Deloitte.

Predicting the future of Cyber Security in Finnish Manufacturing

Cyber Secure Manufacturing in 2021

Contents

Research setting and method

The study was conducted in three phases.

Phase 1: Preparation

Carrying out the literature review, arranging a preparation workshop for 14 cyber security experts, and selecting the professionals for the Delphi panel. The selection of the professionals to the panel was based on the quality of their expertise and diversity of their backgrounds. Therefore, the panel as a group was able to offer a broad view of the future of cyber security in the industry.

Panellist background:

The panellists were from different large Finnish manufacturing companies operating globally, many of which had a turnover of over half a billion euros in 2015. Half of the panellists had at least ten years of experience in cyber security, and most of them had over seven years of experience in their current security role. Even lower year direct cyber security experience professionals still had a lengthy, even decades' long, career in IT where information and cyber security had been part of their daily work.

Phase 2 and 3: Two one-on-one interviews

The purpose of the first interview round was to introduce the topic to the panel. The first propositions from the preparation phase were also tested, and statements and topics for the next round identified. The most popular views of the future of cyber security in manufacturing were identified after the first interviews.

The next interview round was designed based on the findings of the first round. In the second round, the panellists 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.


CUSTOMER SERVICE LEVELS
CHECK FILES
PERSONAL
SERVICE LEVEL AND STATISTICS
TIME SCALE
BIG DATA
FINANCE
NEW BUSINESS
MARKET MEDIA
NEW CLIENTS
GLOBAL STRATEGY
NEW BUSINESS
CUSTOMER SERVICE
NEW INFORMATION
27%
41%

Introduction

Manufacturing is rapidly entering the 4th industrial revolution where the old, complex and formerly closed environments, solutions and systems meet new, connected and more open ones. This offers immense possibilities for the manufacturing industry, and every manufacturing company should harvest the benefits of these innovative solutions to power performance and make their business more successful.

Already today, the network connections from the industrial systems at the "floor level" are rapidly increasing. Every manufacturer of an industrial component or sensor wants to collect all the possible data from their own systems. In a large industrial process, there are dozens of these manufacturers. Each connection to the outside world exposes the systems to cyber risks. In the near future, we will probably see the implementation of 5G mobile networks into each of these sensors. Industrial IoT will not ask users for permission to connect to the Internet; it will be there by default.

The year 2017 saw two large malware campaigns. In April, the case of WannaCry encrypted and hijacked thousands of computers around the world. People were left standing clueless at the shop counters while the registers were locked and inoperable. An even more serious case was yet to come about a month later. The NotPetya case destroyed the information systems that it infected and this time there was a price tag. A large logistics company said publicly that they lost 300 million dollars in the wake of the attack. What is even more alarming is that this company wasn't even a target, but got caught in the crossfire and became collateral damage.

In the midst of these insecure times, we found ourselves with many questions around cyber security in manufacturing. Questions like, what is the near-term role of cyber security in this age of rapid development in manufacturing? Is there a risk that cyber security will be bypassed at this speed of change, and all the benefits of the new solutions diluted? Is there a risk that business benefits of the connected world remain untapped from manufacturing companies because of cyber security incidents? What should manufacturing companies prioritize, and how is this seen by decision makers and industry professionals? Do Finnish manufacturing companies' cyber security professionals feel that they have enough resources, investments, and support from their executives in order to secure the business in the required manner also in the near future?

Above all, what should the focus areas be when planning cyber security road maps to ensure that the manufacturing business also runs smoothly in 2021?

To get the answers to these, we decided to study the subject. In addition to taking a dive into the current literature, we also asked experts. We interviewed a panel of cyber security professionals from large and globally operating Finnish manufacturing companies. We used a known future forecasting method called Delphi, inter alia, in order to ensure the necessary anonymity of the panel members. After and in between many iterative interviews, we analysed the answers and we are now confident that we have:

A VIEW OF THE CYBER SECURITY LANDSCAPE IN FINNISH MANUFACTURING IN 2021

Luckily, we also heard good news about the cyber security in manufacturing. Nevertheless, we found that there will be a lot of work ahead in this field to secure the future of the changing manufacturing business alongside the digitalizing society. Everyone is needed and, therefore, we wanted to share these insights with you.

Please enjoy!

Katariina Kannus
Cyber Risk
Deloitte

Tero Mellin
Director, Cyber Risk
Deloitte

January 2018

What did they say?

To foresee the future of cyber security in manufacturing, it is crucial to understand its current landscape, decisions, desires, and plans, as these give an indication of the future state. Indications include, for example, how manufacturing companies are currently investing or have plans to start investing, what kind of level of cyber security they have decided to reach, and which of the current trends will also occur in the future.

This section includes a brief introduction to the relevant parts of the current landscape which will, according to this study, impact the future of the cyber security in manufacturing. We then move on to summarizing the panellists' view of the future of cyber security in manufacturing before discussing the priorities the panellists had in relation to both literature and Cyber Security Framework.

The current landscape

Developed countries and their manufacturing industry today are increasingly dependent on digital networks and their services. In the future, the dependency will only increase. Cyber security is an enabler of digitalization but when managed poorly it can jeopardize all the benefits that digitalization can bring[1].

