Cybersecurity development and business continuity plan for car dealership

Santeri Valasvuo

2022 Laurea

Laurea University of Applied Sciences

Cybersecurity development and business continuity plan for the car dealership

Santeri Valasvuo

Degree Programme in Security Management

Bachelor’s Thesis

June, 2022

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's thesis

Abstract

Santeri Valasvuo

Cybersecurity development and business continuity plan for the car dealership

2022 Number of pages 27

The purpose of this thesis was to investigate the capability of the case company to meet the challenges of current and growing security threats and to come up with a development plan to increase the level of cyber security and its active monitoring. There was also need for business continuity plan if security will fail.

As a result of the research, the technical and human capabilities to protect against cyber-attacks in business will be determined. The General Data Protection Regulation (GDPR EU 2016/679) generally defines standard requirements for the protection of personal data at EU level, but there are currently no legal requirements for security. But for the GDPR regulation itself to be compliant with the law, it requires good data security.

Process analysis revealed two main threats for cybersecurity in the case company, which are social engineering and ransomware. As data collection methods, the study uses the mapping of relevant systems, analysis together with the IT team, interviews and Traficom's self-assessment tool.

In this study, the company's strengths and weaknesses in cybersecurity were discovered and the development plan was created. Development plan was divided to three stages that forms security layers from foundation to critical processes and key activities.

The case company also wanted to know, what would it cost to improve cybersecurity, so a approximate budget was created by using the request for proposals from possible partner companies. To ensure business continuity we made plan for some manual procedures that will take place if ever needed.

Keywords: Cybersecurity, Cyber awareness, continuity plan, social engineering, ransomware, NIST framework

Table of Contents

1 Introduction 5

2 What is cybersecurity all about 6

2.1 Four-pillars approach to cyber security 6

2.2 Trust as a part of security 8

3 Top cybersecurity threats for car dealers 9

3.1 Focusing on two major threats 9

3.2 Risk management 10

4 Methods 11

4.1 Interview & RFP from partner companies 11

4.2 Traficom’s cybermeter 12

5 Results 14

5.1 Results from interview 14

5.2 Results from Cybermeter 16

6 Development plan 17

6.1 Stages of development plan 18

6.1.1 Stage 1: Foundation security 19

6.1.2 Stage 2: Critical Processes 19

6.1.3 Stage 3: Key Activities 20

6.2 Investment budget for security development 20

6.3 Developing a business continuity plan 21

6.4 Scenarios 23

6.4.1 Used cars sales - Websales not usable 23

6.4.2 New Car Sales – Websales not usable 23

7 Conclusion 24

8 References 25

9 Figures 26

10 Tables 27

1 Introduction

Cyber threats related to information security are growing every day and they are reported daily in Finland also. Especially during the war in Ukraine and discussions on joining NATO are active. Car dealerships can also be attacked, for example when the Internet is down or when a denial-of-service attack prevents systems from operating. Although it is generally thought that the car dealership is not an interesting target all smaller companies, which may not have as good a level of security as large companies are more interesting targets for cyber-attacks. This will make it easier to set up malware and claim ransom. On the other hand, government actors primarily hit supply security chains, operators, and healthcare. The system services operate in common data centers with other service providers, with whom car dealerships may be targeted. So, the risk is real.

The case company of this thesis is a full-service car dealership operating in Finland that sells new and used cars and offers maintenance and spare parts services for them. The size of the staff is about 500 people, and the annual sales volume of cars is 15,000 and the number of repair orders is about 120,000. The company's IT is largely outsourced, but development and risk management are done by the personnel of the company. The industry is facing a significant transformation and profitability in the industry is generally weak. Sales of new cars have frozen due to a shortage of components that started from the Covid-19 and keeps on continuing after the war in Ukraine started. This leads to a limited budget from a security perspective when it is more needed than ever.

Research aim and questions

The aim of this study is to produce a development plan and to provide evidence to the company management to improve cybersecurity and to make investment budget for employee training and other services needed to increase the security. For example, possible soc services. Risks taken into consideration can be personnel, technical ability, processes, or willingness to invest in security.

The research questions are:

- "How to cope with growing needs of cybersecurity threats as a car dealership?"
- "What is the cost of improving cyber security in car dealership?"

2 What is cybersecurity all about

It is protection by technical means, staff training, the feeling that nothing bad will happen. Cyber security concerns us all, it is a new civic skill. Not everything can be protected, so you also must be prepared for the worst to keep your business going.

According to Mahalingam Ramkumar (2016) “The information age is characterized by a steady conversion of national, organizational and personal assets into bits, or digital assets.” The growing need to protect digital assets has drawn researchers from a wide range of disciplines to the emerging field of cybersecurity. On one side, this surge has resulted in a significant rise in the number of tools accessible to address this pressing issue. However, this surge has diluted some of the science of security's core foundations. The risks rise in line with the capability to accomplish more with technology and data. A single security event that compromises the safety of a company's customer might harm the company's reputation and mark the untrustworthy. (Ramkumar 2016.)

Understanding cybersecurity risks and determining measures to decrease them to acceptable levels is only possible when both the human and technological components are considered. These concerns require not only technical answers and solutions, but also responses and interventions from governments, regulators and policymakers, businesses and organizations, and even end users. (van den Berg & Keymolen 2017.)

Every Company should provide a clear measurement of risk and capture current risks to the organization and demonstrate how cyber risks will be managed going forward (Valonen & Halldin). This means that they should provide a clear picture of existing cyber threats and capabilities to address them, assisting companies in understanding why and how to invest in cyber risk management. Also, building a more risk aware culture by training the employees awareness is a important measure to reduce the impact of human behaviour (Valonen & Halldin).

2.1 Four-pillars approach to cyber security

It's a common misconception that cyber security is all about technology. Although technology is an important part of cyber security, it is not enough to protect you from modern cyber threats. Cyber security consists of technologies, processes, and policies to protect people and businesses from cybercrime. Through the deliberate exploitation of systems, networks, and technologies, effective cyber security reduces the risk of a cyberattack. (Dutton 2017.)

An information security management system built on three pillars seen in figure 1: people, processes, and technology. They are required for effective and robust cyber security (Dutton

2017). The company may have the technology in place, but if proper processes are not in place and the employees aren’t trained on how to use it, a company is leaving the business vulnerable to the human factor. During the case study, an extra pillar, such as willingness and risk appetite, was addressed by company's IT manager. The company prefers its resources to business application development and training, rather than security measures.

There are two important aspects to consider. First and foremost, everyone in the company must understand their role in preventing and reducing cyber threats, whether it's handling sensitive data or recognizing phishing emails. Cyber security is a business issue in which everyone has a role to play. A good security awareness program can help to reduce the risk of people being exploited by cyber threats. Secondly, there's the highly trained technical cyber security personnel. They must have the most up-to-date skills and qualifications to ensure that appropriate controls, technologies, and practices are in place to fight the latest cyber threats. Staff who aren't up to date on cyber security issues have an impact on the organization's ability to mitigate and respond to cyberattacks. However, the highly skilled security professionals are usually works for a subcontractor. In case company IT is more focused to developing digital services and basic IT infrastructure, but they must have a basic understanding of security environment. (Dutton 2017.)

