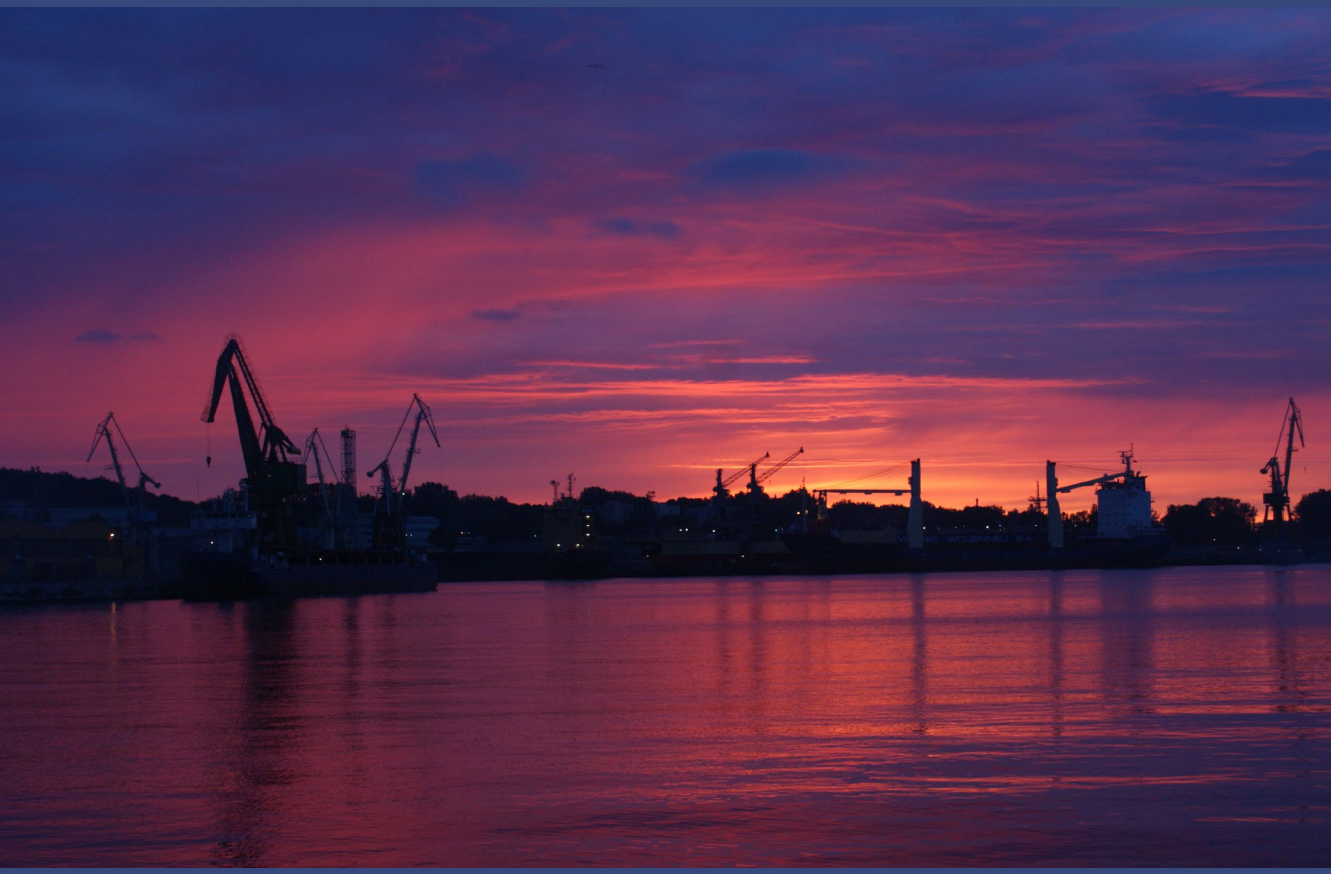

IOT PRODUCTIVITY VERSUS CYBERSECURITY

Is the risk worth it?

Vesa Tuomala

South-Eastern Finland
University of Applied Sciences

Vesa Tuomala

IOT PRODUCTIVITY VERSUS CYBERSECURITY

Is the risk worth it?

South-Eastern Finland
University of Applied Sciences

XAMK DEVELOPMENT 151

SOUTH-EASTERN FINLAND UNIVERSITY OF APPLIED SCIENCES
KOTKA 2021

Authors and South-Eastern Finland University of Applied Sciences
Cover picture: Vesa Tuomala
Layout and printing: Grano Oy
ISBN: 978-952-344-338-9 (PDF)
ISSN: 2489-3102 (ebook)
julkaisut@xamk.fi

Vesa Tuomala, Master Mariner (B.Sc.), Henley MBA, Project Manager

ABSTRACT

As the adoption of IoT devices increases rapidly in modern society, so does the risk of cybersecurity threats and dangers.

This desk study is the second part of the series concerning the Internet of Things (IoT) devices and cybersecurity. The first part of IoT desk study, "Logistics and maritime need to focus on cybersecurity in the Internet of Things (IoT) Technology" was published in Xamk Beyond in December 2020.

The study focuses on the productivity of the Internet of Things (IoT) versus cybersecurity and the risks that affect these IoT devices. The hypothesis is that IoT business can be sustainable with high productivity and profitability.

The methodology of the research was the study of new and relevant information from the papers and articles written by IoT experts. This work is part of a larger desk study of IoT technology that aims to broaden the knowledge of IoT and cybersecurity issues of logistics.

The research concentrates on the growth of IoT technology business, productivity management, the benefits of IoT devices' productivity in different sectors and cybersecurity concerning these devices. As well as focusing on connectivity networks for IoT devices.

The desk study reveals the need for a thorough investigation of the fourth industrial revolution called INDUSTRY 4.0 for the logistics and maritime sector.

KEY WORDS: The Internet of Things, Cybersecurity, Risk Management, Maritime, Logistics, Ports

CONTENTS

ABSTRACT 3

1 INTRODUCTION 5
1.1 Hypothesis of this desk study 5
1.2 Research methods 6
1.3 Roadmap for the study 6

2 DEFINING TERMINOLOGY 7
2.1 The Internet of Everything and Internet of things 7
2.2 Productivity management 7
2.3 Cybersecurity 8
2.4 Risk management 8

3 RESEARCH 10
3.1 Basics and growth of IoT devices 10
3.3 Measuring IoT productivity management 12
3.3 Productivity and IoT devices 13
3.3.1 Smart maintenance strategy 13
3.3.2 Managing comfortable environment in smart offices 14
3.3.3 IoT solutions in logistics and transportation 15
3.4 Cybersecurity and privacy threats 16
3.5 Connectivity to networks 18

4 DISCUSSION 20
4.1 Productivity with better performance generates more profitability 20
4.2 Cybersecurity is important to digitize operations 23

5 CONCLUSION 24

REFERENCES 25

ACKNOWLEDGEMENTS 28

1 INTRODUCTION

This desk study examines the benefits and threats of digitalization for the GET READY project in the logistics sector. GET READY is a cross-border cooperation project between Russian and Finnish academic, scientific, and business partners.