Cyber security professionals in the manufacturing industry need to make decisions in the constantly changing threat landscape. They are dealing with a plethora of both known threats that require instant reactions as well as less well-known and unpredictable future threats. They have to prepare for the unexpected today while planning for the future at least a couple of years ahead. The life cycles of technical systems in Operational Technology are measured in decades rather than in years in conventional IT. It is essential that cyber security plans are connected and aligned with the company's strategy, plans, and vision.

In today's world of constant change, cyber security is not an exception. It is more like a pioneer in regard to change: every hour of every day, attackers are, and will be, using new innovative ways to threaten the manufacturing business by challenging its cyber security. IT systems need to be updated and patched at a very rapid pace to keep up with the vulnerabilities.

Enter the traditional industrial world 'once a year maintenance break' approach in the equation to start to see the challenges that the CSO, CISO, and other cyber defenders are faced with. In the very near future, when manufacturing systems are increasingly entering cyberspace, it will be impossible to run the business without first securing

it properly. Therefore, careful and fact-based planning of a reasonable use of limited cyber security resources as well as the strategic decision-making around the topic is essential for securing the manufacturing business.

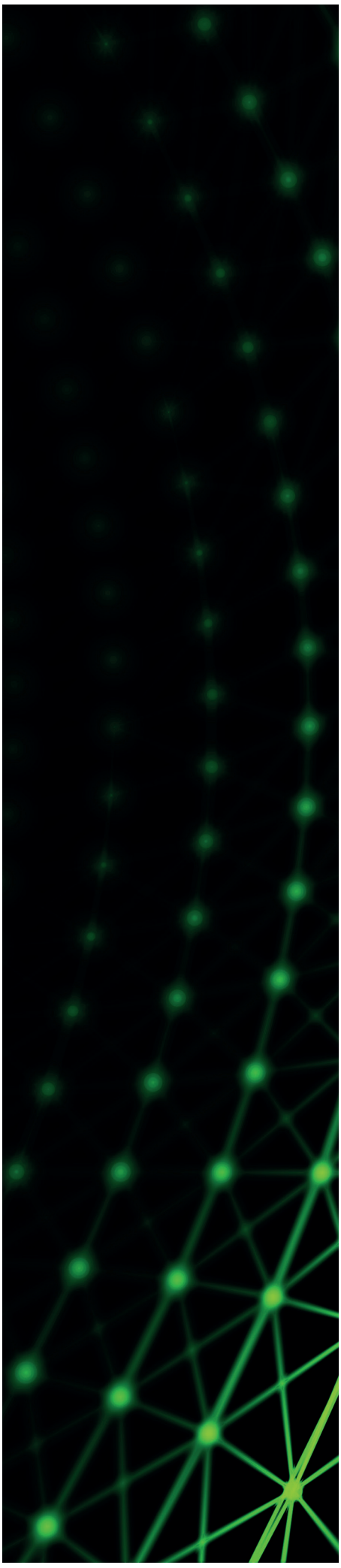
Nowadays, it is highly important that the companies' cyber security is proactive: after a serious cyberattack, the damage is already done. Reactive improvements are too late if, for example, plants are already at a standstill or sensitive information stolen[2, 3, 4]. In addition, the Finnish national cyber security strategy[5] states that preventing cyber security threats needs proactive operations and planning. The new operative environment requires know-how and the ability to react fast and consistently in the right way. To reach proactive cyber security, it is important to know what the priorities will be in the near future, what will not be so important going forward, and what the main objectives are of cyber security.

The manufacturing industry's business and operating environment is increasingly global. More and more operations and stakeholders are spread all around the world. In the future, the changing global operative environment introduces not only opportunities to grow but also challenges[6, 7, 8]. One of the biggest challenges seems to be cyber security management and the contingency planning for the future cyber landscape.

Cyber security does not belong only to the IT department any more[9, 10, 11, 12]. Globally, its importance has been noticed in the corporate boardrooms and the executive interest has been forecasted to rise[12]. New technologies in manufacturing environments bring a new kind of cyber threats with them while the attackers find more and more ways to use the known and unknown vulnerabilities of old systems, technologies, and processes.

Forgetting cyber security could be highly expensive to companies. According to the studies[13, 14], an information security breach can cost the victim company 4-73 million dollars on average. The total impact and costs of cyber security problems, e.g. data breaches, are truly complicated and can only be discovered in the long term[15]. However, according to our study, it seems that Finnish manufacturing cyber security professionals are well aware of the potential costs of security breaches. It also seems that the Finnish manufacturing company executives are becoming more and more aware of the threats and their costs to the business.

Now, the only question seems to be if the rest of the company, e.g. the middle management and daily operations, are aware enough so that the all benefits of the new technologies, innovations, and newly connected systems are not lost.



“If you move slowly with your cyber security you move backwards in relation”

Definition of cyber security

The panellists were asked to define cyber security (in Finnish: kyberturvallisuus) from their point of view. As expected, the answers differed greatly. However, they can be synthesized into a definition: Cyber Security as a term combines traditional information security and a connected world of information systems to the physical world.

Many experts mentioned that cyber security consists of three elements: processes, people, and technology. It was also highlighted how nowadays the problems in cyber security also extend to the physical world: for example, by attacking complex and critical factory systems, it would actually be possible to threaten human lives. It was also noted that most cyber security activity is well-known and normal information security work and practices which should not be forgotten just because of the new term.

