Future Prospects of Cyber Security in Manufacturing: Findings from a Delphi Study

Future Prospects of Cyber Security in Manufacturing: Findings from a Delphi Study

Katariina Kannus
Deloitte
katariina.kannus@iki.fi

Ilona Ilvonen
Tampere University of Technology
ilona.ilvonen@tut.fi

Abstract

Cyber security professionals need to make decisions in a constantly changing threat landscape, with a plethora of known threats that need reacting to in addition to the less well-known future threats. The objective of this paper is to provide insight in the cyber security landscape of manufacturing in 2021, and thus help decision making in the area. The Delphi study found out that internet of things, digitalization, industry 4.0, and the security of the industrial automation would be the most important drivers for the cyber security of manufacturing industry in 2021. The paper presents several important themes to be considered by security professionals.

1. Introduction

In developed countries the manufacturing industry is increasingly dependent on digital networks and their services. The dependency will not diminish, on the contrary, it will increase. Cyber security is an enabler of digitalization but when managed poorly it can jeopardize all the benefits digitalization can bring. [5].

Companies' cyber security should be proactive: after a serious cyberattack the damage is already done. Reactive improvements are too late if, for example, a plant is already in a stand-still, or sensitive information stolen [e.g. 6, 7, 8]. The manufacturing industry is increasingly international. The companies in the industry have growing amount of operations and stakeholders all around the world, and in the future the changing global operative environment introduces not only opportunities to grow but challenges as well (see e.g. [19, 20, 21]). One big challenge is cyber security management and the contingency planning for the future cyber threats.

Cyber security does not belong only to the IT-departments anymore [11, 12, 13, 14] – globally its importance has been noticed in the board rooms of companies and the interest of executives has been forecasted to rise [14]. New technologies in manufacturing environments also bring new kind of cyber threats while the attackers find more and more ways to use the known and unknown vulnerabilities of old systems, technologies and processes.

The Finnish national cyber security strategy [2] says that preventing the cyber security threats needs proactive operations and planning. The new operative environment requires know-how and ability to react fast and uniformly in a right way. To reach proactive cyber security not only business but also the whole society needs high-quality research about cyber security future from different industries' perspectives. In this study cyber security future prospects were studied from Finnish manufacturing organization's point of view: what will be the priorities in 2021, what will not be so important in 2021, and what are the main targets in the near future? 4-5 years as a typical time-frame for strategic planning was selected for the study.

Forgetting cyber security can become highly expensive to companies. An information security breach can cost the victim company 4-73 M$ on average [16, 17]. The impact and costs of a breach are complicated and long-term [18]. According to the results of this study, security professionals are well aware of the potential costs of security breaches. As an example, increasingly connected devices and digitalization, along with the challenges of controlling who uses the organizational networks, were seen to be important challenges for the manufacturing industry in the coming 5 years.

In the next section the results of a literature review as the basis of the Delphi study are presented, followed by findings from the Delphi study itself. The paper is concluded with insights from the study findings and their implications to the manufacturing industry in particular and the cyber security community in general.

URI: http://hdl.handle.net/10125/50488
ISBN: 978-0-9981331-1-9

2. Background

This Delphi study is based on a literature review where the most relevant studies and reports related to the topic were examined. The most important selection criterion to be included in the review was the novelty of the report: the oldest selected reports were from 2015. This criterion was based on the dynamism of cyber security and constant change of the industry under study, thus rendering older studies outdated for the purpose of projecting to the future.

The databases used in this literature review were reached via following search engines offered by the library of the Technical University of Tampere: Tutcat, Scienceport, and Andor. Also, Deloitte's internal search engine KX Research Tools were used to reach e.g. Books 24/7, AMR Research, ALM Intelligence, Gartner's and Forrester's databases. In these search engines the search was done in Finnish and English with a list of relevant search words such as *the future of manufacturing*, *cyber security predictions*, *security of Internet of Things*, *Information Security in Industrial Internet*, and *the future of IoT*. Also during this study, the communication and the e-mail list offered by the Finnish Communications Regulatory Authority Cyber Security Centre were followed for the purpose of receiving the most current cyber security literature and news.

The main results of the literature review are presented in Table 1. They are mapped to the Cyber Security Framework [1] chosen to be used in this study. The framework divides cyber security to four categories: Strategic, Secure, Vigilant and Resilient. In some sources also Governance is used as the name of the first category. [38, 39, 40].

Most of the topics in Table 1 are strongly linked to two topics under Strategic category (the upper left hand corner of Table 1): *IoT* (Internet of Things) and *digitalization*. And of course, those two are linked to each other, too. Not only is media writing a lot about IoT security and risks but also CIOs worldwide see that their companies' IoT investments are growing in the near future [15].

IT spreading widely to industrial automation and control systems has created new vulnerabilities and attack vectors to manufacturing industry's cyber security. According to an international study [9] manufacturing was the second most attacked industry in 2015 right after healthcare. In 2016 manufacturing was also among the top most attacked industries. In addition, according to another worldwide report [10], manufacturing is the third most attacked industry.

