, analytical, having leadership skills, being proactive, acquiring negotiation skills and being able to work with a team but also solely. (JobJob research article n.d).

2.2 Pandemic

Influenza is a sudden inflammatory disease of the respiratory tract caused by the influenza A and B viruses, which occurs worldwide every year as a recurrent of epidemics. During pandemics 5-15% of population is affected with infection. The excessive mortality caused by the seasonal influenza epidemic in Finland usually ranges from a few hundred, rising to over a thousand at worst. Causes of an influenza epidemic significant burden on the healthcare system and can, at worst, disrupt schools and work communities. An influenza pandemic refers to the rapid and worldwide spread of a new subtype of influenza A virus to humans. An epidemic during which the morbidity is higher than the annual during epidemics (25-35%) and the average disease may be more severe than the usual seasonal flu. Unlike seasonal flu, serious forms of the disease can also get previously completely healthy young people. (Contingency plan for an influenza pandemic 2006).

During the pandemic warning period, the pandemic virus may spread from person to person in local clusters or epidemics. If there is no spread from one person to another in pandemic situation has not yet been observed in Finland, the health care activities aim is to target individual infected people that has entered the country, identification of the individual, treatment and isolation of the individual to prevent the spread of infection. (Contingency plan for an influenza pandemic 2006).

The symptoms caused by the flu causes the bodys defense mechanism reaction to work against the viruses and the altered function of the mucous membranes and cells in the body. the immune system activates the inflammatory antibody and inflammatory cells to remove the viruses from the body. The mucous membrane, on the other hand, produces mucus that tries to prevent the virus from getting close to the cells. Mucus surrounds impurities and microbes, making it difficult for microbes to enter mucosal cells. Influenza is also associated with the activation of the immune system throughout the whole body. The bodys symptoms are therefore not limited to the respiratory tract. Typical symptoms are high fever and muscle aches. The inflammatory response in the lungs can sometimes be so strong that a person dies of lung damage. (Huovinen & Ziegler 2011).

Viruses are transmitted primarily through contact, such as in a handshake or as a droplet infection as a result of sneezing or coughing. Flu-causing viruses have been found on TV remotes and toilet cubicles in patients homes, but also in toys at the doctors offices. Researchers at the University of Virginia found out how long the viruses survive on surfaces, dried the mucus from a flu patient containing the virus to light switches, for example, and then monitored how long the viruses were found in them. After 1 hour live virus was detected in one in five subjects and after 3 days in only 3% of subjects. Some influenza viruses remain viable even in the nose goo for days which means there is a lot of difference in viruses as well. (Huovinen & Ziegler 2011).

Researchers have long wondered why both the southern and northern hemispheres during winter are just so liked by the viruses. Namely, the other dozens and hundreds of flu viruses begin to spread quite soon after the summer holidays. American scientists have found a plausible explanation. They came across a coincidental study from 1919 which reported that a Spanish laboratory virus that had then spread over the world unexpectedly killed guinea pigs used as experimental animals. There were no previously available experimental animal models for the spread of the disease because the conventionally used experimental animals did not become ill or became ill with the flu only incidentally. The researchers found that the flu virus infected the guinea pigs best in cold and dry air. Humidity significantly reduced infectivity, as did the rise in temperature. Winter frosts and low relative humidity provide the best conditions for the flu virus to infect. Influenza experts consider the study significant, because it gives a sensible explanation for the mystery that has prevailed for decades. Another lesson in research is that it is good to read studies from decades ago. They can also provide unpredictable tips for current research using modern technology. (Huovinen & Ziegler 2011).

3 Development process

This section explains which methods will be utilized in this thesis and why they are used so the reader can be more aware of what kind of results might be yielded. The main two methods of this thesis are chosen to be: document analysis and semi-structured interviews.

3.1 Document analysis

Document analysis is a qualitative research method that will be the primary method of this thesis. Qualitative research can be described as a process. When in a qualitative research the means of data collection is human, ie the researcher itself, the perspectives and interpretations related to the data can be seen to evolve in the researchers consciousness gradually as the research process progresses. Qualitative research can also be described as a process in the sense that the different stages of the research process may not be structured in advance into clear different stages, but solutions for a research task or data collection, for example, may gradually develop as the research progresses. (Aaltola et al. 2018).

There will be analyzing different sources on current research material that is available to reach and compare existing data and comparison of data that will conjure from this method. The utility of document analysis is to open data from previously gathered posts, articles, or studies and shape them to make sense for the reader. Analyzing documents will also develop the skills for better research once the process starts and will bring forth the thesis's editing while operating it. The gathered data will be professional and accumulated so that the reader can focus on the thesis instead of wondering about the texts authenticity, because all sources that are referred in this thesis have dedicated page at the end of this work. Also, gathered documents will be from reliable and ethical sources so that the reader can backtrack where the text is coming from. This thesis will utilize a lot of public records which includes articles, company posts, mission statements, project scores, reports, syllabis, handbooks and related (Triad 2016).

Advantage of document analysis is that it’s efficient and effective way of acquiring gathered data because documents are time efficient and useful resources. Obtaining and analyzing documents is often far more cost efficient and time efficient than conducting your own research or experiments. Documents are also, non-reactive data sources, which means that they could be read and studied many times and remain unchanged by the researchers influence or research process or time (Bowen 2009).

3.2 Semi-structured interviews

The interview is a qualitative method that keeps asking open, honest questions inside of it. The writer of this thesis will be the interviewer in all of the interviews. The writer will be interviewing corporate management personnel. During the pandemic, most of the interviews will be held via telecommunication software skype, teams or by phone. However, some of the interviews will be face-to-face if the situation requires it or is desirable for possible preferable results. Carrying out semi-structured interview conversationally with controlled phase employs a mixture of open to close-ended questions, usually followed by how or why questions. (Adams 2015).

About an hour is thought to be the maximum limit of time used on this method to not overuse the interviewed person in a way that it could affect the results and feel unpleasant for the person that is being interviewed The interviews will be fully semi-structured. The structures for interviews will be planned. The interview base will be sent for the person who will be interviewed before the interview to give them time to prepare their answers so that the answers are more accurate and professional instead of emotional. That way, the better quality of data will be more guaranteed. There might be limitations for having structure on interviews, such as limited answers or difficulty answering specific questions. However, the benefits will prevail over the negatives by giving less chatter and more data for the interviewer and the thesis research. (Conducting semi-structured Interviews 2015).

Once consent to the interview has been obtained, the time and place must be agreed and any additional materials or the exact subject areas of the interview must be sent in advance. If the data collection schedule is tight, it is a good idea to note that the interviewees calendars may be full. Sometimes the interview has to be arranged weeks, even a few months in advance. Conducting interviews is a challenging part of the research as it is the only stage that requires another person, everything else is up to the researcher. a well-prepared interviewer will normally get good interviews and thus a good research time. (Aarnos, Valli & Raine. 2018).

3.3 Research process

This thesis's research process includes various steps necessary for creating and publishing this thesis with solid and acceptable quality. The thesis could improve working life, which is one of the value points of the University of Applied Sciences in Laurea.

The research process started with identifying the topic and figuring out what could be at the same time relevant to the current situation at 2019-2021 when Covid-19 pandemic was ongoing. The field that was on studying on the author is bachelors degree on safety, security, and risk management, which led the identifying of the thesis to background research about the topic that yielded that there was indeed low availability on data about the title which is both positive and negative.

