Business focused cybersecurity as a competitive advantage: How should this contribute to the success of the company?

Group Leader:
Guro Skari Berger

Group Members:
Kasper Nylander, Marcus Børrud Bjørndalen, Almin Dacic,
Ebba Bakkerud Andersen, Johan Gimse Valseth, Christin Ylva Emanuelsen,
Emil Lie Nesheim-Hauge, Julian Berg & Hilde Rangnes

Supervisor:
Prof. Dr. Bernhard M. Hämmerli

Topic Sponsor and Industry Expert Coach:
Peter Kosel, cyberunity

IMT4115 – Introduction to Information Security Management
Norwegian University of Science and Technology - NTNU

Abstract. Cybersecurity is often viewed by management as a cost factor, not contributing to economic performance. Historically, various methods have been used to justify cybersecurity expenses. However, emerging trends like "business-focused" and "business-centric" cybersecurity aim to secure management buy-in by integrating security with business goals, enhancing resilience, and driving value creation. These approaches position cybersecurity as an enabler of business performance rather than just a defensive measure. Business-focused cybersecurity emphasizes regulatory compliance and high-performance teams, while business-centric cybersecurity embeds security into core business processes to support innovation and growth. These strategies are proactive, integrating threat intelligence and workforce training to create a culture of cybersecurity awareness, crucial against sophisticated attacks like double and triple extortion. In an evolving threat landscape, risk management approaches like Enterprise Security Risk Management (ESRM) and the Factor Analysis of Information Risk (FAIR) model help organizations strategically plan and prioritize resources. Emerging technologies such as AI and cloud computing enhance these strategies, improving threat identification and data management. In Industry 4.0, technologies like Cyber-Physical Systems (CPS) and Industrial Internet of Things (IIoT) require robust security measures. Aligning these technologies with business-focused and business-centric approaches enhances resilience and performance. Overall, this book explores historical and emerging cybersecurity trends, examining their effectiveness in securing management buy-in and enhancing organizational performance. By integrating cybersecurity with business goals and leveraging new technologies, organizations can transform cybersecurity from a cost factor into a strategic asset that drives success in a complex threat landscape.

CONTENTS

Chapter 1

Historical View on Cybersecurity Legislation, Governance, Awareness Campaigns & Education

Kasper Ketilssønn Nylander [10325]

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Keywords: Government Legislation, Awareness campaigns, Cybersecurity.

Abstract. This paper explores the historical evolution of cybersecurity by examining the legislative efforts and different awareness campaigns that have contributed to shape the current cybersecurity landscape. It first examines government legislation, focusing on key legislative frameworks such as the U.S. Computer Fraud and Abuse act (CFAA) of 1986, and the General Data Protection Regulation (GDPR) of 2018. Emphasizing their impact on addressing growing cyber threats and protection of critical infrastructure. The paper then transitions to the role of cybersecurity awareness campaigns, including initiatives like U.S. National Cyber Security Awareness Month, and European Cyber Security month which aims to educate organizations and individuals about best information system practices and potential vulnerabilities. The interplay between these approaches emphasizes the necessity of balancing between a robust governmental legislative framework and culturally adapted educational efforts to encourage an extensive cybersecurity culture. By analyzing global differences, such as western individualistic versus eastern collectivistic messaging, this paper underscores the cultural nuances in addressing cybersecurity. While legislation provides structure and enforcement, awareness campaigns bridge the gap by promoting implementable behavior approaches and changes. Ultimately this paper argues that a holistic approach combining robust legislative framework with educational strategies is essential for countering the growing threat landscape of the cyber-domain.

1 Introduction

In today´s digital age, information security has become a critical component, essential for both public and private sectors. And since the very beginning of exploring the possibilities with the internet, the steady increase in usage of information technology have grown larger and gotten more widespread. The benefits the internet have brought to the world are many and it keeps giving, but with such a powerful tool comes several downsides, as our societies is experiencing more cyberthreats and cyberattacks on a regular basis. The aim for this paper is to enhance the understanding of information security by examining two historic approaches to the topic.

The first topic focuses on government legislation, compliance and their impact on information security. This paper will focus mostly on the western approaches and legislations and examine the United States and their way of handling cybersecurity. This is because of the influence their legislations on the cyberspace have had on the western world. The second topic concentrates on international awareness campaigns and education and how these have contributed to the understanding and the importance of cybersecurity, both on an individual level and on an organizational level. The second topic will also look at the cultural differences in awareness campaigns in different countries.

This paper will focus on the Western world's approach to cybersecurity, with emphasis on U.S. legislation. As for the significant development of both internet and cybersecurity laws originating from the United States. Through examining and analysis of these historical approaches, this paper will highlight how history have unfolded and how different strategies have shaped the current landscape of the cybersecurity domain in the western hemisphere.

This essay examines how both legislative frameworks and awareness campaigns are funded by the government. Therefore, it will not explore in great detail how these funds were raised, since most of the legislation and awareness campaigns mentioned were financed through governmental budgets and decisions made by different nations governmental authorities.

2 A Brief History of Cybersecurity

The historical development of government legislation in cybersecurity has been identified by key moments and milestones. To understand the historical development of cyberspace and cyberthreats we need to analyze the very beginning of the internet. The internets origins trace back to ARPANET, a project funded by the United States department of defense in the 1960s. ARPANET was a development allowing large computers to interact with each other and sharing information through "packets". This made communications more efficient and easier to obtain. This technology laid the foundation of the modern internet as we know it. The internet later transitioned from a military and academic network to a commercial network and went public in the 1990s. As the internet grew larger and got more available, the increase in need for cybersecurity also grew (Savage, 2023)

In the beginning of the 90s, a series of changes happened that were of importance to political history and cyberspace. The cold war had concluded with a dissolution of the Soviet Union (USSR), and the new Democratic president Bill Clinton and vice-president Al Gore had moved into the white house. Some of Clinton's main goals was to turn the world in to a global marketplace for the United States, this goal came along with Al Gore's vision about a future market for information technology. Clinton and

Gore formed a neatly fitted plan to utilize the internet to deliver American goods and services to the world. This would also be an effort for political competitive advantage as this was thought to spread democracy and western human rights for reshaping the post-cold war order (Carr, 2021).

In the earlier years of cyberspace with increasing cyberthreats there was a bigger focus on website defacement. This tended to take place in existing and ongoing political conflicts. Although this kind of cyber-attacks seems both harmless and inconsequential today, these kinds of cyberattacks were considered a new kind of trigger for political conflict (Carr, 2021). And the fact that these kinds of attacks were especially difficult to trace back to the individual executing the cyber-attack, created some anxiety among important world leaders, as these attacks could result in political conflict and more tension between nations (Carr, 2021).

The next wave of cyberthreats came from distributed denial of service (DDoS) attacks on critical infrastructure. Causing massive traffic to the target to overload and make the software and user systems unavailable for the intended user (Carr, 2021). This had already caused great concern, as critical infrastructure like communications and transport services were denationalized and sold to private sector companies and operators. The industrial control systems used to control critical infrastructure were later networked and commercialized (Carr, 2024). This was done due to enhancing efficiency and cutting costs, allowing remote monitoring and management. On behalf of this improvement came the downside in these systems being fairly vulnerable for potential cyber-attacks. And the potential executers behind an attack on such critical infrastructure were expected to be either politically motivated groups or even states (Carr, 2021).

While in democratic nations, when it comes to security in cyberspace, the government are either absent or follows information and communications technology ICT companies' measurements and frameworks for cybersecurity, e.g., Apple and Microsoft. These ICT companies generally focus on global business strategies for their stakeholders and own benefit rather than prioritizing and protecting national interests (Savage, 2023). The threats the ICT companies face, and the government response generates a significant security gap and deficit, as reported in frequent reports of cyber vulnerabilities. Whereas in nondemocratic nations, governments force ICT companies to restrict privacy rights and support authoritarian control through moderation of content and unveiling of encryption keys (Savage, 2023).

As Savage & Reveron (2023) discusses, much of the cybersecurity frameworks implemented in the western hemisphere has emerged from the United States, since decisions made in Washington DC, and the United States technology sector will and have affected American information technology users around the world. One can further assume that these frameworks might have been adopted by the EU as well, as much of Europe are both NATO allies with the United States and share much the same political interests related to geopolitics and commerce.

2.1 Early Legislation and Governance

In the early years of mapping out the cyberspace and its weaknesses, the United States made forward thinking legislative frameworks meant for preventing cybercrimes. In this chapter I will examine two of the earliest legislations regarding cybercrime in the United States, the Computer Fraud and Abuse Act (CFAA) 1986, and the Computer Security Act of 1987, as outlined computer security and the designated responsibilities along with the corresponding penalties (Whitman, 2022).

Computer Fraud and Abuse Act (CFAA) of 1986. Often described as a "anti-hacking law" this act made it illegal to access computers without authorization. The act was amended from the fear of individuals obtaining access to state computers and information's systems and inflicting damage on critical infrastructure (Berris, 2023). This act aimed to implement a cybercrime law, banning a series of computer related actions. The key moments highlighting illegal actions under the CFAA are: Obtaining specific types of information through unauthorized computer access, trespassing a government computer, engaging computer frauds through unauthorized computer access and knowingly causing damage to computers by transference of program, information or command. The original act of CFAA 1986 has since then evolved as technology and the human relations to cyberspace have moved on rapidly. To this day the rapidly changing technological domain presents new legal issues to both the U.S. and the world (Berris, 2023). The Computer Security Act of 1987, aimed at improving the security and privacy of sensitive information in federal computer systems. This act was designed to establish a computer standards program within the national Bureau of standards, currently known as the National Institute of Standards and Technology (NIST). It was expected to provide government computer security and ensure the training of personnel involved in the management operation, and use of federal computers. These acts served as benchmarks for future cybersecurity policies and measurements (U.S. Congress, 1987)

Vassiliadis (2024) further points out how young the cyberthreat domain is, as the European Union Agency (ENISA), which focus is working on strengthening Europe's resilience regarding critical infrastructure and cybersecurity, also helping EU member states implementing relevant EU Legislation was not established before 2004. As well as ENISA the UK cabinet office discusses for the first time the concept of cyber-resilience, and emphasized the need for organizations should adapt due to evolving threats and maintain their daily critical operations as late as 2005 (Vassiliadis, 2024).

2.2 Contemporary Legislation and Governance

In later years the world has gained more knowledge about the potential threats within the cyberspace. In this chapter I will, examine some of the key contemporary legislative frameworks that occur in both the United States, and Europe.

The Information Sharing and Analysis Centers (ISACs), were established in 1998 to encourage information sharing about cyberthreats among members and educate members to mitigate risks and enhance cyber-resiliency. First came the Information Sharing and Analysis Organizations (ISAOs) in 2015, encouraging sharing information about cyberthreats across different sectors. From this initiative came the Cybersecurity and Infrastructure Security Agency (CISA) under the United States Department of Homeland Security. CISA recognized that information sharing with industry and other sectors is important, then launched its new program (Joint Cyber Defense Collaborative) in 2021 (Savage, 2023). This is not a direct legislative framework, but it contributes to maintaining protection as it makes it easier for law enforcement to pose serious punishment on cybercrimes (Savage 2023).

In 2014 the national institute of standards and technology (NIST) published its cybersecurity framework, which pose the guidelines and best practice for further improvement of cybersecurity in different sectors. The measures emphasized the need for organizations to be prepared for an withstand potential cyberattacks, and be able to detect, react and recover from these attacks (Vassiliadis, 2024).

In 2018 the EU General Data Protection Regulation (GDPR) was implemented in the European union. Marking a great increase and investment in cybersecurity in the European hemisphere. This legislation is aimed at protecting the individual's privacy. This act imposes severe punishment for data loss. GDPR also makes it possible for EU citizens to be "forgotten", allowing people to request removal of public personal information on the internet (savage, 2023).

2.3 Funding of Key Legislative Frameworks

As for the funding of these legislations Both CFAA and GDPR are publicly funded through government budgets. According to the U.S. Department of Justice the CFAA was primarily funded as a regular legislative process of the United States Congress. The funding for development and implementation of this framework came from the federal budget designated to the Department of Justice and other agencies connected to law enforcement (U.S. Department of Justice, n,d).

According to the European Commission (n,d), the funding of the GDPR primarily came from the European Union's budget. In addition the GDPR was also supported by EU funding programs such as Citizens Equality, Rights and Values Program (CERV) with around EUR 2.3 million, and the Rights, Equality and Citizenship Program (REC) with around EUR 1.6 million (E.U. Commission, n,d) These programs financed projects focusing on increasing awareness and securing compliance with GDPR across nations and other EU member states (E.U. Commission, n,d).

3 Awareness Campaigns and Education

Governments and commercial organizations make use of information and communication technology, their need for information security is therefore of great significance. To achieve this, the governments / organizations deploy security measures and policies. These specify how to operate information systems in a secure way, as well as they correct user behavior both for citizens and employees. The purpose of cybersecurity awareness campaigns is to influence both businesses as humans to operate information systems in a secure manor (Bada, 2019).

3.1 Western Approach to Awareness Campaigns

Since 2004 the White House and Congress have appointed October to a National Cybersecurity Awareness Month. With the period from 2004 to 2009 focused on cybersecurity "hygiene" in general. Such as implementing strong passwords, and keep your preferred software updated and being cautious of phishing attempts. In 2010 the "Stop. Think. Connect." Initiative begins. This initiative was revealed in 2010 on the yearly Cybersecurity awareness month implemented in 2004. With proclamation from President Barack Obama. This initiative is still operating and are still addressing the human online behavior, as the data breach investigations report stated that the human factor is a key momentum of 74% of breaches today, including cyberattacks like phishing, and misuse (Reed, 2023).

In 2014 a new focus was placed on building security into information technology products. The American nonprofit organization, National Cybersecurity Alliance stated that that security should be an element within the software design, making computers safer to operate for the common man (Reed, 2023). In 2018, former president Donald Trump signed the Cybersecurity and Infrastructure Agency Act. Which made the Cybersecurity and Infrastructure Security Agency (CISA). This agency assists organizations as well as other government agencies in managing cybersecurity issues (Reed, 2023).

In the period of 2019-2022, the "Do your part. #BeCyberSmart" campaign was launched. This campaign emphasizes the importance of individuals and organizations to be responsible for their role in protecting their part of cyberspace, focusing on accountability and making progress towards enhancing cybersecurity (Reed, 2023). In 2023 and beyond, CISA continues to emphasize the general cybersecurity hygiene through recommending strong passwords, two step authentication, recognition and reporting of phishing attacks and frequent software updates (Reed, 2023).

Van steen (2020) also discusses some of the European awareness campaigns. And how they respond to the American approach to cybersecurity awareness campaigns.

The "Cyber Aware" campaign in the United Kingdom, part of the national cybersecurity strategy for 2016-2022. And the European Cyber Security Month, organized by the European Union Agency for Cybersecurity (ENISA) since 2012, that

promote cybersecurity through different activities. Both emphasizing the need for cyber-awareness on an individual and organizational level (Van Steen, 2020).

3.2 Funding of Key Awareness Campaigns

National Cybersecurity Awareness Month 2004 was funded by the U.S. government, especially through funding from the white house and congress (Cybersecurity and Infrastructure Security Agency, 2024). The "Stop. Think. Connect" campaign is funded by a cooperation between the U.S. government, private companies and nonprofit organizations. This campaign was introduced by the U.S. department of Homeland Security, with support from the Whitehouse (Homeland Security, n.d). The "Do Your Part. #BeCyberSmart" campaign is also publicly funded by the U.S. Department of Homeland security and the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, this campaign is supported by the U.S. government and some private sector organizations (Homeland Security, 2021). The European Cyber Security Month is publicly funded by EU programs like the Connection Europe Facility (CEF) and the digital Europe Program. These programs offer financial support for projects that increases cybersecurity awareness and promote sustainable practices across the EU (European Health and Digital Executive Agency, 2023).

3.3 Norwegian Awareness Campaigns

Due to their current sate of a non-membership in the European Union, Norway has some of their own ways to manage cybersecurity and privacy. This chapter will examine, Norway's approach cybersecurity, awareness and education.