Processes are critical to the successful implementation of a cyber security strategy. The key elements for defining how the organization's activities, roles, and documentation are used to mitigate risks to the organization's data. Cyber threats change quickly, and processes need to adapt to stay current. Processes, on the other hand, are worthless if people don't follow them correctly. (Dutton 2017.)

When it comes to cyber security, technology is obviously critical. After identifying the cyber risks that the company may faces, management can start thinking about what controls to implement and what technologies the company needs to do this. Depending on risk assessment and what is considered as an acceptable level of risk, technology can be used to prevent or reduce the impact of cyber risks. (Dutton 2017.)

Based on the interview during the study it seems that small and medium-sized companies find it difficult to make investments to improve cybersecurity, even though they are aware of its importance. They are more likely to believe that their industry is not a target of cyberattacks or that their technology is able to maintain protection, so their willingness to invest is significantly too low. This kind of risk appetite may lead to a cyber-attack that causes economic and reputational losses.

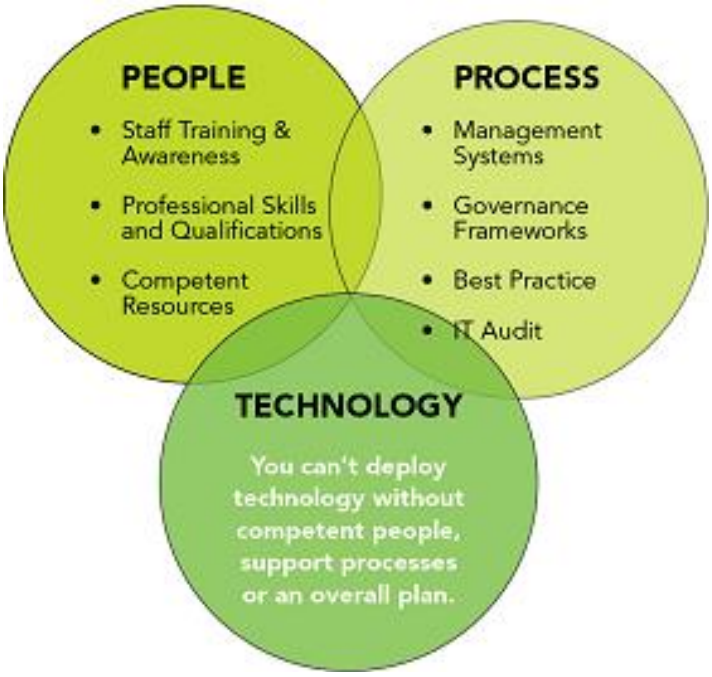

PEOPLE
Staff Training & Awareness
Professional Skills and Qualifications
Competent Resources
PROCESS
Management Systems
Governance Frameworks
Best Practice
IT Audit
TECHNOLOGY
You can't deploy technology without competent people, support processes or an overall plan.

Figure 1: Cybersecurity consist of four parts

2.2 Trust as a part of security

“Without some basic sense of trust, we would not be able to get up in the morning.” (van den Berg & Keymolen 2017). Trust is a technique for dealing with the challenges of life. The fact that we are aware of the unpredictability of the future and that we cannot predict all of the acts of others requires trust in order to set aside some of these uncertainties. To trust is to act as if we know for certain what tomorrow will bring, while in fact we are groping in the dark. Having positive expectations about others' actions is intimately linked to trust. When we put our trust in someone, we want them to act in our mutual benefit rather than their own. (van den Berg, B & Keymolen 2017.)

While employees are essential to any business, they can also be a major source of data loss due to careless or criminal behaviour. Knowing this, an organization's IT personnel must take the appropriate steps to permit various modes and means of working that benefit both people and the business, but without risking sensitive data and systems. (Bush 2019).

3 Top cybersecurity threats for car dealers

Every company is a digital company and digital security (cybersecurity) is about reputation management, ensuring business continuity and customer trust (Limnéll 2022). Resilience is one of the keywords and actions of security for this decade. In a fast-changing world, we will inevitably face different, intentional and unintentional, disruptive and exceptional situations. There is no reason to rely on one card. (Limnéll 2022.)

Security is also a feeling, and achieving it is becoming increasingly difficult. Communication is becoming increasingly important in terms of security, and we must be both active and honest in our communication (Limnéll 2022). Approximately 91 percent of cyberattacks on car dealers involve social engineering, or the use of fraud to trick people into doing something they shouldn't (Reddock, G).

The biggest risk for car dealers of all sizes is the increase in phishing messages (Baggott 2021). Ransomware is a type of malware that typically infiltrates the internet via phishing and phishing emails. When the tightening programme is activated, even the most recent backups are encrypted, making file restoration from the most recent backups impossible. Usually, the only option is to pay a ransom. If the ransom is not paid, the system may be forced to return to a very distant past or rebuild the databases from scratch. (Baggott 2021.)

Customer data is especially vulnerable, as car dealers increasingly rely on harvesting and storing it. Cybercriminals understand the value of this information if it is stolen, and the automotive industry is very likely to be among the top cyber-attack targets. (Baggott 2021.)

3.1 Focusing on two major threats

Cybercrime is the fastest growing type of criminal activity. Almost half of all cyberattacks are directed at small and medium-sized businesses. It is a matter of when, not if, a dealership will be the victim of a sophisticated cyberattack. Auto dealerships are especially vulnerable to social engineering and ransomware attacks. (Nachbahr 2020).

Social engineering is a type of attack that manipulates individuals into doing something that benefits the cybercriminal. This includes phishing, spear phishing, business email compromise (BEC), and CEO fraud. Hackers will send spoof emails appearing as dealership management or other senior executives, requesting to do something for what appears to be a valid reason. The purpose of these attacks is to obtain money. (Nachbahr 2020).

Spoofed emails from employees asking for change to their direct bank deposit are another example of social engineering attacks. Another common way of social engineering is a email from a colleague that asks someone in accounts payable to pay an invoice. Despite the fact that the invoice and company are both fake, the cybercriminals will get the money if paid. Hackers can also gain access to companys network if an employee clicks on a link or opens a attachment file from a phishing email. They may attempt to steal login credentials for financial accounts in order to transfer funds out, or they may locate and steal customer data in order to monetize it. (Nachbahr 2020).

Ransomware is a type of malware that most often infiltrates the network through phishing and spear phishing emails. An example of this is getting an email that looks like it came from a colleague or someone you might know that has a message and a file or a link to a website attached to it. Opening this file or link will download a ransomware on the computer. After that it spreads throughout the computer network of the company. Ransomware is dangerous because it can go dormant for weeks or months. Backups of your data taken during the dormancy period will also include the ransomware. (Nachbahr 2020).