About the future of the cyber security in manufacturing

There is optimism for the future of cyber security in Finnish manufacturing. The panellists saw that work and big steps are needed to manage cyber security but, for example, no one suggested scenarios where Finnish manufacturing would be in some kind of crisis in 2021 because of cyber security problems.

However, the panel shared a view that fast progress is essential to enable valid responses to cyber threats in the future manufacturing environment where:

1. **The dependence on networks and information systems will increase rapidly,**
2. **attacks become smarter and**
3. **cybercrime becomes even more professional.**

Nevertheless, the panel believed that the high education level in Finland as well as the stable operative, political, and geographical environment create a good basis and conditions for strong and viable cyber security. Finnish legislation is also seen as supportive from a cyber security point of view.

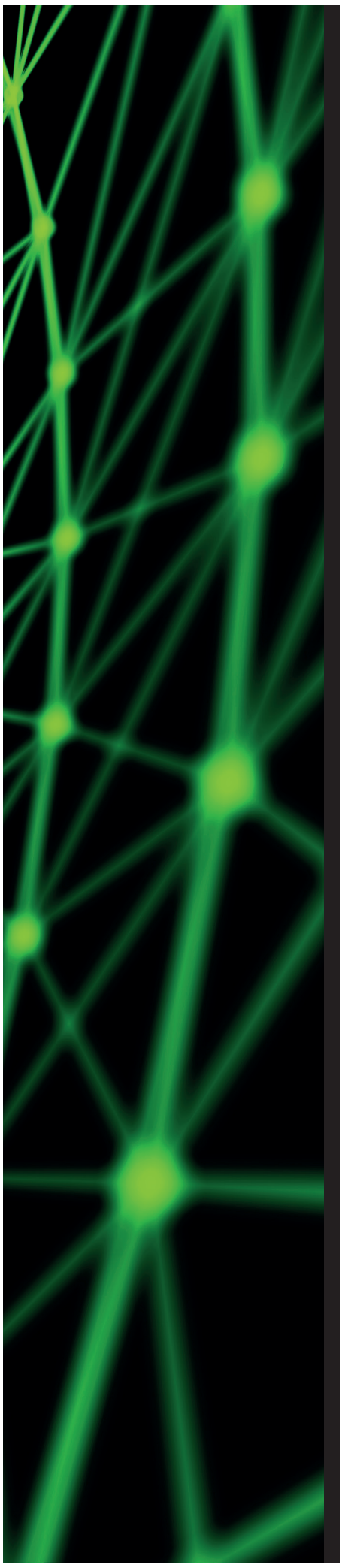
Cyber security efforts can never be scaled down. This will still be the case even if the prevalent situation seems good and there are no imminent threats or security events. One of the panellists put it well: If you move slowly with your cyber security [activities] you move backward in relation [to the threat landscape]. In one company, this was noticed in practice when they reached the cyber security level that they had set, just to realize that, in order to stay at that level, it required new maintenance and work. Criminals seem to be always one step ahead and move much faster than the companies as they make bigger investments and, contrary to legitimate business, criminals do not comply with the legislation.

The panel claimed that in 2021 there will still be differences in cyber security levels between companies even inside Finland. However, at the same time, they estimated with confidence that big and well-networked companies will have their cyber security on the right track.

Cyber security cooperation and networking between different companies and authorities is a necessity. The question of whether competing organizations would have the opportunity (or will) to collaborate in cyber security matters emerged in all the interview rounds. In the second round, the panel concluded that it is possible to collaborate, for example, without breaking any competition laws.

Our study shows, however, that cooperation is easier with organizations that are not direct competitors. In addition, another panellist noted that it is easier to collaborate with companies that have a similar culture and are following similar regulations, e.g. regarding ethical competition.

The study indicated that cyber security has strong potential to become an important competitive and differentiating factor in the manufacturing markets. Catching up with the market leader is perhaps not realistic if they have a head start of several years. This would actually help cooperation when the leading company does not need to worry about losing its advantage. One of the panellists summarizes the topic: “Here, in Finland, we are forced to collaborate because the enemies are so powerful”.



The objectives of cyber security

Which of the following best describes your organisation's future objectives for cyber security?

