Cyberwatch FINLAND

Special media of strategic cyber security

MAGAZINE 2020/2

CYBERSECURITY TOPS THE LIST **OF CRITICAL COMPETENCIES IN A POST-COVID WORLD**

QUARTERLY REVIEW Q2 2020

KVARTAALIKATSAUS Q2 2020

Harri Sundvik: "A seismic shift to digital independence is gaining momentum"

Contents
2020/2

> **CREATING A RELIABLE SITUATIONAL AWARENESS OF CYBER SECURITY IS IMPOSSIBLE IF YOU DON'T UNDERSTAND WHAT IS HAPPENING IN THE CYBER WORLD.**
>
> Aapo Cederberg

Cyberwatch MAGAZINE

Special media of strategic cyber security

Publisher
Cyberwatch Finland
Tietokuja 2
00330 Helsinki
Finland
www.cyberwatchfinland.fi

Producer and commercial cooperation
Cyberwatch Finland team
office@cyberwatchfinland.fi

Layout
Atte Kalke, Vitale
atte@vitale.fi

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

Print house
Scanseri, Finland

Cover and content pictures Shutterstock

AHEAD OF THE GAME, BUT FOR HOW LONG?

– INSIGHTS FROM A BENCHMARKING STUDY ON FINLAND'S CYBERSECURITY LANDSCAPE

For seven years, the annual Digibarometer study has evaluated how well individual countries utilize digitalization and ranked them accordingly. This spring, the Digibarometer 2020 took a special focus on the topic of cybersecurity as a key competence in digitalization. While Finns rank above the European average in cybersecurity performance, the statistics indicate that Finland is falling behind the cutting edge of development.

CYBERSECURITY IS TO DIGITAL PROWESS WHAT AUTOMOBILES ARE TO INDUSTRIAL CAPABILITY

In the field of industrial economics, the automotive industry has often been perceived as a benchmark for the technological prowess of nations. The logic behind this idea is simple: the manufacturing of high-quality automobiles requires a vast set of different kinds of industrial and technological capabilities. If one can build good quality cars, one can build anything—or so the thinking goes.

In many ways, the same is true for the cybersecurity industry in the era of digitalization. Mastering cybersecurity at a high level requires a vast set of various kinds of digital skills and capabilities, as well as broader strategic understanding and ICT business acumen. Therefore, it can be argued that the cybersecurity performance of a country is a good indicator of its overall level of expertise in digitalization. In the relentless world of constantly evolving cyber threats, the attackers are not pulling any punches. Thus, anyone on the defensive side cannot be fooled regarding their own ability.

CYBERSECURITY IS MORE RELEVANT THAN EVER BEFORE

The significance of cybersecurity as a key factor in digitalization has overall increased in recent years. Every year, cyber threats cause losses in the amount of

text:

M.SC. (ECON. & B.A.) JURI MATTILA is a researcher at the Research Institute of the Finnish Economy (ETLA) and a doctoral candidate at Aalto University. In his research, he examines various phenomena of the digital economy. Mattila is also a member of the board of directors for the Lammi Savings Bank.

D.SC. (IND. ECON.) TIMO SEPPÄLÄ is a Principal Investigator (PI) at the Research Institute of the Finnish Economy (ETLA) and a Professor of Practice (Digital Operations) at Aalto University. Seppälä co-heads a collaborative techno-economic and -legal research and policy program between ETLA and University of California, Berkeley, focusing on "Shaping the Future in the Era of Intelligent Tools: AI and Beyond"

hundreds of billions of euros to individuals, businesses and public sectors around the world. In 2016, security software company McAfee estimated the global costs of cybercrime to be 600 billion euros—roughly 0.8 % of the world's annual GDP. If anything, the prevalence of cyber threats has only increased ever since. Log data recorded by Cisco's information security software indicates that the global volume of cyber security incidents quadrupled between 2016 and 2017. Similarly, according to recent estimates by F-Secure, the number of cyber-attacks in the world doubled between 2017 and 2018.

In addition to the increase in the prevalence and the extent of cyber threats, their significance has also grown in recent years. For example, in Europe the GDPR legislation has allowed for stricter sanctions to be imposed on companies for neglecting information security. Thus, the threat of financial consequences from cyber risks has also increased for large corporations and small companies alike.

GROWING INDUSTRY STARVED OF EXPERTISE

Over the years, the ever-growing threat of annual business losses has fuelled the growth of the global cybersecurity sector. In 2017, the annual turnover of cybersecurity companies was estimated to be 150 billion dollars world-wide. The sector's turnover is predicted to grow at an annual rate of approximately ten percent. However, as operators are constantly required to keep acquiring new skills and capabilities, the rapidly changing technological landscape has put companies under a constant cybersecurity skills shortage which is already throttling the growth of the industry.