Regarding to the terms in Strategic category such as *IoT*, *digitalization and industry 4.0* another widely used term is CPPS (cyber-physical production systems). Also *security of industrial automation* in Secure category (in the upper right hand corner of Table 1) is related to CPPS because they are in smart factories. In there, smart ICS (industrial control systems) organize and optimize themselves according to the resource spending and availability, even across company borders. ICS, such as SCADA (Supervisory Control And Data Acquisition), have lately been changed from closed and individual environments to an open architecture and standardized technologies. [29]. Then main ICS challenge is the need for 24/7 availability with no downtime and no disruption to business operations [38].

Table 1. Summary of the literature review mapped to Cyber Security Framework [1].

STRATEGIC / GOVERNANCE	SECURE
Internet of Things (IoT), Digitalization and industry 4.0, Usability vs. information security, Compliance and changes in laws and regulations, Different legislations in different countries, Employees' information security awareness, Lack of information security professionals, Engage young employees to the cyber security culture, Lack and allocation of cyber security resources, Growing performance and real-time requirements.	Security of industrial automation, Ensuring availability, Identity and access management, Old and complex industrial automation and IT systems, Managing expanding amounts of data, Managing changes, patches and updates, Ransom (also IoT ransomware) and terrorism, Defining responsibilities with suppliers and other partners, Mobile devices, Cloud security, Security of robotics, Privacy.
VIGILANT	**RESILIENT**
Increasing use of automation and analytics to improve cyber security, Advanced Persistent Threats (APT), Insider threats, Exploiting zero-day-vulnerabilities, Frauds, Identifying attackers and attacks, Cyber security monitoring systems.	Cyber espionage (including governmental agencies), Preparing to cyber attacks and recovering from them.

Smart factories are an important part of *Industry 4.0* which is under Strategic category in Table 1**.** The term means the fourth revolution of industry where new technologies such as cloud, IoT, augmented reality, big data, machine learning, analytics and automation are changing traditional manufacturing. [41, 42].

One of the main difference between traditional IT systems and industry 4.0. CPPS is the objectives of system's security. The target of the traditional IT system is integrity and confidentiality, and therefore cyber security is often a compromise between availability and security. This means that if a cyber-

attack is detected it is possible to stop it by isolating it from the network, or even by shutting down the whole or a part of the system. Similar approach is not possible for CPPS because their downtime is highly expensive. Hence, the most damaging attacks in manufacturing are the ones when production is delayed and therefore the company suffers from losses of efficiency and revenue. For example, Denial of Service or similar attacks can cause unavailability in manufacturing business [41]. Hence, *ensuring availability* is one of the topics in Secure category in Table 1.

Solving of many kinds of strategic cyber security challenges is mandatory before manufacturing will be able to get all the benefits out of the new technologies introduced above [30, 43, 48]. In the near future the security systems of IoT ecosystems will not be scalable enough so that they could secure broad networks with different kind of IoT devices and CPPS, and fill the *growing performance and real-time requirements* (Strategic category in Table 1) at the same time [37, 41].

Another strategic topic is a conflict between the expectations and investments of executives of the companies. CIOs are expected to take care of the company's cyber security but executives are not investing to it in a scale to meet the expectations. Many CIOs feel their companies are not investing enough in cyber security. However, many of them believe that cyber security investments will grow and cyber security will have a great impact to the business in the near future. [15].

The on-going change is substantial, and it is difficult to know how much security will be compromised in the near future. Predictions say that an average IoT-device is compromised after being in the network for two to six minutes depending on the source of information [10, 44] and before 2020 there will be over 24 billion IoT-devices connected to the network [45]. On the other hand, a somewhat newer prediction says that connected IoT-devices, sensors and actuators will reach over 46 billion before 2021 [46]. Whether or not smart phones are included in the calculation can explain a lot of the differences between predictions.

The security of IoT is a comprehensive concept with many kinds of functions, facilities, actors, platforms, risks, and opportunities. Often when talking about industrial IoT the abbreviation IIoT is used [41]. From an attacker's point of view there is no big difference compared to other targets. However, the impact of a successful attack could be much bigger than in an attack focusing on consumer IoT gadgets [33]. In the future, this fact will increase the popularity of IIoT as an attack vector.

Often old and already used sensors are added to the new IoT environments. It is cheaper than buying new ones but the problem is that the old sensors are not designed to be added to big, open networks and therefore their security level is not high enough. Moreover, old IT security controls and products such as *identity and access management* tools are not sufficient for the IoT security needs. Another security challenge in IoT that needs to be solved in the near future is the use of its vulnerabilities for *ransom and terrorism* (under Secure category of Table 1) [31, 33, 35, 36, 37, 38, 49].

Usually an IoT ecosystem comprises many kinds of organizations and stakeholders across the supply chain. Often all the parts of this chain are processing data. Securing and managing the whole supply chain can be challenging and it is important to define the ownership and life cycle of the data with all the stakeholders. Only then is it possible to be sure that everybody in the supply chain knows their data protection and cyber security responsibilities. [38, 43, 34]. This *defining responsibilities with suppliers and partners* is in Secure category in Table 1.

Each member of the supply chain must consider what information is wise to collect and store. Hence, in the future it is increasingly challenging to companies to know who is dealing with their data and how. Therefore, *identity and access management* (under Secure category in Table 1) is increasingly important, as well as remembering *privacy* and its regulations which differ by region. The latter is needed also when thinking about Vigilant category (in the lower left hand corner of the same table) and *insider threat* in there. It is predicted to be one of the biggest attack vectors in the future of IIoT and from the perspective of its control *privacy* and other similar cyber security legislations can be seen as a challenge. [2, 11, 33, 37, 38, 41, 43, 51, 52].