When the ransomware goes live, your most recent backups will also be encrypted, making it impossible to recover your files from them. The cyber-criminals demand a ransom to break the encryption of your files and restore access to them. There are two options at this point. Pay the ransom or risk losing all of your files and data. To make the transaction untraceable, most cyber thieves demand the ransom in crypto currency. (Nachbahr 2020).

There has recently been an increase in a type of ransomware attack in which hackers threaten to release customer data if they are not paid by the deadline. (Nachbahr 2020.) This makes car dealerships vulnerable, because they store a lot of customer data and if they are leaked by cyber-criminals, the company is responsible for that. Because most small and mid-sized companies can't afford the downtime and inaccessibility to critical data, they often end up paying the ransoms.

3.2 Risk management

Risk management is a key concept in both security and resiliency. Owners and operators of critical infrastructure are uniquely positioned to manage risks to their individual operations and assets, and to develop effective strategies to make them more secure and resilient. (CIS.)

Traficom (Finnish Transport and Communications Agency) provides a free NIST Assessment Tool to help businesses assess and reduce cyber risks. It uses a self-assessment method to assist businesses in doing a cyber risk assessment and implementing cybersecurity best practices.

When dealing with cyber threats, establishing organisational security and resiliency can be particularly difficult. Organizations can invest time up front to ensure they are implementing educated policies and processes by performing a cyber risk assessment. The NIST tool assists organisations in getting started and assessing their cybersecurity against risk-based frameworks.

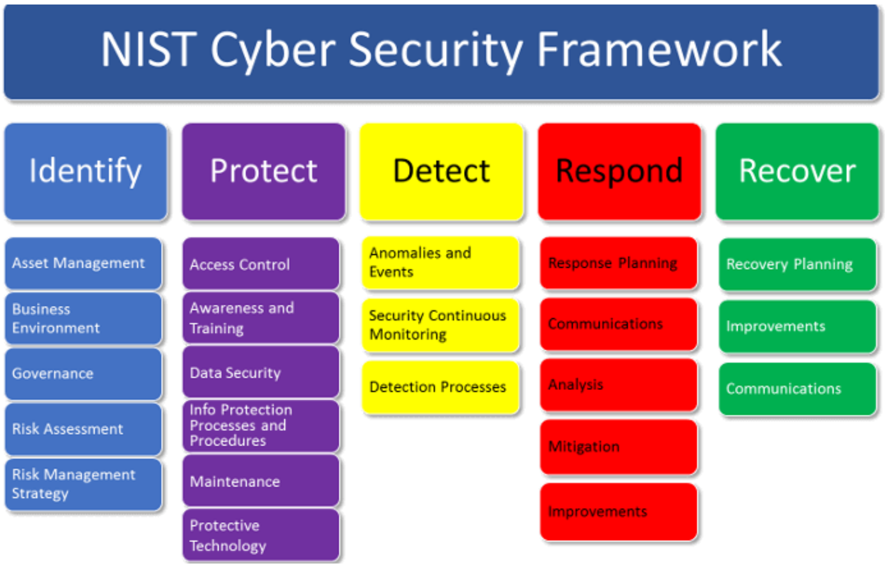


Figure 2: NIST Framework

4 Methods

Methods in this study use both primary and secondary data collections. The primary data collection in process gathers and analyze specific information from mapping of vital systems to Traficom's self-assessment tool (cyber meter) to proffer realistic outcome to the case company. Since this thesis is a development project, the methods will focus on the qualitative interview with the IT team of the company.

4.1 Interview & RFP from partner companies

This research needed some more specific answers from the personnel working at company’s IT department to be able to come up with results for research questions. That’s why an interview with IT people was chosen to gain more knowledge of company’s vital systems, what is the awareness of the employees of the company about cyber threats and how the company has prepared currently for cyberattacks. Interview was carried out by asking pre-made questions from the IT team of the company. The team was given time to prepare for the interview by sending questions in advance. The meeting was organized in company’s premises, where all the topics were discussed through. The answers were written down and used later in the study. The premade questions for the IT team are presented in table 1.

Do the employees recognize what cyber threats are?
Do the employees recognize phishing messages?
Do the employees understand the meaning of passwords?
Does the company's management understand the importance of cybersecurity?
How is secure work reflected in daily work?
How is cybersecurity been developed?
What are most vital systems?
How is the company prepared for cyber threats?
How are company prepared if some of the vital systems are not available?
Has there been any data leakage events?
Is there an annual budget for cybersecurity?

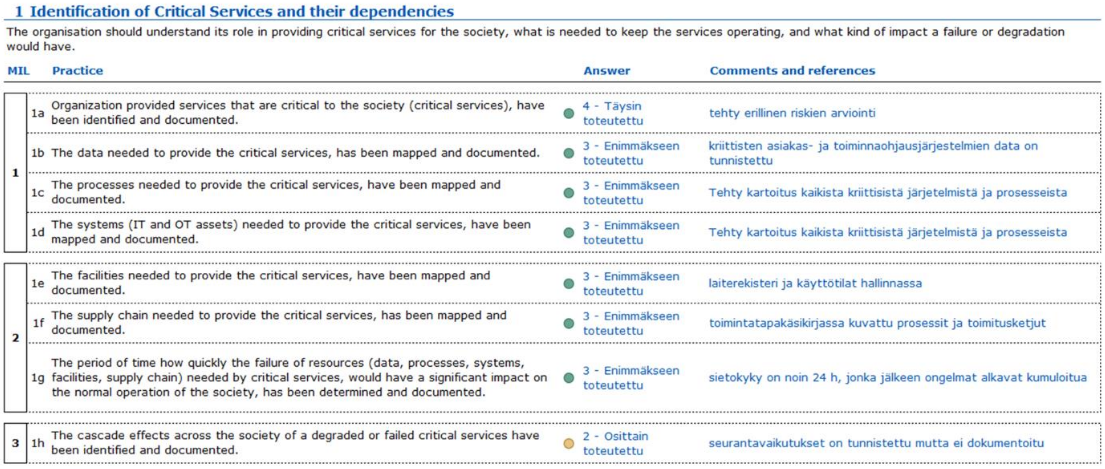
Table 1: Interview questions

Also, a request for proposal (RFP) was asked from few different partner companies to see what it would cost to purchase some of the most crucial cybersecurity services for a company of this size. RFP’s included Network cleaning, SOC services and personnel training.

4.2 Traficom’s cybermeter

One of the main methods used in this thesis was Traficom’s Cybermeter. The National Cyber Security Centre (NCSC-FI) developed Cybermeter, which is based on the international NIST Cybersecurity Framework and Cybersecurity Capability Maturity Model (C2M2). Cybermeter assists corporate executives and organizations in better managing cyber risks and ensuring business continuity. It's a tool that allows executives to see the maturity level of critical operational cybersecurity capabilities per domain and objective. Cybermeter shows how well an organization's cyber risks are identified, protected, detected, responded to, and recovered. It also shows the level of maturity in terms of supply chain management and external dependencies. Furthermore, corporate executives can obtain useful information about their cyber risk preparedness in comparison to the industry average. (Traficom 2021).