Norway has some instances that are supposed to enhance the general knowledge of cybersecurity on a national level. Norwegian National Centre (NCSC) are responsible for managing serious cyber-attacks against critical infrastructure and information. They are also working on increasing Norway's resilience in the digital domain through different campaigns and training programs (NSM, 2024). In addition to this the Norwegian government have worked out a national strategy regarding cybersecurity, in which focuses on strengthening the cooperation between public and private stakeholders as well as increasing cybersecurity competency. This strategy also aims to increase the necessary knowledge for using information systems in a secure manor.

The following campaigns are derived from the Norwegian government (2018) National Cyber Security Strategy for Norway. Norway participates in national exercises and international cooperation, participating with other nations to gain knowledge of potential cyber threats. This campaign is meant to increase both Norway's and the participating countries knowledge and ability to detect and manage cyber-attacks (Regjeringen, 2018). Additionally, there are training and skill development programs which focuses on increasing the competency through education programs at different levels, including elementary school, high school and universities. This also include continuing and postgraduate education. Public and private cooperation is also a key

component, where both government and the corporate sector cooperates to discuss and identify the challenges regarding cybersecurity. This includes sharing experiences and information about potential threats and effective measures. Furthermore, services like "Nettvett.no & Slettmeg.no" provided by Norwegian Center for Securing information (NorSIS), are dedicated to council both individuals and organizations on how to use internet in a secure way (Regjeringen, 2018)

3.4 Individual and Organizational Perspectives

People can sometimes find it stressful to follow security procedures and protocols, especially if they perceive the security measurements as an obstacle. It can also be stressful to remain a certain level of awareness of cybersecurity daily, both in your organization and home. Often when downloading different programs or apps, one can experience several notifications on how you should secure your new profile. This can result so called "security fatigue" and can be hazardous to our society as well as organization (Bada, 2019). In this case, the users of the information systems will become less aware of their actions as they notice no difference whether they follow the security measurements or not. This can potentially be of great threat for organizations or family homes as they become easier targets for cyber-attacks. The following statement highlights the significance of the issue: "When security needs and business needs collide, business wins" (Whitman, 2022, p. 29). Without the business to generate revenue and use the information, the data can possibly loose its significance, rendering it unnecessary. If the business is unable to operate to its core activities, the importance of cybersecurity diminishes. It is therefore crucial to find a balance between the organization's needs for protection of information and the need for operational functionality (Whitman, 2022).

Schneier (2016) also addresses this theme, but with a different perspective expressing that the problem is not the users but how our computers and built in security are designed badly. He also explains that traditionally we have thought about security and usability as a "tradeoff" in such sense that a more secure system is less functional and more annoying for the user, and a more flexible and powerful system is less secure and more vulnerable (Schneier, 2016). Jonathan Reed (2023) emphasized the great importance of the need for built-in cybersecurity into software stated by the national security alliance in 2014. This was also expressed by the United States Whitehouse in 2018, which stressed that one should prioritize improving awareness and transparency of cybersecurity practices and make a bigger market demand for more secure products and services (Van Steen, 2020).

3.5 Cultural Differences

Bada (2019) discusses the cultural differences regarding awareness campaigns in different parts of the world. Reaching maximum efficiency of the campaigns, one need to adapt the message to the targeted population, regarding the recipient's cultural background and values. In western countries the message in cyber awareness

campaigns tend to reach out to individuals, focusing on the individual's benefits gained from following the recommended cyber measurements. This is due to the western individualistic culture. As for the eastern hemisphere the awareness campaigns are more focused on the collective benefit gained from following the recommended cyber measurements, due to their focus on social relations (Bada, 2019).

Bada (2019). refers to the differences between the UK and Africa, regarding the awareness campaigns and the theme of the statement. In the UK the campaigns "GetSafeOnline" and "Cyber Streetwise" give concrete advice on how to protect yourself and your online business, emphasizing the individual responsibility using information systems. In Africa awareness campaigns are aimed in a more collectivistic manor. Campaigns like "ISC Africa" and "Parents" emphasizes teamwork and collective responsibility for cybersecurity (Bada, 2019). One can than conclude that different cultures adapt their awareness campaigns to the country's norms and traditional values. This will also serve a greater purpose when it comes to reaching the wanted result of the awareness campaign.

4 Discussion

Government legislation and awareness campaigns are two critical components in the fight against cyberthreats, each with its own limits and strengths. While legislation gives more of a formal framework for cyber-security, the awareness campaigns aim to educate and inform the public and organizations about best practices within the cybersecurity domain.

Government legislation such as the EU General Data Protection Regulation (GDPR), and the Computer Fraud and Abuse Act (CFAA) in the United States, establishes legal requirements to protect data and respond to breaches. Institutions and frameworks like GDPR, CFAA and Cybersecurity and Infrastructure Security Agency (CISA) create a foundation of security practices that organizations and individuals should follow. Thereby reducing vulnerabilities and ensuring aligned response to cyber incidents (Savage, 2023). GDPR reflects the EU's approach to protection of privacy in cyberspace, contrasting with the more "laissez-faire" attitude of the United States, which seemingly lacks a comprehensive national cybersecurity law comparable to the GDPR (Savage, 2023). Government efforts like the act of developing institutions like CISA also provides mechanisms for enforcement and penalties, which can further prevent irresponsible behavior and encourage compliance (Savage, 2023).

As for the historical development of government legislation in cybersecurity has been marked by milestones, such as the Computer Fraud and Abuse Act (CFAA) of 1986 and the Computer Security Act of 1987 which addresses the earliest of challenges connected to the growth of information systems and the internet (Berris, 2023) & (U.S. Congress, 1987). More modern initiatives like the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA)

show ongoing efforts to adapt and overcome the everchanging threat landscape of the growing cyberspace (Savage, 2023). However, the legislation alone is not sufficient enough to counter cyber-attacks and educate a society on safe cyber practices. The dynamic nature of cyber threats quickly become outdated as the digital world rapidly grows more complex (Savage, 2023). Additionally, as Bada et al. (2019) discusses that compliance with legislation are often seen as a "checkbox" exercise, where organizations do the bare minimum to avoid penalties rather than genuinely improving their cybersecurity systems. It is also known that organizations find these processes affecting the organizations economy as for the expenses linked to cyber systems (Whitman, 2022). This results in organizations cutting the expenses of investing in cybersecurity as they see no difference in their daily operations whether they have a strong cyber defense or not (Whitman, 2022).

Awareness campaigns play a crucial role in connecting the gap between legislation and practical security measures. These campaigns aim to educate organizations and individuals about the latest threats and best practices for mitigating them. By raising awareness, these initiatives can foster a culture of cybersecurity. For example, campaigns like National Cyber Security Awareness Month in the United States and similar alternatives in Europe focus on educating the public about password security, phishing and the importance of software updates (Tommy Van Steen, 2020). Despite the benefits, these campaigns have limitations as well. Their effectiveness depends largely on the initiative and participation of the targeted individuals, as well as the continuous effort and resources to stay with the fast-growing threat landscape (Bada, 2019).

Schneier (2016) adds another dimension to this discussion by emphasizing that the problem is not the user but the designs of the computer systems themselves. He argues that security and usability have been seen as a "tradeoff", where more secure systems are less functional and more annoying for users, and more flexible systems are less secure to operate. His perspective suggests that improvement of the design of security systems is a necessity and can enhance cybersecurity. This is also emphasized in the National Cybersecurity Alliance statement about how security should be a component within the software design, making the computer safer to operate (Reed, 2023).

The interplay between government legislation and awareness campaigns is complex, yet somewhat logical in a sense that they fulfill each other. While government legislation provides a necessary framework for the legal challenges and enforcement mechanisms (Carr, 2021), awareness campaigns complement these initiatives by promoting a preventive cybersecurity culture both in business and for individuals of a society (Bada et al., 2019). However, both approaches have their limitations and flaws. For instance, despite the strong legislative frameworks, the growing landscape of cyberthreats challenges old legislations and pushes governments to implement new regulations to counter the new threats (Carr, 2021). Aligned with this, awareness campaigns address a main issue to bad computer habits as "security fatigue", where users of information systems find it exhausting to maintain proper cybersecurity in their

daily life and operations, which further lead to creation of a bad security culture both in business and on an individual level (Bada, 2019).

Furthermore, awareness campaigns in the western hemisphere are often tailored for western needs and specific western interests and can possibly contain a different message than eastern campaigns. Bada et. al (2019) discusses that Western campaigns tends to emphasize protecting national and economic interests, whereas southern campaigns might emphasize a different set of priorities like teamwork and shared responsibilities, reflecting different political strategies. In addition, the differences in government legislation in countries as Russia, China, and the United States. Whereas throughout history the United States have shown a more liberal view on cyber-security which focuses on business and protection of civil liberties. This goes for the EU as well, as they have implemented privacy laws as GDPR allowing individuals to request removal of public personal information. In contrast, eastern countries like China and Russia focus on control and surveillance in cyberspace (Savage, 2023).

5 Conclusion

The historical and modern approaches to cybersecurity, extensive government legislation and awareness campaigns, highlight the criticality of robust and adaptive frameworks in a rapidly evolving digital landscape. Legislation like General Data Protection Regulation (GDPR), Computer Fraud and Abuse Act (CFAA), provides legal frameworks for addressing cyberthreats and protecting data. In parallel, awareness campaigns connect the gap between legal compliance and practical implementation, encouraging a culture of cybersecurity both on individual and organizational levels. However, both approaches have their limitations. Legislative frameworks risk becoming outdated as the cyberthreat landscape quickly evolves, while awareness campaigns often suffer from inconsistencies in implementation as people find the awareness and security processes exhausting. As highlighted, cultural differences and varying political strategies and beliefs, makes a further impact on the efficiency of these efforts globally. Ultimately, a collaborative approach is essential. One that combines robust legislative measurements with proper education and system design improvements. Integrating security withing technological innovation, as emphasized by experts like Bruce Schneier, alongside continuous awareness efforts, can help to build a society more resilient cyberattacks. By learning from former incidents and adapting to emerging challenges, societies can navigate the complexities of the growing cyberthreat landscape and protect the interconnected world.

6 Reference List

Berris, P. G. (2023) Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress. *Congressional Resaerch Service* , (p. 31).

https://crsreports.congress.gov/product/pdf/R/R46536 (Accessed: 15 November)

Carr, M. (2021) A Political History of Cyberspace. I P. Cornish, *The Oxford Handbook of Cyber Security* (ss. 50-70). Oxford Academic. https://books.google.no/books?hl=no&lr&id=p6pJEAAAQBAJ&oi=fnd&pg=PA49&dq=A+Political+History+of+Cyberspace&ots=7o-74StTzA&sig=odXi_7neyPT00BU8v0U8vV3lH4s&redir_esc=y#v=twopage&q&f=false (Accesed: 17 November)

Cybersecurity and Infrastructure Security Agency (n.d) "Cybersecurity Awareness Month." Last modified 2024. https://www.cisa.gov/cybersecurity-awareness-month. (Accessed: 12 December)

European Commission, (n.d) EU funding supporting the implementation of the General Data Protection Regulation (GDPR). https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en (Accessed 12 December)

M. Bada, A. M. (2019) *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Cornell University: https://arxiv.org/abs/1901.02672 (Accessed: 12 November)

NSM. (2024) *Norwegian National Cyber Security Centre (NCSC)*. nsm.no: https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/ (Accessed: 1 Desember)

Reed, J. (2023, October 27) The evolution of 20 years of cybersecurity awareness. *Security Intelligence*.https://securityintelligence.com/articles/20-years-of-cybersecurity-awareness/ (Accessed: 28 November)

Regjeringen. (2018) *National Cyber Security Strategy for Norway.* Accesed Regjeringen.no:https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (Accesed: 15. November)

Savage, D. S. (2023) 1-The Emergence of Cyberspace and Its Implications. I D. S. Savage, *Security in the cyber age* (pp. 13-34). Cambridge University Press.

Schneier, B. (2016, October 25) Stop Trying to Fix the User. *IEEE Security & Privacy*. https://ieeexplore.ieee.org/document/7676198 (Accessed: 27 November)

Tommy Van Steen, E. N. (2020, 12 12) *What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?* Accesed Oxford academic: https://academic.oup.com/cybersecurity/article/6/1/tyaa019/6032830 (Accessed: 8 November)

U.S. Congress. (1987) Computer Security Act of 1987. Available at: https://www.congress.gov/bill/100th-congress/house-bill/145 (Accessed: 12. December)

U.S. Department of Homeland Security, (2021) *Be Cyber-Aware This Month (and All Year!)*. https://www.dhs.gov/science-and-technology/news/2021/10/04/be-cyber-aware-month-and-all-year (Accessed: 12 December).

U.S. Department of Homeland Security, (n.d) *Stop. Think. Connect. campaign fact sheet*. https://www.dhs.gov/xlibrary/assets/stop-think-connect-campaign-fact-sheet.pdf (Accessed 12 December)

U.S. Department of Justice, (n.d) Computer Fraud and Abuse Act (CFAA). https://www.justice.gov/jm/jm-9-48000-computer-fraud (Accessed: 12 December)

Vassiliadis, V. T. (2024) *Tracing the evolution of cyber resilience: a historical and conceptual review.* Accesed Springer.com: https://link.springer.com/article/10.1007/s10207-023-00811-x (Accessed: 8 November)

Whitman, M. E. (2022) *Information security: principles of information secirity (7th ed.).* Cengage learning.

Chapter 2

Historical view on cyber security standards and insurance

Marcus Bjørndalen [10390]

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This paper investigates two historic approaches to promoting and funding cybersecurity: the development of cybersecurity standards and the adoption of cyber insurance. The research focuses on how these methods have evolved over time and their impact on cybersecurity practices globally, with a specific look at Norway as a case study. The study draws from a combination of peer-reviewed articles, industry reports, and historical analyses to explore the emergence of frameworks such as ISO 27001 and the NIST Cybersecurity Framework, alongside the growth of specialized cyber insurance policies. It examines how standards provide structured methodologies for managing risks and how insurance offers financial protection while incentivizing better security practices. Findings reveal that while these approaches have significantly enhanced the cybersecurity landscape, challenges remain, including the lack of reliable data, limited adoption in certain markets, and difficulties in integrating standards into insurance practices. By understanding these dynamics, the paper sheds light on the importance of these tools in managing modern cyber threats and highlights opportunities for further development.

Keywords: Standards, Insurance, Cyber Security

1 Introduction

Cybersecurity has escalated to a major business function globally due to the ever-increasing complexity and frequency of cyber threats. This research aims to provide a comprehensive analysis of the evolution of cybersecurity standards and insurance, their impact on cybersecurity practices and funding, and the challenges and opportunities they present.

Firstly, this chapter will give a establish and reason why cyber security is such an important part of our everyday lives. Secondly, will the paper take you through a literature review by elaborating on the history of cyber security standards and insurance, and how these two interplay. Further, we will elaborate on the history of selling standards and insurance, and how funds were gathered. As cyber security standards and insurance are a relatively new field of study, there is not that many peer reviewed articles that provide historic views on how they were sold. We will elaborate on how lack of data is limiting the field later in the chapter. Therefore, this paper will bear mark of

information gathered through peer reviewed articles and blog posts from acknowledged organizations, with relevant authors. As most of the research and development of cyber security started in the U.S., it will also be articles and examples mostly from the U.S. I will touch upon cyber security in Norway at the end.

To end the chapter, I will conclude the research and be looking into the future of cyber security standards and insurance. By analyzing these historic approaches, we can better understand the current position of cyber security and its future destination.

1.1 Growing Importance of Cyber Security

The cybersecurity landscape has undergone an incredible transformation since the 1990s. What started as a niche concern to some companies has become a vital part of risk management and organizational strategy. This shift is driven by the rise of increasingly complex cyber threats and a growing awareness of the financial and reputational damage cyber incidents can cause, creating significant challenges for organizations worldwide.

(Sayegh, 2024). Today, the global cyber workforce has grown to around 4.7 million people (101 Cybersecurity Statistics and Trends for 2024, 2024). Plus, 93% of organizations say they plan to boost their cybersecurity budgets within the next year (The CISO Report, no date). This highlights just how crucial cybersecurity has become.