One future challenge in managing data is under Secure category in Table 1: *managing expanding amounts of data* securely will be increasingly challenging in the future with development and popularity of *mobile devices*, big data, IoT and similar technologies. [30, 33, 43, 49].

Cloud security (under Secure category in Table 1) is another information sharing and identity management related concern, which is much discussed in the literature [2, 37, 43, 49]. The increasing use of cloud services as well as their development bring not only opportunities but also new threats to cyber security in manufacturing industry. Companies are transferring increasing amounts of data and services to the cloud. Hence, growing amounts of business critical data will be stored to different kinds of cloud services. But, cloud

services do not have to be more unsecure than other IT services. From security point of view, it is essential to ensure that the services have the right kind of configuration. [37].

Trust in cloud solutions is predicted to grow which will increase the amount of sensitive data stored in them. Therefore, cloud services will become more interesting as a target of cyber-attacks. However, companies are predicted to store their most valuable data in their own trusted networks and data centers. One of the future challenges will probably be outdated authentication systems in cloud services which leads to identity thefts and brute-force attacks against maintenance credentials of cloud services [37].

In the last category presented in lower right hand corner of the Table 1 is Resilient. Both of its topics, *cyber espionage* as well as *preparing to cyber-attacks and recovering from them* are mentioned quite often by the literature. Both are important in the proactive future of cyber security, especially in manufacturing because of, for example, high costs of downtime or intellectual property loss [5, 6, 7, 27, 28, 30, 32, 50, 43, 49, 53, 54, 55].

Overall, every new employee, stakeholder, or IoT device connected to the ecosystem or system is a new attack vector against CPPS [35, 38, 41, 47, 48]. It is predicted that during the coming years there will not appear a pervasive and uniform IoT security system which is ideal for business, security, and users. Instead, the reality will be different kind of separate systems and security systems linked to them one by one. [35].

3. Research setting and method

This study conducted in three phases. The first stage comprised careful preparation: carrying out the literature review, arranging a preparation workshop for 14 cyber security experts, and selecting the experts to the Delphi panel. The thoroughness in the preparation phase was important so that it was possible to avoid weaknesses of the Delphi method, such as wrong kind of experts in the panel, poorly designed interviews or unjustified and over-guiding propositions. The selecting of the professionals to the panel for this study was based on the quality of their expertise and diversity of their backgrounds. [22, 23, 24]. Hence, the panel as a group was able to offer a broad view of the future of cyber security in the industry.

The panelists were from different Finnish manufacturing companies, which were large and operating globally. (More than a half of them had a turnover over 5000 M€ in 2015). The role titles of the panelists were Vice President Information Technology, Head of IT Risk and Information Security Management, Information Security Director, Cyber Security and Quality Manager, Chief Security Officer, Manager IT Security and Compliance, Chief Information Security Officer, and Head of ICT Security. Half of the panelists had at least ten years' experience in cyber security, and most of the panelists had over seven years of experience in their security role. If a panelist did not have so many years' experience directly in cyber security they still had had a long, even decades', career in IT where information and cyber security had been part of their daily work.

During the next two phases of the study the panelists were interviewed alone two times each: in the first iteration round the purpose was to introduce the topic to the panel. First propositions from the preparation phase were also tested, and statements and topics for the next round identified. After the first round the most popular views of the future of cyber security in manufacturing were identified. The next iteration round was designed based on the findings of the first round. In the second round the panelists were presented with more specific topics raised from the first round, and they argued for and against not only their own but also others' opinions and statements.

In this study cyber security is defined as actions which an organization takes to protect against cyber-attacks and their impacts. The structure and elements of the cyber security strategy and program depend on organization's calculated threat factors and risks. Thus, the base of the cyber security is organizational risk or threat analysis. [3] The definition to cyber security, however, is not commonly agreed upon. Therefore, the panelists were asked to state their own understood definition for cyber security. In addition to serving a research purpose, this was done to find agreement on terms and definitions used in the interviews.

Technical problems of industrial systems were left out of this study because they are usually considered internal weaknesses instead of external threats. In this study a cyber threat was defined as an external threat by using the thematic from the SWOT-analysis which is commonly known among risk management professionals [4, 53]. Hence, in this study the internal weaknesses were considered to become external threats only when an attacker could use them in a malicious way. Thus, production downtime caused by an unintended programming mistake was not considered a cyber-threat in this study even if, from information security point of view, it is a threat against availability and its impact to business could be substantial.

4. Results

In this section the key findings of the Delphi study are presented. In the analysis phase of the study and already during the Delphi rounds the understanding of the cyber security landscape was created based on the views of the panel. In the context of this study the word "panel" refers to all the panelists. It is used when the panelists can be seen as having a common understanding about a topic. In this chapter the topics which emerged from the first round for validation on the second round are highlighted with *italics*.