The positive side is that the topic is new and has a lot to research on. The negative is that there is not that much suitable data available to research that could easily be accessible which is the one of the research problems of this thesis. The most reasonable cause of this problem is that there has not been such impactful pandemic in our near history such as Covid-19 that has affected the industry. (8 Steps in Research Process 2021).

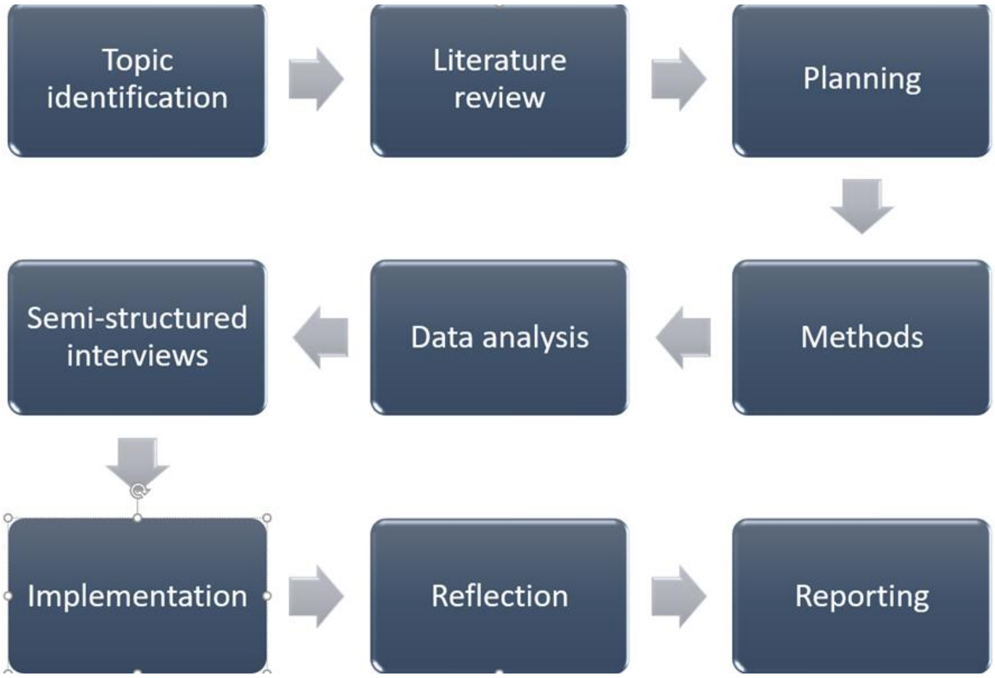


Table 1 Research process

3.4 Ethics and reliability

The subject is ethically correct since the purpose of this thesis is to research whatever the security management field has changed from pandemic. Goal is to only benefit the actual people working on the field and not to harm them or their employees in any way, also on ethical standpoint, this thesis is not trying to achieve a market advantage of any kind. The research subjects include human beings, so sensitivity is required since people should not be listed as objects as premises can be. The thesis goal is not to gather sensitive data or data that may violate anyones privacy or cause harm.

This writings reliability is on point since only reliable sources will be used. Every interview, research, study or article will be traced so that the reader can find reliably where the data is gathered from. No profit is searched from making of this thesis which is purely made to improve the researched working field.

Any sensitive data that could harm certain companies' privacy or publish classified information is strictly forbidden and will not be published in this thesis. The interviewed personnel will be informed of the terms and reasons for the interviews.

3.5 Estimate of resources and costs

This thesis data will come from legitimate sources and have traces on them, as mentioned in the ethics part. This thesis's costs will be approximately from 0€-1000€ depending on what kind of services or possible paid research data will be used doing this thesis. Using document analysis as one of the methods of this thesis could follow that some articles or research results may be under a paywall.

4 Results

Results has two sections. First section includes data by document analysis: research data that is found from existing studies, articles and books that are related to security management during pandemic. Second section goes through semi-structured interviews at Caverion that the author held for this thesis.

4.1 Research data

Business continuity is an essential target for security managers preparing for a pandemic. Many valuable European commission guidelines and council recommendations targeting business continuity and recovery of these sectors and hopes that member states will contribute to coordinated management of the crisis as recently requested by the European Parliament. Coordination of the response to the pandemic at the EU level has been too slow to develop the Covid-19 crisis but has nevertheless proven to be valid. (Private security and Covid in Europe 2020).

Considering that most of the security and risk teams are now mostly operating in completely different environments and mindsets than before pandemics the incident response plans and protocols might become challenged or need to be adjusted to pandemic. Even incidents that would normally be well-managed risks can become bigger issues if the team can’t respond effectively under the new set-ups. (Panetta 2020).

Below a table of survey provided by company named Randori illustrates that the pandemics, especially the Covid-19 does affect the security industry a lot. Attacks have increased, modern challenges have come with the pandemic and organization sizes have changes. The methodology for the survey was done in a way that Randori corporate partnered with a Market Cube which is a third-party research company and they surveyed more than 400 security decision-makers globally to comprehend how Covid-19 pandemic affected their security operations. (How Covid-19 challenged security leaders 2021).

How COVID changed security	(Includes responses of more than 400 security decision-makers nationwide)

75% increase of attacks during pandemic	55% increase spending
55% admit that protecting their attack surface has become more difficult since	44% organizations grew their security teams during pandemic
One in two understand less than 75% of their real-world attack surface	All thought, 25% organizations had to cut security staff of their rosters
42% have been compromised because of shadow IT*	-

Table 2 How Covid-19 challenged security leaders (Randori 2021.)

Sluggish responses to the coronavirus pandemic leaves organizations vulnerable to security breaches. Security and risk teams must remain vigilant and focus on strategic areas. (Security areas to focus on during Covid-19. 2020).

During a pandemic, the security manager should conduct a risk assessment based on the identified threats and update the company's risk registers. Good security management and risk management require an organization to have transparent governance and control of protective security management infrastructure. As so-called risk owners, senior leaders need to be conversant with the fundamental principles of protective security to guide their strategic decision-making. (Managing security risks throughout Covid-19. 2021).

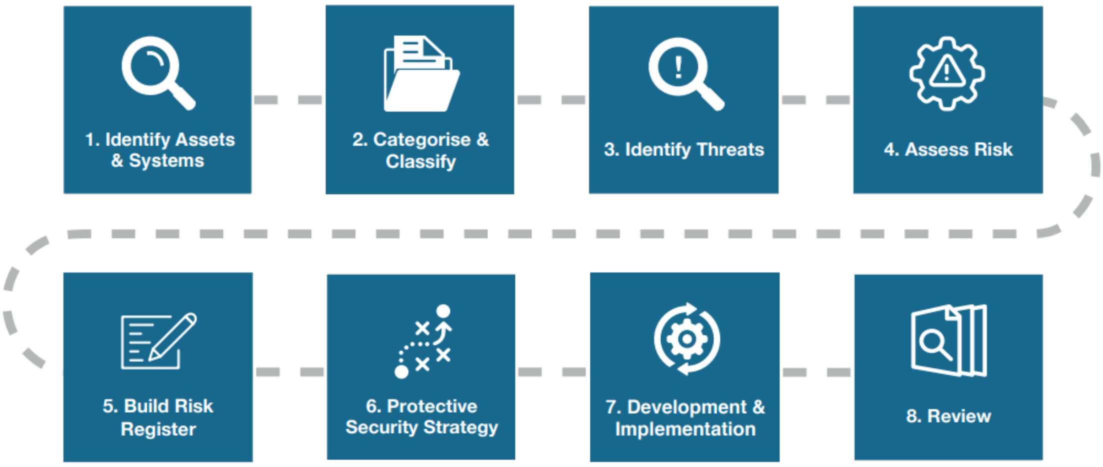

1. Identify Assets & Systems
2. Categorise & Classify
3. Identify Threats
4. Assess Risk
5. Build Risk Register
6. Protective Security Strategy
7. Development & Implementation
8. Review

Figure 1 Protective Security Risk Management, Centre for protection of National Infrastructure 2019.