The main objective of the GET READY project is to create interest in increasing environmentally sustainable development awareness and readiness for the stakeholders in the vulnerable coastline. One of the objectives is to search for best practices for the development of the digitalization of port owners and operators, as well as shipping companies. This framework aims to create innovations for sustainable ports, protecting the environment, and mitigating climate change. The project is implementing capacity building in professional competencies via education and training, training content of digitalization of ports and cases of smart ports, and managing environmental issues.

One of the project objectives is to investigate possible best practices for the development of the digitalization of port owners and operators, as well as shipping companies.

The first IoT desk study for the project, "Logistics and maritime need to focus on cybersecurity in the Internet of Things (IoT) Technology" was published in Xamk Beyond in December 2020. This second study continues the theme of digitalization articles for the project. The research question for the digitalization challenges is: *IoT productivity versus cybersecurity - is the risk worth it?*

This desk study focuses on IoT productivity and the cybersecurity challenges in logistics. First, the study unpacks the terms of the research question. Second, the information and research about IoT productivity is examined, in order to develop an adequate and accurate productivity measurement system. These results will be examined in a correlation of benefits, expenses and cybersecurity threats. The third part of the study focuses on the discussion of productivity and explores whether it is more beneficial than the cybersecurity risks for IoT devices in industry.

1.1 HYPOTHESIS OF THIS DESK STUDY

In 1987, Robert Solow came up with a paradox of information technology and productivity, he stated "You can see the computer age everywhere but in the productivity statistics." Solow's Paradox is defined as the "discrepancy between measures of investment in information technology and measures of output at the national level". (Goldin, et al. 2020.) It means the rate of productivity appears to be slowing dramatically in the age of the Internet. Is it possible that this phrase will change in the era of growth of the IoT devices?

The study was carried out as a part of the Master of Engineer studies' Networks and Cybersecurity course of the productivity of the Internet of the Things (IoT) devices versus cybersecurity. The research interest is whether the productivity benefits of these devices outweighs the possible threats of cybersecurity, and is the risk worth it?

The paper's hypothesis is that, increasing profit with the use of IoT is a sustainable way to achieve higher productivity. I research productivity and cybersecurity issues to see how these subjects are entangled and examine targets for productivity enhancement. My argument is that these points of views are not mutually exclusive rather they are complementary.

1.2 RESEARCH METHODS

The study method is qualitative content analysis. In order to understand the fundamentals of IoT productivity and cybersecurity threats to these devices, this desk study uses open access research done by universities, researchers, companies, and intellectuals. In order to grasp a more holistic picture, the study also utilises material from the producers of IoT devices as well as material on IoT productivity from IoT, cybersecurity, and risk managed experts.

The research is qualitative and executed with the FINER method (Fandino 2019). The FINER criteria mean that research needs to be feasible, interesting, novel, and confirming, refuting, or developing previous research. In this context, feasibility means that there need to be enough subjects, technical expertise, and be manageable in scope. The research also needs to be carried out following ethical principles and be relevant. In this study, relevancy focuses on scientific knowledge and researching the future. The FINER method is a very effective and suitable tool to examine productivity and research cybersecurity.

1.3 ROADMAP FOR THE STUDY

My reason to research cybersecurity is two-fold, on the one hand, I am interested in helping organizations prevent incidents and mitigate the results of data breaches. On the other hand, in writing these studies I gain more information for myself about topic research that interests me and I can better teach the future generations of students.

This paper proceeds as follows, I define the terminology used in this study. After reviewing the literature and data collection of the qualitative research, I examine the data in the research section. In the discussion section, I review the findings and analyse the gathered research information. The final part of the study concludes the issues raised and includes recommendations for further research.

2 DEFINING TERMINOLOGY

2.1 THE INTERNET OF EVERYTHING AND INTERNET OF THINGS

The Internet of Everything (IoE) describes future machine-to-machine (M2M) communications for people, structures, vehicles, systems, and processes. In practice, Internet of Things (IoT) devices mean new applications for smart sensors, information, and communications technology to connect the billions of devices around the world. Additionally, IoT means the connectivity of physical objects such as vehicles, devices, buildings, and electronics, and the networks that allow them to interact, collect and exchange data. The Industrial Internet of Things (IIoT) refers to the manufacturing industry, improving the industry's connectivity, efficiency, scalability, timesaving, and cost-savings. IIoT specifically refers to increasing efficiency and improving health and safety. (Tuomala 2020.)

IoT technology enables future digital transformation and the exchange of information between human to machine, and between machine to machine, collecting massive data from us to the systems. These IoT devices become a part of our everyday normal life and help us in the home, healthcare, logistics and transport technologies, and industrial networks. (Tuomala 2020.)

2.2 PRODUCTIVITY MANAGEMENT

Peter Drucker, a well-known American management consultant for modern business theory, said: "Without productivity objectives, a business does not have direction. Without productivity measurement, a business does not have control" (SPRING 2011).

The definition of productivity is commonly described as the unit output per a given unit of input. It means that productivity is an ever-increasing range of performance. The company's results become how a business is operated with the resources of people, processes, business function units, and with suppliers. If business operations are improved to become more efficient, then productivity is improved. Productivity is an additional output that can be produced by companies with cost savings. The mathematical expression of this is **Productivity = Output / Input**. (OECD 2001; SPRING 2011; GSMA 2019.)

The output measures could be the physical quantity and financial value. In some fields, the physical value can be units produced and the financial value could be increasing sales, production value and valued-added. The input measures can be numbers of hours worked, the number of workers or the cost of labour. Productivity indicators are labour as value-

added per worker (effectiveness) and capital productivity. Capital productivity is a result of improvements in the machinery and equipment used. (SPRING 2011.)

2.3 CYBERSECURITY

The British Cambridge Dictionary defines cybersecurity as "the things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet". The European Union Agency for Cybersecurity (hereinafter ENISA), bases their definition of cybersecurity on the principles of 'Confidentiality', 'Integrity' and 'Availability' or CIA for short". Thus, information security means that the information is under the purview of confidentiality, integrity and availability of information (CIA). Confidentiality means that information is not available or disclosed to unauthorized individuals, entities, or processes. Integrity requires that the information is accurate and complete. Availability means that the information is accessible and usable upon demand by an authorized entity. (ENISA 2015.)

Therefore, information security means that the information is available when needed, intact (original) and confidential, so that no one else can access it without permission. In this case, we can say that the security risks are under control. Information security is a key factor in cybersecurity. It proactively manages cyber threats and effects operations in the physical world. A security threat and the event endangers security, which causes a cyber-disruption situation. A cyber threat or an event in process affects the cyber environment that endangers the security of society. The cyber threat may be directed against vital societal activities, infrastructure or citizens. A cyber-attack is a realized cyber threat that endangers the operation of an organization or system. The management of cyber incidents divides into preparedness, situational awareness, prevention and recovery. Cybersecurity means that the threats and risks to society's necessary functions are under control. (Turvallisuuskomitea 2017.)

2.4 RISK MANAGEMENT

The Ministry of State in Finland guidelines describes risk management as a function that manages and controls organizational risks. The impact of the risk can be positive or negative compared to what is expected. According to the guidelines, risk means the effect of uncertainty on goals and a deviation from expectations. Risk refers to the impact of uncertainty on objectives and it can have positive or negative, or both effects. Risk is a deviation from expectations that creates opportunities or threats. The risk can concern people, animals, property, information systems, and the environment or community values. Risk assessments are one way of preparing for different threats. Following a risk assessment threat models are created. These models are refined through continuous and regular risk assessments and the models are updated regularly. Risk management is systematic and

goal-oriented operations, organizational management and development. (Rousku 2017; Turvallisuuskomitea 2017.)