Already in the first round the expert panel seemed quite optimistic about the future of the cyber security in the Finnish manufacturing. This impression strengthened in the second round. Of course, the panelists saw that work and big steps are needed so that cyber security will be managed but, for example, no one suggested scenarios where Finnish manufacturing would be in some kind of trouble or crisis in 2021 because of cyber security problems.

However, the panel saw that making progress is essential so that manufacturing is able to respond to cyber threats in its future environment where the dependence on networks and information systems will be increasing rapidly, and when at the same time attacks become smarter and cybercrime becomes even more professional. Nevertheless, the panel believed that the good education level in Finland, and stable operative, political and geographical environment, create a good base and conditions for strong and viable cyber security.

Cyber security efforts cannot settle down even if the prevalent situation seems good and there are no imminent threats or security events. One of the panelists puts it well: *If you move slow with your cyber security [activities] you move backward in relation [to the threat landscape]*.

In one company this was noticed in practice when the panelist said that they reached the cyber security level they want just to realize that to stay at the level requires maintenance and work. One of the panelists commented that criminals move much faster than the companies and make bigger investments, and, contrary to the legal business, the criminals do not need to comply with legislation.

According to the panel the threat landscape of manufacturing is changing rapidly, which naturally challenges the companies' cyber security management. These are reasons why manufacturing will have to invest in its cyber security also in 2021.

4.1. Cooperation with others

The panel thought that in 2021 there will be still differences in cyber security levels between companies even inside Finland. However, at the same time they trusted that big and well-networked companies will have their cyber security on the right track. The panelists emphasized many times during the study cyber security cooperation and networking between different companies and authorities. The question *whether competing organizations would have the opportunity (or will) to collaborate in cybersecurity matters* emerged from the first round to the second. In the second round the panel concluded that it is possible.

The panelists added that it is possible to collaborate, for example, without breaking any competition laws. One of the panelists, however, saw that cooperation is easier with organizations that are not direct competitors. In addition, another panelist noted that it is easier to collaborate with companies that have a similar culture and are following similar regulations e.g. regarding to ethical competition.

A panelist added to this that in the future cyber security might be an important competitive and differentiating factor even in the manufacturing markets. Nevertheless, he continued that catching the leader organization is perhaps not realistic when they have done work many years in the field of cyber security. This of course helps the cooperation when the leading company does not need to worry about losing its advantage. One of the panelists summarises the topic: "Here in Finland we are forced to collaborate because the enemies are so powerful".

4.2. The definition of the cyber security

In the first round the panelists were asked to define cyber security from their point of view. As expected, the answers differed greatly. However, they were possible to synthesize into a definition: *Cyber security is mainly a new term on the top of the information security, and the word 'cyber' extends it to apply also e.g. to the IoT and industrial environments.* In the second round the panel agreed with this definition.

Many experts mentioned in the first round that cyber security consists of three elements: processes, people and technology. Some of the panelists also highlighted how nowadays the problems in cyber security extend also to the physical world: for example, by attacking the large systems in the factories it would be possible to threaten human lives.

However, couple of the panelists noted that most of the cyber security activities are known and normal

information security work and practices which should not be forgotten just because of the new term.

4.3. The objectives of cyber security in manufacturing

In the second round the panel was asked about the objectives of their companies' cyber security. Based on the first Delphi round the panel was given preselected options and from there all of them selected all that were relevant to their company's plans. Almost every panelist chose more than one of the options.

Fulfilling the requirements were clearly selected the most frequently by the panelists - only one of them left it out. One of the panelists said that it is just "mandatory". The next most popular option was *being among the bests* and *gaining competitive advantage by cyber security*. Both were selected four times and only one of the panelists gave both of the options as their company's objective for cyber security.

The competitive advantage was seen to be reached when the clients see the company more trustworthy than its competitors or through the secure industry 4.0. High quality, and the certainty to supply, were seen as enablers for company's trustworthiness. And both of which was mentioned to become weaker by poor cyber security management. However, it is not easy and one of the panelists commented that reaching the competitive advantage via cyber security is a challenge in big global companies.

One of the panelists, who selected *being among the bests* as their company's objective, told that their CEO made it very clear that for cyber security activities he/she is excepting world-class solutions. Nevertheless, couple of the panelists saw that their company has no need to *become the best in cyber security*. For instance, one panelist's opinion was that "of course, being the best would be great but unnecessary for our core business". *Become the best in cyber security* objective was selected only by one panelist who said that it is one of their company's value. However, he also added that "of course all the steps have to be taken to become the best and it is not happening quickly.

For none of the panelists' companies only *surviving* was the objective of cyber security. However, *reaching the same level as other companies such as competitors* was given as their objective by two panelists. One of them described that the company's cyber security should be in the level where "you are not the slowest prey moving".

One of the panelists reminded that the objective of cyber security could be changing depending on who asks: the executives could have a very different view of it comparing to shareholders or cyber security professionals.

Among the objectives the panel was also asked who are the ones they are comparing their cyber security level with – for example, who are "the leaders". To some panelists this was clear and they told that they are comparing themselves against e.g. their own industry. Some panelists mentioned critical self-evaluation and comparing against own performance history to be the best metric because "comparing directly to other companies does not tell you everything".