This tool was used for finding the strengths and weaknesses of current state of cybersecurity in the case company, by filling up the tool with answers. After that the tool gave results on how well the company is doing whit its current practices. The tool itself is very extensive, so not everything can be gone through during this thesis. That why some critical ones were chosen to present on this research.

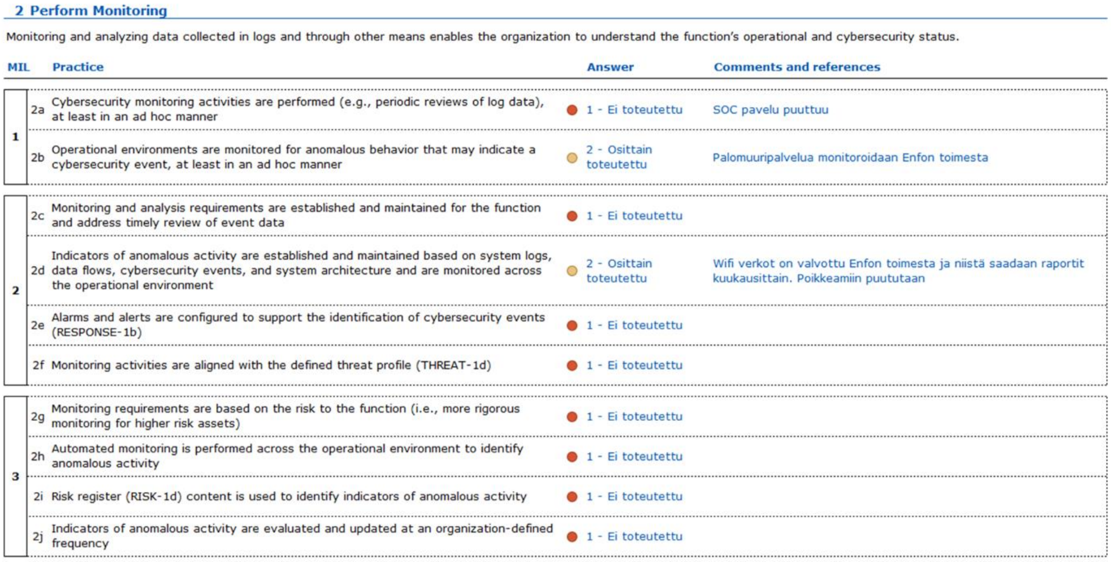


1 Identification of Critical Services and their dependencies

The organisation should understand its role in providing critical services for the society, what is needed to keep the services operating, and what kind of impact a failure or degradation would have.

MIL		Practice	Answer	Comments and references
1	1a	Organization provided services that are critical to the society (critical services), have been identified and documented.	● 4 - Täysin toteutettu	tehty erillinen riskien arviointi
	1b	The data needed to provide the critical services, has been mapped and documented.	● 3 - Enimmäkseen toteutettu	kriittisten asiakas- ja toiminnaohjausjärjestelmien data on tunnistettu
	1c	The processes needed to provide the critical services, have been mapped and documented.	● 3 - Enimmäkseen toteutettu	Tehty kartoitus kaikista kriittisistä järjetelmistä ja prosesseista
	1d	The systems (IT and OT assets) needed to provide the critical services, have been mapped and documented.	● 3 - Enimmäkseen toteutettu	Tehty kartoitus kaikista kriittisistä järjetelmistä ja prosesseista
2	1e	The facilities needed to provide the critical services, have been mapped and documented.	● 3 - Enimmäkseen toteutettu	laiterekisteri ja käyttötilat hallinnassa
	1f	The supply chain needed to provide the critical services, has been mapped and documented.	● 3 - Enimmäkseen toteutettu	toimintatapakäsikirjassa kuvattu prosessit ja toimitusketjut
	1g	The period of time how quickly the failure of resources (data, processes, systems, facilities, supply chain) needed by critical services, would have a significant impact on the normal operation of the society, has been determined and documented.	● 3 - Enimmäkseen toteutettu	sietokyky on noin 24 h, jonka jälkeen ongelmat alkavat kumuloitua
3	1h	The cascade effects across the society of a degraded or failed critical services have been identified and documented.	● 2 - Osittain toteutettu	seurantavaikutukset on tunnistettu mutta ei dokumentoitu

Figure 3: Critical services protection (example of low risk)

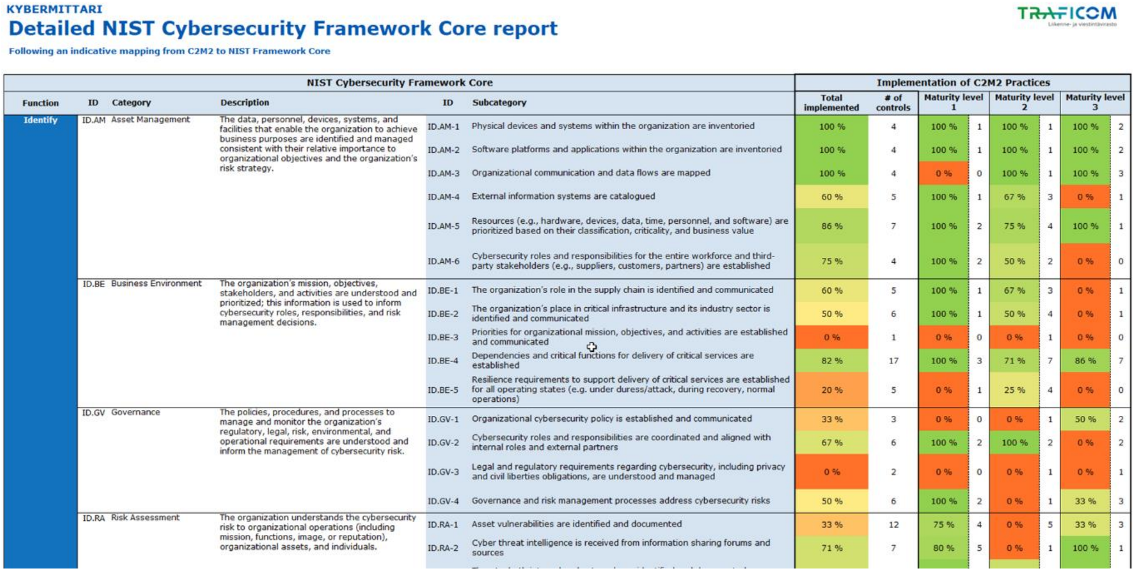


2 Perform Monitoring

Monitoring and analyzing data collected in logs and through other means enables the organization to understand the function's operational and cybersecurity status.