Above figure illustrates a risk assessment formula that could be used by security manager (not a calculatable assessment matrix but practical). Security teams are suggested to perform a risk assessment before formulating security policies and procedures to answer pandemic adapted working practices. Afterwards these teams should communicate any updates to the security policies and procedures manifestly across the whole corporate network and keep reminding the network about the continued security threats during the period. Important task is to keep proving wellbeing support and clear security guidance to the networks and employees (one way would be to pin to other alert messaging), especially to that are performing remote working. (Pandemic Security 2020).

Since the beginning of the Covid-19 pandemic, the utilization of remote working in companies has been generalized by a lot, forcing people to get comfortable with new ways of working by the usage of their home laptops and new ways of communicating with their colleges and forepersons via skype, teams, or other similar style communication softwares.

At this point, many people working in the office environment have become familiar with remote working to at least understand the concept if not forced or willingly unitizing it. Remote work significantly affects security managers since observing the daily workings inside the company's office buildings has significantly changed. No longer can security manager have a clearer picture of who goes in and out of the company at what time with timestamps from access control instead observing (if needed) of movement of the employees has to be done via online now forcing new ways of observing company infrastructure devices (again if needed.) With the new digital environment, more challenges approach even the management team scheduling their own time and attention to those that need to be managed. As social human beings have less frequent times when seeing each other face-to-face, we will negatively affect our social satisfaction levels, especially those who lack some or any social life connections in personal life outside of the official circles.

Many companies are forcing them to use remote work from the start of the recent Covid-19 pandemic that has made a considerable change in their way of work from the 2020s and counting. A survey published by a time tracking software company in the US called Hubstaff included 400 business owners who were all above the age of 25. 76,75% of the companies that answered the survey were not fully remote before the Covid-19 pandemic, and 23,25% were fully remote already before the pandemic. The survey came up with remarkable results, including that: 66% of companies said that remote work helped them to prevent layoffs due to the pandemic. 44.25% expect remote work to increase profitability and 45.5% productivity. Also, 63.75% of companies expected remote work to make their employees happier. While this result might controversial since it is the business owner’s opinion, still it lights up a thought that new ways of working could make us happier. That way allows us to have a long commitment to the company. The exciting result is that 87.7% of companies reported that employees are interested in continuing remote work possibility after the pandemic. (Pandemics impact on remote work 2020).

The pandemic that boosts people to work from home is creating new challenges for the companies security managers and departments related to security and information. Companies are forced to accelerate their cybersecurity standards to large numbers of employees or face external parties' consequences.

Two-fifths (43%) of people admitted to making a mistake at work that had security consequences, while almost half (47%) of people working in the tech industry told they've clicked on a phishing posts at work. Properly typing, most data breaches occur because of human errors. Hackers aware of this situation and know how to manipulate people into slipping up on them. That's why emails scams, also known as phishing, are so successful. (The psychology behind phishing scams 2020).

47% of individuals fall for phishing scams while working at home

Figure 2 Nabe 2021. People getting scammed by working at home 2021.

Survey states that most data breaches occur because of human errors, so a higher amount of training for company staff should be in place. Employees should be taught to have suspecting feelings towards information security, meaning that if one is starting to suspect feelings from an unknown sender of an email, the employee should contact the companys IT/Cyber department before glancing at the email. If right off the bat, the email title says you have won X then the employee should not in any case open the email. When in doubt one should ask. In most cases it is either a hack or a scam. If one has opened an email even highlighting a mouse over the press here to claim your price button will show the actual link behind the button. Between early of 2020 and middle 2020, more than 500 thousand people worldwide were impacted by data breaches in which the personal data of video conferencing users was stolen and sold on the dark web. The personal data of video conferencing services users (name, passwords, email addresses) was stolen and sold out on the dark web. To perform this attack, some hackers utilized an instrument called OpenBullet. Hackers also use credential stuffing techniques to gain access to employees credentials and the stolen data is then traded to other cybersecurity outlaws. (Nabe 2021).

Having your face or personal data sold on the dark-web or anywhere else does not seem beneficial for one's privacy. Cybersecurity teams on companies should make sure that the communication platform they are using is secured. The device they are connecting from to the meeting online is protected with the company's proper antivirus protection. Also, utilizing VPN at home should be considered by companies to their employees working remotely. (Nabe 2021).

Federal Bureau of Investigation released guidance on defending against video teleconferencing hijacking and performing so called Zoom-bombing. Zoom is a widely used platform in many schools in Finland and globally. Organizations also use this teleconference platform. These guidance tips are do not make meetings or online event public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control guests' admittance. One should not share a link to a teleconference or classroom on publicly available social media post, because it could draw unwanted consequences. Provide the link directly to specific people that are known and are linked to the meeting. Manage screen sharing options. In Zoom, change screen sharing to host only. Ensure users are using the updated version of remote access/meeting applications. Outdated versions are in a bigger risk. In January 2020, Zoom updated its software. In their security update, the software provider added passwords by default for meetings and disabled the ability to scan for meetings to join randomly. Lastly, ensure that your organization’s telework policy or guide addresses requirements for physical and information security. (Online hijacking during Covid-19 Pandemic 2020).

The Wi-fi of households should also be at an intense level since it can provide a gateway for outsiders to access company devices. Creating a unique and robust password is necessary. No one should ever be able to guess ones password. In the optimal case, if resources would allow, home wi-fi should be adequately secured by the company’s IT/Cybersecurity department. This for sure is near impossibility in large-size corporates. However, on smaller to medium-scale companies, it could and should happen. These passwords should ideally include a mixture of lower case and upper-case letters with punctuations and numbers. Kaspersky highly recommends VPN. (Cybersecurity tips for working from home n.d).

Spike in cyberattacks has also happened during the Covid-19 pandemic because small to medium-sized companies have brought the bring your own devices (BOYD) approach to the offices, which practically means that employees are allowed to use their own laptops, tablets, and phones to access companies information. This brings opportunities for attackers to more reliably to get access to companys data. (Nabe 2021).

There has been case where a company employee gave his/her phone to a child to let the child play for a while. The child ended up downloading a gaming portal app which happened to have viruses that infested the company phone and gave a gate away for attacker to gather classified data.