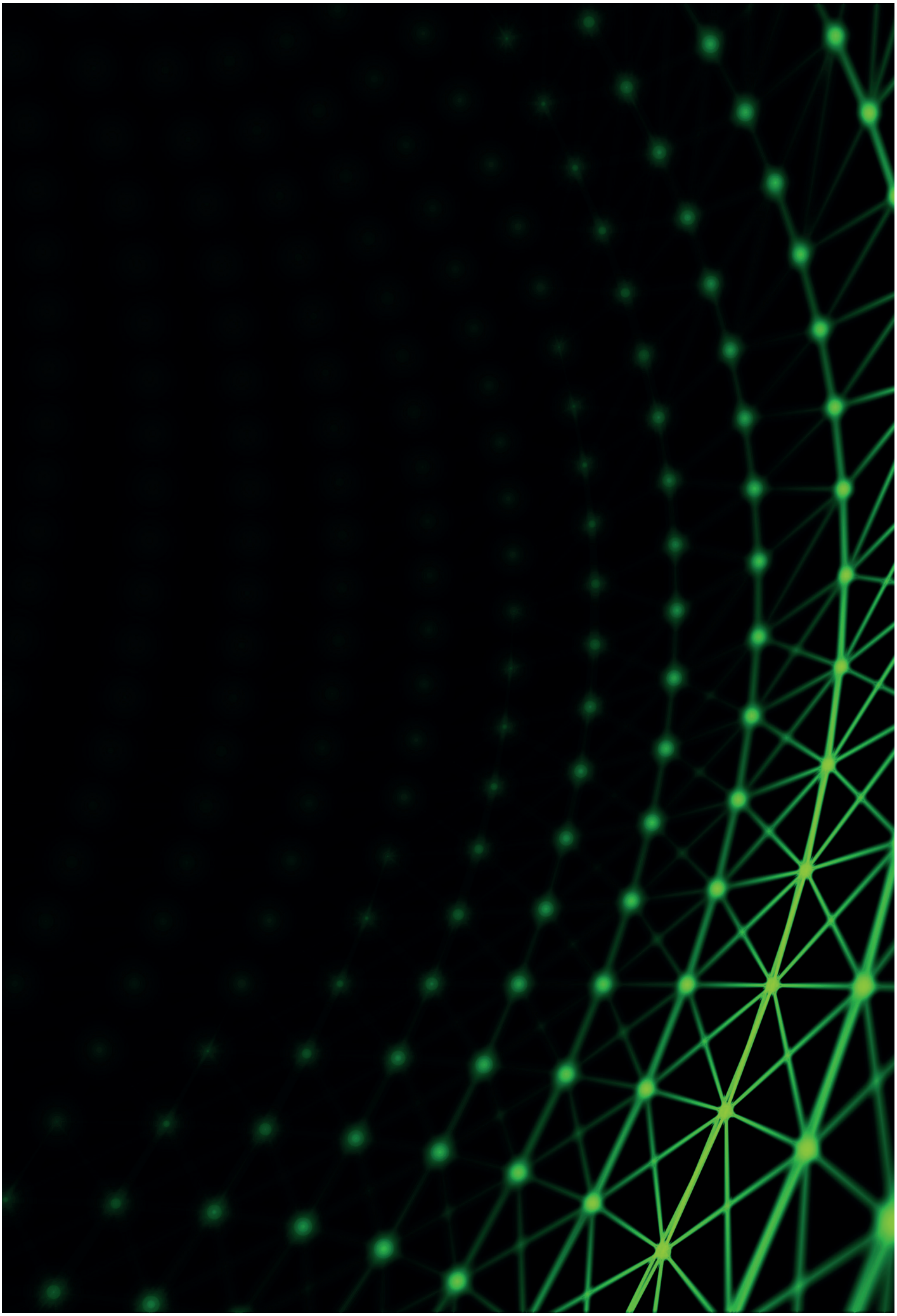
Meeting the compliance requirements was clearly among the most important cyber security future goals. Only two of the panellists left it out. It was described as "just mandatory". None of the panellists chose *only surviving* as their cyber security objective. It was mentioned that the objective of cyber security could be changing depending on who asks: the executives could have a very different view of it compared to shareholders or cyber security professionals.

For some of the panellists, *reaching the same cyber security maturity level as other companies such as competitors* was the future goal of their companies' cyber security. One of them described that the company's cyber security should be at the level of where "you are not the slowest prey moving".

One of the most popular future goals was *being among the best* and *gaining competitive advantage by cyber security*. This was seen to be reached through clients viewing the company as more trustworthy than its competitors or through the secure industry 4.0. High quality and the certainty to supply were seen as enablers for companies' trustworthiness. Both of which were mentioned to weaken by poor cyber security management. However, it is not an easy road, and one of the panellists commented that reaching competitive advantage via cyber security is and will be a real challenge in big global companies.

One of the panellists, who selected *being among the best* as their company objective, pointed out that their CEO is expecting world-class solutions in cyber security. Some panellists said that their company has no need to become the best in cyber security. One comment was, for example, that "of course, being the best would be great but unnecessary for our core business". *Becoming the best in cyber security* was selected only by one panellist who said that it is one of their company's values.

Our study also asked who the manufacturers are comparing their cyber security level with – for example, who are "the leaders" mentioned by the panellists. To some, this was clear and they stated that they are comparing themselves against e.g. their own industry. Some panellists, however, saw critical self-evaluation and comparing against own performance history to be the best metric because comparing directly to other companies did not give them a satisfactory overview.



Cyber security priorities in manufacturing in 2021

Figure 2 shows a summary of the priority topics that, according to this study, manufacturing business and cyber security professionals can start with when planning 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.

In Figure 1, the priority topics are divided under the categories of the Deloitte Cyber Security Framework[16]. The categories of the framework are Secure, Strategic, Vigilant, and Resilient. As seen in Figure 1, the Internet of Things, digitalization, industry 4.0, and security of industrial automation will be the most important drivers for cyber security in the manufacturing industry in 2021. In addition, identity and access management as well as ensuring availability will most likely be priorities.

Moreover, a group of weakly trending topics was identified. The "possibly important" topics are collected in Figure 1 in relation to all of the Cyber Security Framework categories.