According to the Ministry of Finance of Finland, risk management assesses the risks that an organization takes in setting strategic goals and how they are managed to achieve the goals. A Project's success is achieved by ensuring good risk management. Risk assessments must be carried out in day-to-day work and when faced with significant changes. According to the guide, many risks are not able to be eliminated, so the consequences must be prepared for in advance. Risk management should be done in cooperation with the people involved and includes risk analysis, measures to be planned and implemented, and to monitor and correct the situation. In addition to taking a risk, there should be other ways to avoid or negate it. If necessary, the risk can be minimised by sharing it or by preventing damage. Adequate resources for operations must be determined in risk management. (Rousku 2017; Turvallisuuskomitea 2019.)

3 RESEARCH

The VTT Technical Research Centre identified three key threats in Finland in 2013: loss of manufacturing capability, early retirement combined with an increased life expectancy, and limited energy and raw materials. The environmental policies and reducing Co2 emissions may affect the competitiveness of Europe. Therefore, it is important to improve productivity to achieve greater output, fewer work-years, more value for less raw materials and energy with better sustainability. (VTT 2013.)

In this section, I present forecasts of the growth of IoT devices and industries, which may improve productivity with the next level of sensing and automatizing of the processes.

3.1 BASICS AND GROWTH OF IOT DEVICES

VTT defines IoT for core technologies as sensing, processing, communication, refining and managing information. The supporting technologies are energy harvesting and low-power embedded systems. IoT brings together the digital and physical worlds. (VTT 2013.)

IoT devices are sensors and actuators with a connection to computing systems via a network. Figure 1 presents the exponential growth of devices globally between years 2010-2018. IoT connections have increased by 40 per cent per annum from 76 million in 2010 to 1102 million devices in 2018. Chinese IoT investments in connected cars, smart metering, payment terminals, industrial applications and smart cameras has made these growth IoT areas. (Edquist, et al. 2019.)

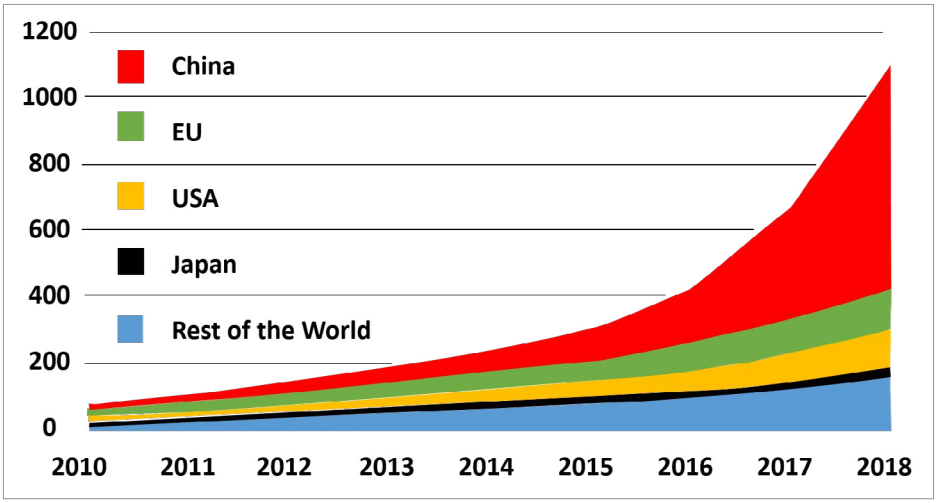

Figure 1. Number of total cellular IoT connections in the world (in millions). Source: GSMA Wireless Intelligence Database 2019 (Edquist, et al. 2019).

The growth of IoT connections will be on average 21 per cent a year from 2017 to 2025. Industrial IoT connections account for 14 billion worldwide, over half of the expected connections by 2025. The productivity benefits are estimated to be worth over $370 billion (USD) per annum in 2025, which means 0.34 per cent of global GDP. IoT companies ae projected to generate over $1 trillion in revenues by 2025. Consumer IoT connections are expected to reach over 10 billion worldwide. According to the research company IDC, IoT Edge markets will grow by 30 per cent to $2,1 billion between years 2016-2021. (Cisco 2019; GSMA 2019.)

Total IoT connections are projected to double between 2019 and 2025, reaching 24 billion. The forecast for 2020 was cut as a result of the pandemic and growing cost pressures in the SME and corporate markets. IoT revenues are expected to triple globally by 2025, from 381 billion dollars to 906 billion dollars. Connected vehicles are the most vulnerable, due to slowdowns in new car sales and the increasing use of ride-sharing, public transportation and working from home. Business sector IoT volumes are now more exposed due to the economic slowdown resulting from the pandemic. Cities and building operators will be the most negatively affected, followed by utilities. The current crisis will also reshape retail, manufacturing, and health. (GSMA 2020.)

The IoT market grows each year and now there are more IoT connections (connected cars, smart home devices, and connected industrial equipment) than non-IoT connections (smartphones, laptops, and computers). Of the 21.7 billion active connected devices worldwide, 11.7 billion (or 54%) are IoT device connections by the end of 2020. By 2025, it is expected that there will be more than 30 billion IoT connections, almost four IoT devices per person on average. (IoT analytics 2020.)

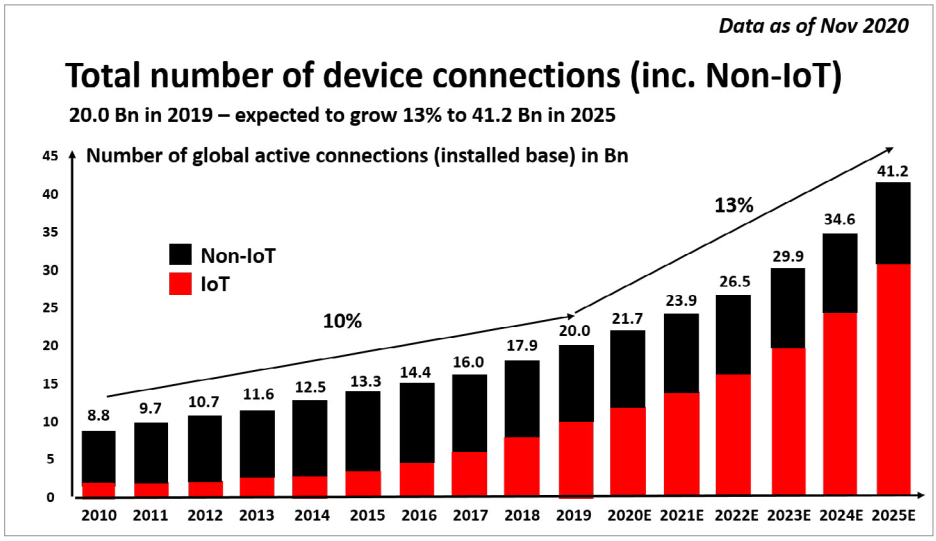

Figure 2. Estimation of global connections until 2025 by IoT Analytics

Cisco estimates that IoT devices collect 867 zettabytes or 867,000,000,000,000 Gb of data per year by 2021. IoT costs are expected to be $1.2 trillion by 2022. IoT solutions as application development, device hardware, system integration, data storage, security, and connectivity are projected to be $6 billion. The estimate for investments is to generate $13 trillion by 2025. (GetSmarter 2019.)