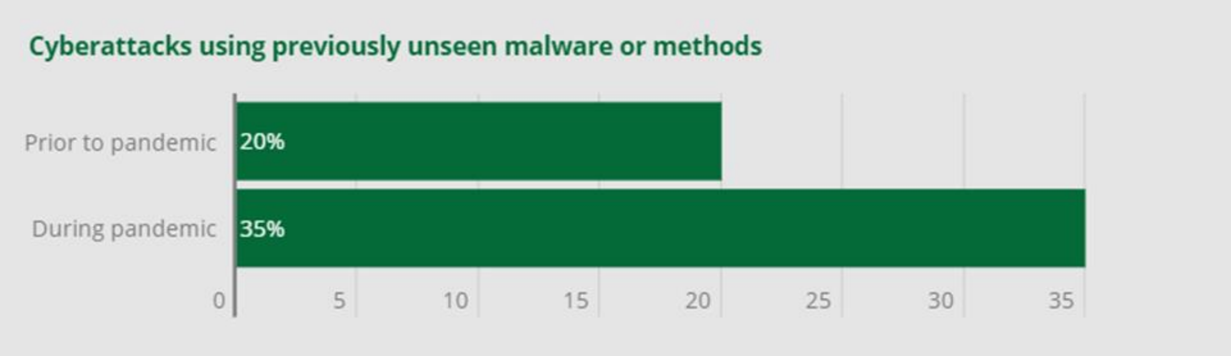


Figure 3 Nabe 2021. Prior to pandemic versus during pandemic cyberattacks 2020.

If working as a security manager on and off pandemic, then Katakri information security auditing tool for authorities should be considered since it is a guideline when arranging the company's facility security clearance and evaluations of the security of authorities information systems. Also, many new possible clients in Finland will most likely ask for it. Also, the public administration's digital security management team's VAHTI-guideline should be considered with Katakri. The minimum requirements based on national legislation and international requirements are gathered in the Katakri. Katakri does not set any strict requirements for information security, but instead the requirements collected in Katakri are based on the legislation and the international information security requirements binding on Finland. (Finnish Ministry for Foreign Affairs. 2021).

Discussed in the book of managing of information security by Whitman and Mattord (2014) managers that are operating a lot of their time in the information security field should familiarize themselves with the ISO/IEC 27001 standards that focuses on information security management (International Organization for Standardization/International Electrotechnical Commission: 27001 Information Security Management 2021). Some companies security managers have to more or less to deal with information security depending on the size, field, country, and organizational style of the company. Also, international SFS-ISO 31000:2018 risk management standards should be considered for achieving excellent security levels by security professionals. (International Organization for Standardization 31000:2018 Risk Management 2021).

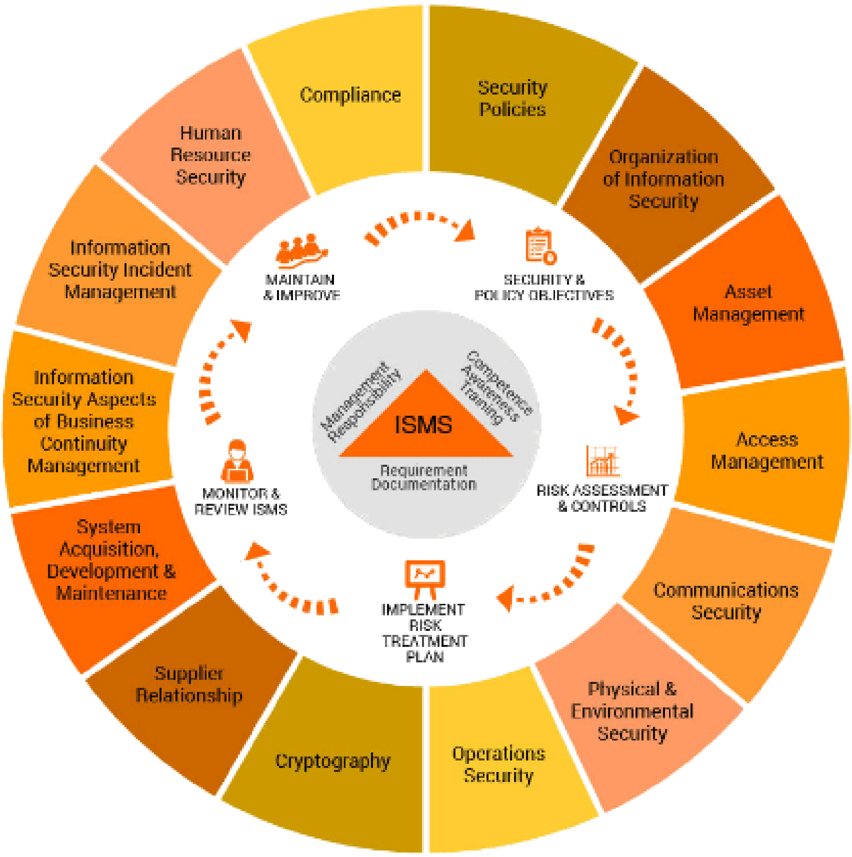

Compliance
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
MAINTAIN & IMPROVE
SECURITY & POLICY OBJECTIVES
RISK ASSESSMENT & CONTROLS
IMPLEMENT RISK TREATMENT PLAN
MONITOR & REVIEW ISMS
ISMS
Management Responsibility
Competence Awareness Training
Requirement Documentation

Figure 4 Information Security Management Cycle (ISO/IEC 27001 2020)

Ways of communication have rapidly changed via the way people work during the pandemic, which forces cultural changes in working life and affects working forever—in contrast, working from home, the role of supervisor changes. To understand communication and how offices will change in the future, security managers must internalize how the industry is changing and how they need to respond to it. Recent covid-19 pandemic has further developed the teleconference systems and overall, the communication and ways of working remotely which allows companies to grow their technology standards. (Dufva 2020).

Seeing how someone is doing cannot be done no more at the office by seeing if they act differently or their mood seems down. Being in touch has a different meaning now by supervisors being regularly and often in contact with employees to know how they are doing and see possible changes in their mood or behavior that could affect work or even in security at some level. Remote supervising importance for social and mental health is grand. That is why remote supervisors responsibility is tremendous and allows supervisors to have a new kind of role in employee’s life. Not so much a boss currently but more of a supervisor who supports their employees in their daily working life. (How the pandemic can change workplace culture for the better 2020).

For many people the lockdown has meant social isolation, a harm many have endured in silence. Theres a reason why solitary confinement is used as a punishment in prisons. Leaders can respond by engaging with their teams and use collaborative technologies to maintain social contact. Before the pandemic mental health awareness was sometimes a slogan. Now it is a necessity. (Thomas 2019).

Working from home has decreased small talks in the office and reduced overall communication. This can have a negative impact on ones social life. Saving money for remote work is a thing for some people by saving on travel costs, food, and time to get to the office and back. Working and life balance are hard to measure since it has increased and decreased, yielding inconsistent results. Working alone creates a less stressful environment for not having peers staring at one's work but can increase the feeling of being alone with work, which can create stress. Having to spend days at home and have more time to leisure and not travel will allow people to have more time to spend with family. Sometimes even too much for some to intake. (Slack Technologies Inc collaboration 2020).

Slacks research found that out of 4,700 workers, only 12% want to return to the full-time office working environments. The rest, 72%, want to implement a hybrid for working remotely and at the office. (BBC online article Coronavirus: How the world of work may change forever n.d). On paper, this could mean that an employee spends a five-week working day mainly at the remote home office but has one to two office days at the week depending on the schedule and if there are meetings, pieces of training, project launches or ceremonies. (Slack Technologies Inc collaboration 2020).

Not for everyone. Workers sense of belonging can suffer while working remotely. The experience of remote work varies across job roles, genders, seniority, and other factors. For instance, experienced remote employees tend to report higher levels of satisfaction and productivity than their less-experienced peers. (Slack Technologies Inc collaboration 2020).