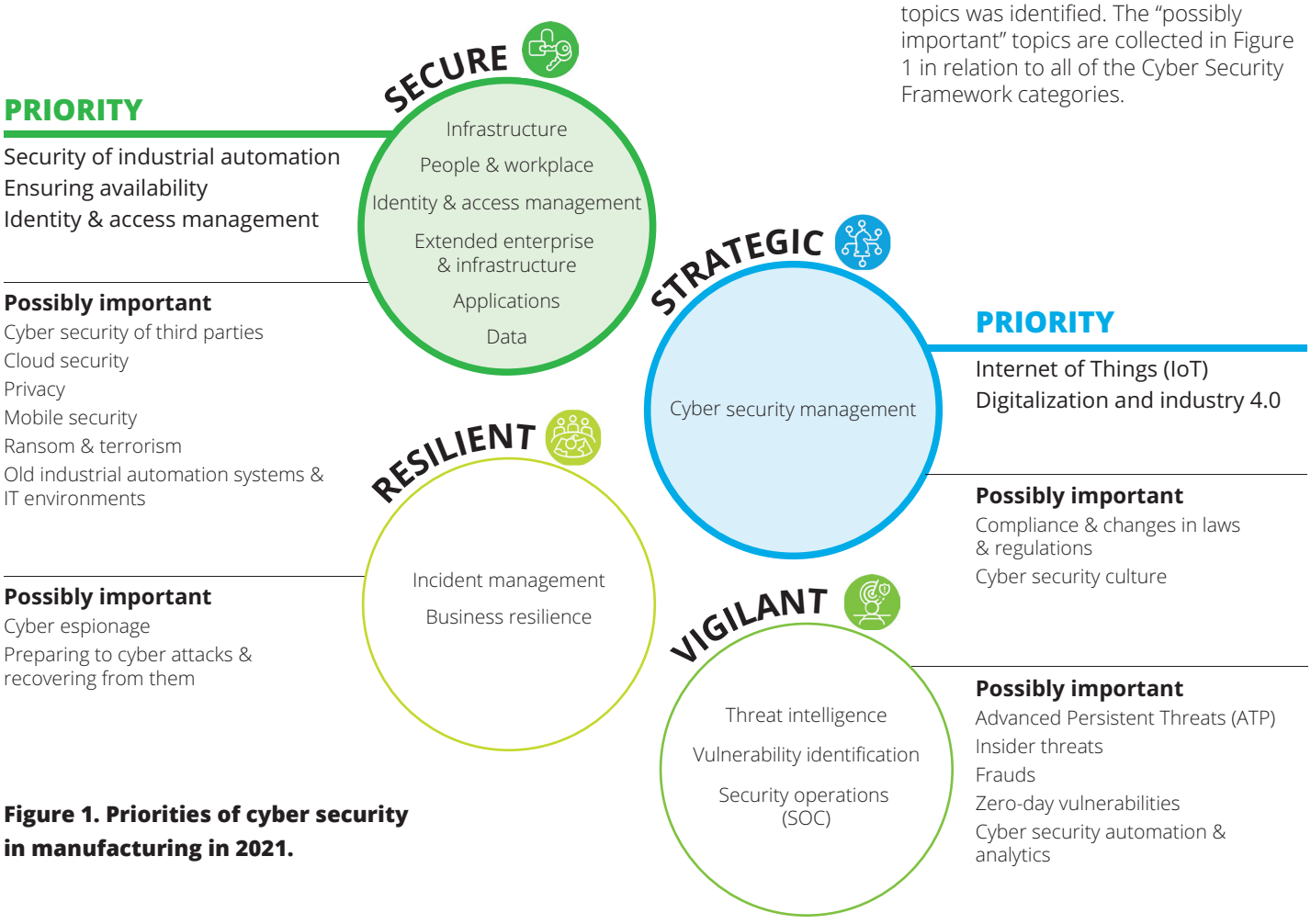


Figure 1. Priorities of cyber security in manufacturing in 2021.

“All the steps have to be taken to become resilient against incidents in cyber security; there are no shortcuts.”

As visible in Figure 1, the priority topics fall under Secure and Strategic categories of the Cyber Security Framework. However, there were also possibly important topics, which were considered important by both the panel and in the literature, under the Vigilant and Resilient categories. A good example of those was increasing use of cyber security analytics and automation.