Advances in technology, AI, and machine learning have transformed security monitoring and threat detection. These tools are now must-haves for any modern cybersecurity plan. With the rise of cloud services, smartphones, tablets, and IoT devices, the landscape of cybersecurity has changed, pushing for stronger methods to combat attacks. While technology simplifies life, it also ramps up security risks (Slonopas, 2024).

In response to these new challenges, two approaches have emerged in the cyber security world: the development and adaption of cyber security standards, and the growth of cyber security insurance. These two approaches have played a crucial role in successful funding cybersecurity initiatives.

2 History of cyber security standards and insurance

The development of cybersecurity standards and insurance has been key to overcoming early challenges, like the absence of clear guidelines. These tools have also helped build trust and ensure financial protection for investments in cybersecurity. This analysis dives into how they’ve evolved over time and shaped the cybersecurity field.

2.1 Historical development of cyber security standards

Early stages and emergence of standards

The cyber security landscape evolved significantly in the early 2000s. As businesses grew more dependent on digital systems, it became clear that a structured way to protect them was needed. One of the first big milestones was the British Standard 7799, which eventually became the ISO 27001 standard, which is a very popular certification worldwide (Culot *et al.*, 2021).

The ISO 27001 standard was designed and published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which marked a milestone for cybersecurity standards. It outlines how organizations can set up, run, maintain, and improve an information security management system (ISMS), within the context of the organization (Culot *et al*., 2021). Several technological providers including Amazon Web Services, several Microsoft business units and recently Facebook marketplace have gained widespread attention for achieving ISO 27001 certification (Venters and Whitley, 2012; Culot *et al*., 2021)

Evolution of NIST Frameworks

Alongside the development of international standards, the National Institute of Standards and Technology (NIST) in the U.S. has been researching risk for computing devices since the early 1970s. NIST has focused on risk management as the key driver for cybersecurity and privacy investments (National Institute of Standards and Technology, 2022).

NIST has over the years created several guidelines and standards, and the most influential being the NIST Cyber Security Framework. This framework was an executive order by former President Obama, demanding better collaboration in identifying, assessing, and managing cyber risk in both public and private sector (Cisternelli, 2024). The NIST Cybersecurity Framework has seen significant updates over time, with the latest being CSF 2.0 which expands its applicability beyond critical infrastructure to a wider array of organizations (National Institute of Standards and Technology, 2024). “The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors including industry, government, academia, and nonprofit - to manage and reduce their cybersecurity risks” (National Institute of Standards and Technology, 2024, para. 1)

Comparative analysis of standards

ISO 27001 and the NIST Cyber Security Framework have gained worldwide adoption, but they differ in their focus and approach. Organizations often follow best practices from international standards like the ISO-27,000 series, which are created by groups like ISO or government agencies. These standards lay out guidelines to make

sure systems, processes, and services work effectively and meet their goals, and are designed to be applicable globally (Andersson, Hedström & Karlsson, 2022). ISO 27001 also requires a formal certification, which involves a thorough evaluation of an organization's ISMS to ensure it meets the standard's requirements. It addresses various areas, including risk assessment, asset management, access control, incident management, and business continuity planning (ISO 27001 vs NIST cybersecurity framework, 2023).

Information security standards provide a solid baseline for organizations to manage risks and stay efficient. They hold a lot of influence because people trust their benefits. For standardizing groups, it's all about building legitimacy so stakeholders see the value in adopting them (Andersson, Hedström & Karlsson, 2022).

NIST frameworks offer a flexible approach, allowing organizations to customize their security programs to fit their specific needs without requiring formal certification. Developed by the National Institute of Standards and Technology, a non-regulatory U.S. government agency, these voluntary frameworks help organizations manage and reduce cybersecurity risks. They provide practical guidelines and best practices for strengthening security measures and are designed to be adaptable for organizations of any size or industry (Vicente, 2023; Palatty, 2024).

The constant evolution of these standards and frameworks reflects the ever-growing cyber security threat landscape, and the growing acceptance of cyber security as a critical business concern. As cyber threats become more sophisticated, will standards also continue developing to guide businesses and organizations of all sizes.

2.2 Evolution of cyber security insurance

Historical development of cyber insurance

What is cyber insurance? Insurance companies, in the early days of the Internet, primarily offered insurance that covered general liability, and less for data-related risks. As the cyber threat picture grew alongside the development of the Internet, insurance companies realized that they needed more specialized policies (Bloxberg, no date). Granato and Polacek (2019) explains that the history of cyber insurance often is traced back to Steven Haase. He helped AIG create the first internet security liability policy in 1997, and these policies were initially designed for IT companies managing networks and systems for other businesses and consumers. Over time the cyber insurance market has grown and is now offering three main types of coverage: third-party coverage, first-party coverage and implicit silent cyber coverage (Granato and Polacek 2019).

Third-party liability cyber insurance covers costs that clients face due to data breaches, malware, or other cyberattacks caused by the business. Granato and Polacek (2019) draws comparison to medical malpractice, with businesses insured against harm they may inflict on their clients. Early cyber insurance policies were mostly of this type.

In the mid-2000s, cyber insurers started to introduce first-party expense coverage, opening options for any company using technology. This type of insurance helps businesses cover costs from cyberattacks that directly impact the business. Policies can be tailored to a company's needs and may include expenses like credit monitoring, hiring crisis management consultants, negotiating ransom payments, and recovering lost data (Granato & Polacek, 2019).

Granato and Polacek (2019) further explains the third type of coverage, silent cyber coverage. This isn't a cyber security policy per se, but really a term that refers to potential cyber related losses that fall under traditional property and casualty policies not specifically meant to cover cyber risks. Since this isn't a cyber security-specific policy, I won't go into further detail about this.

Impact of major cyber incidents

High-profile cyber incidents have played a big role in the demand for cybersecurity insurance. Events like the Target breach in 2013 and the Equifax breach in 2017 were major wake-up calls. These breaches showed how vulnerable organizations can be and the huge financial and reputational damage a breach can cause a business (Granato & Polacek, 2019). The NotPetya attack in 2017 caused over $10 billion in global damages and was another key moment in cyber security history. It highlighted the need for robust cyber insurance to cover large-scale, cascading failures. Incidents like this have raised awareness of cyber risks and pushed organizations to look for insurance to protect against similar threats in the future (Granato & Polacek, 2019).

2.3 Interplay between insurance and standards

The connection between cybersecurity standards and insurance is both complex and complementary and the same time. Research shows that cyber insurance can encourage organizations to adopt better cybersecurity practices. An analysis from Adriko and Nurse (2024) on insurance application forms examining how cyber insurance promote cyber security best practice, showed how they align with cybersecurity standards like ISO 27001 and NIST. This highlighting how cyber security insurance policies promotes compliance with these frameworks. For example, insurance applications often require companies to follow specific protocols, which can push them to align with standards like ISO 27001 or NIST (Adriko & Nurse, 2024). This may indicate that the insurance industry is starting to integrate established standards into their processes.

However, integrating cybersecurity standards into insurance practices comes with challenges. The article "Cyber Insurance and the Cyber Security Challenge" by MacColl, Nurse and Sullivan (2021) highlights the difficulties the industry faces in moving from theoretical frameworks to real world applications. They mean cyber insurers are theoretically in a strong position to promote the adoption of established cybersecurity

frameworks like ISO 27001 or NIST. This could be achieved by requiring certification as a condition for insurance coverage, or by structuring insurance questionnaires around these standards. Some insurers have expressed positive views on security standards like ISO and Cyber Essentials during interviews. However, there's no consistent evidence that certification to these standards is a routine requirement for obtaining cyber insurance. Additionally, how well these standards are reflected in insurance questionnaires varies, with some key topics occasionally missing entirely (MacColl, Nurse and Sullivan 2021).

3 Government and private organizations

An important part of cyber security's development in standards and insurance, is played by government and organizations. Governments are a crucial part of setting and implementing standards through legislation and regulatory frameworks. The government can set out a standard and define what is an acceptable level of security. Haleliuk (2023) writes that cyber security vendors often support and lobby for stricter standards and regulations that will help customers prevent potential cyber incidents, and ultimately drive demand for their products and services.

Fadia, Nayfeh and Noble (2020) discusses how governments can combat cyber security risks. They explain that many governments have created national cybersecurity strategies that include setting up dedicated cybersecurity agencies, like The United Kingdom's National Cybersecurity Agency. These agencies lead the charge by defining standards, driving the cybersecurity agenda, and enhancing the skills of cybersecurity professionals. They further address a study done by ISC2 from 2017 where they predicted that the world would be 1,8 million short of cyber-skilled individuals by 2022. (ISC2, 2017 as cited in Fadia, Nayfeh and Noble, 2020). A new study from 2024 found that the world is now 4,8 million skilled individuals short of the global demand (ISC2, 2024)

Private organizations, especially those in tech and cybersecurity sectors, play a key role in developing and promoting industry standards and best practices. They drive innovation by investing in research and development to create new and advanced security solutions that often meet or surpass established standards (Etzioni, 2011).

4 How was cyber insurance historically sold?

Cyber insurance got a big wakeup call in 2013 and 2017 with the Target and Equifax breach, as we mentioned earlier in the chapter. The market for cyber insurance has gotten huge, and by 2018, businesses in the U.S. was spending 1.1 billion dollars on standalone cyber insurance policies, and $922 million on packaged policies (Granato and Polacek, 2019). This growth has continued, and the global market for cyber security insurance was valued at 7.60 billion dollars in 2021 and is projected to reach 20.43 billion dollars by 2027 (Cole, 2024). The Swiss Re (2024) explains in their report that

the market has shifted to slower growth and lower insurance rates. Data from 2023 and 2024 shows that many players overestimated the market's potential, leading to overly optimistic premium projections. For 2025, Swiss Re is estimating a market premium of 16.6 billion dollars, which estimates to +8% over 2024 (Swiss Re, 2024).

Granato and Polacek (2019) gives an interesting view on the adoption rates in different sectors in their article from 2019. About 58% of large businesses have a standalone cyber insurance policy, and small businesses have just about 21%. Their article also shows that education and healthcare sectors have higher adoption rates at 66% and 62% respectively, while financial institutions and manufacturing have lower rates at 27% and 30% (Granato and Polacek, 2019). These different adoption rates highlight the different perceptions on risk, security and regulatory processes across industries.

4.1 Historical approaches to sell cyber insurance

We remember from earlier in the chapter that cyber insurance policies initially were add-ons to traditional liability coverage when they first dropped in the late 1990s. These early policies focused on third-party liabilities such as losses to a business's clients, rather than first-party direct losses to the business itself. 2010s saw the rise of ransomware attacks, which significantly impacted the cyber insurance landscape. Cryptocurrencies started emerging and facilitated untraceable ransom payments, increasing the frequency and severity of ransomware attacks (Watts, 2024). MacColl, Nurse and Sullivan (2021) explain that ransomware is still the most pressing challenge facing the industry. They call it a societal problem, but insurers have received massive criticism for facilitating ransom payments to cyber criminals. These factors throw fuel on the fire by encouraging cyber criminals to engage in ransomware attacks and giving existing criminals the resources to invest in and expand their operations.

The early market of cyber insurance was hindered by some challenges. Collecting and sharing reliable cyber risk data, which is essential for informing underwriting and risk modeling, plus a general lack of awareness among decision-makers, which contributed to limited demand. This lack of data hampered insurers' ability to accurately assess risks and price policies accordingly, further limiting the effectiveness of any incentives that could be offered (MacColl, Nurse and Sullivan, 2021).

A good strategy employed by insurers has been to incentivize better cybersecurity practices among policyholders. They did this by rewarding organizations that demonstrate good risk management, and insurers did not only reduce their own risk exposure but also promoted the adoption of best practices in cyber security (MacColl, Nurse and Sullivan, 2021). Although some has insurers has done this, most of the industry has struggled to implement effective financial incentives or security obligations (MacColl, Nurse and Sullivan, 2021). The insurance industry faces difficulties in collecting and sharing reliable cyber risk data. The data is essential for informing underwriting and risk modeling. This lack of data stops insurers' ability to accurately assess risks and

price policies accordingly, further limiting the effectiveness of any incentives that could be offered (MacColl, Nurse and Sullivan, 2021).

4.2 Cyber insurance funding

Government grants and programs, like the State and Local Cybersecurity Grant Program by America's Cyber Defense Agency, are being used in supporting cyber security initiatives. These programs provide funding to strengthen cybersecurity at state and local levels. These indirectly impacts the cyber insurance market by lowering risks and encourage more organizations to invest in coverage (Brown, 2024).

Public-private partnerships have been key to funding cybersecurity initiatives, by combining the strengths of both private and public sectors to improve infrastructure and capabilities. The International Counter Ransomware Initiative is a great example. During their fourth gathering, the members of CRI reaffirmed their joint commitment in developing resilience to ransomware and support other members if they are faced with attacks (The White House, 2024). This is showcasing how these partnerships tackle ransomware, a major threat covered by cyber insurance.

5 How were standards historically sold?

The promotion and selling of cyber security standards to organizations and industries have involved various strategies. We touched slightly upon this earlier in the chapter where we explained the origin of cyber security standards.

Businesses have historically sold standards by highlighting their role in improving security and ensuring compliance requirements. Frameworks like NIST and ISO 27001 provide solid foundations for managing cybersecurity risks, with adoption often influenced by the industry in which an industry is located and their specific needs. The choice between the two frameworks is influenced by factors such as the desired level of standardization and the specific risks faced by the organization (Maharaj, 2024). The cost and flexibility are key advantages of these frameworks. NIST, for example is free of charge. It also lets organizations implement the framework at their own pace. adapting it to fit their budget and needs (Vicente, 2023). This flexibility can make NIST especially appealing to organizations that are just starting to build their cyber security risk management plans.

On the other hand, ISO 27001 requires purchasing the standard and undergoing expensive certification audits, which can cause a barrier for some organizations. But despite the cost of ISO 27001, the certification process remains a strong selling point by offering globally recognized validation of an organization's information security practices. ISO 27001's formal certification is widely viewed as a sign of operational maturity and a commitment to rigorous security standards (Vicente, 2023).

6 The Norwegian market

Now that we've covered the history of standards and cyber insurance, as well as how they've been marketed globally, let's shift our focus to how these cybersecurity measures are applied in the Norwegian market.

Norway is a technologically advanced country. They ranked fourth in the World Economic Forum's Networked Readiness Index in 2016. Singapore, Sweden and Finland were the only countries above them (Breene, 2016 as cited in Bahşi, Franke and Friberg, 2020). Even though this ranking is 8 years old it still proves that Norway is an advanced technological country. Nevertheless, Norway are being called the cyber insurance laggard amongst the other Nordic countries (Franke, 2017 as cited in Bahşi, Franke and Friberg, 2020). This might be because Norway's estimated cyber loss is 0.64 per cent of GDP, 23 percent above the EU average of 0.41 per cent (McAfee and CSIS, 2014 as cited in Bahşi, Franke and Friberg, 2020).

Bahşi, Franke and Friberg (2020) further explains that the Norwegian market is similar to many others, especially their Swedish neighbors. These similarities are that they have low adoption rates relative to the total number of companies, few claims are being filed to insurers, and rapid marked growth by new product launches. However, one key difference stands out. According to all interviewees in the study by Bahşi, Franke and Friberg (2020) has Norway a lower cyber insurance uptake compared to its Nordic neighbors.

The low number of claims that are filed to insurers highlights a major challenge in the cyber insurance industry, namely the lack of reliable and comparable data. We also mentioned this earlier in the chapter "Historical approaches to sell cyber insurance". This creates a gap that makes it harder for insurers to price their products accurately and leaves policymakers, researchers, and the public with limited insight into the state of cyber insurance (Bahşi, Franke and Friberg, 2020).

Earlier studies highlighted GDPR as a driver of increased cyber insurance activity, not only in Norway but in Europe as well. The GDPR regulations is supposed to protect personal data, and took effect in the EU on 25 May 2018, and in Norway on 20 July 2018 (Bahşi, Franke and Friberg, 2020). Breaches in personal data must be communicated to the data subject and the national supervisory authority within 72 hours of the data controller becoming aware of the breach (EPEC, 2016a as cited in Bahşi, Franke and Friberg 2020). While GDPR has had a modest impact on the Norwegian cyber insurance market so far, it's proven useful for insurers as a conversation starter. Many use it to highlight the importance of protecting personal data and managing cyber risks, making it easier to introduce cyber insurance as a valuable tool for compliance and risk mitigation (Bahşi, Franke and Friberg, 2020).