Working at home indeed has its disbenefits since employees are not allowed to see personally during pandemic parts. Having employers host smallish events for teams such as morning coffees and taking walks outside of the house in the nature via having the meeting/conversation running simultaneously will increase the feeling of belonging to the company and decrease loneliness. Referring to the second quarter CNBC/SurveyMonkey Workforce Survey, workers are happier with their jobs than they were pre-pandemic, yet more than half (54%) say their jobs have become increasingly more difficult. On the other side of things, some companies are finding strength from their culture, having been able to successfully navigate during these times. (How post-pandemic office spaces could change corporate culture 2020).

Premises security and office premises play as the platform of many security managers on and off a pandemic. Off from pandemic, they are less occupied, but when pandemic starts going, they usually go on lower occupation. Premises are also affected by pandemics in a different way than people are. The usage percentage of premises, especially office buildings, are reduced to low numbers making the buildings occupancy rate drop highly. From a security standpoint, this can be both negative and positive thing. Positive things are that maintaining and surveilling access control is more accessible, but the negatives cannot be outlooked. (RSA Insurance 2020).

Since most offices are nearly empty during a pandemic, it opens up many opportunities to external forces such as burglary, data stealing, breach, mischief and access to server rooms, and many other possible adverse outcomes to occur. Having the office building on low occupation also dangers the premises to fire and water risks since fewer eyes notice the risks. Gladly modern office premises are usually equipped with at least decent fire and water protection. Following points regarding premise security should be notified by the security managers when premises are occupied on low staff percentage. Have security rounds around the office premises regularly and site checks by security guarding company or appointed security staff from the company. Have the external security lightning on the premises even though they are not occupied. Having lights on premises already mitigates the risk of someone thinking that the premises are clear and empty. (RSA Insurance 2020).

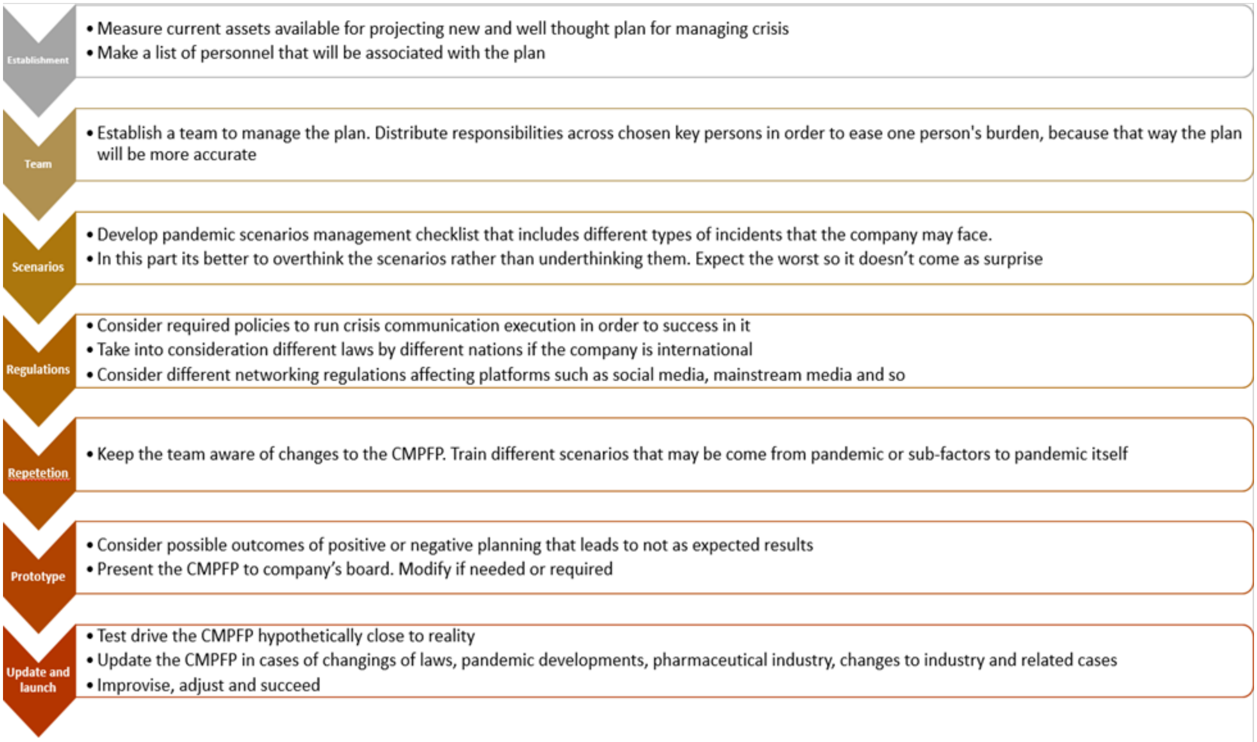
Fire doors should be closed most of the time, but especially if the premises are empty If some parts of the premises are unused during the pandemic isolating. Unused water supplies should be considered (Ones that are not required by fire protection systems or other similar devices) to be closed. Even if the premises are on low occupation, some waste can still be created, which can accumulate into a large pile of waste material that can be a fire risk. This can be a mistake that should be avoided by adjusting the cleaning companies' services depending on the premises' usage. Maintaining a good state of cleanliness helps keep the premises healthy, which is another reason to keep the cleaning services running even though the pandemic might financially hit the company. When company staff starts to return to the office once the pandemic little by little ease, it is much more comfortable to return to clean working environments than to a trashcan. (RSA Insurance 2020).

Unsafe conditions should be rectified, meaning that unoccupied parts of the premises should be maintained as safe environments, if possible, for those with legitimate access to them. Verify that all security and fire alarm systems are fully functioning and having personnel and backup personnel responsible for them identified with a proper action plan in the event of alarm or malfunction. Making sure all locking devices are secure and functioning correctly is essential. Maintain security and fire system checking intervals. Verify that sprinkler valve sets are set to locked/secured on the open position and that systems are live and check that data transfer between security and fire devices is operating correctly. Limit hot works such as soldering, cutting, grinding, brazing, welding, and spark generating unless essential. If the hot works site is sprinklered, avoid hot work if sprinklers are impaired. Hot works shall not be performed unless the required number of trained staff is available. (RSA Insurance 2020).

Securing safe passage on emergency exits even if it would be rare for someone to utilize that exit. Emergency lights also need to function correctly in case of a fire emergency. Checking their condition is crucial. On premises where there are no security lights picking off the dust from sticky labels of emergency indicators should be performed. (RSA Insurance 2020).

Pre-Covid many companies had for business continuity plans for a financial crisis. For example, the 2007-2009 financial crisis is still in many large companies memory (Financial Crisis 2015). However, not many could predict the future that the early 2020s brought and how the vital responsible people for companies' business continuity should have planned beforehand.