Recent research of IoT and economic growth, estimate a potential economic impact from IoT of $3 900–$11 100 billion per annum and a contribution of approximately 4–11 per cent of total world GDP in 2025. The study of "The Internet of Things and economic growth in a panel of countries" shows, that IoT connections have increased 30 per cent per annum. It means that the Total Factor Productivity (TFP) is equivalent to $592 billion based on World GDP of $85,804 billion in 2018. TFP is 0,69 per cent of World GNP. The growth of IoT investments are high, while user costs and income will initially be low due to the new technology of IoT. The estimation is that TFP growth may be larger than expected. (Edquist, et al. 2019.)

IoT devices also include micro-electromechanical systems sensors (MEMS). The price of MEMS sensors fell by 30–70 per cent from 2010 to 2015, approximately 6–14 per cent a year. This shows that there is fast technological progress in the production of IoT equipment. (Edquist, et al. 2019.) Sensors gather valuable data with more effective condition-based maintenance strategy. There is a large range of smart sensors for monitoring electrical currents, moisture, ultrasonic, vibration and temperature. (Short 2020.)

The wider economy results in productivity gains and more government revenue as taxes. Taxes are paid on corporate income and sales. Due to productivity gains, $22 billion was contributed to government revenue, which will rise to $47 billion worldwide by 2025. (GSMA 2019.)

3.3 MEASURING IOT PRODUCTIVITY MANAGEMENT

Productivity has many perspectives and the measurement system for IoT productivity need to develop first. According to the Guide of Productivity Management (SPRING 2011), there are five steps of a structured system. First, is the need to form a task force comprising senior management, a representative from different departments with knowledge of operations and processes, customers and suppliers. It is a good to include some employees in the measurement process. The second step is to decide what to measure, and to create productive goals and objectives. The third step is to create, indicators that are significant, meaningful, and action-oriented. These racking indicators need to be reliable and practical, related together, and used at the industry level. The fourth step is to design a system and implement it to collect, analyse and report performance indicators. There is a need to have a common understanding of the objectives. The fifth step is to monitor and review the results periodically and to enhance the system and its relevance as necessary. (SPRING 2011.)

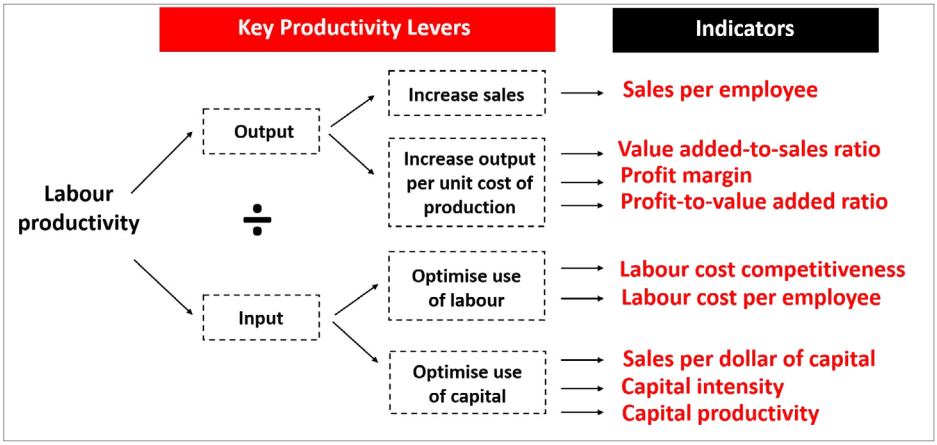

Figure 3. Key Management Indicators illustrate how indicators are found from Labour productivity (SPRING 2011).

Both developed and developing economies have slowing economic productivity and are faced with a major challenge to achieve higher standards of living and prosperity. The productivity of industry operations can improve with IoT installations. Smart factories can easily monitor the performance of equipment and predictive maintenance, tracking volume, and the location of stock and equipment. Quality assurance can reduce production waste through assessment and by focusing on product quality. (GSMA 2019.)

In Finland, we have similar challenges with the loss of manufacturing capability and limitations for energy and raw materials. Productivity may increase with monitoring and sensing processes with IoT devices.

3.3 PRODUCTIVITY AND IOT DEVICES

IoT can increase productivity by enabling faster decision-making, real-time control, service time reduction, process optimization, and the development of new business models and enhanced operational efficiency, and resource conservation globally. (VTT 2013.) The manufacturing sector, including consumer electronics and automotive, comprises a large share of the total global economic output, and some 50 per cent of the total global productivity impact. Using IoT, companies report savings globally on average of between 4 per cent and 6 per cent of operating costs. (GSMA 2019.)

3.3.1 SMART MAINTENANCE STRATEGY

An IoT manufacturing process can monitor factory assets using smart sensors to detect and notify of an incident occurring in real-time. Broken or breaking components can send data to let the relevant people know to replace those before causing damage. To shut down

a factory or an operation entirely may be very expensive, far better to replace components before damaged is caused (GetSmarter 2019.)

Productivity can improve by reducing the number of necessary service calls, resulting in fewer working hours. Productivity increases when using IoT devices as the production machines downtime and vehicle breakdowns are shorter. Condition-Based Maintenance (CBM), also called Preventive Maintenance, uses IoT with wireless sensors for increased control efficiency in the cloud services. Machines can then analyse and optimize their state and the whole process further. This enables global and efficient real-time process tuning and learning. Accordingly, maintenance changes from reactive repair to predictive and preventive maintenance. However, data transmission leads to huge security risks as the number of broadcasting sensors increase. (VTT 2013.) The technical product sensors detect, diagnose faults, and alert before faults appearances. Then they send information to the appropriate technician for a scheduled repair. IoT minimizes or even eliminates downtime time and saves the time of customer service workers. The spare part can be ordered in advance and the technician solves the problem in one visit, rather than two or three. Some of the repairs can even be automated after alerts. (Bedell 2019.)

3.3.2 MANAGING COMFORTABLE ENVIRONMENT IN SMART OFFICES

In this section, we'll discuss the role of IoT systems in office spaces rooms and smart scheduling systems controlled by IoT systems improve collaboration, coordination and space management between employees. Meeting rooms equipped with sensors are able to sense people entering the room and turn the equipment on. (Bedell 2019.) Smart sensors are also used to investigate the most occupied spaces where employees spend the majority of their time. This can be used to schedule meetings more efficiently, make better use of available resources, and minimise unnecessary expenses through smart heating and lighting systems. (GetSmarter 2019.) Improving productivity with the right kind and amount of lighting in occupied locations can remove unnecessary costs and the discomfort of non-optimized lighting. Smart control lighting might save 70 per cent more energy when using sensor information and novel luminaires. (VTT 2013.)

An office equipped with IoT sensors recognizes how and when employees are moving through the office space; this data can be used to improve traffic flows. The office can be rearranged to provide easier access to conference rooms and other resources to minimize disruption. IoT can also be used for the location tracking of equipment and devices. Smart homes and offices could use intelligent thermostats to adjust the temperature or window controls to open and close curtains and connected smart video cameras to reduce the risk of theft. (Bedell 2019.)

Productivity means more efficient processes that often translate into cost savings for companies.