7 Conclusion and future research

This paper highlights the evolution and impact of cybersecurity standards and insurance, two crucial approaches in cyber security. From the establishment of ISO 27001 to the emergence of specialized cyber insurance policies. These strategies have grown significantly, addressing both risk management and financial protection. Their interplay where insurance incentivizes compliance with established standards, demonstrates a promising synergy for enhancing cybersecurity globally. However, challenges like the lack of consistent data and standard integration into insurance policies hinder broader adoption. For Norway, as a technologically advanced yet lagging market in cyber insurance, addressing these gaps could unlock significant potential.

Cyber threats are becoming more sophisticated and frequent, driven by rapid technological advances such as artificial intelligence and cloud technology. These developments have increased the complexity of cyber risks, making it challenging for organizations to protect themselves adequately. The global cost of cybercrime is expected to hit $13.8 trillion annually by 2028, underscoring the growing financial toll of cyber threats (Munich Re, 2024).

On a personal note, I strongly encourage both Norwegian and international businesses to invest in ISO certification and cyber insurance, particularly policies that cover third-party losses. Achieving a certification like ISO 27001 demonstrates a commitment to robust information security management, ensuring the confidentiality, integrity, and availability of client data. This not only reassures existing clients but also serves as a powerful tool to attract new customers. Additionally, having insurance that covers third-party losses can be a great selling point, if a client's data is compromised in a cyberattack, they'll know they're covered and can be compensated.

Looking forward, more research is needed to explore how AI-driven tools could revolutionize cybersecurity frameworks and insurance models. Additionally, studying underrepresented markets, such as Norway, might offer valuable insights into overcoming adoption barriers. By understanding these dynamics, the industry can better prepare for the escalating complexity of cyber threats while ensuring resilience and trust in digital ecosystems.

8 Reference list

1. Adriko, R. and Nurse, J. R. C. (2024) Does cyber insurance promote cyber security best practice? An analysis based on insurance application forms, *Digital Threats*, 5(3), Article 25, 39 pages. Available at: https://doi.org/10.1145/3676283(Accessed: 22 November 2024).

2. Andersson, A., Hedström, K. and Karlsson, F. (2022) Legitimacy in information security standardization: A study of the ISO/IEC 27000 series, *Information & Management*, 59(2), pp. 1–13. doi: 10.1016/j.im.2022.103623.

3. Bahşi, H., Franke, U. and Friberg, E. L. (2020) The cyber-insurance market in Norway, *Information & Computer Security*, 28(1), pp. 54–67. doi: https://doi.org/10.1108/ics-01-2019-0012 (Accessed: 27 November 2024).

4. Bloxberg, D. (no date) What is cyber insurance and why do you need it?, *Vipre Security Group*. Available at: https://vipre.com/glossary-terms/what-is-cyber-insurance-and-why-do-you-need-it/?srsltid=AfmBOor-JqkJYY2th2rE-EAZE7s3N0WlW0KV2pgL4P2Jz3xShYiI3qON (Accessed: 15 November 2024).

5. Brown, K. (2024) 14+ Unexpected Sources of Cybersecurity Funding for State and Local Governments, *Blumira*, April 3. Available at: https://www.blumira.com/blog/14-unexpected-sources-of-cybersecurity-funding-for-state-and-local-governments (Accessed: 26 November 2024).

6. Cisternelli, E. (2024) 7 cybersecurity frameworks to reduce cyber risk, *Bitsight*, 27 February. Available at: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (Accessed: 14 November 2024).

7. Cole, N. (2024) 23 Eye-Opening Cybersecurity Insurance Statistics, *Network Assured*, August 7. Available at: https://networkassured.com/security/cybersecurity-insurance-statistics/ (Accessed: 24 November 2024).

8. Culot, G., Nassimbeni, G., Pedrecca, M., Sartor, M. (2021) The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda, *The TQM Journal*, 33(7), pp. 76–105. Available at: https://doi.org/10.1108/TQM-09-2020-0202 (Accessed: 14 November 2024).

9. Etzioni, A. (2011) Cybersecurity in the private sector, *Issues in Science and Technology*, 28(1). Available at: https://issues.org/etzioni-2-cybersecurity-private-sector-businesses/ (Accessed: 25 November 2024).

10. Granato, A. and Polacek, A. (2019) The growth and challenges of cyber insurance, *Federal Reserve Bank of Chicago*, No. 426. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426 (Accessed: 22 November 2024).

11. Haleliuk, R. (2023) The government's role in shaping the future of cybersecurity, *Venture in Security*, June 29. Available at: https://ventureinsecurity.net/p/the-governments-role-in-shaping-the (Accessed: 28 November 2024).

12. ISC2. (2024) Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen, *ISC2*, 11 September. Available at: https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen (Accessed: 25 November 2024).

13. MacColl, J., Nurse, J. R. C., Sullivan, J. (2021) Cyber Insurance and the Cyber Security Challenge, *Royal United Services Institute for Defence and Security Studies*. Available at: https://static.rusi.org/247-op-cyber-insurance-fwv.pdf (Accessed: 22 November 2024).

14. Maharaj, R. (2024) Navigating Cybersecurity Frameworks: A Comparative Analysis of NIST CSF and ISO 27001, *LinkedIn*. (Accessed: 27 November 2024).

15. Munich Re. (2024) Cyber Insurance Risks and Trends 2024. Available at: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html#:~:text=Munich%20Re%20experts%20expect,at%20scale%20in%20all (Accessed: 27 November 2024).

16. National Institute of Standards and Technology. (2022) Risk management. *National Institute of Standards and Technology*. Available at: https://csrc.nist.gov/nist-cyber-history/risk-management/chapter (Accessed: 14 November 2024).

17. National Institute of Standards and Technology. (2024) The NIST Cybersecurity Framework (CSF) 2.0. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed: 14 November 2024).

18. National University. (2024) 101 Cybersecurity Statistics and Trends for 2024, *National University*. Available at: https://www.nu.edu/blog/cybersecurity-statistics/#:~:text=The%20cybersecurity%20sector%20is,estimated%20at%204.7%20million (Accessed: 6 November 2024).

19. Palatty, N. J. (2024) ISO 27001 vs NIST Standards: Differences and Requirement, *Astra*, 2 September. Available at: https://www.getastra.com/blog/compliance/nist/iso-27001-vs-nist/ (Accessed: 15 November 2024).

20. PrivacyEngine (2023) ISO 27001 vs NIST cybersecurity framework, *PrivacyEngine*, 10 November. Available at: https://www.privacyengine.io/blog/iso-27001-vs-nist-cybersecurity-framework/ (Accessed: 6 November 2024).

21. Sayegh, E. (2024) The evolving role of cybersecurity operations in a rapidly changing world, *Forbes*, June 11. Available at: https://www.forbes.com/sites/emilsayegh/2024/06/11/the-evolving-role-of-cybersecurity-operations-in-a-rapidly-changing-world/ (Accessed: 6 November 2024).

22. Slonopas, A. (2024) Cybersecurity trends: Looking over the horizon to the future, *American Public University*, April 16. Available at: https://www.apu.apus.edu/area-of-study/information-technology/resources/cybersecurity-trends/#:~:text=The%20rise%20of%20cloud%2Dbased,security%20during%20the%20last (Accessed: 6 November 2024).

23. Splunk (no date) The CISO Report, *Splunk*. Available at: https://www.splunk.com/en_us/campaigns/ciso-report.html(Accessed: 6 November 2024).

24. Swiss Re (2024) Reality check on the future of the cyber insurance market. Available at: https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html (Accessed: 24 November 2024).

25. The White House. (2024) International Counter Ransomware Initiative 2024 Joint Statement. Available at: https://www.whitehouse.gov/briefing-room/statements-

releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/#:~:text=with%20the%20private%20sector,counter%20the%20scourge%20of (Accessed: 26 November 2024).

26. Venters, W. and Whitley, E.A. (2012) A critical review of cloud computing: researching desires and reality, *Journal of Information Technology*, 27(3), pp. 179–197. doi: http://dx.doi.org/10.1057/jit.2012.17.

27. Vicente, V. (2023) NIST vs. ISO: What's the Difference?, *Auditboard*, 24 April. Available at: https://www.auditboard.com/blog/nist-vs-iso-whats-the-difference/ (Accessed: 15 November).

28. Watts. J. (2024) How the cyber insurance industry has shaped the ransomware landscape, *The Stack*, November 19. Available at: https://www.thestack.technology/how-the-cyber-insurance-industry-has-shaped-the-ransomware-landscape/(Accessed: 26 November 2024).

Chapter 3

Historical View on Antivirus Software, Firewall- and Network Security

Almin Dacic

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This chapter examines the historical development and commercialization of antivirus software and firewalls from the 1980s to 2000, highlighting their role in addressing emerging cybersecurity threats such as computer viruses and network intrusions. It explores the funding strategies, marketing approaches, and technical advancements that facilitated their evolution. The study highlights the contrast between the usability of antivirus solutions for individuals and the complex design of firewalls for enterprises, demonstrating how these technologies laid the foundation for modern cybersecurity practices.

1 Introduction

The period from the 1980s to 2000 marked a crucial era for cybersecurity, driven by the explosive growth of personal computing and the internet. As digital systems became an integral part of daily life for individuals and businesses, they introduced significant opportunities for communication, productivity, and commerce. However, this rapid technological adoption also brought new challenges, such as computer viruses and network-based attacks, which exposed vulnerabilities in these systems. These threats underscored the urgent need for robust tools to safeguard data and systems, leading to the development of antivirus software and firewalls, which became foundational components of cybersecurity during this period. (Szor, 2005).

The emergence of computer viruses in the 1980s, such as Elk Cloner and the Brain virus, was among the earliest signs of the risks posed by malicious software. Elk Cloner spread through floppy disks, causing minor disruptions to Apple II systems, while the Brain virus, more advanced in design, infected the boot sectors of floppy disks, operating hidden and compromising system functionality. These early threats served as wake-up calls, demonstrating the ease with which malicious code could propagate and the growing necessity for detection and removal tools. Companies like McAfee and Symantec stepped into this evolving market, creating antivirus solutions that addressed these risks and laid the groundwork for the cybersecurity industry. (IBM, 2023)

The 1990s brought further complexity with the widespread adoption of the internet, which connected systems globally but also exposed them to advanced threats. The Morris Worm of 1988, for example, exploited vulnerabilities in UNIX systems, causing widespread disruption and signaling the need for network-level defenses. This incident

caused the creation of firewalls, which were designed to control data flow, monitor network activity, and prevent unauthorized access. These tools became crucial for protecting the growing interconnected world of the internet age, especially for organizations handling sensitive information. (Spafford, 1989)

Regulatory frameworks also shaped the cybersecurity landscape during this period. The Computer Fraud and Abuse Act (CFAA) of 1986, for instance, classified unauthorized access to computer systems as a federal crime, establishing a legal foundation for digital security. This legislation encouraged organizations to invest in protective measures, driving the development of both antivirus software and firewalls (Congress.gov, 1986).

Beyond the technical challenges, companies faced funding and marketing obstacles in an developing cybersecurity industry. Venture capital enabled rapid growth for firms like McAfee (Guthrie, 2019), while freemium pricing allowed users to sample antivirus features before upgrading. Partnerships with hardware manufacturers expanded market reach, and fear-based marketing highlighted risks to drive adoption (Ayala, 2016). In contrast, firewalls, designed for enterprises, offered advanced solutions through collaborations with firms like Cisco and Check Point (Cheswick & Bellovin, 1994).

This chapter explores the development, commercialization, and lasting impact of antivirus software and firewalls during this transformative period. Drawing on interviews, company reports, press releases, white papers, and academic sources, it examines how these tools evolved to meet the challenges of their time. By analyzing their funding strategies, marketing approaches, and technical innovations, the chapter sheds light on the creative solutions and enduring lessons that continue to shape modern cybersecurity practices.

2 Identification of Cybersecurity Threats

In the late 20th century, personal computing and the rapid growth of the internet change how people and organizations worked. While these innovations brought incredible benefits, they also introduced some significant vulnerabilities, making cybersecurity a critical concern.

During the 1980s, the first notable computer viruses, such as Elk Cloner and the Brain virus, emerged, revealing significant vulnerabilities in personal computing systems. Elk Cloner was one of the earliest viruses that could replicate itself. spreading through floppy disks, and causing minor disruptions to Apple II systems. Although it was more of a minor issue than a serious threat, it demonstrated how quickly malicious code could spread. On the other hand, the Brain virus was more complex and worrisome. It infected the boot sectors of floppy disks, compromising computers without the user's knowledge and disrupting their functionality. These early viruses demonstrated how quickly malicious software could evolve and highlighted the urgent need for tools

to detect and remove such threats. This led to the creation of the first antivirus programs. (Szor, 2005)

Fred Cohen played a key role in the development of antivirus technology. In 1984, he introduced the term "computer virus" during his experiments with self-replicating software (Cohen, 1984). His research was groundbreaking, as it not only defined the concept of computer viruses but also provided the foundation for creating tools to detect and combat them. Cohen's work greatly advanced the understanding of how malicious software works, leading to the development of early prevention and detection methods. Filiol (2004) later emphasized the significance of Cohen's contributions in shaping the evolution of antivirus technology.

At the time, floppy disks were widely used to share and distribute software, but their popularity made them a common target for malware. This highlighted the importance of antivirus software capable of scanning and removing these threats. Although floppy disks were eventually replaced by CDs and USB drives, the challenges they presented in the 1980s and 1990s played a crucial role in the growth of the cybersecurity industry. (Szor, 2005)

The general adoption of the internet in the 1990s marked a transformative period for cybersecurity. This brought about more complex and large-scale threats, including the Morris Worm in 1988. This worm exploited vulnerabilities in UNIX systems and caused widespread disruption across early internet-connected systems. The incident served as a wake-up call, showcasing the damaging potential of network-based threats. In response, cybersecurity practices evolved, and the first Computer Emergency Response Team, CERT - was created to help organizations respond to such incidents. (Spafford, 1989)

The lessons from the Morris Worm illustrated the importance of network level defenses, leading to the development of firewalls. These tools became crucial for controlling access and keeping data safe in an increasingly connected world. Alongside antivirus software, firewalls became a foundation of cybersecurity, addressing the increasingly complex threats of the digital age. (Spafford, 1989)

3 Collection and market growth

Antivirus software was introduced as a commercial product in the 1980s, representing a key milestone in the evolution of the cybersecurity industry. Growing concerns about computer viruses, including their potential to cause data loss and financial harm, drove the need for reliable solutions. Companies like McAfee and Symantec responded by promoting antivirus tools as essential, often relying on fear-based marketing to emphasize the dangers of malware.

To reach a wider audience, antivirus companies adopted innovative marketing and distribution strategies:

1. Freemium model: Companies offered free basic antivirus software with limited features while charging for premium options like real-time scanning, advanced heuristics, and customer support. This strategy built trust and familiarity with the product, encouraging users to upgrade to paid versions over time. Gold, S. (2011).

2. Bundling with hardware: Antivirus software was pre-installed on computers through partnerships with manufacturers. This ensured users were protected as soon as they started using their devices, seamlessly integrating antivirus tools into the computing experience. (Kimball, Z. 2023)

These strategies were highly effective in driving adoption and making antivirus software a household name. However, they also had drawbacks:

- Fear-based marketing: While it successfully raised awareness, relying on fear to sell antivirus software may have created unnecessary anxiety among users. This approach often led users to focus on immediate threats rather than understanding long-term cybersecurity strategies. (Gamayun, 2023)
- Limited consumer choice: Bundling antivirus software with hardware made it convenient for users because the software was already installed when they bought a new computer. However, this approach often gave users no choice but to use the pre-installed antivirus, even if it wasn't the best fit for their needs. It also reduced competition, as people were less likely to explore or buy alternatives, leaving them stuck with what was provided.