Establishing a crisis management team prior to the pandemic outbreak is strongly advised. Having a team ready to take and report activity to the company is essential to its survival in any crisis. Looking at Security Snapshots online interview with Phillip’s Global Head of Physical and Personnel Security Michael toe Water. Water states that they have an operational crisis management government group is below the board and executive members. Under the crisis management team, there are human resources, insurance, and real estate. It is easy to have crisis management meetings and coordinate efforts returning to work, supply chain, manufacturing security, and related factors. Having an operational team below the group crisis team makes it very easy for them to align with all enabling functions in Phillips. Having a specific minimum number of employees to work at specific working tasks needs to be thought out carefully so that when pandemic starts/evolves, the company’s assets match the required need of people to perform critical tasks to keep the company competitive running. Challenges such as quarantines reduce the number of people available to carry out jobs requiring physical presence such as factorys, cleaning, security guarding, retail, and so on. Having a set amount of number for minimum capacity before the company starts to recruit available people to carry out the minimum number to carry out critical jobs for the corporates survival needs to be thought of. Utilizing hiring companies or reserve staff for the company could come into play and decide whether the pandemic is lethal or not. (Snapshot 2020).



Establishment

- Measure current assets available for projecting new and well thought plan for managing crisis
- Make a list of personnel that will be associated with the plan

Team

- Establish a team to manage the plan. Distribute responsibilities across chosen key persons in order to ease one person's burden, because that way the plan will be more accurate

Scenarios

- Develop pandemic scenarios management checklist that includes different types of incidents that the company may face.
- In this part its better to overthink the scenarios rather than underthinking them. Expect the worst so it doesn't come as surprise

Regulations

- Consider required policies to run crisis communication execution in order to success in it
- Take into consideration different laws by different nations if the company is international
- Consider different networking regulations affecting platforms such as social media, mainstream media and so

Repetetion

- Keep the team aware of changes to the CMPFP. Train different scenarios that may be come from pandemic or sub-factors to pandemic itself

Prototype

- Consider possible outcomes of positive or negative planning that leads to not as expected results
- Present the CMPFP to company's board. Modify if needed or required

Update and launch

- Test drive the CMPFP hypothetically close to reality
- Update the CMPFP in cases of changings of laws, pandemic developments, pharmaceutical industry, changes to industry and related cases
- Improvise, adjust and succeed

Table 3 Crisis management plan for pandemic. n.d. (CMPFP)

Above is a development guideline based on research that gives a hand to security managers wanting to develop precisely. A crisis management plan for pandemic (CMFPF) targets to improve the conditions of companies that are willing to develop a plan for pandemic crisis management. Without a plan, the companies are more likely to falter. Better to be well prepared than not prepared. Currently, in Finland, where the pandemic is still roaming, the required number of days that one needs to be quarantined is 14 days (Finnish Department of Health and Welfare 2021). Meaning for two weeks, one employee/employer is away for a task that may be critical. Multiplying that number hundreds or even thousands can be devastating for a company with no plan to survive such a fatal incident. A business continuity plan for significant hazards or accidents should also be considered not straightly for pandemics but the company's overall crisis capability. For example, a large internal explosion in a nuclear power plant would lead to catastrophic events not only for the company's revenue but also for the environment and people affected by the range of explosion, not to mention the brand damage that would come out of it.

4.2 Interviews

interview from Caverions corporate security and premises manager Juha E. Salminen on how the security management has changed from pandemics, the reply was that: clearly security management has changed to more hectic, the changes of Covid-19 have required more and more following of the situation and wide subordinate on a national level. Co-operations and communications with different organizational departments on the company have increased regarding the companys security. These departments are, for example, human resources, business management, company wellbeing, and property managers. After the pandemic has been going on for some time the security planning should be upgraded to match the current situation and requirements to fulfill the same security level as when the pandemic is off. The requirement for the business is that the level of security does not change whatever happens. This is part of business continuity, and if it is not possible for the corporation, aiming for it must be a high priority. (Salminen 2021. Personal communication).

What things should security managers take to their attention on new everyday work when the pandemic is still going: Again, pandemic or not the security needs to be at the same level in the company. The most affected aspects would be occupational safety and personal safety, with health security being one of the biggest challenges. Also, the way that the companys office squares are used has been taken into a note so that a safe working environment stays for those who wish to work at the office. (Salminen 2021. Personal communication).

How the pandemics has affected the security of the premises: the security of the premises is not so much affected since it keeps itself inside a shell of protection, camera surveillance, access control, and related devices, but the importance of premise security devices has increased in that way that there are less pair of eyes at the office. Systems must be functional even when fewer people are looking after companys or customers information material. (Salminen 2021. Personal communication).

Some companies security managers have more than one primary job description on their arsenal; for example, Caverions security manager is currently also handling the companys premises management. When asked how the pandemics changed office premises management, the reply was that rethinking usage of office squares in smarter way is in order so that costs and space efficacy are adjusted so that the facilities match the purpose needed. Certainly, the pandemics has taught many companies for future usage of premises and will surely affect companies usage percentage in future. (Salminen 2021. Personal communication).

How pandemics had changed business continuity planning: Business continuity plans before Covid-19 were made, but this kind of pandemic on such a large scale was not straightly anticipated. Thoughts of staff civil protection, evacuation, and related were. However, the battle for acquiring disinfectant machines and face masks was unexpected for many companies out there. After a pandemic, for sure, there will be considered that did the plans match the actual Covid-19 pandemic that happened. Gladly a deviation and crisis planning guideline for crisis communication was made before the pandemic started, which helped a lot since on the launch of the Covid, a crisis messaging channel for Caverion was made by the IT department. A team responsible for maintaining its informative part was established, making the pandemic start optimally as possible for the company. (Salminen 2021. Personal communication).

Interviewing Caverion's quality- and environmental manager Jorma Kekki, who is also responsible for information and cybersecurity in Caverion, about how the pandemic has affected information/cybersecurity in the company: Covid-19 from the companys perspective started in a general hassle in the beginning. Despite of everything, the situation came unexpectedly. People were sent to work remotely and counting of resources and capacity when doing so was aloft. Moving to remote work was quick, and the so-called growing to it happened fast. At this point, Caverions remote work is at its highest, and the office is silent. Regarding information and cybersecurity, one of the issues at starting of the pandemics was the information technologys limitations, also issues such as how people know how to use the right tools to complete their work and guiding key personnel. Establishing practical living to manageable brings the base for normal working conditions and knowing how to use tools securely even and especially from home. Affection to present time in such a way that it has developed perspectives and experiences from the topic and how the level of information and cybersecurity has been upgraded even at a technical level. It could be said that pandemic has brought positive and negative things from that perspective. Maybe firstly the negatives and after the positives. (Kekki 2021 Personal communication).

One of the biggest concerns regarding people working from home, in general, is how much the pandemic affected classified information handling. Are the documents kept safe physically safe from outsiders and even family members and accesses denied from any other than the staff member to company devices? In that way, information security has also been affected negatively since the devices are taken away from secure office premises to secure home establishments. The same level of security regarding classified information should be kept no matter what the physical location of the document is. (Kekki 2021. Personal communication).

What things should be considered so that working remotely from home could be safe: The standard classified information rules should be followed. Caverion has even a set of rules regarding the topic (cannot show on this thesis because of classification). The rules keeps inside a checklist that requires the security requirements fulfilled for the work to happen at any working place site. They also have a data classification guideline on usage of data and its distribution, mitigating or even preventing mistakes from the company staff members themselves. (Kekki 2021. Personal communication).