3.3.3 IOT SOLUTIONS IN LOGISTICS AND TRANSPORTATION

The Harvard Business Review states that digital transformation is not just about technology, it is guided also by the broader business strategy and the reorganization of working methods. Supply chains are global. Customer expectations grow at the same time logistics have staff shortages in transportation and fragmented markets and low margins. The logistics process needs to be more efficient and planned with the right loading capacity. IoT technology requires networks, sensors and actuators, and scalable cloud services for the large amount of data. (Boberic et al. 2020; Solistica 2019: Tabrizi et.al 2019.)

Logistical IoT devices in supply chains and warehouses are used in real-time tracking, automation, paperwork, forecasting and inventory solutions. Supply chain transparency is growing to enable consumers to make environmentally friendly choices. IoT devices can track location and stocks, as the entering and exiting of goods in a warehouse are registered and recorded. Volume, weight, humidity, temperature, damage prevention and theft detection sensors for transports provide safe conditions for products. Data from warehouses can be delivered by automated systems resulting in less responsibility for workers, for example with processing a bill of lading. Accurate automated forecasting provides information for supply chain managers, decreases human errors, and saves time for manual collection. IoT Asset Tracking analyses stock levels and can prevent shortages, and location information with an inventory tracking system. Smart tags and sensors keep track of inventory levels in a warehouse or store in real-time for more efficient resupply, improving the company's cash flow. Inventory tracking also reduces over-ordering and make sure that the most popular products are in stock in order to maximise profits. (Bedell 2019; Nicholas 2019; Solistica 2019; Supply Chain Digital 2020.)

IoT sensors can also improve the fleet management of vehicles maintenance levels for trucks, vans, forklifts and cranes, fuel consumption, and emission control and even the drivers' wellbeing. Devices track the transport and delivery of products monitoring accurately arrival times and logistics. IoT can improve fuel efficiency in smart cities using connected traffic lights. This can help to reduce traffic jams and fuel consumption by automatically routing traffic during rush hour by controlling traffic lights. Last-mile deliveries are the best-routed, streamlined, faster and optimized for better customer service. (Bedell 2019; GetSmarter 2019; Nicholas 2019.)

Edge technology drives intelligent infrastructure for connected and automated mobility (CAM). Edge intelligence combines sensors, radar, LIDAR, video-based detection, connected traffic signals and remote monitoring capabilities, and transform roadway junctions, busy corridors and difficult roadway connectivity sections. Systemic changes are a key part of the Green Deal, for making sure Europe reaches the ambitious goals of reducing carbon emissions across many different sectors of our society and economy. The localisation of data

and computation can improve privacy, security, reliability, resilience and safety, which, taken together, comprises trust. (Cisco 2019; European Commission 2020.)

Edge computing drives decentralisation and decarbonisation in support of the European Union's Green Deal with cloud services, the importance of integrating connectivity and computing with artificial intelligence (AI) based reasoning and automation. Digital platforms and IoT Edge devices make it possible to gather all the massive data IoT devices collect and transfer it to the cloud computing services via networks. A cloud platform enables the rapid scaling of data storage, while machine learning identifies critical patterns. IoT Edge devices process data locally faster with improved security and low latency, before sending it to the cloud service. An IoT device has five core features for complex event processing, machine learning and artificial intelligence models, applications, and offline support and data management. (Cisco 2019; European Commission 2020.)

3.4 CYBERSECURITY AND PRIVACY THREATS

Cyberattacks are no longer fiction but reality. Cybersecurity becomes more important as companies digitize manufacturing operations. 100 per cent of large enterprises plan to report annually on cybersecurity risks to their boards of directors in 2020 versus 40 per cent in 2019. Organization need to update critical software and firmware minimizing overall cybersecurity risks and securing cyber threats. (Kaspersky 2020; Fahrni et al. 2020.)

When developing an IoT strategy, the security aspect needs to be considered from the very beginning. The three drivers of overall equipment effectiveness (OEE) are availability, performance, and quality. 5G networks give effectiveness and strong connectivity. Kaspersky's study shows IoT components are critical for new 5G communication networks. The study believes that new connectivity standards and embedded security are at a high level. Cybersecurity enables better visibility across the supply chain, allowing a more rapid response to disruptions. (Fahrni et al. 2020; Kaspersky 2020.)

In IoT, security is the most serious concern and the top priority for technology developers. The other concern is privacy; managers can track the movements of devices and vehicles. As everything that is connected to the internet can be hacked, including IoT devices, cybersecurity risks will continue to grow. Industrial control systems (ICS) and their automation components were never considered a potential security risk before now. (GetSmarter 2019; Myler 2015)

Kaspersky's survey found several typical ICS cyber threat challenges in 2020. The effects after an attack and the resulting costs were especially important (Kaspersky 2020):

- the most important challenge for industrial cybersecurity is to protect employees from injury or death
- damage to product/service quality

- loss of proprietary or confidential information
- cost of incident response and mitigation
- loss of customer confidence
- damage to equipment

The Industrial Cybersecurity Maturity Model has been developed to ensure the secure deployment of new devices. This model has been adapted from Kaspersky's ARC model and it provides a practical tool for industrial cybersecurity strategies through standards, guidelines for edge gateways, new practises as Key Performance Indicator (KPI), and the integration of Information technology (IT) and Operational Technology (OT) cybersecurity. The model highlights the need to balance the discrepancy between technology investment and human resources. (Kaspersky 2020.)

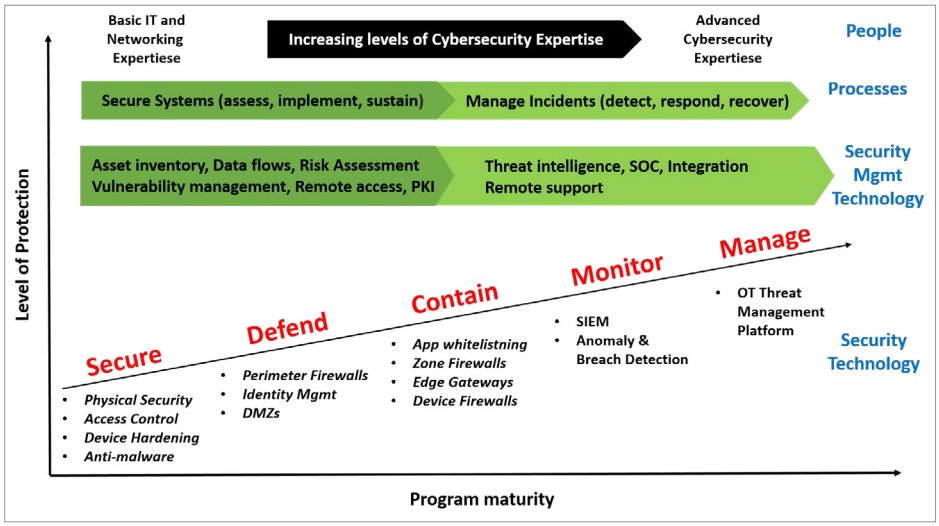

Figure 4. The Industrial Cybersecurity Maturity Model by Kaspersky (2020).

Network monitoring refers to the protocoling and analysis of data. In the network, data streams are mainly used to detect anomalies that influence the automation processes. Anomalies are unexpected deviations from the normal rules. The detection of anomalies is a suitable method for generating cyber-warnings and enabling more effective forensics. Anomaly detection is one of the basic methods of detecting cyberattacks. (Kaspersky 2020.)