MIL		Practice	Answer	Comments and references
1	2a	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	● 1 - Ei toteutettu	SOC pavelu puuttuu
	2b	Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event, at least in an ad hoc manner	● 2 - Osittain toteutettu	Palomuuripalvelua monitoroidaan Enfon toimesta
2	2c	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data	● 1 - Ei toteutettu	
	2d	Indicators of anomalous activity are established and maintained based on system logs, data flows, cybersecurity events, and system architecture and are monitored across the operational environment	● 2 - Osittain toteutettu	Wifi verkot on valvottu Enfon toimesta ja niistä saadaan raportit kuukausittain. Poikkeamiin puututaan
	2e	Alarms and alerts are configured to support the identification of cybersecurity events (RESPONSE-1b)	● 1 - Ei toteutettu	
	2f	Monitoring activities are aligned with the defined threat profile (THREAT-1d)	● 1 - Ei toteutettu	
3	2g	Monitoring requirements are based on the risk to the function (i.e., more rigorous monitoring for higher risk assets)	● 1 - Ei toteutettu	
	2h	Automated monitoring is performed across the operational environment to identify anomalous activity	● 1 - Ei toteutettu	
	2i	Risk register (RISK-1d) content is used to identify indicators of anomalous activity	● 1 - Ei toteutettu	
	2j	Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	● 1 - Ei toteutettu	

Figure 4: Situational Awareness (example of high risks)



KYBERMITTARI

Detailed NIST Cybersecurity Framework Core report

Following an indicative mapping from C2M2 to NIST Framework Core

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	100 %	4	100 %	1	100 %	1	100 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	100 %	4	100 %	1	100 %	1	100 %	2
				ID.AM-3	Organizational communication and data flows are mapped	100 %	4	0 %	0	100 %	1	100 %	3
				ID.AM-4	External information systems are catalogued	60 %	5	100 %	1	67 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	86 %	7	100 %	2	75 %	4	100 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	60 %	5	100 %	1	67 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	50 %	6	100 %	1	50 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	82 %	17	100 %	3	71 %	7	86 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	0 %	1	25 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	33 %	3	0 %	0	0 %	1	50 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	67 %	6	100 %	2	100 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	50 %	6	100 %	2	0 %	1	33 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	33 %	12	75 %	4	0 %	5	33 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	71 %	7	80 %	5	0 %	1	100 %	1

Figure 5: NIST Report

5 Results

In this section, the results of the data collection will be presented. The methods that were used were an interview with the IT department of the company and the self-assessment tool from Traficom (Cybermeter). These results are used to produce a cybersecurity development plan for the case company.

5.1 Results from interview

The interview was executed with the company's IT department. During the interview, it was clear that the company has some work to be done what comes to cybersecurity. The results of the interview will be separated to few topics.

The first topic was about the employee's awareness to the subject. According to company's IT department, some of the employee's recognize what cyber threats are, but there are many who don't care. Some of the employee's don't even understand what it means. During the interview of this topic came up, that just recently there was a phishing email test done by Silverskin for 34 keypersons in the company, where the company setup a fake email and sent message to the pilot group and required them to click the link that directed them to a familiar looking website. The website required them to log in to their work email. If the employee logged in, the website showed an error message. The test showed that from 34 employee's tested, 11% gave their information and almost third of the employee's opened the link. During this phase of the interview also came up that most of the employee's don't keep their password secured, but also give them to other employees in some cases, i.e during vacation time when employees are helping each other. The highest management of the company understand the meaning of information security and are aware of the problem. That's why they try to maintain the awareness by training events.

Another topic was about how the security shows on company's day to day activities and the company's cybersecurity development. According to IT department, most employees are using multi-function authenticators when logging in to their M365 accounts (Microsoft subscription for office apps). This means that not only the password is enough to gain access to the employees account, but it needs another verification like a code from the accounts owner's phone Authenticator app. The company is also using geo-blocking on all their employee's accounts. With this they ensure that the accounts cannot be accessed from outside of Europe. They also require employees to change their passwords regularly and complexity of password is prescribed. Car Sales system (Websales) is protected by two-way authentication with SMS code if logged in outside company network. Car Service system (Automaster) is protected by VPN tunnel. Users need to be logged in from the company network or via VPN if working remotely. Continuous monitoring of systems and internet traffic is not currently used in the company.

Next topic was about the company's most vital systems and how are they prepared to cyber threats. The most vital systems for the company are the sales systems. For car sales the sales system is Websales and for repair services the system is Automaster. Without them, doing business in the company would be much harder and time taking. From a risk analysis standpoint, car sales and maintenance operations must be placed in a different position. Cars that are not sold today can be sold or billed tomorrow if the systems work. Cars that have not been serviced today will not be serviced tomorrow, as the cars scheduled for the following day will arrive. As a result, even two days of maintenance for one day is not possible. This is a serious business risk that immediately jeopardizes the company's cash flow.

The company has been thinking about a plan for a moment when these vital systems are unavailable, but there is not one yet. The company has prepared for cyber threats with technical actions on workstations and servers by encrypting the data on laptop hard discs, so the information cannot be stolen easily. Also, they have firewall in their WAN (Wide area Network), LAN (Local area network) has been blogged from each other areas, Wi-Fi LAN area are monitored and analyzed by the partner (ENFO), Symantec antivirus and end point protection systems on every workstation and without admin IDs, the user of workstation can't really defile it that easily.

The last topic was about the company's annual budget for cybersecurity and if there has been any data leakage events before. According to IT department, the company does not have an annual budget for cyber security. The budget has been combined with the IT budget, which might be too low to invest in cybersecurity services as the management seems to be willing to invest more on business technology than cyber threads. There has also been one incident, where the critical information has been leaked. which led to a conversation with the police. The crime was corrected by technical means.

5.2 Results from Cybermeter

The results from the Cybermeter were very deep and analytic and there was so much data, that it all cannot be presented in this study. The overall results are presented in figure 6 and explained in this section and some examples of parts that were executed well and poorly in the company are also explained.

The Cybermeter tool is divided in many different cybersecurity categories and they all are included to one of the five main functions. These functions are Identify, Protect, Detect, Respond and Recover. Answering to questions in different categories, the tool evaluates the company's acquirements in that area by maturity levels from 0 to 3. 0 being the worst result and 3 being the best result. After answering to all categories, the tool evaluates an overview of all the main functions.