4.4. The important and less important cyber security topics in manufacturing in 2021

Corporate cyber security consists of many different parts, and investing similarly to all of them is not possible. Hence, it is important to decide how to allocate the limited resources. In the first Delphi round 31 topics (presented in Figure 1) emerged as the priorities for manufacturing cyber security in 2021. Besides, Figure 1 demonstrates what the panel selected as the most important topics for the cyber security in manufacturing in 2021 and what were given less emphasis.

As seen in the Figure 1 the panel was not unanimous with their opinions about many of the topics. Nevertheless, a few of the topics were quite clear priorities and some of them were clearly ranked as less important. There were also so-called controversial topics which are typical for Delphi studies. In futurology the topics with no clear trend are quite common. However, Delphi is known as a challenging method to study those weak trends because of its features which are designed for finding a consensus. [23, 26].

Nevertheless, in this study the reasons behind the disagreement of the panel about many topics could be explained by the different education, backgrounds and employer histories of the panelists as well as the size, clients and strategy of their employer organization. In addition, the panelists could interpret the meaning of the topics differently.

In some topics there was inconsistency between the answers during the interviews and the answers for the prioritization of the topics. For example, only one of the panelists named cyber security culture and employee awareness as a priority in 2021. However, during the other parts of the Delphi interviews many of the panelists were talking about cyber security culture related improvements and investments which

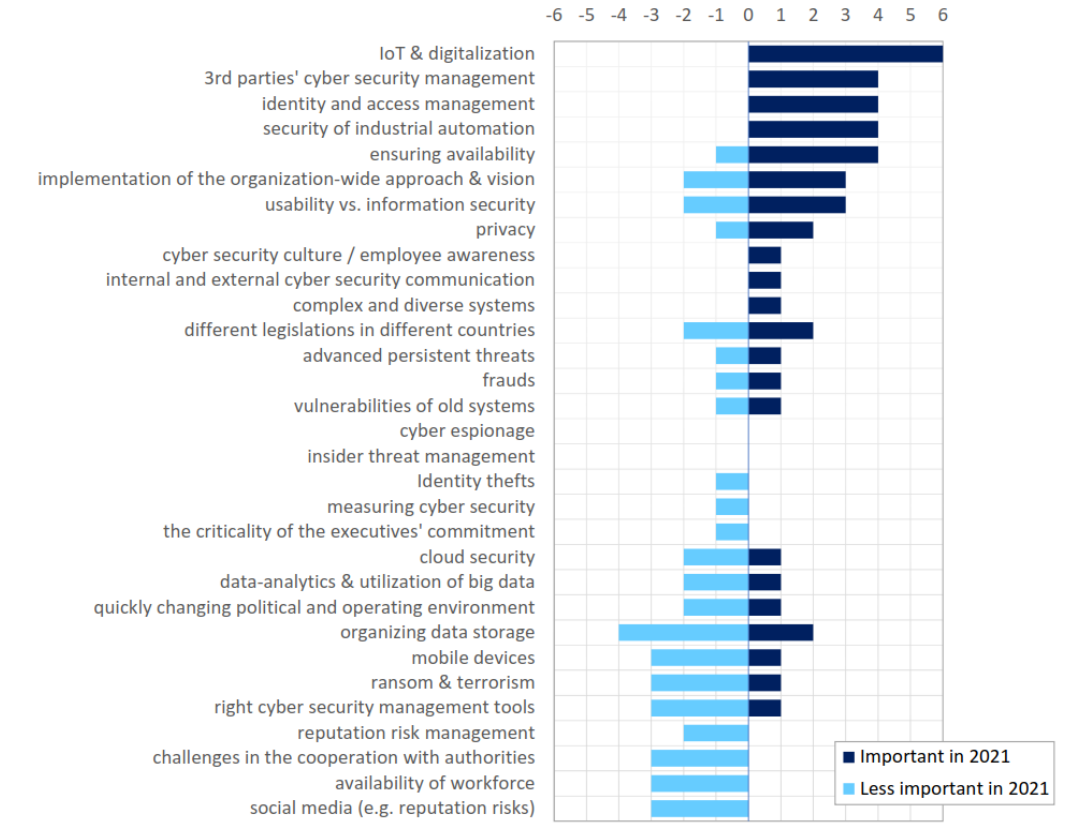

Figure 1. The important and less important cyber security topics in manufacturing in 2021.