Cybersecurity threats need to be taken care of in all industries. New technologies make it possible for hackers to attack almost everything and this is compounded by the fact that IoT devices are one of the easiest peripherals to break into. There is no sense to improve productivity if information and cybersecurity issues are not being considered at the strategic level of the company.

3.5 CONNECTIVITY TO NETWORKS

The key drivers for IoT connectivity have been cellular (2G, 3G, 4G, 5G) and LBWA (Low-Power Wide-Area) networks last 5 years. The connections grow 43 per cent from 2010 to 2019 and are expected to grow 27 per cent in the future (Compound Annual Growth Rate, CAGR). LoRA and Lorawan technologies operate in the unlicensed spectrum have 41 per cent market share in the LBWA networks today (2020 H1) and are estimated to be same at 2025. (IoT analytics 2020.)

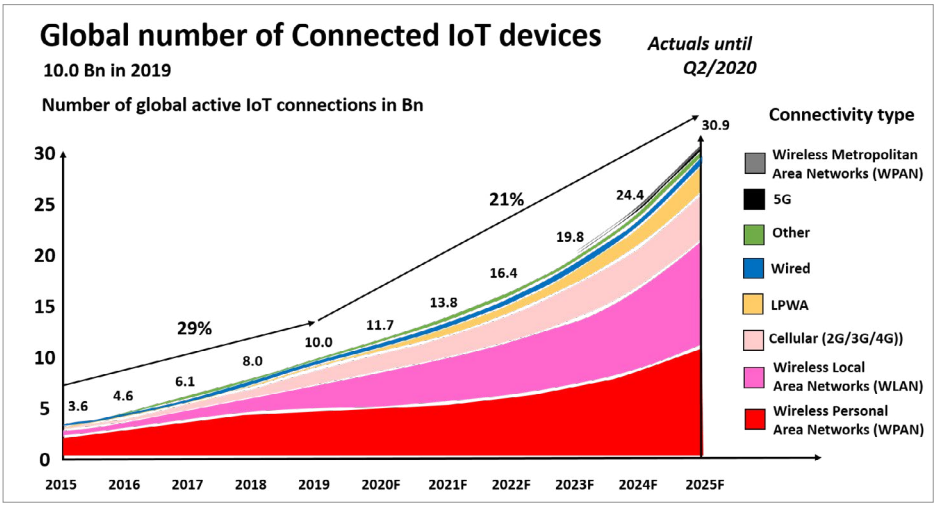

Figure 5. Estimation of global connected IoT devices until 2025 by IoT Analytics

Wireless or radio-based connectivity networks are suitable for IoT. The important challenges relate to power consumption and the range of the connectivity network. Low-power wide-area networks (LPWANs) have accelerated the development of IoT-applications. A wide range of connectivity networks all have their specific particularities, from short-range networks such as Bluetooth, to global connectivity via satellite networks and the radio spectrum frequency. The technical comparison should be considered as follows:

- Is there a public network available?
- Can a private network be deployed?
- What about manufacturer dependence?
- What would be the difference in costs when choosing for a network A vs network B over the lifetime of the application?

(Vannieuwenborg et al. 2017)

The speed of data rate and the range of connection is expressed in the picture below. Cellular and Wi-Fi connections are fastest, and the signal of transmission and receiving rate are the most efficient.

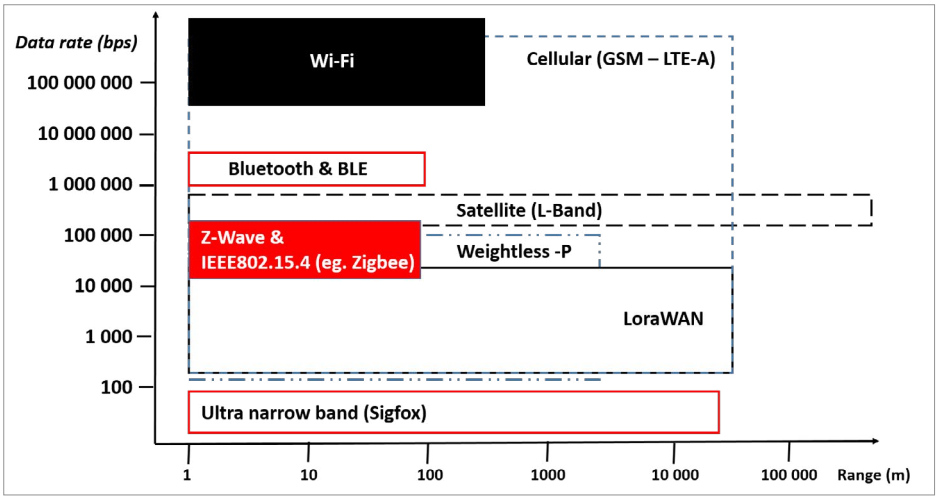

Figure 6. Wireless connectivity networks overview: data rate vs range (Vannieuwenborg et al. 2017).

5G connection increases the speed, responsiveness and reach of self-driving cars, drones, virtual reality and the IoT. The convergence of Artificial Intelligence (AI) and IoT devices with intelligent Cloud and Intelligent Edge services offer local AI tasks with cloud management and real-time data insights. (GetSmarter 2019.)

4 DISCUSSION

There are two lines of IoT technology business, consumer IoT and enterprise Industrial IoT devices on the market. Companies can produce new business models with new services with Industrial IoT devices for the logistics sector. Consumers have had IoT products in their wristwatches to investigate their health for many years. The IoT devices of the Industrial Revolution will become a huge success during the next few years. Companies need to be aware of cybersecurity in all level of production to the delivery. End-users need to have support to update and patch the software and hardware of the IoT devices.

This study examined the productivity of IoT devices for industry, focusing on logistics sector. The primary question was how to measure productivity and what are the benefits of using IoT devices in the logistics industry. This will be discussed in additional detail in this section.

4.1 PRODUCTIVITY WITH BETTER PERFORMANCE GENERATES MORE PROFITABILITY

The estimates for IoT growth and expansion speed is huge. Depending on the source, the growth of IoT devices may reach more than 30 billion device connections by the year 2025. IoT companies' revenues are expected to generate $ 1 trillion dollars by 2025. This has the potential to lead to huge cybersecurity risks as the number of connection-based sensors are increasing rapidly.

As this study has shown, productivity means enhanced performance with the company's units, employees, machinery, equipment and its vendors. If these resources are used more effectively, productivity can be seen as increasing. Productivity improves with increasing sales, production value and value-added. Additionally, it improves through cost savings with fewer working hours and labour. Enhanced productivity increases outputs, less work, raw material and energy, which means more sustainability in the long term. The indicators of productivity are effectiveness and capital productivity. Growing capital productivity can be achieved though the enhancement of machines and equipment.

For the IoT strategy and objectives, a company needs to have support from the senior management, process owners, customers, suppliers, and employees for an effective productivity management system.

IoT devices and actuators are used via a connection network for security, sensing, smart metering, and processing, refining, and managing information. These devices can communicate in terminals, vehicles, and machines with industrial applications. IoT

technology collects a massive amount of data with these smart sensors for condition-based maintenance by monitoring temperature, humidity, moisture, vibration, lighting, ultrasonic, and electrical currents. IoT technology also requires a scalable cloud service for this large amount of data. The overall equipment effectiveness (OEE) of IoT devices are measured by availability, performance, and quality.