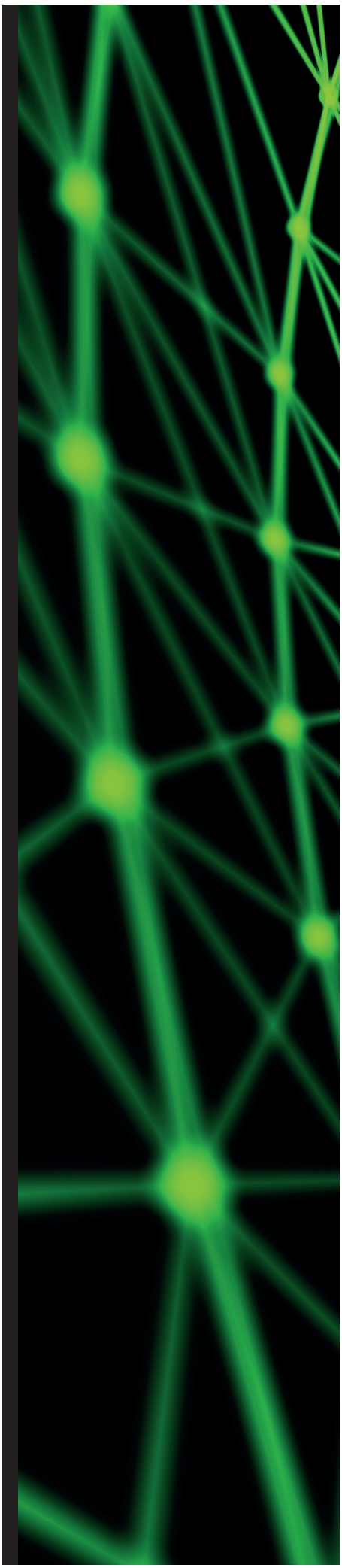
In this study, less important cyber security related topics, in which the manufacturing industry will not focus on so much in the future, were also identified. Those were the commitment of companies’ executives, reputation risk management, challenges in the cooperation with authorities, and measuring cyber security. The panel considered many of these to be in order in 2021 and, therefore, the work and costs related to them will mainly come from maintenance. Therefore, the panel said that manufacturing in 2021 will mainly be allocating resources and investing in other cyber security topics.

In the literature review, there were a couple of topics from the Strategic category that were not mentioned by the panel at all, or were considered less important. For instance, a lack of cyber security professionals and young employees’ commitment to a cyber-secure culture were mentioned as serious threats in the literature. The panel, on the other hand, was not very concerned about these, which reflects the positive attitude of panellists toward the future of cyber security.

It has also been emphasized in the literature for quite some time that senior management needs to be committed to cyber security and endorse its importance. This study indicates that this has become self-evident in the Finnish manufacturing organizations, as the panel considered executives’ low commitment will no longer be one of the priority risks in their organizations in 2021.

Compared to the findings in the literature, the panel did not seem to experience special pressure on increasing real-time requirements. Even as the panellists admitted that the business may unintentionally forget cyber security when in a hurry, they seemed to trust that employees don’t want to violate cyber security on purpose if the secure habits and actions are made easy enough to follow.

One of the intriguing topics of the Resilient category is cyber espionage. None of the panellists prioritized it as important or less important, while in the literature and media it was considered an important topic especially for manufacturing[1, 2, 17, 18, 19, 20, 21, 22].



Conclusions

So far, the main decisions regarding cyber security seem to be mainly on the strategic level, and have not been fully implemented to a company-wide operational level. This study indicates that in 2021 it can still be a huge risk to manufacturing not to implement cyber security solutions simultaneously with newly connected systems.

Besides new solutions in manufacturing, ensuring the availability of manufacturing systems as well as the integrity of control data was also identified as a future priority. These are not new priorities for manufacturing, but rather become even more important and challenging in the coming years as 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 defence against leaking data and responding quickly to detected attacks. In the future, ensuring that systems and environments are proactively secured is vital for the business as even a short downtime in manufacturing can become extremely expensive.

An interesting finding was also that the panel ranked identity and access management among the most important topics but, by contrast, no one selected identity theft as an important topic. It was mentioned a couple of times during the interviews and there are also references in the literature to this as a problem especially for the manufacturing industry[23]. One of the panellists even ranked it as a less important topic for the Finnish manufacturing in 2021.

For the view noted hereinabove there could be many reasons. First, identity theft is probably considered easier to solve than the whole identity and access management. According to the panel, identity and access management will also 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 external partners, meaning, vendors, suppliers, and customers will need even more attention from the cyber security point of view. The literature as well as the panel reminded everyone that as industry 4.0 with cyber physical systems, smart factories, and IoT will soon be part of the everyday life, in manufacturing it means that systems, industrial machines, hardware, software, or even a coffee maker or a light bulb will also need their own identities.

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 panellists named cyber security culture and employee awareness as a priority in 2021. However, during the other parts of the Delphi interviews many of the panellists talked about cyber security culture related improvements and investments which their company is making within the next five years.

This contradiction indicates that cyber security culture will most likely be a more important topic in the future than how the panel prioritized it. As a whole, the panellists indicated that their company's investment in cyber security will either grow during the next 5 years or remain at the current level. The latter was indicted in cases where it had grown substantially during recent years.