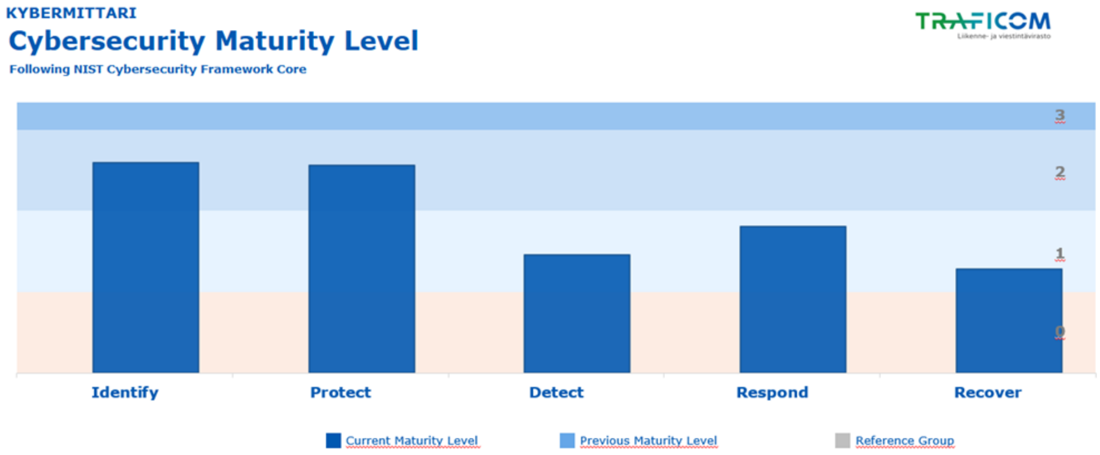


Figure 2: Maturity level

According to the research with the Cybermeter, the current state of case company's cybersecurity has been evaluated. As shown in the cybermeters maturity level diagram (figure 6) the case company got 78% out of 100% in Identify function overall, which indicates maturity level 2 out of 3. This means that although the organization's ability to identify and manage cybersecurity risks to systems, people, assets, data, and critical services is strong, there are some areas where it falls short. This could lead to some cyber risks remaining unaddressed, compromising the organization's overall resiliency.

In function of Protect the company got 77% out of 100%, which indicates the maturity level of 2. This means that the company has a strong capability to protect critical services from cyber security threats and incidents, but it still has some control gaps. While all critical services and information may be protected, the implementation leaves grey areas or gaps in the protection, resulting in unnecessarily high costs and incident numbers.

In function of Detect the company got 43% out of 100%, which indicates the maturity level of 1. This means that although the company has a basic data collection capability, the ability to detect cyber incidents is hampered by data quality and coverage, as well as analysis capability. This could lead to delayed response and that the actions taken are not based on a complete understanding of the situation, leaving the company vulnerable to major breaches and damage despite the initiated response.

In function of Respond the company got 54% out of 100%, which almost reaches to the maturity level of 2 but is still level 1. This means that the company has the basic capability to respond quickly to a cyber incident, but the process may not be well coordinated and practiced. This could mean that, even if the breach was detected early, the response will most likely fail to contain the breach and damage.

In the last function of Recovery, the company got 38% out of 100%, which is their lowers score and indicates the maturity level of 1. This means that the company's basic capability to initiate and execute recovery from a cyber incident is limited. This could mean that recovery will not cover all aspects of the business, will not be executed in the best order, or will not be fast enough to meet the business needs, resulting in business disruption, costs, and impact that could have been avoided.

6 Development plan

In the case company cybersecurity is about reputation management, ensuring continuity, and building customer trust. Security is always a feeling, which is why communication is especially important in a disruptive situation. According to the interview with the IT department of the case company, system crashes or crashes caused by cybercrime (hacking, phishing) or system failure are the most significant business security risks for the company. Leakage of customer or personnel information to the public is also a significant risk, which can result in serious reputational damage. Customer loss and business closure are the worst-case scenarios.

6.1 Stages of development plan

By implementing foundational securities and critical processes, a company can stop or significantly reduce the risk of a breach occurring. According to an article written on EideBailly (2020), the foundation of good cybersecurity consists of three stages. The development plan of the company will be based on this model.

The stages are presented in figure 7.

1) Foundation security, which is the basis of the cyber security. This includes adminstative access, data backups and recovery, email gateway, Phising exercise, endpoint protection, firewall and MFA.
2) Critical processes, which is the second step when developing the cybersecurity plan. This includes vulnerability management, incident response retainer and training and awarness.
3) Key activities, which is the third step, includes remote access and monitoring.

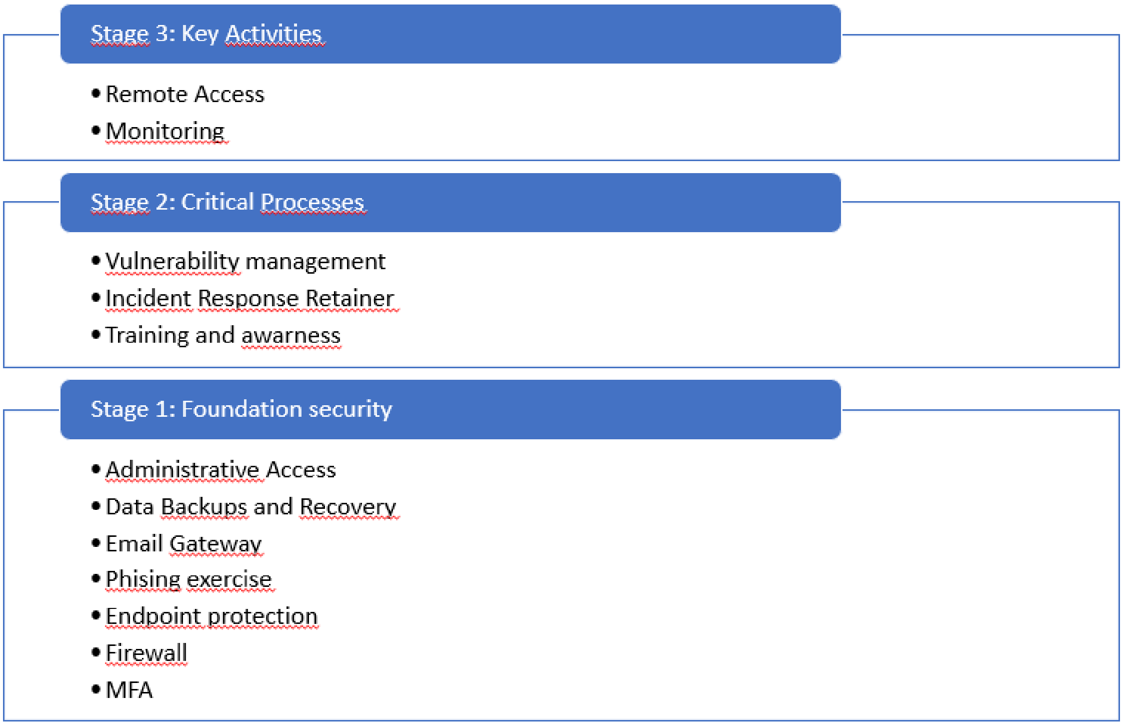


Figure 3 : Security stages model

6.1.1 Stage 1: Foundation security

According to the interview with the company’s IT team and the research with the Cybermeter, the administrative access has been executed well in the case company. Only the IT personnel have the administrative rights on devices and are able to create new users and install software. After the phishing test, online learning system (Vuolearning, is an easy-to-use online learning platform that enables fast e-learning course production) has been introduced in the company and the employees of the company have been informed about the learning system on the intranet. The company is regularly updating their firewalls, antivirus systems and fully automated patching (Microsoft security updates), so the endpoint protection, which takes place on workstations, is covered on an acceptable level. The company is using an email gateway security, which stops most of the harmful emails and they are also using the multifactor authentication system to increase the security of employees’ accounts. What comes to data backups and recovery, according to the Cybermeter, the company’s capability to recover and backing up vital data is limited.