So why did the freemium model work so well for antivirus software? The freemium model worked well for antivirus software because it allowed users to try the basic features for free, building trust and familiarity with the product. This approach reduced the initial cost barrier, making it accessible to a wide audience. Once users experienced the value of the software, many were motivated to upgrade to paid versions for advanced features like real-time scanning and better support. This strategy not only increased user adoption but also generated steady income for companies.

Despite these challenges, the commercialization of antivirus software played a key role in establishing the cybersecurity industry. By using creative marketing strategies and building on the growing awareness of digital threats, companies were able to drive widespread adoption and shape the future of cybersecurity tools.

3.1 Emergence and evolution of firewalls

In the 1990s, as the internet became a key part of communication and business, protecting networks became more important. Security moved from focusing on individual devices to safeguarding entire systems. Firewalls became an essential tool to defend

against network threats like unauthorized access, data spying (packet sniffing), and denial-of-service (DoS) attacks. Companies like Cisco, Check Point, and Juniper Networks led the way in developing firewalls with features such as intrusion detection systems (IDS) and virtual private networks (VPNs). These tools were especially important for businesses handling sensitive information, such as banks and healthcare organizations. (Cheswick, W. R. 2003). Firewalls and Internet Security)

Firewalls were mainly sold to large businesses, but their high price and complexity made them hard to access for smaller businesses and individual users. This created a gap in cybersecurity, where smaller groups could not get the protection, they needed. On top of that, advertising often focused on firewalls as tools only big companies needed, leaving out the smaller networks that also required security. (Cheswick, W. R. 2003). Firewalls and Internet Security)

3.2 Market drivers and challenges

In the late 1990s, several factors boosted cybersecurity growth. Events like the Y2K problem (Elgan, 2022) and regulations such as the Gramm-Leach-Bliley (Federal Trade Commission, 2002) The act led to investments in tools like firewalls. However, these efforts often focused on quick fixes to meet requirements instead of building stronger systems, leaving organizations open to new threats. Although, many organizations focused only on meeting the minimum legal requirements, leaving them unprepared for new and more advanced threats.

Globalization also played a central role in expanding the cybersecurity market. Companies like Symantec and McAfee extended their products to new regions, Aspray and Cortada (1999) addressing growing global demand. However, less wealthy areas often struggled to access effective security tools due to high costs and limited infrastructure. (Świątkowska, 2020)

In the 1990s, cybersecurity experienced significant advancements with the introduction of heuristic detection and stateful packet inspection. Heuristic detection enabled tools to identify unknown malware by analyzing behavior patterns, moving beyond reliance on known signatures. Stateful packet inspection enhanced firewalls by tracking the state of active connections, providing robust protection against unauthorized access and denial-of-service attacks. (Ingham and Forrest, 2002)

Despite these innovations, the cybersecurity industry often focused more on creating marketable features than on solving long-term security challenges. Companies prioritized adding eye-catching features to attract customers, sometimes overlooking important issues like scalability, integration, and long-term management. This approach led to products that were complex and full of features but lacked strong and sustainable security. As a result, organizations remained vulnerable to new and evolving threats. The pressure to quickly adopt new technologies often created fragmented defenses,

where tools did not work well together or were not properly maintained, failing to address the root causes of cyber risks. (Khan, 2023)

3.3 Critical reflections and implications

The development of firewalls and antivirus software used two different approaches to address cybersecurity needs. Antivirus software focused on being easy to use, making it a good option for individuals and small businesses. Firewalls, on the other hand, were created for large companies, offering advanced and customizable features. These two approaches helped shape today's cybersecurity by balancing simplicity with more complex protection.

The development of firewalls and antivirus software used two different approaches to address cybersecurity needs. Antivirus software focused on being easy to use, making it a good option for individuals and small businesses. This simplicity was especially valuable in combating threats like scareware, which (Ayala, 2016) describes as "a form of malicious software that uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software." Firewalls, on the other hand, were created for large companies, offering advanced and customizable features. These two approaches helped shape today's cybersecurity by balancing simplicity with more complex protection. (Ingham and Forrest, 2002)

Challenges still exist. Antivirus software often used scare tactics in marketing, which made people focus on reacting to threats instead of preventing them. Firewalls, designed mainly for big companies, were too expensive and complicated for smaller businesses to use. These issues show the need to improve cybersecurity by considering both technical systems and the people using them.

3.4 Lessons from historical cybersecurity failures

In the early days of cybersecurity, as said most tools focused on reacting to threats after they happened rather than preventing them. This approach left users vulnerable because attackers often stayed one step ahead. Over time, cybersecurity experts realized the importance of being proactive. Today, modern solutions prioritize identifying and stopping threats before they cause harm. Tools like threat intelligence systems, machine learning, and real-time monitoring have become key to detecting risks early. These improvements show how cybersecurity has evolved to handle more complex and fast-changing challenges. (Szor, P. 2005)

3.5 Ethical considerations in marketing

In the past, many antivirus companies used fear to sell their products. They scared people by highlighting the dangers of cyber threats, which often caused panic and reduced trust in their tools. Today, companies are taking a more ethical approach. Instead

of using fear, they focus on educating users about risks with clear and honest communication. This helps users feel informed and confident, building trust and stronger relationships with customers over time.

By addressing past mistakes and enhancing both technical methods and ethical practices, modern cybersecurity has become more effective and user-friendly. These improvements show the importance of combining advanced tools with clear, responsible communication to develop solutions that benefit everyone. (Cheswick, W. R. 2003)

4 Analysis

Antivirus software was designed to be simple and easy for individual users, while firewalls were built for businesses, offering advanced and flexible solutions for large networks. These differences show how each tool was created to meet specific security needs and target different types of users. Antivirus software focused on being simple and easy to use, aiming to help individuals and small businesses. These tools included user-friendly features like clear interfaces and automatic updates, so people did not need much technical knowledge. Marketing often highlighted immediate dangers, like losing data, to show why antivirus software was important for both personal and work use. However, this approach mainly dealt with specific threats, not bigger security weaknesses, leaving some gaps in protection. This difference between fixing small issues and addressing larger problems highlights a key challenge in improving cybersecurity tools.

Firewalls, on the other hand, were built to protect the complex networks of large organizations. Companies like Cisco, Check Point, and Juniper Networks created customizable tools with advanced features such as intrusion detection systems (IDS) and virtual private networks (VPNs). These tools required technical knowledge and were mainly targeted at industries like finance and healthcare, where strong network security was critical. However, focusing on large businesses often left smaller organizations and individual users behind, as the tools were too expensive and complicated, leading to unequal access to cybersecurity protection.

Trends in IT security shaped the adoption of antivirus software and firewalls. Laws like the Gramm-Leach-Bliley Act (Federal Trade Commission, 2002) and Sarbanes-Oxley Act pushed organizations to implement stricter cybersecurity measures, leading to increased use of these tools. However, many organizations aimed only to meet the basic legal requirements rather than investing in stronger, more adaptable systems. This approach left them exposed to new and evolving threats.

Antivirus software and firewalls evolved to keep up with new threats. Antivirus programs added features like real-time scanning and heuristic detection to spot unknown malware. Firewalls introduced scalable designs and stateful packet inspection to help

organizations monitor and secure their networks. These advancements laid the groundwork for modern cybersecurity, offering accessible tools for everyday users and powerful solutions for large organizations.

Despite their achievements, these tools revealed challenges in cybersecurity. Antivirus software's reliance on fear-based marketing promoted a reactive approach to security, while firewalls, designed mainly for large enterprises, left smaller organizations with limited access to protection. To close these gaps, a more inclusive and proactive approach is needed. One that addresses both technical issues and human vulnerabilities to create a stronger, more secure digital environment.

5 Funding and strategies

The growth of antivirus software and firewalls in the 1980s and 1990s relied on strategic funding from sources like venture capital and business partnerships. This funding helped companies create new technologies, expand their reach, and respond to evolving cybersecurity challenges.

5.1 Venture Capital: Driving innovation in antivirus software

Venture capital (VC) was essential for the early growth of antivirus companies such as McAfee, Symantec, and Dr. Solomon's Software. It helped close the funding gap for innovative but high-risk projects, especially during the phase when new technologies were being brought to market. VCs often targeted industries with rapid growth, offering both financial support and strategic advice to help these companies expand successfully (Zider, 1998).

These companies convinced investors by highlighting the growing risks of malware and the increasing need for digital protection. VC funding supported:

- Product Improvement: Companies used the funds to develop better detection methods, such as heuristic analysis, to find both known and unknown threats. (Szor, P. 2005)
- Global Reach: Funding allowed these companies to expand internationally, making antivirus tools available to more users and businesses.
- Marketing: With VC support, companies launched major advertising campaigns to raise awareness and position antivirus software as essential for online safety. A notable example is John McAfee's antivirus firm, which secured a better funding deal through the efforts of VC analyst Sonja Hoel Perkins. Her strategy enabled the company to retain partial ownership while receiving $10 million in first-round funding, facilitating McAfee's expansion and eventual IPO. (Guthrie, 2019)

5.2 Business partnerships: Supporting firewall development

Firewalls were primarily developed for large organizations like banks, hospitals, and government agencies. Companies like Cisco and Check Point partnered with these organizations to fund development. This funding was used for: (Cheswick, W. R. 2003). Firewalls and Internet Security)

- Custom solutions: Firewalls were designed to meet the specific needs of large organizations, such as scalability and system integration.
- Advanced features: Investments helped create tools like intrusion detection systems (IDS) and stateful packet inspection, essential for protecting networks.
- Training programs: Companies funded certifications and training, such as Cisco's programs, to ensure professionals could manage firewalls effectively.

5.3 How funding was used

Both antivirus and firewall companies used their financial resources strategically:

- Research and development: Antivirus companies improved detection technologies like real-time scanning, while firewall companies enhanced tools to analyze and secure network traffic.
- Standing out in the market: Funding enabled companies to add unique features, making their products more appealing and competitive.Almin Dacic Term-paper 2024 IMT4115

5.4 Challenges with funding

While funding was important for growth, it also led to some challenges:

- Focus on large clients: Firewalls were expensive and complex, making them hard for smaller businesses and individuals to afford or use.
- Fear-based advertising: Antivirus companies often used scare tactics in marketing, which encouraged users to react to threats rather than focus on long-term prevention.

6 Importence of cyber security

In the 1980s and 1990s, antivirus software and firewalls were essential for tackling new digital threats. Antivirus programs helped individuals and small businesses stay safe from malware, while firewalls protected large companies from network attacks. Together, they worked to create a safer online environment.

As technology becomes a central part of our lives, whether in businesses, personal devices, or government systems, the need to safeguard these systems has grown seriously. Without proper cybersecurity, the consequences can be severe, including financial losses, damage to reputations, and disruptions to critical services.

The internet's rise in the 1990s made digital systems even more interconnected and vulnerable. Attacks like ransomware, which locks users out of their data until a ransom is paid, and phishing, where people are tricked into revealing sensitive information, show how cyber threats target both technology and human behavior. These risks make cybersecurity necessary for individuals and organizations alike.

Cybersecurity is also crucial for protecting economies and society. Data breaches can lead to stolen intellectual property or loss of customer trust, which can harm businesses. On a larger scale, attacks on essential systems like hospitals, power grids, or transportation could cause widespread chaos. By ensuring systems are secure, cybersecurity helps maintain trust and stability in a digital world.

Additionally, strong cybersecurity enables organizations to embrace new technologies, such as cloud computing and artificial intelligence, while meeting legal and ethical standards. It also helps prepare for modern, advanced threats that require not just technical defenses but also policies and user education. (Świątkowska, 2020)

7 Conclusion

The period from the 1980s to 2000 was crucial in shaping modern cybersecurity, with the development of antivirus software and firewalls addressing emerging threats. Antivirus software provided a simple and effective way to protect individual users and small businesses from early computer viruses like Elk Cloner and the Brain virus. Companies like McAfee and Symantec introduced innovative strategies, such as free basic versions and pre-installed software on computers, which made antivirus solutions widely available and contributed to their success.

Firewalls, on the other hand, were developed to secure networks and protect against more advanced threats like the Morris Worm. They were essential for large organizations, such as banks and hospitals, where network security was critical. However, their high cost and complexity made them less accessible for smaller businesses, creating a gap in cybersecurity protection.

Both approaches, antivirus software for individual devices and firewalls for networks highlighted different needs in the digital landscape. Together, they established the foundation for modern cybersecurity practices by addressing a range of threats. However, challenges such as fear-based marketing and limited accessibility for smaller businesses show that early cybersecurity solutions were not perfect.

Comparing antivirus software and firewalls shows the importance of creating cybersecurity tools that are both simple to use and strong enough to handle different needs. By learning from these early examples, modern cybersecurity can aim to develop tools that work well for both individuals and organizations.

Looking back at these early strategies, we can see how they shaped the development of today's cybersecurity tools. They also remind us of the importance of balancing simplicity, accessibility, and advanced protection to meet the needs of all users. By learning from the past, we can create more inclusive and effective cybersecurity solutions for the future.

Looking Beyond 2000, the work done in the 1980s and 1990s laid a strong foundation for handling new challenges in the 2000s. The focus on antivirus software and firewalls helped prepare for more complex threats, like botnets (Checkpoint, 2024) that took control of many devices, ransomware that locked users out of their data, and the need to secure cloud systems as more businesses moved online. These early tools showed the importance of adapting to changing threats and helped shape modern cybersecurity solutions to handle an even wider range of risks.

8 References

1. Cohen, F., 1984. Computer Viruses: Theory and Experiments. Available at: https://www.cnsr.ictas.vt.edu/QEpaper/cohen.pdf [Accessed 1 Sep. 2024].
2. Zider, B., 1998. How venture capital works. Harvard Business Review. Available at: https://hbr.org/1998/11/how-venture-capital-works [Accessed 3 Sep. 2024].
3. Guthrie, J., 2019. The woman who saved John McAfee from an epically bad deal. Wired. Available at: https://www.wired.com/story/the-woman-who-saved-john-mcafees-biscuits/ [Accessed 5 Sep. 2024].
4. Filiol, E., 2004. Computer Viruses: From Theory to Applications. Available at: https://books.google.no [Accessed 7 Sep. 2024].
5. U.S. Congress, 1986. Computer Fraud and Abuse Act of 1986, H.R. 4718, 99th Congress. Available at: https://www.congress.gov/bill/99th-congress/house-bill/4718 [Accessed 9 Sep. 2024].
6. Aspray, W. and Cortada, J.W., 2015. Before it was a giant: The early history of Symantec, 1982–1999. IEEE Annals of the History of Computing. Available at: https://ieeexplore.ieee.org/document/7436658 [Accessed 5 Sep. 2024].
7. Gold, S., 2011. The future of the firewall. Network Security, (6), pp.10–12. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1353485811700150 [Accessed 6 Sep. 2024].
8. Malin, C.H., Gudaitis, T., Holt, T.J. and Kilger, M., 2017. Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communications. Elsevier. Available at: https://www.perlego.com/book/1830304/deception-in-the-digital-age-exploiting-and-defending-human-targets-through-computermediated-communications [Accessed 15 Sep. 2024].