How modern companies handle business continuity? Business continuity is partly made more secure having proper guidelines and processes. Incorporate security continuity and risk management are part of the well-planned wholeness of the companys security. Just by securing remote working does not fix the whole problem but is a part of a bigger picture. Pandemic is “just a thing” that could have came earlier and is only one risk out of many of them out there. On the brighter side of things, at this point, the recent pandemic has been lived for more over a year, and problems have been solved if and when they have shown up. At this point, our performance rate is excellent even though the company is performing mainly remotely. In public, it has been shown that remote working is here to stay in the future, and business continuity plans should be adjusted accordingly. (Kekki 2021. Personal communication).

The same problems regarding remote workings information security are here to stay until the technology and industry supporting life between office and home working have advanced further. Gladly people can now communicate faster than ever (easier scheduling, data transfer, no traveling times, or restrictions, and so on), which has actually developed companies that in contrast require the following of security regulations even deeper, so that security could still be kept in acceptable level. It could be said that a pandemic is such a wake-up call and test for companies to see if the homework was done before Covid. Observing bigger picture, it could be said that pandemic has brought much learning and things have been developed rapidly for sure in many of the companies. (Kekki 2021. Personal communication).

5 Conclusions

Conclusion section is a comparison between the document analysis research data found in results section and the Caverion semi-structured interviews section. There are clear similarities between the found data and the interviews. The interviewed personnel representing Caverion are aware of business continuity, crisis management and the affects of moving employees to work remotely so that the company may emerge better from pandemic. As for the impact of pandemic on case company security seems to be mild, but more so the impact has been on premises management and employees ability to work more safely on remote working conditions. Since being able to work remotely greatly decreases the changes of getting infected by co-workers possible infection. Adjustments on how premises are managed more securely are done in companies in general but, also in case company since less pair of eyes are observing the premises meaning that the importance of alarm systems has increased a lot.

Like many companies also the case company had business continuity plan for pandemic, but not on such large as we have had the pandemic. Gladly nothing crucial has happened and the companys operations have been adjusted in safer way. Business continuity plans will be updated for sure for the future.

Researched data states that attacks on companies has increased during pandemic by third. Fortunately, case company seems to be unaffected by such attacks. As many companies has had challenges on new ways of working remotely so has the case company. Handling classified data on outside of company premises is still a challenge as not all staff members take or notice safety and security as important as the people working on the field. Classified data may be on kitchen table, phones might be borrowed to children and laptops left without locking.

Researched data states that crisis management team should be established prior to pandemic. When pandemic started case companys IT department launched company communication portal for case companys security team to manage, which was a great way to inform the company staff of the evolvement of Covid-19 so that stakeholders could better inform the situation of pandemic to employees more easily. This was due well planned crisis management plan. This declares that having a well-made business continuity and crisis management plant will help companies to thrive through pandemic on better results than they would have without them. The most affected aspects of Covid on case company would be occupational safety and personal safety, with health security being one of the biggest challenges. This leads us to conclusion that yes, security management during pandemic indeed has changed on case company and, also on other companies worldwide which just raises the importance of qualitative security management on enterprises.

References

Printed

Aaltola, J., Laajalahti, A., Valli, R. 2018. Ikkunoita tutkimusmetodeihin. 2, Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. PS-kustannus.

Aarnos, E. & Valli, R. 2018. Ikkunoita tutkimusmetodeihin. 1, Metodin valinta ja aineistonkeruu. PS-kustannus.

Huovinen, P., Ziegler, T. 2011. Influenssa: pandemiaviruksen päiväkirja. Duodecim.

Korhonen, E., Moisio, J., Tuominen, K. 2003. Turvallisuusjohtaminen. Benchmarking Ltd Oy.

Whitman, E. & Mattord, H. 2014. Management of Information Security 4th Edition.

Electronic

Algosec. Examining the Impact of Security Management on the Business. Accessed 2 March 2021.
https://www.algosec.com/wp-content/uploads/2016/03/impact_of_security_management_on_the_business.pdf

Centre for the Protection of National infrastructure 2021. Managing security risks throughout COVID-19. Accessed 8 June 2021.
https://www.cpni.gov.uk/security-risks-throughout-covid-19-0

Geller, J., & León, R. CNBC 2020. How post-pandemic office spaces could change corporate culture report. Posted 18 May 2020.
https://www.cnbc.com/2020/05/18/how-post-pandemic-office-spaces-could-change-corporate-culture.html

COVID-19 and Crisis Management Planning Security Snapshot interview. 2020. Directed by ASIS International. Accessed 12 February 2021.
https://www.youtube.com/watch?v=PPu5emGm-L8

Nabe, W. 2020. Deloitte. Article impact of Covid-19 on Cybersecurity. Accessed 15 February 2021.
Impact of COVID-19 on Cybersecurity (deloitte.com)

Bowen, G. 2009. Document Analysis as a Qualitative Research Method. Accessed 27 December 2020.
https://www.researchgate.net/publication/240807798_Document_Analysis_as_a_Qualitative_Research_Method

Setera, K. 2020. FBI Boston. Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. Posted 30 March 2020. Accessed 20 May 2021.
https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Finnish national contingency plan for an influenza pandemic 2006. Helsinki, Finland.
https://laurea.finna.fi/Record/valto.10024_73712

Linnanmäki, E. n.d. Finnish National institute of public health. History of influenza Pandemics. Accessed 5 March 2021.
https://www.julkari.fi/bitstream/handle/10024/90766/duo95933.pdf?sequence=1

Panetta, K. 2020. Gartner. Security Areas to Focus on During COVID. Posted 18 November. Accessed 2 January 2021.
https://www.gartner.com/smarterwithgartner/7-security-areas-to-focus-on-during-covid-19/

iEduNote. Guide on Research Process: 8 Steps in Research Process. 2021. Accessed 13 May 2021.
https://www.iedunote.com/research-process

International Organization for Standardization. 2021. 31000:2018 Risk Management.
https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-31000-riskienhallinta/

International Organization for Standardization/International Electrotechnical Commission. 2021. 27001 Information Security Management. Accessed 7 June 2021.
https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization/International Electrotechnical Commission. 2020. 27001 Information Security Management Figure.
ISO/IEC 27001 Information Security Management - ServiceDesk Academy

JobJob. n.d. Online job description to security management. Accessed 29 December 2020.
https://www.jobisjob.com/security+manager/job-description

Kaspersky. n.d. Cyber Security Risks: Best Practices for Working from Home and Remotely. Accessed 3 January 2021.
https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

Finnish Ministry for Foreign Affairs. 2021. Katakri. Accessed 11 May 2021.
Katakri – tietoturvallisuuden auditointityökalu viranomaisille - Ulkoministeriö (um.fi)

Randori. 2021. Look at how COVID-19 challenged security leaders. Accessed 16 August 2021.
https://www.randori.com/how-covid-19-changed-security/

Thakor, A. 2015. The Financial Crisis of 2007–2009: Why Did It Happen and What Did We Learn? Article from Oxford Academic. Accessed 7 June 2021.
https://academic.oup.com/rcfs/article/4/2/155/1555737

Behaviours Centre for Protection of National Infrastructure. 2020. Pandemic Security. Accessed 9 June 2021.
https://www.cpni.gov.uk/system/files/documents/13/ca/CPNI%20Pandemic%20Security%20Behaviours%20Update%20-%20Nov%202020.pdf

Finnish Department of Health and Welfare 2021. Quarantine and Isolation. Accessed 16 March 2021.
https://thl.fi/fi/web/infektiotaudit-ja-rokotukset/ajankohtaista/ajankohtaista-koronaviruksesta-covid-19/tarttuminen-ja-suojautuminen-koronavirus/karanteeni-eristys-ja-karanteenia-vastaavat-olosuhteet