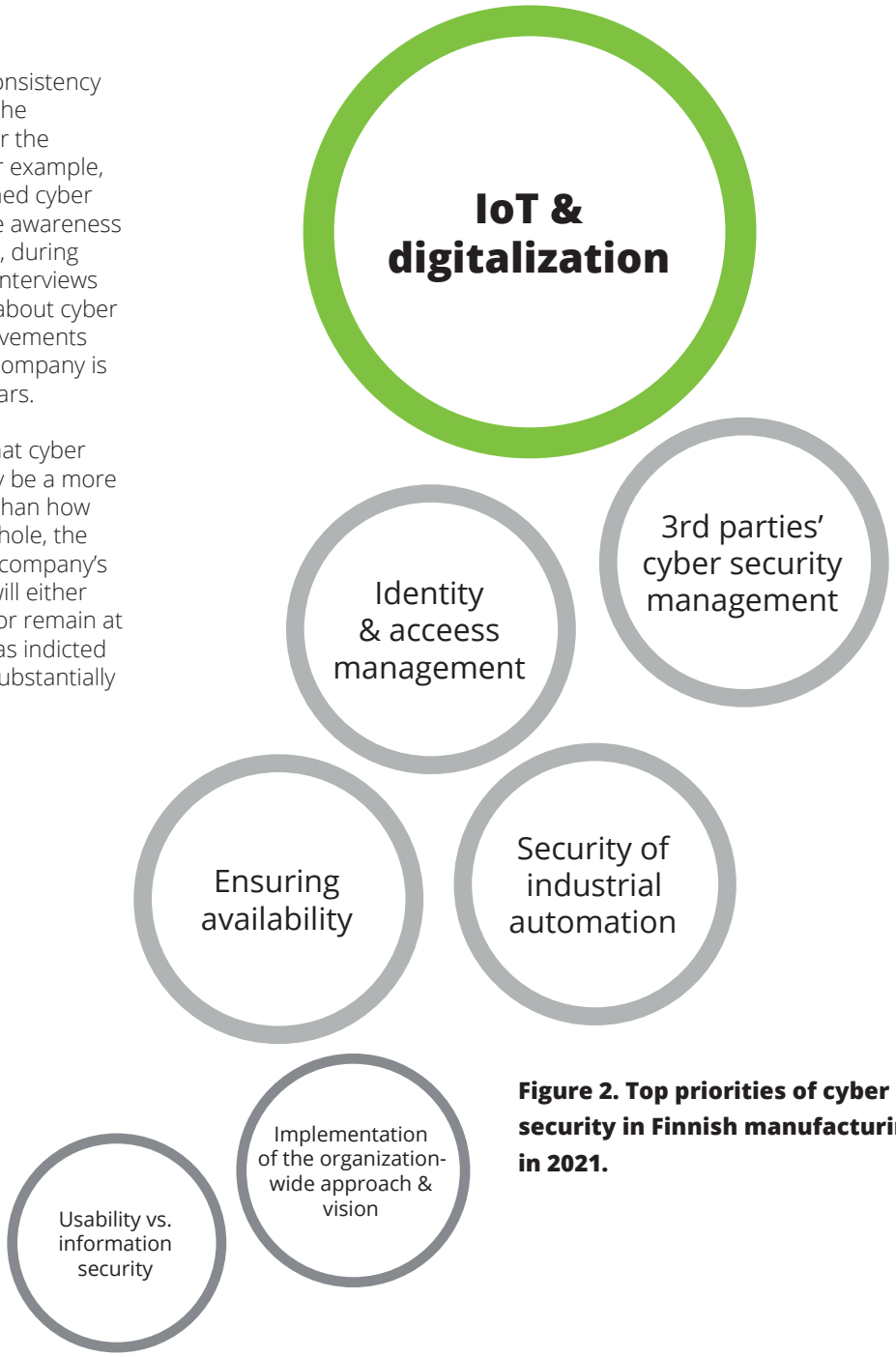


Figure 2. Top priorities of cyber security in Finnish manufacturing in 2021.

And here's what we say

According to the study, cyber security will still be an important topic within Finnish manufacturing in 2021 as industrial systems, products, and environments are increasingly complex, Internet-enabled and interconnected. In 2021, the field of cyber security will continue to be ever-evolving and new threats will continue to appear on an, at least, daily basis. Many Finnish manufacturing companies are leaders in innovative, new connected technologies, and creators and early adapters of solutions that help business succeed. Cyber security will be indispensable not only for earning client trust but also in keeping the critical infrastructure, people, and business running.

At the same time, boards and senior management have an increasingly important role in providing oversight of cyber security strategy execution, monitoring the manufacturing companies' cyber security posture, and being prepared to respond to investor, client, analyst, and regulator questions about the actions taken on cyber security.

The study indicates that in the 2020s there will still be a risk that manufacturing companies will see cyber security only as a cost and not as an opportunity or as a business enabler. Managing cyber security risks keeps companies out of trouble. However, cyber risk management techniques can also be used in positioning for success. Operatively thinking: How to leverage risk to power performance? Therefore, in the near future, it is crucial that manufacturing companies view cyber risks through a different lens. Instead of thinking of the risks only in terms of the number of attacks or the actual value that could be lost, they should consider how better cyber risk management would allow them to reach more customers, maintain better relationships, or manufacture more products.