9. Świątkowska, J., 2020. Tackling cybercrime to unleash developing countries' digital potential. Available at: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf [Accessed 18 Sep.2024].
10. Khan, A., 2023. Guarding the gates: The rise of network protection in the 1990s. Available at: https://smartermsp.com/guarding-the-gates-the-rise-of-network-protection-in-the-1990s [Accessed 18 Sep. 2024].
11. Elgan, M., 2022. Blast from the past: What the Y2K bug reveals about cybersecurity today. Security Intelligence. Available at: https://securityintelligence.com/articles/y2k-bug-cybersecurity-today/ [Accessed 18 Sep. 2024].
12. Federal Trade Commission, 2002. How to comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act. Available at: https://www.ftc.gov/business- guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act [Accessed 28 Sep. 2024].
13. Kimball, Z., 2023. Hardware-as-a-service (HaaS) bundles to drive sales and profitability. Available at: https://blog.hardfin.com/hardware-as-a-service-haas-bundles-to-drive-sales-and-profitability [Accessed 1 Oct. 2024].
14. Gamayun, 2023. The art of fearmongering: A critical look at security sales tactics. Available at: https://gamayun.uk/2023/12/27/the-art-of-fearmongering-a-critical-look-at-security-sales-tactics/ [Accessed 1 Oct. 2024].
15. Matt, B., 2018. Computer Security: Art and Science. Available at: O'Reilly Media. [Accessed 10 Oct. 2024].
16. Brown, M., 2020. Fear-based cybersecurity content marketing. Available at: https://www.ndash.com/blog/fear-based-cybersecurity-content-marketin [Accessed 4 Oct. 2024].
17. Lynn, M.S., 1989. The Computer Worm: Report from the Provost of Cornell University. Available at: https://simson.net/ref/1989/Cornell_Worm_Report_1989.pdf[Accessed 4 Oct. 2024].
18. Spafford, E.H., 1989. The Internet Worm Program: An Analysis. Available at: https://spaf.cerias.purdue.edu/tech-reps/823.pdf[Accessed 10 Oct. 2024].
19. Grimes, R.A., 2001. Malicious Mobile Code: Virus Protection for Windows. O'Reilly Media. [Accessed 15 Oct. 2024].
20. Seeley, D., 1989. A tour of the worm. Available at: https://www.cs.unc.edu/~jeffay/courses/nidsS05/attacks/seely-RTMworm-89.html [Accessed 1 Nov. 2024].
21. National Institute of Standards and Technology (NIST), n.d. NIST cybersecurity program history and timeline. Available at: https://csrc.nist.gov/nist-cyber-history[Accessed 1 Nov. 2024].
22. Szor, P., 2005. The Art of Computer Virus Research and Defense. Addison-Wesley. Available at: Amazon. [Accessed 2 Nov. 2024].
23. Ingham, K. and Forrest, S., 2002. A history and survey of network firewalls. Available at: https://www.cs.unm.edu/~forrest/publications/firewalls-05.pdf [Accessed 15 Nov. 2024].
24. Singer, P.W. and Friedman, A., 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. Akademika. [Accessed 15 Nov. 2024].
25. Cheswick, W.R. and Bellovin, S.M., 2003. Firewalls and Internet Security: Repelling the Wily Hacker. 2nd ed. Available at: https://cdn.preterhuman.net [Accessed 15 Dec. 2024].
26. BM. The History of Malware. IBM Think Blog. 2023. Available at: https://www.ibm.com/think/topics/malware-history [Accessed 1 Dec. 2024].
27. Checkpoint. (n.d.). What is a Botnet? 2024, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-botnet/ [Accessed 1 Dec. 2024].

Chapter 4

The Goals and Context of Business-Focused Cyber Security

Ebba Bakkerud Andersen

Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This chapter explores business-focused cyber security, emphasizing the integration of security measures that align with business goals, to enhance resilience and continuity. It discusses the importance of regulatory compliance, cyber security teams, and risk management. The chapter also highlights the role of high-performance teams and cyber security as a competitive advantage, advocating for proactive adaptation to evolving threats and regulations.

Keywords: Business-focused cyber security, goals and context, risk management, competitive advantage

1 Introduction

"There are only two kinds of companies in the world, those who have been breached and know it and those that have been breached and don't know it" (Schlein, 2024).

This quote underscores the critical importance of cyber security in businesses. Wherever valuable information exists, there is a risk of losing it. Therefore, implementing security measures is crucial to prevent such losses (Hasani et.al, 2023).

Cyber security measures are crucial for businesses to protect their information assets and ensure operational continuity. Effective cyber security measures help mitigate risks associated with digital attacks and incidents. Such measures are important for maintaining confidentiality, integrity and availability of information (CIA). These principles are the foundation of information security (Whitman and Mattord, 2021). While not directly profitable, cyber security measures are essential for risk management. They do not generate immediate value, rather they protect existing assets and profit by preventing digital attacks and minimizing potential losses, thus ensuring the organization's long-term stability. Therefore, businesses must implement these measures to strengthen their organization (Hasani et.al, 2023). This is the essence of business-focused cyber security, to implement security measures that align with, and even supplement the vision and goals of the business. The two should go hand in hand, not work against each other (Dalal et.al., 2022).

The trend business-focused cyber security has no universal definition. Nonetheless, this chapter will proceed based on the following definition of the term:

Business-focused cyber security involves implementing and managing security measures that align with and enhance the vision and goals of a business.

The ongoing development of digital devices and services, coupled with the increasing threat of cyber security attacks, forms the basis for international and national cyber security laws and regulations. DORA (Digital Operational Resilience Act) is an EU regulation that intents to strengthen digital operational resilience in the financial sector. The regulation comes into effect in 2025 and applies to all financial institutions within the EU/EEA area (Finanstilsynet, 2024). Furthermore, it is part of the EU's plan to put cyber security on the agenda. Meanwhile, in 2023, the Norwegian Parliament and Government developed a new digital security law. However, it has not yet come into effect, as the government is unaware of the regulations from DORA. In anticipation of this, many Norwegian businesses have put digital security measures on hold. In the digital age, businesses cannot afford to wait passively for cyber security regulations to initiate action. Cyberattacks can occur at any time and from any location, posing significant risks, especially when protective measures are lacking. Norwegian business leaders and board members should proactively address cyber security, rather than waiting for regulations. Many Norwegian companies are currently not prepared for such threats. The new EU regulations present an opportunity to enhance both security and profitability, despite potential burdens. The NIS2 directive, replacing NIS1, will impose stricter cyber security requirements across various sectors. These developments underscore the necessity for Norwegian, and non-Norwegian businesses to proactively adapt to these regulations to reduce potential risks (Bock, 2024).

2 Purpose, limitations and plan for the chapter

The purpose of this chapter is to elaborate on the trend of business-focused cyber security, explaining its goals and context. It will discuss potential use of business-focused cyber security as a strategic business approach. Additionally, the chapter will argue that legislation and directives shape the context of this trend. This chapter will not cover historical approaches to cyber security, as these are addressed in other chapters. However, it will discuss cyber security as an enabler, high-performance teams, competitive advantages, risk management, and challenges and solutions related to cyber security.

This is the basis of the following problem statement;

"What is business-focused cyber security, and why is it important?"

3 Defining Business-focused Cyber Security

What is business-focused cyber security? The term can be broken down into several components. “Business” refers to the activity of working, trading, selling, and buying goods or services with the goal of gaining profit or value. Thus, having a “business-focused” refers to directing attention towards business activities. When a business has a business-focused, it acts purposefully, ensuring that its actions align with its goals and interests 14 (Oxford English Dictionary, 2024).

The word “cyber” pertains to the use and activity of digital devices, typically connected to the internet, whereas “security” means protection, or keeping something safe. Security involves safeguarding assets from potential harm caused by others, whether their actions are intentional or not. Organizations must implement multiple layers of security to protect their personnel, operations, infrastructure, functions, communications, and information (Whitman and Mattord, 2021). Therefore, “cyber security” refers to measures implemented to protect an entity and its computer information from crimes or attacks carried out via the internet. Consequently, “business-focused cyber security” refers to a business aiming to create value and profit within the organizations, while implementing cyber security measures that align with its business goals (Dalal et.al., 2022).

The CIA triad is a fundamental concept in information security, illustrating three critical principles: Confidentiality, Integrity, and Availability. These principles ensure that information remains protected from unauthorized access, remains accurate and original, and is available to authorized users when needed (Whitman and Mattord, 2021, page 8). The importance of the CIA triad lies in its ability to address the essential aspects of information security that provide value to organizations. However, as threats evolve, ranging from accidental damage to intentional and unauthorized modifications and harm, the need for more complex and comprehensive models has grown. Maintaining the security of information through the CIA triad is crucial for preserving the trust, functionality, and resilience of any organization. Therefore, these three principals are important in business-focused cyber security (Whitman and Mattord, 2021).

4 Business Context and Integration

Business and industry are constantly operating in a society that is rapidly changing. Therefore, government and institutions must regulate the market. Norwegian and other international businesses are on the brink of an exciting era that will bring both demands and responsibility.

Firstly, there are international standards that provide frameworks for risk management, amongst them are the ISO standards and the NIST framework. Both focus on identifying and mitigating risks by following structured processes that involve documentation, reporting and complying to regulations (Ngalim, 2023). Moreover, ISO and

NIST also focus on aligning security measures with organizational objectives and ensuring that these measures support the overall goals of the organization (Whitman and Mattord, 2021). Hence, they are both great examples of business-focused cyber security. (Ngalim, 2023)

The EU's directive on security of network and information systems (NIS directive) is one of EU's responses to the increasing threats related to cyber security (Calder, 2018). In an environment such as the EU, many organizations operate across national borders. Therefore, the total number of threats and incidents compose a great threat to the hole continent of Europe. Overall, the goal of the NIS directive is to contribute to cyber resilience and create a community in EU where the member states can cooperate to increase this resilience. Hopefully, this will increase cyber security in European countries (Calder, 2018).

Moreover, Dora is a new legislation that highlights and sets requirements for risk management in financial market infrastructures in the EU. It emphasizes the importance of addressing and managing risks associated with outsourcing crucial functions, services, and ICT systems. The overall goal of DORA is to encourage businesses to adopt and institutionalize cyber security measures, systems, and functions. Additionally, it aims to foster a collaborative environment where businesses and countries can share knowledge across national borders (Duggan, 2024). On the one hand, the burden of DORA may involve investments, recruiting new staff, driving innovation, new work tasks, and creating new technologies. However, DORA is also an opportunity for European organizations to increase global financial stability by participating in a collaborative sector (Buttigieg and Zimmermann, 2024). Surely, this is only the beginning of legislation that demand better information security in Europe.

As a result of EU legislation, the Norwegian government has too developed a digital security law. Therefore, it will be important for Norwegian businesses to increase their focus on cyber security (justis- og beredskapsdepartementet, 2023). In total, these legislations and directives illustrate the context of the need for cyber security measures in businesses. If businesses want to continue their success, they must adapt to their environment.

5 Goals of Business-focused Cyber Security

Ultimately, the goal of business-focused cyber security is to enhance and support business resilience and continuity by protecting sensitive data and ensuring regulatory compliance (Blum, 2020).

This alignment facilitates that measures regarding information security do not hinder the business's strategic goals. Most businesses invest in risk management to some extent. Part of managing an organization is mitigating risks that can impact the operations

of a business. Implementing cyber security measures will protect against loss and attacks.

Moreover, businesses typically wish to maintain and improve operational efficiency. For instance, cyber security measures can help businesses by removing disruptions such as security incidents or system crashes etc. Furthermore, these measures may improve communication and collaboration across the organization. Safe and efficient data systems can help the organization by collecting information and making it available to more people. Documents and systems can be accessed by authorized personnel, making it easier to work separately whilst collaborating. This is helpful for businesses that aim to improve efficiency and knowledge among their personnel (Blum, 2020).

Companies must act responsibly and ensure that they comply with regulations and the CIA triad. This is important to ensure the daily operation of the organization, as well as maintain the trust that customers and authorities have in them (Blum, 2020). Therefore, organizations must implement cyber security measures that are forced by regulations and laws.

6 Cyber security as an enabler

T. Mosley (2024) argues that the alignment of cyber security initiatives with overarching business goals [...] is a fundamental necessity. In his article “Aligning Cyber security with Business Goals: A Roadmap for Executives”, he explains that businesses must internalize cyber security measures that support the business goal in order to protect themselves whilst cyber attackers are becoming more sophisticated, and harder to recognize (Mosley, 2024). When doing so, cyber security becomes an enabler.

Furthermore, Mosley (2024) claims that there are six factors that contribute to understanding the trend of business-focused cyber security. Firstly, the business must acknowledge cyber security as an enabler, and an internal part of the organization. Furthermore, the business must create a common language between different teams or departments, to facilitate communication and cooperation between different teams. Also, cyber security leaders must be included in the strategic decision-making process in the company, to make sure that the different teams have common goals that align with the overall goals of the company. Efficient distribution of the resources within the organization comes from prioritizing which assets do- and which assets do not make an impact on the goals of the organization. Moreover, Mosley claims that fostering a security focused culture is important. This can be done through education and training. Lastly, measuring success is a key to ensuring progress, therefore the company may establish a Key Performance Indicator that illustrates the alignments between the achievements of the cyber security team, and the goals of the organization (Mosley, 2024).

Furthermore, Wong (2024) supports cyber security as an enabler in his article "Cyber security as a Business Enabler: How to Justify Cyber security Spending to Business Leaders". The article illustrates how companies can utilize cyber security to

achieve their goals. Rather than viewing cyber security as an expense, businesses can think of it as a tool that will facilitate success. However, this requires an understanding of the endless number of risks, and how disaster can impact on the company. When a company has established an overview of the risks they face, they can start to make decitions regarding cyber security investments. This approach facilitates protection of the operations and data of the business, whilst supporting the business strategy of the companies (Wong, 2024).

7 High-performance Teams

Kosel, N., Schumm, J., and Kosel, P. (2024) explain how businesses can maintain strong cyber security teams that protect their digital assets whilst supporting the organizations overall success. To achieve this, they might take inspiration from a sports team. In a team, a chain is only as strong as its weakest link. Therefore, the team must perform as a unity. This is what is conveyed in the article "How can we build high-performance teams (HPTs) in cyber security and support their successful development through exceptional" by Kosel et.al (2024).

Firstly, a high-performance team must complete tasks efficiently and effectively. Team efficiency is crucial for maintaining cyber security, as this field may require quick and accurate responses to threats. Efficiency can save a company from significant losses as time is of the essence in the cyber security field (Kosel, 2024).

All teams must have a caption or a coach. Good leadership is vital for any business, especially in cyber security teams. Many hands make light work, and the leaders' task is to make sure that everyone is working towards the same goal. This can be challenging, as the team players sometimes have to work under pressure. Therefore, the purpose of the leader is to inspire and motivate the team players (Kosel, 2024).

Clear and measurable goals are important to any team. In a business context, this refers to the business' ability to set specific goals for the cyber security team to achieve. As the teams achieve their goals, they will be able to track their progress. By doing so, the team can become more motivated, and it will ensure that their work aligns with the business' overall goals (Kosel, 2024).

A team consists of several teammates. A supportive environment facilitates the motivation and well-being of each team player. In a cyber security team, such environments might create innovation and cooperation, as the employees might feel comfortable with sharing ideas and thoughts with each other (Kosel, 2024).

Lastly, a high-performance business-focused cyber security team must be given autonomy. The team members must also have a wide extent of autonomy in their work, as they are the first responders when an attack occurs. During an attack, the member

must be confident that it can act without the permission of a leader. Therefore, autonomy is important to a high-performance team member (Kosel, 2024).

The article concludes that high-performance teams are crucial in any business-focused cyber security team, because it ensures effective responses to threats and protection of assets, whilst leveraging solid leadership and collaborations (Kosel, 2024).

8 Competitive Advantage through Cyber Security

All businesses rely on their ability to deliver a good or service to a user. If this good or service has attributes that outperform other substitutes, the business has gained a competitive advantage in the market (Wen-Cheng et al., 2011). How can cyber security measures create competitive advantages for businesses?

Firstly, many digital businesses can benefit from implementing cyber security measures. Strengthening their systems can build trust between the business and their users, and the users may achieve better safety in their personal information. If that same level of safety is not provided by competing firms, it will be a competitive advantage to the business in question (Mmango et al., 2024). This will also help the business by differentiating it from others, which can attract new customers. Moreover, following international standards and other regulations will give the business the benefit of avoiding legal issues. Operational efficiency may improve, as firms can switch analog and slow procedures and systems with modern, digital systems. For instance, collecting all procedures in one data cloud may help the user to more easily find and access the information. Furthermore, focusing on cyber security may also foster innovation. Different standards and regulations will point out problematic operations within the business, which again will push the business to find new and modern solutions. Creating and leading high-performance cyber security teams may also foster learning, innovation, and a healthy work environment (Kosel, 2024). Overall, implementing and maintaining a focus on cyber security measures may influence the reputation of the organization positively. When attacks occur, the businesses with the best cyber security defense will come out ahead (Mmango et al., 2024). These businesses will signal that even if attacks happen, they will keep their organization and customers safe. Ultimately, implementing cyber security measures can generate a positive effect, strengthening businesses' competitiveness (Hasani et al., 2023).