The company's operational productivity improves with the monitoring of the industry's machinery for predictive maintenance, volume tracking and location of the equipment. Smart sensors detect, diagnose and collect data from equipment. Devices pre-emptively warn of damage or problems by asking for the replacement of broken components beforehand and this can result in decreased machinery downtime. The spare parts are ordered in advance and replaced by the technician in less service time.

Enhanced operational efficiency with faster decision-making and real-time control increases productivity through a reduction in maintenance time and the optimization of processes. The productivity increases optimize maintenance by switching from reactive repair to predictive and preventive maintenance. At the same time, the product quality improves and waste is reduced by optimization.

IoT devices also sense people. Offices and workplaces can be equipped with smart sensors for switching security equipment and various machines on and off, and adjusting the temperature and lighting system of the space. This may save unnecessary costs and could create a more comfortable environment in the office. Smart seating and the location of the workstations can be determined by IoT technology for more comfort and increased productivity. The smart office is the term for sensors connected to automated systems that improve employee productivity by adjusting energy consumption, creating safer workstations, better source management, and a well-conditioned climate with effective space management.

Logistic supply chains are global. These processes need to be more efficient and provided with the right loading capacity. IoT devices used in logistics collect data from tracking, location, forecasting and inventory, automation and paperwork. Sensors measure volumes, weight, humidity, temperature, pressure, chemical content, liquid and solid levels, damages, theft detection and protection, and also can decrease human error.

Sensors and smart tags are used for keeping track of inventory levels in real-time in logistics. The sensors can also track products in transport, store and warehouse. These parameters may save costs for the company.

Vehicle sensor IoT devices track fuel consumption and the emissions of trucks, vans, forklifts, and cranes. Transport and delivery sensors monitor traffic, arrival times, location, and logistics for sustainability. Traffic routing can be automated to reduce unnecessary stops in traffic jams and to get the optimized and best-routed delivery to guarantee good customer

service. Vehicles can be equipped with sensors, radar, LIDAR (meaning laser imaging, detection, and ranging) and cameras for remote operating or autonomous driving. The amount of collected data is processed in the IoT EDGE device, which sends secure data to the desired cloud service. Security creates the most concern in IoT technology, as everything, which connects to internet is hackable.

IoT connections are used mostly on mobile cellular networks nowadays. In four years until 2025, Wireless Local Area Networks (WLAN), Wireless Personal Area Networks (WPAN) and Low Power Wide Area Networks (LPWAN) rule the connectivity of IoT devices. Fast 5G cellular networks with high responsiveness and wide-range allow IoT usability in autonomous vehicles, drones and for Virtual Reality (VR). Wireless and 5G communication enable many possibilities together with cloud services for increasing productivity.

Solow's Paradox refers to the fact that the rate of productivity increase appears to be slowing dramatically in the age of the Internet. At the beginning of the research, I asked the question whether it is possible that this will change with the growth of IoT devices. The growth estimates for an IoT business model are very positive on the global level. Over the next five years, new business models of IoT technology will contribute approximately 4 to 11 per cent of the World Gross National Product. Some research estimates that IoT growth will be even larger.

IoT productivity goals and objectives found in this research are presented in figure 7. These productivity enhancement indicators are significant, meaningful and action-oriented, relating to each other. These performance indicators collect, analyse and report, monitor and review periodically.

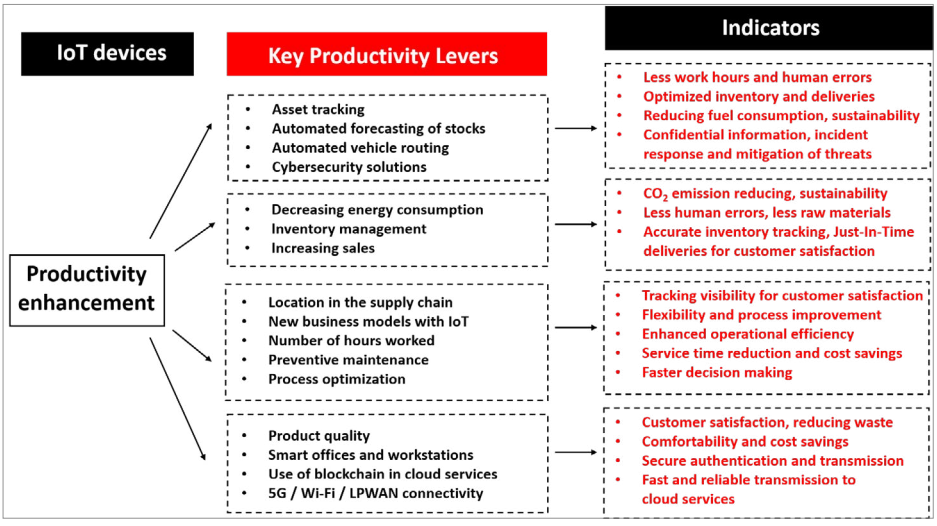

Figure 7. The Key Management Indicators of IoT productivity, modified from the Spring Singapore model (SPRING 2011).

4.2 CYBERSECURITY IS IMPORTANT TO DIGITIZE OPERATIONS

Cybersecurity protects against crimes and attacks carried out against businesses, and their information and operational technology systems on the internet. The most well-known definition for cybersecurity is the acronym CIA, which comes from Confidentiality, Integrity, and Availability of information, and means that the cyber threats and risks are under control. Cybersecurity management can be divided into preparedness, situational awareness, prevention, and recovery.

The cybersecurity strategy needs to be considered immediately in the beginning. The strategy should define the target state as an operating environment that can be trusted, and that its operation is secure using adequate and appropriate information security. In that case, information security threats would not necessarily actualize.

The potential security risks are attacks to the company's Industrial Control Systems (ICS), which may cost the loss of quality, confidential information and incident response and mitigation of threats. The new information and operational technology need to secure and defend, contain, monitor and managed. Security management technology needs to upgrade, incidents need to be managed in the processes and employees need to receive more advanced cybersecurity education.

5 CONCLUSION

The research question asked whether the risk of cybersecurity threats is worth the benefits of IoT productivity. Risk can always be an opportunity or a threat, meaning the impact can be positive or negative with the ongoing process. Digital transformation is a combination of new strategies, technology and working methods. The company sets strategic objectives and includes risk management in their daily work with risk analysis.

This desk study was not able to confront IoT productivity versus cybersecurity challenges and future risks. The growth of IoT possibilities is so enormous, that those cybersecurity companies and solution providers are faced with a win-win situation. It means, that industrial companies need to rely on the expertise of cybersecurity consulting companies and their ability to provide solutions for protecting information and operational technology systems. Cybersecurity can control the threats and risks for the company's necessary functions. Threat models need to be updated continuously with regular risk assessments carried out. As the phrase goes, locks are only for honest people. All technological peripherals, which connect to the internet, are hackable.

IoT technology enables higher productivity, which means better performance and therefore more sustainable profitability.

It is recommended that a research group would be established to investigate new perspectives to use IoT devices in the ports and logistic stakeholders. In the working group, one topic worthy of study would be the idea to combine innovative approaches on how to enhance work machines, cranes and vehicles operational use in ports and the entrance to ports.