Triad, T. Research methodology in education. 2016. Introduction to document analysis. Posted 9 March 2016. Accessed 21 December 2020.
https://lled500.trubox.ca/2016/244

Adams, W. 2015. ResearchGate. Conducting Semi-Structured Interviews. Accessed 14 January 2021.
https://www.researchgate.net/publication/301738442_Conducting_Semi-Structured_Interviews

Resources Workable. n.d. Security Manager description. Accessed 5 February 2021.
https://resources.workable.com/security-manager-job-description

RSA Insurance. 2020. Covid-19 Outbreak: Premises Safety and Security Risk report.
https://www.rsabroker.com/system/files/RSA%20Risk%20Control%20Bulletin%20-%20COVID-19%20Outbreak%20Premises%20safety%20and%20security%20v.3.pdf

Dufva, M. 2020. Sitra. Technology brings opportunities and threats to post covid era. Accessed 7 July 2021.
https://www.sitra.fi/artikkelit/teknologia-tuo-koronanjalkeiseen-aikaan-paljon-mahdollisuuksia-ja-muutamia-uhkia/

Slack Technologies Inc. 2020. Collaboration survey. Accessed 3 January 2021.
https://slack.com/blog/collaboration/workplace-transformation-in-the-wake-of-covid-19

Thomas, J. Strategy&. 2019. How the pandemic can change workplace culture for the better. Accessed 17 March 2021.
https://www.strategyand.pwc.com/m1/en/articles/2020/how-the-pandemic-can-change-workplace-culture-for-the-better.html

Sadler, T., & Hancock J. Tessian. 2020. Why We Click: The Psychology Behind Phishing Scams and How to Avoid Being Hacked.
https://www.tessian.com/blog/why-we-click-on-phishing-scams/

Confederation of European Security Services (CoESS). 2020. The New Normal 2.0: Private Security and COVID-19 in Europe. Accessed 16 May 2021.
https://www.coess.org/newsroom.php?news=Beyond-COVID-19-Private-Security-Services-call-for-Political-Action

Nevogt, D. 2020. Hubstaff. The Pandemics Impact on Remote Work & Where We Go From Here. Published 20 August 2020. Accessed 16 January 2021.
Exclusive Report: The Impact of the Pandemic in Remote Work (hubstaff.com)

Wellcome 2020. From equality to global poverty: how Covid-19 is affecting societies and economies. Accessed 12 March 2021.
https://wellcome.org/news/equality-global-poverty-how-covid-19-affecting-societies-and-economies

Online website Caverion 2021. About Us. Accessed 25 December 2020.
https://www.caverion.com/about-us/

Wikipedia. 2021. Last modified 13 November 2021. Article On Security Management. Accessed 5 May 2021.
https://en.wikipedia.org/wiki/Security_management

Unpublished

Crisis management plan for pandemic (CMPFP)

Kekki, J. Quality- and Environmental Manager. Caverion Suomi Oy. Interview with the author 4.2021. 1.4.2021a. Vantaa. Personal communication.

Kekki, J. Quality- and Environmental Manager. Caverion Suomi Oy. Interview with the author 4.2021. 1.4.2021b. Vantaa. Personal communication.

Salminen, J,E. Corporate Security and Premises Manager. Caverion Suomi Oy. Interview with the author. 1.4.2021b. Vantaa. Personal communication.

Salminen, J.E. Corporate Security and Premises Manager. Caverion Suomi Oy. Interview with the author. 1.4.2021a. Vantaa. Personal communication.

Figures

Figure 1 Protective Security Risk Management, Centre for protection of National Infrastructure 2019. 15
Figure 2 Nabe 2021. People getting scammed by working at home 2021.......... 17
Figure 3 Nabe 2021. Prior to pandemic versus during pandemic cyberattacks 2020. 19
Figure 4 Information Security Management Cycle (ISO/IEC 27001 2020) 20
Figure 5 Thesis timetable plan 36

Tables

Table 1 Research process.......... 13
Table 2 How Covid-19 challenged security leaders (Randori 2021.).......... 15
Table 3 Crisis management plan for pandemic. n.d. (CMPFP) 24

Appendices

Appendix 1: Thesis timetable plan 36

Appendix 1: Thesis timetable plan

The idea and planning for this thesis started on 8.2020, but for a while was on thinking/pause period since working and studying at the same time was taxing for the thesis. After completing internship and most of the other studies the thesis had full attention which was on around the late of 2020. Early of 2021 to late of 2021 was the major time period this thesis was done.

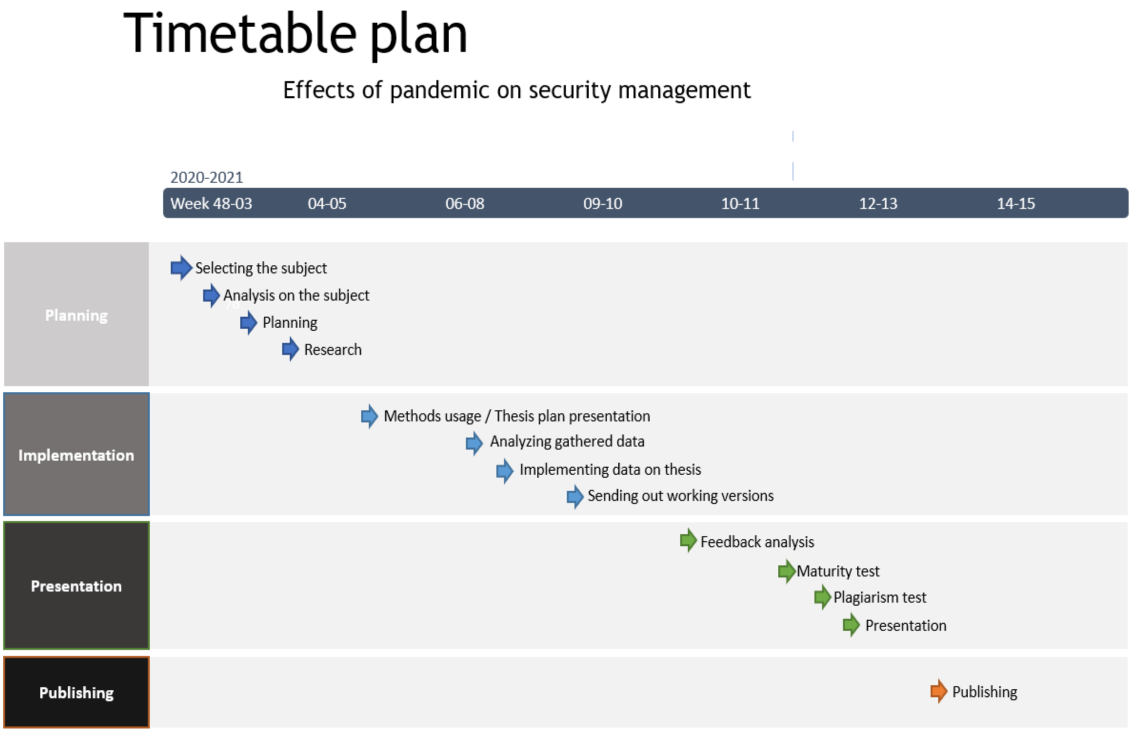


Figure 5 Thesis timetable plan