9 Risk management

If businesses wish to understand cyber security as a strategic enabler that supports overall business goals, they must also understand and value effective risk management. As a crucial approach, it helps businesses navigate the complex environment of cyber threats, such as phishing, malware functions, and hackers (Whitman, et.al., 2021).

Risk management in cyber security refers to the act of identifying, assessing and mitigating risks. The goal of cyber security is to protect the organization's ability to perform its mission, as well as to safeguard its assets. In fact, this process is essential to the strategy of the organization, and it is closely integrated into the Systems Development Life Cycle (SDLC), a methodology that facilitates the implementation of information systems (Whitman, et.al., 2021).

According to Whitman and Mattord (2021), there are four key components of risk management. The first is risk identification, which involves recognizing harmful threats. Threats, like us humans, come in all shapes and sizes, some are natural disasters whilst others appear very sophisticated, or hard to recognize. However, the ability to recognize a threat early on will allow the organization to take time to prepare and implement controls. The process of evaluating the threat and finding appropriate controls is called risk assessment. During this process, the organizations must create an overview of the likelihood of the actual risk and the potential damage or harm it poses. This can be done using NIST Risk Management Framework. Moreover, risk mitigation refers to the decision-making process regarding the addressing of the threats. Sometimes, organizations can implement technical controls, such as firewalls, other times they implement managerial controls, such as policies. Regardless, the goal is to mitigate the risk, not entirely, but to an acceptable level. Costs, trust, reputation, and other factors will influence this decision. Finally, the organization must facilitate continuous monitoring of risks and threats. Risk management is an ongoing process, an attack is always on the way. Continuous monitoring emphasizes the importance of maintaining effective security measures, so that future risks can be identified quickly. Risk management is not a linear, but a circular process (Whitman, et.al., 2021).

For cyber security to become an enabler, security measures must align with the organization's business objectives. This involves integrating security practices, ensuring that all employees understand their responsibilities regarding the security of the company. Training is essential to foster a security culture (Whitman, et.al., 2021).

This proactive approach should create resilience in a world full of cyber threats.

10 Challenges and Solutions

On the contrary, implementing business-focused cyber security, which aligns cyber security measures with overall business goals, can present several challenges. Whitman and Mattord (2021) present several arguments that can be related to the challenges and solutions of implementing a successful business-focused cyber security strategy.

The authors value the balance between security and usability. Cyber security measures must create security without wearing the users down. Employees must manage the use of cyber security tools, however, they must not lack quality, as this will pose a risk.

Moreover, the book states that the threat landscape is highly dynamic. Threats vary from malware to ransomware, worms, trojan horses, viruses, and so on. To keep up with these changes is hard, and it requires continuous monitoring. Another argument is that ensuring that cyber security measures support and do not disrupt business processes can be challenging. Employees and leaders must be aware that implementing cyber security measures can cause disruptions at their workplace. This can include resource allocations, as cyber security measures require significant resources in technology, personnel, awareness, and training. Such allocations often influence the other areas of the organization, leaving them less. Lastly, organizations must ensure compliance with various regulations and standards, such as ISO, DORA, or national laws. Naturally, this too can cause disruptions and a need for allocation of resources within the organization (Whitman et.al., 2021).

However, Whitman and Mattord (2021) present several factors that can contribute to successful implementation of cyber security measures that are business-focused. First of all, there are several risk management frameworks, such as the NIST Framework (RMF). Frameworks like this provide a comprehensive approach to managing cyber security risks. Continuous monitoring helps the organization mitigate risks, and therefore protect them. This also ensures that the organization is constantly adapting to its environment. Employee training and awareness help maintain policies and procedures, as well as helping reduce the risk of human error. Having a proactive approach may also help the organizations in following directives such as ISO, which will influence their reputation and ensure that they are ahead of future threats. Incident Response Planning is also important to any organization that wants to recover from potential attacks. Such plans will prepare the organization for cyber incidents; therefore, it makes them more resilient (Whitman et.al., 2021).

Technology and innovation are part of cyber security. As threats evolve, so do regulations and legislation, as well as technology. Innovation can be an enabler to organizations, just like the computer or internet was once. Implementing a business-focused cyber security strategy can help the organization find new technology, measures and controls, whilst following regulations and international standards. However, implementing a business-focused cyber security involves addressing various challenges. By adopting good practices, organizations can enhance their cyber security posture (Whitman et.al., 2021).

11 Conclusion

This chapter intends to provide an introduction to the trend business-focused cyber security, which emphasizes the importance of integrating security measures with the overall goals and strategies of an organization. First, the chapter introduces general cyber threats and modern legislations, regulations and international standards. These form the

context of the trend. The text discusses complex topics such as risk management and cyber security measures in a relatively superficial manner. However, it becomes clear through literature that cyber security is not just about protecting information, but also about ensuring business continuity and resilience in a constantly developing society.

The importance of this text lies in its attempt to highlight how modern businesses must adapt to an increasingly complex threat landscape. Cyber security is not only a technical challenge, but a strategic necessity that requires leadership engagement and integration across all parts of the organization. By adhering to international standards and directives such as ISO, NIST, and EU regulations like DORA and NIS2, this chapter argues that businesses can not only protect themselves from threats but also achieve competitive advantages and improved operational efficiency. However, getting ahead of these legislations rather than waiting for them to come into force, is what creates the biggest competitive advantage in the field of business-focused cyber security.

Moreover, the chapter explores how the trend business-focused cyber security involves an approach that includes risk management, compliance with laws and regulations, and continuous monitoring. The text has explored articles that provide insights into how businesses can build high-performing security teams, foster a security culture, and use cyber security as an enabler for business success. In total, the chapter tends to underscore the importance of being proactive and prepared, rather than waiting for regulations to force action.

12 References

1. Blum, D. J. 2020. Rational Cyber security For Business : The Security Leaders' Guide To Business Alignment. Berkeley, CA: Springer Nature.
2. Bock, S. H. 2024. Mens Vi Venter På Digitalsikkerhetsloven. Og Forskriften. Og Dora. Available at: Https://Www.Digi.No/Artikler/Debatt-mens-vi-venter-pa-digitalsikkerhetsloven-og-forskriften-og-dora/551836 [Accessed 04.10.2024].
3. Buttigieg, C. P. & Zimmermann, B. B. 2024. The Digital Operational Resilience Act: Challenges And Some Reflections On The Adequacy Of Europe's Architecture For Financial Supervision. *Era-forum,* 25**,** 11-28.
4. Calder, A. 2018. A Concise Introduction To The NIS Directive : A Pocket Guide For Digital Service Providers. 1st Ed. Ely, England: IT Governance Publishing.
5. Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J., & Brummel, B.J. (2022). Organizational Science And Cyber security: Abundant Opportunities For Research At The Interface. Journal Of Business And Psychology, 37, Pp. 1-29. Available At: Https://Link.Springer.Com/Article/10.1007/S10869-021-09732-9 [Accessed 2 Dec. 2024].
6. Duggan, D. 2024. The Impact Of The Digital Operational Resilience Act On Financial Market Infrastructures In Europe. *Journal Of Securities Operations & Custody,* 16**,** 344-350.

7. Finanstilsynet. 2024. *Forordning Om Digital Operasjonell Motstandsdyktighet I Finanssektoren (DORA)* [Online]. Finanstilsynet.No: Finanstilsynet. Available at: Https://Www.Finanstilsynet.No/Tema/Forordning-om-digital-operasjonell-motstandsdyktighet-i-finanssektoren-dora/ [Accessed 04.11.2024 2024].
8. Hasani, T., O'reilly, N., Dehghantanha, A., Rezania, D. & Levallet, N. 2023. Evaluating The Adoption Of Cyber security And Its Influence On Organizational Performance. *SN Bus Econ,* 3**,** 97-97.
9. Justis- og beredskapsdepartementet (2023) *Lov om digital sikkerhet (digitalsikkerhetsloven)*. Available at: https://lovdata.no/dokument/NL/lov/2023-12-20-108 (Accessed: 12 December 2024
10. Kosel, N., Schumm, J., & Kosel, P. (2024) 'How Can We Build High-performance Teams (Hpts) In Cyber Security And Support Their Successful Development Through Exceptional Leadership?', Cyberunity. Available At: Https://Cyberunity.Io/En/How-can-we-build-high-performance-teams-hpts-in-cyber-security-and-support-their-successful-development-through-exceptional-leadership/ (Accessed: 5 December 2024).
11. Mmango, N., Gundu, T., Gerber, A. & Gerber, A. 2024. Cyber security As A Competitive Advantage For Entrepreneurs. Switzerland: Switzerland: Springer.
12. Mosley, T. (2024). Aligning Cyber security with Business Goals: A Roadmap for Executives. Available at: https://www.securit360.com/blog/aligning-cyber security-with-business-goals-a-roadmap-for-executives/ (Accessed: 5 December 2024).
13. Ngalim, B. 2023. Integrating NIST And ISO Cyber security Audit And Risk Assessment Frameworks Into Cameroonian Law. *Journal Of Cyber security Education, Research & Practice,* 2024.
14. Oxford English Dictionary. (n.d.). Business. In Oxford English Dictionary. Retrieved December 12, 2024, from https://www.oed.com/dictionary/business_n?tl=true
15. Oxford English Dictionary. (n.d.). Business. In Oxford English Dictionary. Retrieved December 12, 2024, from focus, v. meanings, etymology and more | Oxford English Dictionary
16. Schlein, T. (N.D.). Venture Capitalist Ted Schlein On The Future Of Cyber security. Kleiner Perkins. Available At: Https://Www.Kleinerperkins.Com/Perspectives/Venture-capitalist-ted-schlein-on-the-future-of-cyber security/ [Accessed 2 Dec. 2024].
17. Wen-cheng, W., Chien-hung, L. & Ying-chien, C. 2011. Types Of Competitive Advantage And Analysis. *International Journal Of Business And Management,* 6.
18. Whitman, M. E. & Mattord, H. J. 2021. *Principles Of Information Security,* Boston, Massachusetts, Cengage.
19. Wong, P. (2024) 'Cyber security as a Business Enabler: How to Justify Cyber security Spending to Business Leaders', Enterprise Security Magazine. Available at: https://cybersecurity.enterprisesecuritymag.com/cxoinsight/cyber security-as-a-business-enabler-how-to-justify-cyber security-spending-to-business-leaders-nid-3854-cid-21.html (Accessed: 5 December 2024).

Chapter 5

Business-Centric Cyber Security as a Driver of Value Creation

Johan Gimse Valseth (10059)

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. We have established the term business-centric cyber security to provide insight on the approaches business-focused and -centric, how they differ and why they can drive value, with the main emphasis on business-centric. This is done through a qualitative approach with literature review and varied sources. We found that business-centric cyber security can drive value creation through facilitating agile business processes and security innovation, which in today's landscape is important to thrive. Thus, facilitating ever-changing intangible processes, ROI is hard to calculate.

Keywords: Business-centric, business-focused, cyber security.

1 Introduction

As we explored in the previous chapter regarding business-focused cyber security, there are several approaches on how to obtain and maintain robust and expedient cyber security for a given business. To introduce this less thoroughly, this can include both general goals to protect the business from encountering problems, or more, call it ambitious thoughts, on how to integrate cyber security measures in a way that can add value rather than just protecting for the lowest possible direct cost. Cyber security can, when rightly applied, fuel a thorough understanding of the business, including customers and the threats to the products, creating and improving a competitive advantage (Broquist, Kratzert and Mosquera, 2021; Kosutic and Pigni, 2022).

Now that we have presented two, somewhat flimsy views on cyber security, the value increase could potentially be made through gaining competitive advantages such as improving profitability, including cost savings as well as top line growth, but also other thinkable positive outcomes as promoting innovation, knowledge and competence development or strengthening value proposition(s) to customers and so on. Holley (2024) states that the cyber security imperative can be turned into "a powerful driver of business value and growth". Another aspect of this is how investments and resource allocation can be sold in either to convince or inform employees or the board of directors of the importance of simply taking on the matter.

To be perfectly inaccurate, there are numerous desired approaches, effects and outcomes that the convenient cyber security strategy potentially could lead to. With that said, we find it appropriate to investigate what business-centric cyber security means,

how it differentiates from business-focused cyber security and how it can contribute to the business' competitiveness by striving to increase value creation through the cyber security approach which, judged by the name in any case, puts the business at the center of the solution. This chapter will strive to gain more insight into which cyber security investments that yields the most expedient results for a business, and how these investments could be sold in and communicated both to the board of directors and employees within the business.

Firstly, the chapter will figure out and elaborate on the background of the term "Business-Centric Cyber Security", attempting to establish and define it through gathering information from several sources. As it is hard to find an established definition of the term, this includes both academic publications as well as posts from social media and blog platforms from established firms and industry experts. Thus, this involves the necessity of the author reasoning oneself to establish a plausible and credible definition to build an understanding of, and contextualize the subject for further exploration.

Secondly, we will provide an extensive literature review, elaborating on the meaning of value creation, shedding light on cyber resilience, KPI's and accounting of investments, including insight on the matter of finances regarding sell-in of security.

The literature review will as an extension of the latter chapter, look upon aligning cyber security to the business, for better understanding the differences between the approaches. This includes viewing what value contribution an Information Security Management System (ISMS), certifications and standards can have to the business.

To wrap up the literature review, we will try to understand how a holistic approach to cyber security can drive value creation. This through strategic team building and leadership, cross-functional functionalities and information sharing, security culture and engagement as engrained in every process.

The chapter will then provide a methodology review before discussing the term, approaches and their value contributions, and eventually concluding findings and recommendations for future research.

2 Background and establishing the term

In the past, companies defined themselves through their product offering, which mostly consisted of tangibles (Lustenberger, 2015). The product offering has been a matter of radical change in the last decades, where the share of intangibles has increased, changing the business models (Lustenberger, 2015). The business model is a description of how the value is created through architecture or design, delivery and the employed mechanisms (Teece, 2010). For today's businesses, they can operate in both the physical and digital domain, offering intangibles as products or dealing with them

as systems in production or in the office. Therefore, Lustenberger (2015) both states that the companies producing hardware have been hardware-centric, and further raises the question of whether organizational structures have adapted, considering the changes that manufacturers have gone through. We will come back to this, which could prove to be relevant regarding security.

Today, the most valuable assets are digitized, and information systems are critical for building assets based on knowledge and competitiveness (Kosutic and Pigni, 2022). When digitalizing, using components in the digital domain or even having them as an intangible product, the business must take the new environment into consideration. This means that the business operates also in the cyber domain, where security can be an element as in manufacturing. The definition of cyber security, as originally interpreted, is "The ability to protect or defend the use of cyberspace from cyber attacks" (NIST, n.d.). As we understand from the definition, the idea of capturing or developing value from security strategies and measures within the cyber domain has not necessarily been a matter of logical course. On the contrary, cyber security has been perceived as a necessary evil, a financial burden taking care of defensive measures (Carson, 2023). To exemplify, we find it reasonable to assume that the board of directors of an LLC has a strong focus on delivering shareholder returns, as it is one of their responsibilities as members of the board. A report that was published by the insurance company AIG presented results from a study conducted in UK, where "52% of companies said they either rarely or never discussed information security in board meetings" (AIG, n.d., as cited in Ajmani and Kumar, 2017, p. 11). This can tell us that information is not considered as a source of either a potential loss of value or fueling value creation among many members of the board of directors, at least at their top-of-mind.

With that, we understand that cyber security logically has been sold to boards and managements with potential arguments like sufficient protection in the cyber domain for the lowest possible price – because the purpose is only protection, and the protection costs either money, other resources or both. More concrete examples of sell-in arguments could be protection against data breaches, viruses and attacks in various forms (Agrafiotis *et al.*, 2018).

As the world progresses, there are natural developments when it comes to wanting to maximize outcomes of input factors as mentioned. Thus, cyber security is, in line with other activities, subject to attempts of improvement and optimalization. As a result of that, there are several approaches to cyber security, whereas there are variations on how profound or concrete they are, or whether they are of such nature that have a sole or more holistic purpose proposal.