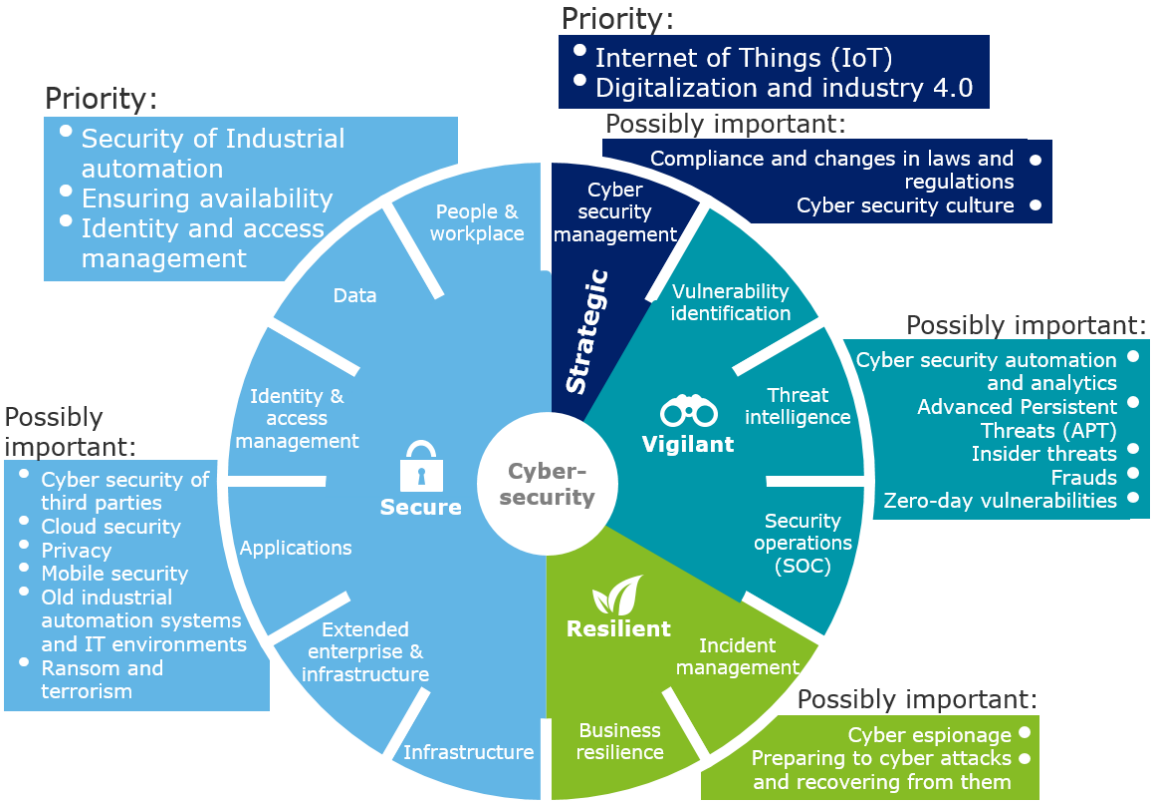

Figure 2. Priorities of cyber security in manufacturing in 2021.

their company is making within the next five years. This and other comments indicates that cyber security culture will likely be a more important topic in the future than how the panel prioritized it. As a whole the panelists indicated that their company's investment to cyber security will either grow during the next 5 years, or in case it had grown substantially during the recent years, remain in the current level.

The most important results of this study are divided under the topics of the Cyber Security Framework. As seen in Figure 2, the most important topics that will affect cyber security in manufacturing in 2021 will be IoT, digitalization, industry 4.0 and the security of the industrial automation. Also, identity and access management as well as ensuring availability will probably be priorities. Moreover, a group of weakly trending topics was identified. The "possibly important" topics are collected in the Figure 2 in relation to all of the Cyber Security Framework categories.

In this study less important cyber security related topics, in which manufacturing industry will not focus on so much in the future, are at least the commitment of companies' executives, reputation risk management, challenges in the cooperation with authorities and measuring cybersecurity. Many of these things the panel considered to be in order in 2021 and the work and cost related to them are mainly just because of maintenance. Hence, the panel said that manufacturing in 2021 will be allocating resources and investing in other cyber security topics.

As seen in Table 1 and Figure 1, even if the experts had many similar views as there was in the literature they did not select some of the topics mentioned in the literature as priorities for manufacturing in 2021. For example, both literature and the panelists saw that IoT, digitalization and industry 4.0. will be important drivers for the cyber security in manufacturing in 2021.

Other important topics identified were the security of the industry automation (ICS), identity and access management, as well as ensuring availability. These topics included mainly under Secure and Strategic categories of the Cyber Security Framework. However, possibly important topics which both the panel and the literature review considered important were also under Vigilant and Resilient categories. A good example of those was increasing use of cyber security analytics and automation.

In the literature review there was couple of topics from Strategic category that were not mentioned by the panel at all, or were considered less important. For instance, *lack of cyber security professionals* and *young employees' commitment to the cyber secure culture* were mentioned as serious threats in the literature but on the contrary, the panel was not very concerned about them. This reflects the positive attitude of panelists toward cyber security future.

Compared to the literature, the panel did not seem to experience special pressures about *increasing real-time requirements*. Even if the panelists admitted that in a hurry the business may unintentionally forget cyber security, they seemed to trust that no one of the employees wants to violate cyber security on purpose if the secure habits and actions are made easy enough to them.

Interesting was also the finding that panel ranked *identity and access management* among the most important topics but by contrast, nobody selected *identity thefts* as an important topic – even if it was mentioned couple of times by the panelists during the interviews and the literature mentions it as a problem especially for the manufacturing industry [e.g. 10]. One of the panelists even ranked it as less important topic for the Finnish manufacturing in 2021.

For the view noted above there could be many reasons. First, identity thefts were probably considered easier to solve than the whole *identity and access management.* Also according to the panel, *identity and access management* will be progressively related to third party management when in 2021 companies will have their own employees' identities managed but, for example, the identities for the externals, vendors, suppliers, and customers will need even more attention from the cyber security point of view. Besides, the literature as well as the panel during the Delphi rounds reminded that when industry 4.0 with cyber physical systems, smart factories and IoT will be soon part of the everyday life in manufacturing it means that also systems, industrial machines, hardware, software, or even a coffee maker or a light bulb will need their own identities.

