63rd FTTCE International Congress
26 - 28 September 2024, Kraków, Poland

ChangeTechno-Economics of IoT and OT security

Morten Falch and Reza Tadayoni

Aalborg University Copenhagen, DK

Abstract

Cybersecurity has become a serious challenge for businesses around the world. PwC has reported cybercrime to be the most widespread kind of economic fraud [1]. Cryptocurrencies valued at more than 400 mil. dollars were paid to ransomware addresses in 2020. This represents a growth of more than 400% in one year. Malware increased by 358%. Distributed Denial of Service (DDOS), ransomware and other kinds of cyberatacks are happening more and more frequently, and for businesses they can lead to severe consequences, e.g., interruption of work processes and customer services, loss and compromising of data, violation of data protection and privacy laws, a lot of time wasted, and large costs. The ongoing process of digital transformation is affecting all businesses and organisations, large and small, and this puts further focus on the challenges related to cybersecurity. In the latest Global risk report published by the World Economic Forum the issue of cybersecurity reappeared to be among the top 10 global risks, as cyberatacks on critical infrastructure was seen as one of the risks with the largest potential impact on a global scale [2]. This concern is partly due to cyberatack against Ukraine in 2022. Also cyberatacks jeopardizing privacy of vulnerable citizens is seen as a global risk. In this regard IoT and OT security is becoming still more important. The number IoT devices has exploded within the past decade, and many of these are not sufficiently protected. Many IoT devices lack built-in capabilities for updating software, which makes it difficult to maintain security. Hackers can not only hamper their functionality but can also use them as a gateway to other IT systems and devices. Especially badge readers, cameras and printers are of concern from a security perspective.

Likewise, OT security has gained in importance, as this is a key issue for securing critical infrastructures. Compared to IoT, OT devices are lower in quanties, but more valuable. Many critical infrastructures are highly dependent on OT devices, and disruption of their operations may have detrimental impact on the functions of the society. Cybersecurity as a policy issue has atracted a lot of atention both from a regulatory perspective and in economic literature. The EU has published a common strategy on cybersecurity [3], and several major initiatives are being launched by the EU to increase awareness and protect critical infrastructure, e.g., the NIS2 (Network and Information Security 2) Directive [4]. The EU

Cyber Resilience Act will impose security demands on manufacturers of hardware. Likewise in the US the Executive Order 14028 is issued to protect critical infrastructures.

The economics of cybersecurity is a relatively new area of research. While much research has been published on development of technical solutions and strategies for implementation strategies, the economic foundation of any regulation and strategies for remedy cybercrime is still under development. This is in particular the case for IoT and OT security. This paper will provide an overview of the IoT and OT security challenges, and techno-economic characteristics of possible cybersecurity measures to be taken. What are the market failures to be addressed? Finally, the paper will identify the regulatory challenges that follows from this analysis, and how are they being addressed in current regulation? More specifically the paper will discuss cybersecurity issues related to IoT and OT, how they can be addressed by the market, and where regulatory intervention is needed. First the paper will identify IoT and OT cybersecurity challenges [5] [6] [7]. Second the economic characteristics of different security measures will be discussed. This discussion will as departure be based on current research on cybersecurity as an economic good including [8] [9] [10]. Compared to these C contributions, we will take an approach, where the characteristics of the specific security measures identified in the technical analysis of IoT and OT are taken into account. Based on this, regulatory challenges regarding market intervention will be identified.

References

[1] PwC, »PwC's Global Economic Crime and Fraud Survey 2022,« PwC, 2022.

[2] World Economic Forum, »Global Risk Report 2024,« World Economic Forum, 2024.

[3] European Commission, »JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final,« Brussels, 2020.

[4]"NIS2 Direcﬁve," 16 Dec. 2020. [Online]. Available: https://eurlex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b01aa75ed71a1.0001.02/DOC_1&format=PDF.

[5] W. H. Hassan, »Current research on Internet of Things (IoT) security: A survey,« . Computer networks, nr. 148, pp. 283-294, 2019.

[6] R. Mahmoud, T. Yousuf, F. Aloul og I. & Zualkernan, »December. Internet of things (IoT) security: Current status, challenges and prospecﬁve measures.,« i 10th international conference for internet technology and secured transactions (ICIT), IEEE, 2015, pp. 336-341.

[7] W. A. Conklin, »IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience,« i 49th Hawaii International Conference on System Sciences (HICSS) , Koloa, HI, USA, 2016, pp. 2642-2647.

[8] I. Brown, »The economics of privacy, data protec�on and surveillance.,« i In Handbook on the Economics of the Internet. , Edward Elgar Publishing, 2016.

[9] H. Asghari, v. Eeten og &. B. J. M. M., » Economics of cybersecurity. In Handbook on the Economics of the Internet.,« Edward Elgar Publishing, 2016.

[10] A. Odlyzko, »Cybersecurity is not very important,« ACM, 2019.