As a conclusion of stage one, the foundation security in the case company is on the right track and most things have been executed well. The company must develop its capability to recover from possible cybersecurity adversities and backing up the vital data. Currently, the company trusts heavily to Microsoft cloud services that has some backups by itself. It is useful to mitigate missing files or data in daily operations, but it may not be enough when a total disaster occurs, and the entire Microsoft platform must be recovered. There are lots of vendors that provides this kind of services to improve basic protection against MS cloud data from MS tools, such as emails, Teams, Sharepoint and Onedrive files.

6.1.2 Stage 2: Critical Processes

According to the research with the Cybermeter, vulnerability management is one of the weakest areas for the company. They are not continually gathering their cybersecurity vulnerability information and their operative systems are not monitored. The workstation security in enhanced with automated updates and antivirus software’s. Network penetration testing, which shows, how the company’s network looks like for an intruder, has never been done. Also, internal network vulnerability scan has not been done either. This test would show, what an intruder could exploit if it got into the company’s network.

If an incident happens, the company has a response policy which includes how an employee should act. The employees should first inform their closest supervisor, then the information should transfer to IT personnel and from there to CEO of the company. This policy is good if all the employees acted towards it. This of course requires training of the personnel.

Cybersecurity training is an important part of securing the company’s information. The company is using the Vuolearning online learning system, but as shown on a phishing test done by Silverskin, they should also do regular phishing tests to improve personnel awareness, otherwise it will be left to the onboard process alone and will be forgotten over time.

As a conclusion of step two, the company should invest more on vulnerability management by doing regular penetration tests and continually gathering cybersecurity vulnerability information. They should also do more personnel training by regular phishing test and training events.

6.1.3 Stage 3: Key Activities

According to the research with the Cybermeter and the interview with the company’s IT team, the company is using transport layer security (TLS) with reliable partners like financing companies and vehicle importers. This means that the emails between these partners are encrypted and safe. The company is also using VPN, which secures their network usage for remote users too. Wi-Fi networks are divided to many SSID’s and monitored by routers, applications, clients and devices and analysed periodically (90 days) by telecommunication specialists. Specialists are making suggestions for developing Wi-Fi even more secure. What comes to data and log information monitoring, the company is not using any kind of technology for that.

As a conclusion of stage 3, the company has executed remote access control well, but they don’t have any kind of monitoring of their data. The company should consider investing in monitoring services like for example Security Operation Center services (SOC) to increase their capability to detect cybersecurity incidents and be able to respond to them more effectively.

6.2 Investment budget for security development

Based on the results of the research, the company must invest more to cybersecurity to accomplish daily business security and continuity. Cybersecurity development can be focused in three main areas. The first one being, how to make sure Wide Area Network (WAN) will be working even in situations when it will be subjected to extra traffic such as Ddos attacks. This can be managed by operator’s network cleaner called Shield service (Elisa 2022).

The second being personnel training that needs to be ongoing so that cyber threats are on everybody’s mind every day. HoxHunt for example, provides phishing mail training based on micro learning and it has a constantly evolving set of metrics that measures the improvement of the company’s awareness (Hoxhunt 2022).

The third area would be to see what's happening in networks and systems in real time. This would needs more technical systems, such as Secure operation center services (SOC). Many security companies provide this kind of service where they read system logs and analyze that data. Log data is so massive that people are unable to monitor it. It needs to be analyzed first with artificial intelligence and secondly with just one permille with the help of cybersecurity experts. There may also be false positive alerts that a company's IT needs to consider and whether they are real risks or normal operations. The complexity of operations raises the cost of processing that can be a hurdle for the investment willingness. (Securecloud 2022.)

The fourth topic is Microsoft 365 cloud backup services. In cloud services, data is always the customer's responsibility. Human errors are the main cause of data loss and intentional or unintentional destruction of data is mostly an internal measure. That means that all files, Teams channels and Sharepoint online can be restored if data would be lost.

The investment budget consists of these levels and the amounts are based on RFPs made during the study. The Shield service (1) is approx. 10 000 euros annually, Micro learning training (2) is approx. 20 000 euroa annually and SOC (3) is starting from 100 000 euros annually (4) MS 365 backup and restore services 20 000 euros annually.

6.3 Developing a business continuity plan

When business systems fail, business continuity and resilience become vital otherwise the company may run into the serious problems and finally lose their customers, cash flow and in the worst case even get in bankrupt.

The term 'resilience' means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Business continuity plan consists of policy of internal and external communication when company is in crisis and preparing and testing of manual procedures in case the vital IT-systems are down.

Communication plan

A preliminary communication plan was made with the company's IT team. The things to consider were, when an incident happens, how should the employees act and who should be contacted and how?

A procedure was made where the employee who notices the incident, will immediately report to the closest supervisor. The supervisor makes an assessment of the situation with his team and his supervisor, after which an immediate communication chain is launched. In order, the first to be notified is the Head of the Department, who will then notify the Unit Management and after that the CEO will be notified. The CEO coordinates internal and external communications with personnel and CIOs, as well as other senior management as appropriate.

Internal Communication

The head of the unit is in charge of the office's and department's immediate internal communication.

HR and the CEO will have more centralised internal communication. Internal notifications are drafted under their supervision and in collaboration with the appropriate parties (e.g., disrupted entity, information management, car sales, aftersales).

If the situation requires communication with the personnel other than via company's e-mail, Yammer or intranet and the personnel's contact information cannot be obtained from the systems, they can be found in the personnel department in hard copy, on a USB stick and stored on the phone. Units may not have personal records stored outside the personnel management system due to privacy concerns.

External communication

All external communication is routed through the Chief Human Resources Officer, to whom all possible media contacts are also directed. He and the CEO will work together to create the necessary bulletins, which will be distributed to all parties involved. Sales managers and service managers ensure that customers are contacted if the situation affects customer orders and delivery times or scheduled appointments. Through the marketing department, information about the disturbance is available on the company's website and on Facebook. Situation is used for communication, but if the disturbance causes changes in opening hours and agreed delivery times, up-to-date information on the Internet is important.

Manual procedure plan

When business systems are down, the company moves to a manual operational process, where the data generated by the systems is manually recorded in Excel or ultimately on paper with the assistance of customers at the time of the encounter.

Table 2 presents the package that every manager should always have available.

• Templates for making car sales offers and workshop work orders by hand.
• Latest terms of conditions for maintenance and repair of motor vehicles
• Sales contract form for a used vehicle
• Fire and rescue plan
• A USB memory stick with all the above in electronic format

Table 2: Manual procedure tools

6.4 Scenarios

In this section, a few examples scenarios, where the incident has happened, were created with in cooperation with the company’s IT team. The scenarios Include the preliminary procedure, how the company should act, when the vital systems are unavailable.