According to a study conducted by the Cyber Security Competence for Research and Innovation Consortium (CONCORDIA), in the near future, cybersecurity experts will be required to master a total of 200 different competences and 90 practical skills. Respectively, a recent survey of the Finnish Information Security Cluster (FISC) found that approximately 60 % of Finnish cybersecurity companies feel that there is a shortage of cybersecurity professionals in Finland. The demand for labour is particularly dire for expertise in digital identities, competence in cloud architecture and talent with business competence in addition to cyber-security competence. Consequently, professionals with such expertise are mostly recruited from abroad, *e.g.* from India.

Finland is beating the average but losing the race

In the field of cybersecurity, simply improving one's performance is not enough. To keep up with the competition, one has to make progress—and one has to do it quickly. For example, according to the Global Cybersecurity Index by the International Telecommunications Union, Finland improved its global cybersecurity

ranking from 23rd position to 19th place in 2014–2018. However, Finland's index score from 2014 would have only been good enough for the 66th position in 2018. The figurative comparison paints a strong image of how detrimental just a few years of stagnation can be in the cybersecurity arms race.

Based on Eurostat's statistics, the overall cybersecurity situation in Finland was relatively good compared to the rest of Europe in 2019. Finland ranked clearly above the EU28 country average on most indicators. However, the statistics indicate that Finland is clearly falling behind the countries at the cutting edge of development. Comparison of the Nordic countries shows that Finland is overshadowed by Sweden and Denmark on most indicators.

WHY DOES FINLAND STUMBLE ON INFORMATION SECURITY?

While Eurostat's data does not reveal the intricate reasons behind the survey answers, information security appears to stand out as particularly concerning factor for Finland. With regard to smart devices in particular, the information security behaviour of consumers seems to be marked by disinterest in how personal data is used, rather than lack of information or knowledge. While 25 % of the Finnish smart device users never restricted the rights of their installed applications, only 4 % was oblivious to this opportunity.

Data leaks also appeared to have a pronounced role as a cybersecurity issue for domestic companies. According to Eurostat, data leaks were three times more prevalent in Finland than in the EU28 countries on average in 2019. Moreover, one in six Finnish large-scale companies had had their sensitive data compromised in one way or another—a proportion over twice as high as in Sweden.

In Finland, small businesses were the best performing in the business size comparison. By nearly all indicators, the management of cybersecurity in small Finnish companies was above the European average. Even though the management of cybersecurity in large companies was clearly more advanced than in small businesses, large Finnish companies underperformed compared to other EU countries. The situation of medium-sized domestic companies also leaves something to be desired, especially in comparison to our counterparts Sweden and Denmark.

Compared to the rest of Europe—or even just other Nordic countries—Finland invests more heavily in the teaching of digital skills.

IS FINLAND PREPARED FOR THE FUTURE OF CYBERSECURITY?

It is anticipated that the current tools and practices of cybersecurity will be comprehensively transformed and challenged by the developments in the upcoming years. For example, as more and more devices are connected to the Internet, more pronounced digital device identities will be required. Products, services, and the companies providing them need similar level identifiers as are used to identify human individuals today. While some initiatives are already working on the problem, Finland should be looking to engage in the development of digital device identification methods on a more systemic national level.

Another example of a disruption looming overhead is the development of quantum computers. While most estimates suggest that practical applications of quantum computing are still 15–20 years away, the quantum threats to data cyphering and digital identification are already very real. While numerous quantum-resistant encryption methods are known, none can offer a direct plug-and-play transition. In order to prepare for the era of quantum computing, Finland should without further delay draw up a roadmap on how critical systems will be updated to quantum-resistant encryption. Sectors with long equipment life cycles should also already start considering the possibilities of quantum cryptography when planning and designing future systems.

WORKING HARD OR WORKING SMART?

Compared to the rest of Europe—or even just other Nordic countries—Finland invests more heavily in the teaching of digital skills. Although the effects of these investments cannot be seen instantly, the trendlines in cybersecurity performance raise the question of whether Finland is investing in the right areas to create a comprehensive range of competences in digitalization. According to the Digibarometer study, only 5 % of all the Finnish businesses have included any kinds of cybersecurity-related communications on their public websites. The low hit rate leaves one wondering, do Finnish companies suffer from a lack of commitment to develop their cybersecurity capabilities?

Whatever the reasons behind the declining trendlines may be, the signs are clear. Without a course correction in cybersecurity performance, Finland may soon be facing the imminent threat of losing its digital edge entirely. The country must readjust its take on cybersecurity and start perceiving it as a key competitive factor in the digital era, much like the automotive industry has been perceived in the industrial era. In the rapidly growing and transforming industry of cybersecurity, Finland has enormous potential. The question is, how do we turn that potential into performance—and how do we do it fast?