This desk study has highlighted the need for further research on IoT. One such area of study would be the investigation of the fourth industrial revolution or INDUSTRY 4.0, which refers to the convergence and digital transformation of additive manufacturing, augmented reality (AR), autonomous robots, Big Data, cloud computing, cybersecurity, IoT, simulation, and system integration. A study of Artificial Intelligence (AI) and new Blockchain technology would complete the next step of IoT research.

IoT devices have a huge potential to increase productivity in many industries, including the logistics sector. Together with effective cybersecurity and research of future demands, I believe that the risk is worth taking to develop productive and secure cyber services and products for the logistics sector!

REFERENCES

Bedell, C. 2019. 5 Ways IoT Technology Can Boost Productivity. IoT World Today. https://www.iotworldtoday.com/2019/10/02/5-ways-iot-technology-can-boost-productivity/ [Accessed 14 December 2020].

Boberic, D., Krotki, K., Michalas, L., Ott, L., Rütten, M., Schlehahn A. and Stulle M. 2020. How IoT can improve the logistics process. Deloitte. Available at: https://www2.deloitte.com/de/de/blog/internet-of-things-blog/2020/how-iot-improves-logistics.html [Accessed 17 December 2020].

Cisco. 2019. Five components of IoT edge devices. Available at: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-edge-devices.html [Accessed 18 December 2020].

Edquist, H., Goodridge, P., Haskel, J. 2019. The Internet of Things and economic growth in a panel of countries. Available at: https://www.tandfonline.com/doi/full/10.1080/10438599.2019.1695941 [Accessed 14 December 2020].

ENISA, European Union Agency for Network And Information. 2015. Security Definition of Cybersecurity Gaps and overlaps in standardization. ISBN 978-92-9204-155-7. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Accessed 2 December 2020].

European Commission. 2020. Building an ecosystem where IoT, edge and cloud converge towards a computing continuum. Available at: https://ec.europa.eu/digital-single-market/en/news/building-ecosystem-where-iot-edge-and-cloud-converge-towards-computing-continuum [Accessed 18 December 2020].

Fahrni, S., Jansen, C., John, M., Kasah, T., Körber, B. and Mohr, N. 2020. Coronavirus: Industrial IoT in challenging times. McKinsey & Company. Available at: https://www.mckinsey.com/industries/advanced-electronics/our-insights/coronavirus-industrial-iot-in-challenging-times [Accessed 16 December 2020].

GetSmarter. 2019. How the IoT Can Improve Business Productivity. 2U.com. Available at: https://www.getsmarter.com/blog/market-trends/how-the-iot-can-improve-business-productivity/ [Accessed 14 December 2020].

Goldin, I., Koutroumpis, P., Lafond, F. and Winkler, J. 2020. Why is productivity slowing down? OMPTEC Working Paper No. 2020-1. Available at: https://www.oxfordmartin.ox.ac.uk/downloads/academic/ProductivitySlowdown.pdf [Accessed 7 December 2020].

GSMA Intelligence. 2019. The contribution of IoT to economic growth. PDF. [Accessed 15 December 2020].

GSMA Intelligence. 2020. Global Mobile Trends2021. https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=58621970&file=141220-Global-Mobile-Trends.pdf [Accessed 15 December 2020].

Tabrizi, B., Lam, E., Girard, K. and Irvin, V. 2019. Digital Transformation Is Not About Technology. Available at: Digital Transformation Is Not About Technology (hbr.org) [Accessed 27 April 2021].

IoT Analytics. 2020. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. Available at: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ [Accessed 16 December 2020].

Nicholas, M. 2019. Six Ways the Supply Chain Benefits From the IoT. IoT Evolution. Available at: https://www.iotevolutionworld.com/smart-transport/articles/442715-six-ways-supply-cha-benefits-from-iot.htm [Accessed 17 December 2020].

Kaspersky. 2020. The state of Industrial Cybersecurity in the era of digitalization. Availability at: https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf [Accessed 15 December 2020].

Myler, T. 2015. How the Internet of Things will Impact our Productivity. Availability at: https://www.infoq.com/articles/iot-impact-productivity/ [Accessed 11 December 2020].

OECD. 2001. Measuring Productivity, measurement of aggregate and industry-level productivity growth. Available at: https://www.oecd.org/sdd/productivity-stats/2352458.pdf [Accessed 11 December 2020].

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriö. Available at: http://julkaisut.valtioneuvosto.fi/handle/10024/80013 [Accessed 2 December 2020].

Short, T. 2015. 3 Critical Maintenance KPIs an Optimal CMMS Dashboard Should Have. Available at: https://www.softwareadvice.com/resources/top-3-kpis-for-cmms-dashboard/ [Accessed 14 December 2020].

Short, T. 2020. 3 Smart Maintenance Solutions to Get More from Asset Data. Available at: https://www.softwareadvice.com/resources/3-smart-maintenance-steps/ [Accessed 14 December 2020].

Solistica. 2019. The IoT and its uses in logistics. Available at: https://blog.solistica.com/en/ithe-iot-and-its-uses-in-logistics [Accessed 18 December 2020].

SPRING Singapore Solaris. 2011. A Guide to Productivity Measurement. Available at: https://www.academia.edu/8016777/Guidebook_productivity_measurement [Accessed 11 December 2020].

Supply Chain Digital. 2020. Five benefits of an IoT-enhanced supply chain. Available at: https://www.supplychaindigital.com/logistics/arm-competitive-edge-logistics-through-esim [Accessed 17 December 2020].

Turvallisuuskomitea. 2019. Suomen Kyberturvallisuus-strategia. ISBN: 978-951-663-051-2 pdf. Available at: https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/ [Accessed 2 December 2020].

Tuomala, V. (2020). Logistics and maritime need to focus to cybersecurity in the Internet of Things (IoT) Technology. Xamk Beyond publication. Available at: http://urn.fi/URN:ISBN:978-952-344-279-5 [Accessed 18 December 2020].

Tuomala, V., Brunila, O-P. & Hannula L. (2020). Getting ready for the cross-border challenges towards digitalization. XAMK Logistics and seafaring yearbook. Available at: XAMK kehittaa 129 Ville Henttu ja Pauli Potinkara Suuntaa antamassa (theseus.fi) [Accessed 17 December 2020].

Turvallisuuskomitea. (2017). Kyberturvallisuuden sanasto. Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf [Accessed 2 December 2020].

Vannieuwenborg, F., Verbrugge, S. Colle, D. (2017). Choosing IoT-connectivity? A guiding methodology based on functional characteristics and economic considerations. Available at: https://www.researchgate.net/publication/324615120_Choosing_IoT-connectivity_A_guiding_methodology_based_on_functional_characteristics_and_economic_considerations [Accessed 16 December 2020].

VTT Technical Research Centre of Finland. 2013. Productivity Leap with IoT. Available at: https://www.vttresearch.com/sites/default/files/pdf/visions/2013/V3.pdf [Accessed 15 December 2020].

ACKNOWLEDGEMENTS

I need to praise Xamk's publication organization and the most important persons for me to finalize this study. Thank you Soila Eräniemi for helping me with all kind of questions concerning publishing my research and Cai Weaver for helping translate this study to accurate English.

I am super happy!

Vesa

XAMK
DEVELOPMENT