6.4.1 Used cars sales - Websales not usable

Since the prices of used cars are displayed on the car windows, offers can be made in Excel or on a hard copy. The templates for that can be found at the garage manager. Applications for funding can be made by telephone if the banks have sufficient resources for the telephone service. GT-X modeling can be omitted in such a situation. The range of used cars is not updated with online services, which must be considered in customer service. Customers may receive inquiries about cars that have already been sold. New ones exchanged will not be revealed. After the incident is over the systems must be updated to recover. Cash payments are normally charged, but billing must be done manually.

6.4.2 New Car Sales – Websales not usable

New car price lists and accessory price lists can be found on import, if necessary, but the car tax calculation for each car type is difficult to calculate. In practice, offers for new cars and sales contracts cannot be made.

If Traficom's service has been blocked for example due to Internet problems, Traficom's service can be accessed via a VPN connection remotely. Cars can be registered at the nearest inspection office if they have access to Traficom's service.

Car Service – Automaster not usable

If use of the Automaster is prevented in the middle of a day, all work orders for the entire day should be printed and the necessary spare parts collected the previous day, so that work can be carried out at least for the most part. Billing, etc. will be moved to the next day.

If the Automaster is still out of operation the next morning, no parts have been collected or work orders have been printed the day before. When the customer brings the car in the morning, it can be clarified with the customer, what has been agreed in the appointment. The workload can be done on paper and the template can be found at garage managers, but spare parts cannot be collected when the system is down.

In practice, only troubleshooting electrical repairs or other work that does not require Automaster could work normally. If the internet connections is not working properly, the work at the workshop is completely interrupted, as the connection of cars to factory systems is prevented.

7 Conclusion

After studying NIST analysis and employee’s awareness for cybersecurity, it is obvious that company must invest more for cybersecurity in coming years to ensure business continuity. The company has the base for cybersecurity at a satisfactory level, but they should improve their personnel training program, security monitoring and capability to recover from incidents. Cyber security and training must be included to the budget and start to take steps toward better security. The company’s management has to decide, what areas of cybersecurity they are ready to invest in and what they are ready to put under the risk. In the future, government actors may enact regulations for cyber risk management as they did already in GDPR. Manufacturers, importers, and other stakeholders may also set new rules, contracts, and regulations how to protect product pipeline. The cybersecurity is not just a one player task but a common for all. Risks and threats can be transferred and mitigated by data protection agreements, but this does not eliminate the fact that when a company's cyber security is compromised, its profitability and reputation may lead to a loss of trust and eventually even business closure.

8 References

Electronic

Ramkumar, M. 2016. Cybersecurity: It’s All About the Assumptions. Accessed 02.05.2022 https://www.researchgate.net/profile/Mahalingam-Ramkumar/publication/303991366_Cybersecurity_It's_All_About_the_Assumptions/links/5762096f08aeeada5bc50487/Cybersecurity-Its-All-About-the-Assumptions.pdf

van den Berg, B & Keymolen, E. 2017. Regulating security on the Internet: control versus trust. Accessed 10.05.2022. https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1298504

Bush, C. 2020. Trust is a two-way street when it comes to cybersecurity. Accessed 19.05.2022 https://www.itproportal.com/features/trust-is-a-two-way-street-when-it-comes-to-cybersecurity/

EideBailly, 2020. What You Need to Know About Cybersecurity At Your Dealership. Accessed 20.05.2022. https://www.eidebailly.com/insights/articles/2018/9/cybersecurity-at-dealerships

Traficom. 2021. Kybermittari – Cybermeter. Accessed 29.04.2022. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

Limnéll, J. 2022. Linkedin. accessed 29.04.2022 https://www.linkedin.com/posts/jarno-limn%C3%A9ll-08699720_t%C3%A4n%C3%A4%C3%A4n-puhumassa-espoon-elinkeinoforumissa-activity-6916991475968868352-Q6sb?utm_source=linkedin_share&utm_medium=member_desktop_web

Dutton, J. 2017. Three pillars of cyber security. Accessed 10.6.2022. Three pillars of cyber security - IT Governance UK Blog

CIS. 2021. A Short Guide to Infrastructure Security and Resiliency. Accessed 24.04.2022. https://www.cisecurity.org/insights/blog/a-short-guide-to-infrastructure-security-and-resiliency

WhiteHOuse. 2022. FACT SHEET: Act Now to Protect Against Potential Cyberattacks. Accessed 01.05.2022. FACT SHEET: Act Now to Protect Against Potential Cyberattacks | The White House

Securecloud. Cloud SOC - tietoturvavalvomo pilvestä. Accessed 25.05.2022. SOC, Cyber Security palveluna | Secure Cloud | Helsinki

Nachbahr, E. 2020. Top 2 Cybersecurity threats for auto dealers in 2020. Accessed 20.05.2022 https://www.autosuccessonline.com/top-2-cybersecurity-threats-for-auto-dealers-in-2020/

Otorio. 2021. Ransomware: The Cyber Attacks on The Automotive Industry. Accessed 23.04.2022. https://www.otorio.com/blog/ransomware-the-cyber-attacks-on-the-automotive-industry/

Threatmodelet. 2020. Fastest Frowing Types of Cybercrime. Accessed 29.04.2022. https://threatmodeler.com/fastest-growing-types-of-cybercrime/

Nguyen, J. 2018. Five Ways to Prevent Social Engineering Attacks. Accessed 24.04.2022. https://www.mdsny.com/5-ways-to-prevent-social-engineering-attacks/

Zhang, E. 2020. Is Your Auto Dealership Secure? Top Cyber Risks and Tips to Protect Your Dealership. Accessed 24.04.2022. https://zeguro.com/blog/is-your-auto-dealership-secure-top-cyber-risks-and-tips-to-protect-your-dealership

Baggott, J. 2021. Experts warn cybercrime threat for car dealers increasing as conmen use pandemic quirks to steal cash. Accessed 25.04.2022. https://cardealermagazine.co.uk/publish/experts-warn-cyber-crime-threat-for-car-dealers-increasing-as-conmen-use-pandemic-quirks-to-steal-cash/217569

Reddock, G. 2022. Why Auto Dealers Should Make Cybersecurity a Priority. Accessed 05.05.2022. https://www.foason.com/2020/04/28/why-auto-dealers-should-make-cybersecurity-a-priority/

Unpublished

Mattsson, M. IT Team. Company x. Personal interview.

9 Figures

Figure 1: .... **Error! Bookmark not defined.**

Figure 2: NIST Framework 11

Figure 3: Critical services protection (example of low risk)...................................... 13

Figure 4: Situational Awareness (example of high risks) 13

Figure 5: NIST Report 14

Figure 6: Maturity level .... **Error! Bookmark not defined.**
Figure 7 : Security stages model 18

10 Tables

Table 1: Interview questions 12
Table 2: Manual procedure tools 23