One of the interesting parts of the Resilient category is *cyber espionage*. None of the panelists raised it as important nor less important, while in the literature and media it was considered an important topic especially for manufacturing [5, 6, 27, 28, 32, 53, 54, 55].

5. Discussion

The results of this study provide a future view of cyber security in the Finnish manufacturing industry in 2021. Although the study comes from a small geographic area, the global operating environment of the involved companies allows to generalize the results to manufacturing cyber security in the developed countries. Figure 2 shows priority areas

that manufacturing business and cyber security professionals can start with when planning for example cyber security investments and the direction of future security efforts. Each organization has and will have their unique cyber security background and challenges. However, in many organizations the priority risks seem to have common root causes.

The manufacturing systems seem to enter cyberspace faster than ever. Therefore, not only manufacturing companies' IT department but also their business and daily operations level need to see the necessity of the proactively addressed security in those newly connected environments such as in industrial automation and industry 4.0 systems. In many manufacturing companies the implementation of the new solutions and the connecting of old systems have already been started. Despite this, the main decisions regarding cyber security seem to be still mainly on the strategic level only, and has not been fully implemented to the company-wide operational level. This study indicates that in 2021 it can still be a huge risk to manufacturing not to implement security solutions simultaneously with newly connected systems.

Besides new solutions mentioned, other future priorities identified are ensuring the availability of manufacturing systems as well as the integrity of their control data. Those are not new priorities for manufacturing. Nevertheless, this will also become even more important and challenging in the coming years when formerly closed manufacturing environments will increasingly be connected to open networks. This increases the possibility of an outsider to disrupt the system. Traditionally cyber security has been seen as defending against leaking data and quickly responding to detected attacks. However, even a short downtime in manufacturing can become extremely expensive, and hence ensuring that systems and environments are proactively secured is vital for the business.

It has been emphasized in literature for a long time that senior management needs to be committed to cyber security and endorse its importance. This study indicates that this has become given in organizations, as the panel considered executives' low commitment will no longer to be one of the priority risks in their organizations in 2021. Although this result is very positive from the standpoint of security scholars, future studies should look more into the attitudes of managers in operational level toward cyber security to find out if this study indeed reflects a more general rooting of management's and business' commitment to cyber security.

While the findings of this study mirror the findings in literature, it is important to note that all attempts to look into the future reflect the present. Within the five-year span there might be upcoming disruptive innovations in the field. Forecasting such disruptions is difficult. Thus, it is good to keep in mind that the findings of a Delphi study are always only a glimpse into the future. Security managers can find possible pointers for direction from this study, but they should also keep in mind that it is vital to be prepared for the unexpected.

The impact of manufacturing's cyber security problems will not only be very costly to the business but also increasingly seen in the physical world. For example, cyberattacks may threaten people's health, or suddenly stop whole factories around the world. Therefore, in 2021 cyber security cannot be addressed separately from the business and operations anymore. This study indicates strongly that not later than now is the time for manufacturing companies to make sure that they will include and implement the security not only in their newly connected solutions but also in their daily business, operations, environment, and culture. Only if addressing the risks proactively it will be possible for companies to focus on the cyber security priorities in 2021.

Because the topic of the study is wide and recently there has not been similar research, there are still questions that need to be answered concerning the future of cyber security in manufacturing, and other industries. Future endeavours could extend to concern longer time period than until 2021. Also, in 2021 it would be interesting to study if the predictions became realized and if so, why. This would help in predicting cyber security in the future.

6. References

[1] Deloitte Cybersecurity Framework, 2017

[2] Suomen kyberturvallisuusstrategia ja taustamuistio (Finnish Cyber Security Strategy), Turvallisuuskomitea (Finnish Safety Committee), 2013

[3] M. Lehto and A. Kähkönen, Kyberturvallisuuden kansallinen osaaminen, The University of Jyväskylä, 2015

[4] SWOT, The Finnish Risk Management Association (FinnRima), 2013, http://www.pk-rh.fi/index.php?page=swot.

[5] M. Lehto, J. Limnéll, E. Innola, J. Pöyhönen, T. Rusi, and M. Salminen, Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtionneuvoston kansliasivistys- ja tutkimustoiminta, 2017

[6] Verizon 2017 Data Breach Investigations Report, Verizon, 2017

[7] Verizon 2016 Data Breach Investigations Report, Verizon, 2016

[8] Renault stops production at some sites after cyber attack, Daily Mail, MailOnline, 2017,