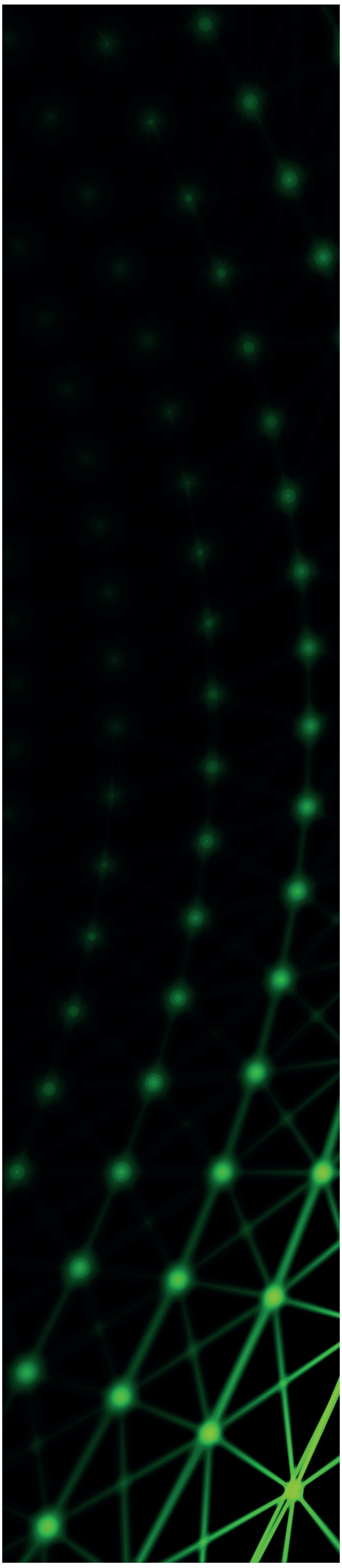
It is vital that manufacturing companies continue to invest in cyber security capabilities strategically. Investments need to be continuous not only because threats keep on evolving, but also to keep the competitors behind. By focusing on the right areas, manufacturing companies can become resilient organizations that can quickly and proactively respond to new threats and attacks, while remaining flexible to meet today's market needs.

The impact of manufacturing industry cyber security problems will not only be very costly to the business but also increasingly visible in the physical world. For example, cyberattacks may threaten people's health, or suddenly stop whole factories around the world. Cases like NotPetya in 2017 showed us that even a single incident can take up a lot of skilled cyber security resources to help large organizations recover.

If the impact is truly global and takes down multiple large enterprises at the same time, there simply is not enough help available. ISACA predicts that there is a lack of more than two million cyber security specialists globally already today[24]. Therefore, in the 2020s, cyber security cannot be addressed separately from the business and operations.

Cyber security in manufacturing is and will be a topic that has to be in place to enable the digital society to run smoothly. The first truly clever and disruptive uses of AI in cyber security will probably be done by nation state hackers or organized criminal groups with healthy budgets and resources.

This study strongly indicates that now is the time for manufacturing companies to make sure that they will include and implement security not only in their newly connected solutions but also in their daily business, operations, environment, and culture. It will only be possible for companies to focus on the necessary cyber security priorities that will keep manufacturing secure and safe in business in 2021 and beyond if addressing the risks proactively.



Contact us

Katariina Kannus
Cyber Risk
Deloitte

+358 (0)50 3309 164
katariina.kannus@deloitte.fi

Tero Mellin
Director, Cyber Risk
Deloitte

+358 (0)50 3580 316
tero.mellin@deloitte.fi

References

1 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

2 Verizon 2017 Data Breach Investigations Report, Verizon, 2017

3 Verizon 2016 Data Breach Investigations Report, Verizon, 2016

4 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.

5 Suomen kyberturvallisuusstrategia ja taustamuistio (Finnish Cyber Security Strategy), Turvallisuuskomitea (Finnish Safety Committee), 2013

6 Industry 4.0: An Introduction, Deloitte, 2015

7 J.Paasi and N.Wessberg, Menestyvää liiketoimintaa suomalaisissa valmistavan teollisuuden yrityksissä 2020-luvulla – Neljä skenaariota, VTT, 2016

8 Pictures of the Future, Siemens, 2016, https://www.siemens.com/innovation/en/home/pictures-of-the-future.html.

9 Threat Horizon 2019: Disruption. Distortion. Deterioration., Information Security Forum, 2017

10 AT&T Cybersecurity Insights: What Every CEO Needs to Know About Cybersecurity - Decoding the Adversary, AT&T, 2015

11 Tech Trends 2017: The kinetic enterprise, Deloitte University, 2017

12 EMEA 360 Boardroom Survey, Deloitte, 2016

13 Cost of Data Breach Study, IBM Security: Ponemon Institute, 2016

14 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2016

15 E. Mossburg, H. Calzada, and J. Gelinne, Beneath the surface of a cyberattack: A deeper look at business impacts, Deloitte. 2016

16 Deloitte Cybersecurity Framework, 2017

17 ENISA Threat Landscape 2016, ENISA, 2017

18 ENISA Threat Landscape 2015, ENISA, 2016

19 Kaspersky Security Bulletin: Predictions for 2017 'Indicators of Compromise' are Dead, Kaspersky Lab, 2016

20 B. Gertz, China cyber espionage continues, The Washington Times, 2016, http://www.washingtontimes.com/news/2016/ sep/28/china-cyber-espionage-continues/.

21 2016 Manufacturing Report, Sikich, 2016

22 Yearbook 2016: National security is a joint effort, the Finnish Security Intelligence Service, 2017

23 2017 Internet Security Threat Report, Symantec, 2017, https://www.symantec.com/security-center/threat-report.

24 ISACA: Cyber Security Skills Gap, 2016. https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

This report is based on a study completed in the first quarter of 2017.
The study was conducted in cooperation with Tampere University of Technology.

https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/24932/Kannus.pdf?sequence=3&isAllowed=y

www.deloitte.fi