http://www.dailymail.co.uk/wires/reuters/article-4502266/Renault-stops-production-sites-cyber-attack.html.
[9] 2016 Cyber Security Intelligence Index, IBM X-Force, 2016, http://www-03.ibm.com/security/data-breach/cyber-security-index.html.
[10] 2017 Internet Security Threat Report, Symantec, 2017, https://www.symantec.com/security-center/threat-report.
[11] Threat Horizon 2019: Disruption. Distortion. Deterioration., Information Security Forum, 2017
[12] AT&T Cybersecurity Insights: What Every CEO Needs to Know About Cybersecurity - Decoding the Adversary, AT&T, 2015
[13] Tech Trends 2017: The kinetic enterprise, Deloitte University, 2017
[14] EMEA 360 Boardroom Survey, Deloitte, 2016
[15] Navigating legacy: Charting the course to business value, Deloitte University, 2016
[16] Cost of Data Breach Study, IBM Security: Ponemon Institute, 2016
[17] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2016
[18] E. Mossburg, H. Calzada, and J. Gelinne, Beneath the surface of a cyberattack: A deeper look at business impacts, Deloite. 2016
[19] Industry 4.0: An Introduction, Deloitte, 2015
[20] J.Paasi and N.Wessberg, Menestyvää liiketoimintaa suomalaisissa valmistavan teollisuuden yrityksissä 2020-luvulla – Neljä skenaariota, VTT, 2016
[21] Pictures of the Future, Siemens, 2016, https://www.siemens.com/innovation/en/home/pictures-of-the-future.html.
[22] Delfoi-metodi, eDelfoi, 2012, https://edelfoi.fi/viewbulletin.page?bulletinId=5.
[23] O. Kuusi, Delfoi-menetelmä, Metodix, 1999
[24] R. Popper, How are foresight methods selected? Foresight, 2008, pp. 62-89
[25] C. Okoli and p. D. Pawlowski, The Delphi Method as a Research Tool: An Example, Design Considerations and Applications, Information & Management, 2003
[26] V. Valtonen, Turvallisuustoimijoiden yhteistyö operatiivistaktisesta näkökulmasta, Maanpuolustuskorkeakoulu, Taktiikan laitos, 2010
[27] ENISA Threat Landscape 2016, ENISA, 2017
[28] ENISA Threat Landscape 2015, ENISA, 2016
[29] Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, ENISA, 2015
[30] AT&T Cybersecurity Insights: The CEO's Guide to Securing the Internet of Things, AT&T, 2016
[31] L. Kessem, Ransomware: How consumers and businesses value their data, IBM X-Force Research, 2016
[32] Kaspersky Security Bulletin: Predictions for 2017 'Indicators of Compromise' are Dead, Kaspersky Lab, 2016
[33] N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad, and P. Berg, Secure Information Sharing in an Industrial Internet of Things, University of Agder, Norway, 2016
[34] T. Davenport and A. Amjad, The future of cybersecurity, Deloitte University, 2016
[35] R. Contu and E. Perkins, How the Internet of Things Will Impact Cybersecurity, Gartner, 2016
[36] S. B. Alaybeyi, Don't Be Misled by the IoT Security Myths, Gartner, 2016
[37] 2017 Threats Predictions, McAfee Labs, 2016
[38] I. Saif, p. Peasley, and A. Perinkolam, Safeguarding the Internet of Things, Deloitte University Press, Deloitte Review, 2015
[39] RBI Guidelines for Cyber Security Framework, Deloitte, 2016
[40] Services: Cyber Risk, Deloitte Global
[41] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, Security and Privacy Challenges in Industrial Internet of Things, Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE
[42] S. Wang, J. Wan, D. Li, and C. Zhang, Implementing Smart Factory of Industrie 4.0: An Outlook, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, 2016
[43] AT&T Cybersecurity Insights: The CEO's Guide to Data Security, AT&T, 2017
[44] A. Spadafora, The Average IoT Device is Compromised after Being Online for 6 Minutes, ITProPortal, 2016, http://www.itproportal.com/news/the-average-iot-device-is-compromised-after-being-online-for-6-minutes/.
[45] Will the Internet of Things be bigger than the Industrial Revolution? Business Insider Nordic, 2016, http://nordic.businessinsider.com/will-the-internet-of-things-be-bigger-than-the-industrial-revolution-2016-9/.
[46] 'Internet of Things' Connected Devices to Triple by 2021, Reaching over 46 Billion Units, Juniper Research, 2016, https://www.juniperresearch.com/press/press-releases/'internet-of-things'-connected-devices-to-triple-b.
[47] Internet of Things; A Vision for The Future, OTA, Online Trust Alliance, 2016, https://otalliance.org/news-events/press-releases/ota-publishes-vision-future-internet-things.
[48] J. Lee et al., Introduction to cyber manufacturing, Manufacturing Letters, Society of Manufacturing Engineers (SME), no. 8, pp.11-15.
[49] AT&T Cybersecurity Insights: The CEO's Guide to Navigating the Threat Landscape, AT&T, 2016, 28 p.
[50] H. Shey et al., The Cybercriminal's Prize: Your Customer Data And Intellectual Property, Forrester, 2015
[51] How the Internet of Things will affect security & privacy, Business Insider, 2016, http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?IR=T.
[52] Report on Workshop on Security & Privacy in IoT, European Commission, AIOTI, 2017,
[53] B. Gertz, China cyber espionage continues, The Washington Times, 2016, http://www.washingtontimes.com/news/2016/sep/28/china-cyber-espionage-continues/.
[54] 2016 Manufacturing Report, Sikich, 2016
[55] Yearbook 2016: National security is a joint effort, the Finnish Security Intelligence Service, 2017
[56] M. Abdi, M. Azadegan-Mehr, and S. Ghazinoory, SWOT Methodology: A State-of-the-Art Review for the Past, a Framework for the Future, Journal of Business Economics and Management, 2011