With that said, we can talk about purposeful centricity, orientation and positioning of cyber security. The business-centric cyber security term consists, in contrast to the already mentioned cyber security, of an extra part: the business-centric addition to the term. We therefore must establish the meaning of the whole new term.

According to Cambridge Dictionary, the suffix -centric can mean having a "thing as your most important interest" (Cambridge University Press & Assessment, 2024a). Also, Lustenberger (2015) emphasized the focus on product research and manufacturing as a product-centric approach, while underscoring that *business-centric* structures think in terms of business processes and models, although in an organizational context. Nevertheless, we therefore find it reasonable to assume that the term "Business-centric cyber security" positions the business in the center, perhaps in an interpretation where it is reasonable to view the core business as the most important component to maximize the performance of. We therefore make the reservation that the meaning behind business is the core activities the business has, and therefore are the subject to whom it is attempted to be taken care of, for unleashing inherent potential and further releasing and fueling value creation. As we already have noted, today's businesses are different from before, and the business model is emphasized when delivering an intangible product to the customers, facilitating for an ever-changing business model to create value (Teece, 2010; Lustenberger, 2015). Business models can be agile and rapidly changing, therefore making cyber security dependent on this, rather than the cyber security framing or limiting the opportunities the business model encounters.

As explained above, this approach can contrast with what we would call the traditional cyber security, that often focuses on the technology and system tools only (Adams and Makramalla, 2015, as cited in Grobler, Gaire and Nepal, 2021). Furthermore, under the assumption that the business, as of business model(s) and processes is the most important component, we find it reasonable to claim that the *business-centric cyber security* must be defined as an approach to cyber security that searches to firstly maximize business performance through integration of cyber security within the core activities and implement measures within the business, viewing cyber security as an enabler. This in comparison to the previous chapter about *business-focused cyber security*, where the strategy and measures in business-centric cyber security will not only strive to be aligned to the business' goals to promote competitiveness, but rather strive to be tailored to capture and add further value through using cyber security for releasing potential. How this can be done will be the subject of further exploration and discussion in the latter parts of this chapter.

3 Literature review

3.1 What is value creation?

Value can be defined as the amount of money that can be received for, or the importance of, something (Cambridge University Press & Assessment, 2024b). *Value creation* can be defined as "the processes aimed at increasing value generation" (Chesbrough, Lettl and Ritter, 2018; Dyer, Singh and Hesterly, 2018; Visnjic, Neely and Jovanovic, 2018, as cited in Sjödin *et al.*, 2020). Value generation can therefore be defined as the process of producing value, with the value creation as the process of increasing, improving, this value generation.

3.2 KPI's and accounting

To have the value generation processes going, the business probably will need to form resilience. This is, as elaborated on earlier, the traditional view on cyber security – prevention against breaches, interruptions, losses. However, there can be found value in prevention.

Return on investment (ROI) is a metric to measure what the organization get out of an investment made for risk mitigation, expressing the reduction in risk as a benefit, subtracting the total cost of mitigation actions then divided on cost – ROI then only good if it ends up with a positive value (Alsaleh, Al-Shaer and Husari, 2017).

A twist on ROI, another way of measuring the usefulness of security measures, is through the KPI "Return On Damages Not Incurred" (RODNI), which shows the board the resilience of the company through exemplifying potential damage amount minus investment amount (simplified) (Peter Kosel, 14. November 2024, industry contact guidance meeting).

A business striving to accomplish an expedient return that stakeholders can be satisfied with can require working thoroughly with calculations. A tool to continuous management of investments, viewing them as fixed or intangible assets, is by activating costs incurred to acquire assets according to the Norwegian Accounting Act § 6-2 when the requirements are met, requirements such as identifiability, control and positive net present value (Regnskapsloven, 1998; Norsk Regnskapsstiftelse, 2022). However, these requirements can often not be satisfied, and then the ROI and RODNI could come in handy. The general rule is that an intangible asset that generates positive cashflow and that is owned and controlled by an LLC should be activated as an asset in the company's balance sheet (Norsk Regnskapsstiftelse, 2022). For example, an identifiable knowledge asset that is in the LLC's possession that succeeds in providing demonstrable positive ROI, for example as proven data systems as a permanent structural knowledge capital, could and should be activated (Westeren, 2013; Norsk Regnskapsstiftelse, 2022). With that said, it can be a complex task to determine and appraise the value of such knowledge capital – systems that facilitate for value through prevention can be hard to evaluate, especially regarding identifying the correct net present value associated with the possession of it.

3.3 Business-aligned cyber security as a value generator

We have now mentioned that investments in cyber security can provide business resilience. Furthermore, from establishing the business-centric cyber security term, we have also opened for a possibility for businesses to profit from the introduction of business-centric principles in the cyber security strategy and operational measures, as well as integration of this mindset in the daily activities.

While the business-centric approach has the intention of adding further value to the business, it must be noted that also the business-focused approach, as earlier elaborated on in the latter chapter, intends to add value to the business. We must say the we find it appropriate to assume that every approach to cyber security intends to maximize the value creation ability of the firm in total, but we observe that the mindset and ambitions for both the approach and output varies – from for example the intention of having the lowest possible direct costs associated with cyber security incurred, to viewing cyber security as a resource to fuel value creation.

When it comes to cyber security as a contributor to enhancing value creation, one could seek to align the cyber security measures to the business in an expedient manner, for example through implementing an ISMS with specific goals. To control the ISMS for quality, it can both be worked on to fulfill the expectations of known standards and to be taken to review and further get assessed to decide if it could get acknowledged with certifications like the ISO 27000 series (Whitman and Mattord, 2019). Certifications like the ISO 27 000 series are a common type of investment in cyber security (Malliouris and Simpson, 2019). The ISO 27001 can be a flexible and adaptable standard for different businesses regarding implementing and establishing, operating and monitoring an ISMS, facilitating for sustainable information security (Kamil, Lund and Islam, 2023). An internal assessment process, prior to a formal certification process, can even add value by being subject to reviewing and assessing what is an expedient security program for the business (Whitman and Mattord, 2019).

Exercises regarding quantification of effects on organizational resilience, security breach impact and breach likelihood are difficult to execute (Verendel, 2009; Thomas *et al.*, 2013, as cited in Malliouris and Simpson, 2019). With that said, certifications and standards like the ISO 27001 and TISAX can add value to the business by both ensuring an efficient ISMS that takes care of mitigation measures on confidentiality, integrity, availability and technicality as well as building industry-specific customer recognition and trustworthiness (DNV, n.d.a; DNV n.d.b).

Another certification is the Cyber Essentials (Plus). While ISO 27001 has 114 potential controls, although the business only needs to pass those who are relevant, the Cyber Essentials framework emphasizes five security controls that include reducing impact of threats such as malware, network attacks, password-guessing, phishing and ransomware (IT Governance, 2022; IT Governance, n.d.). In contrast to ISO 27001, the Cyber Essentials plus scheme focuses on specific, technical requirements that yield high ROI, a focus which are to be found and visualized in form of higher returns in the stock market (Malliouris and Simpson, 2019; IT Governance, 2024). While ISO 27001 has a risk-based approach, making it pragmatic and flexible, the Cyber Essentials are more specific and cost-effective (IT Governance, 2024). Time is what builds trust, but certifications and standards can help convincing the market about the cyber security posture of the company, with the Cyber Essentials being more suitable for smaller organizations as it associated with less complexity despite the flexibility of ISO 27001 (Broquist, Kratzert and Mosquera, 2021; IT Governance, 2024).

3.4 Building momentum with Business-Centric Cyber Security - creating value through a holistic approach

Although acknowledgements and accomplishments as certifications and evidence of fulfilling standards can add value to the business, it may not incorporate the principles of business-centric cyber security. Broquist, Kratzert and Mosquera (2021) for example, states that everything that impacts the product impacts its cyber security characteristics, and that the cyber security therefore "must be engrained in every process with checks and balances to ensure that security is being managed every step of the way".

As Lustenberger (2015) stated, adoption of the internet facilitated transformation from hardware-centric production to business models with intangible products, demanding an ability of rapid adoption and innovation of new, agile products. Lustenberger (2015) further emphasized the importance of cross-functional, interdisciplinary units in a horizontal organization rather than vertical silos, working business-centric in form of business processes and models, making decisions based on business value.

This is where the term High-Performance Teams (HPT) comes in. We have gone through organizational facilitation for value creation, where Lustenberger (2015) stated that an organizational structure that is continually adapted and expedient for the nature of the company, can support flows and business models in positive ways. Companies can thrive in a world that is becoming more interconnected and complex, but this requires embedding security in every corner of the business in a holistic, proactive manner and viewing it as a continuous journey with a culture aware of security across the organization (Holley, 2024). This does not only require an organizational structure that facilitates for more information exchange beyond neighboring silos or pillars as a sequential way of manufacturing a product, but also horizontal, cross-functional units with agile qualities, open communication and a culture of trust (Lustenberger, 2015; Kosel, Schumm and Kosel, 2024).

Both Holley (2024) and Kosel, Schumm and Kosel (2024) emphasize fostering a security-aware culture. As approximately 80% of total vulnerabilities that is exploited by attackers is of human character (Adams and Makramalla, 2015, as cited in Grobler, Gaire and Nepal, 2021), whereas phishing alone in 2019 accounted for 52% of breaches (Porsche Consulting, 2021), the user behavior and security awareness are essential components of an expedient cyber culture. In addition to this, companies must both facilitate for a psychologically healthy and expedient work environment for the user to experience autonomy, ensuring security to triumph convenience and strive to let their motivation thrive through leadership of HPT's, this including building psychological safety (Grobler, Gaire and Nepal, 2021; Kosel, Schumm and Kosel, 2024). Ensuring psychological safety and constructive communication, facilitating for making mistakes and learning from them, will lead to more innovative teams, driving security innovation, competitiveness through security features included in development (Kosutic and Pigni, 2022; Kosel, Schumm and Kosel, 2024). Incorporating secu-

rity-related values and norms across the organization helps promote security practices, and once dynamic cybersecurity capabilities is embedded in the daily operations, the cyber security can be leveraged strategically (Kosutic and Pigni, 2022; Zachar, 2022).

4 Research approach and methodology

This study targets to establish the term business-centric cyber security, nuance the differences between business-centric and the business-focused approach to cyber security, with their objectives and further clarify their respective value-generating capabilities. Thus, using a qualitative approach with written sources through a literature review, this study aims to differentiate, compare and elaborate on key capabilities of the two approaches. This is done through extensive searches on scientific online libraries with keywords as well as obtaining relevant sources from industry experts and blog- and social media posts written by experts. As the term is not thoroughly explored, it was found necessary to include sources of less academic character to give flavor to the terms and interpretations of the literature. The relevant sources are then compared and applied.

To have a high degree of credibility, the research must ensure validity and reliability (Leedy and Ormrod, 2021). Unfortunately, the literature selection, interpretation and discussion does stand at risk for subjectivity and biases from the researcher, as the researcher must engage. To ensure validity, the approach must match what the research aims at achieving, in nature of being context-dependent (Leedy and Ormrod, 2021). Further, regarding reliability, the research with findings must be applicable and contribute to the field by getting the same results as another researcher would achieve (Leedy and Ormrod, 2021).

5 Discussion

In the background section, we established the term “Business Centric Cyber Security” to partly embrace the business as the component of the most important interest. However, one could argue that the “business” is the unity that all the cyber security approaches strive to maximize the performance of, and to facilitate for. With that in mind, we still found that the “business” part of the term should be interpreted as focusing on the business processes, the intangible processes directly aimed at generating value, processes that nowadays often must be agile and ready for thriving in rapid surroundings and changes. With that, the processes can be driven by knowledge, be either made of or handled by humans, probably raising demand for security measures among employees and cross-functional teams.

As for value creation, we found that it means producing something worthy of cash or worth of importance. The value creation could appear in several forms, including providing pure resilience through securing operations and core activities, maintaining generation of value, or by making and/or releasing potential for example through

triggering something that drives top line growth as fueling innovation, branding the company as certified or compliant with standards, building industry-specific trust. This be through controlling process with ISO 27001 or fulfilling technical requirements to meet Cyber Essentials Plus. But on the other hand, this doesn't necessarily put the business as the most important component to release the inherent potential of.

This can facilitate different sell-in strategies of the measures towards the board of directors and the employees. A CISO will likely want to sell in the expedient actions with arguments of convincing nature, such as illustrating downside with a worst-case scenario or an upside with tempting targets. We have seen a development from prevention to enablement of cyber security, making it a case about stakeholder returns, where one of them – the shareholder, represented by the board of directors – are likely to prioritize returns in form of shareholder remuneration, mostly dependent on the LLC's competitiveness through long-term profitability. While concrete preventative measures can be decided with a precalculated and determined investment cost, proven through a ROI-calculation, more holistic approaches could turn out to be harder to calculate, giving a qualitative decision basis. One could also do a calculation with RODNI, taking potential related costs into consideration, for example through expected ransom from ransomware introduced from careless employees. As some investments in intangibles such as software, rights or patents can be activated as assets and not accounted as expensing as incurred, there can be argued that the management of such assets can be more visible if done – as a result of visualization through higher equity and market value - although there seems to be difficult to activate cost related to cyber security as they don't fulfil the requirements for activation in line with the accounting act and intangibles standard, because of difficulties with isolating the asset and proving it to yield tangible returns. From this point of view, it may be plausible to assume that a way of activating investments within the cyber security domain could make it easier to make the numbers add up.

As we barely touched on in the first paragraph in this section, there is demand for human competency regarding cyber security, individually and in teams. This could also lead to innovation materializing in cash flow if successful. We found that agility and the ability to thrive in rapidly changing environments are key components today – making demand for an aligned cyber security approach. With that said, a point of appeal against the business-focused alignment strategy can be that it is not agile enough to thrive in change, possibly making external uncertainties and changes challenging for the business. Embedding cyber security into every corner of the business, making it business centric, encapsulating it in every employee and team, could be argued to facilitate for agility, requiring people process and competency change, rather than cumbersome system change.

On the other hand, required investments in human resources, through time-usage, planning and mapping etc., could be difficult to quantify when approaching also in holistic manner. But although not necessarily possible to quantify, some experts will argue that the proactive, information sharing and security culture facilitates develop-

ment for further resource utilization, weeding out common errors committed by individuals, but also stimulating agility and innovation while navigating in both changing customer demand and cyber security landscape.

6 Conclusions and future research

We have established business-centric cyber security as an approach that views cyber security as an enabler that could improve business performance through embedding cyber security to the core activities and implement measures within the business processes. Thus, taking cyber security further from stimulating to achieve goals through customization of sets of defensive capabilities, including processes or technicalities. This customization could also be through recruiting customers through branding the company as compliant with standards or certifications.

We have found that accounting management and communication of investments in cyber security is difficult, both from a governance perspective and as a tool (for CISO) to sell-in to the decision-makers (executives and the board), but that business-centric cyber security could have lower "implementing cost" barriers, although it needs allocation and reallocation of resources to drive security innovation, demanding organizational and cultural update and maintenance. Thus, also being associated with little tangible return on isolation of investment of resources, but may materialize in tangible returns overall, as the culture should permeate cross-functional.

Business-centric cyber security can contribute to value creation by weeding out vulnerabilities of human character, providing resilience for maintaining value generation, as well as cultivating motivation and innovation in a security culture. This giving ability to continuously be agile and catch opportunities while still having an expedient cyber security is an advantage in a landscape where the companies thriving are those able to create value by updating their business processes which are generating value.

In this research, we did not manage to concretize returns in business-centric cyber security. To further contribute to the field, we recommend research on how to gain more insight in isolating the performance of business-centric approaches and measurable KPI's, both for observing what tangible returns that are, but also forming selling points to decision makers on non-defensive cyber security investments.

References

1. Agrafiotis, I. et al. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of cybersecurity (Oxford)*. 4(1), pp. 1-15. doi: 10.1093/cybsec/tyy006
2. Ajmani, N. and Kumar, D. (2017) Next Practices: Business-Centric Security and Risk Management. *Achieving and Sustaining Secured Business Operations*. Berkeley: Apress, pp. 9-33.
3. Alsaleh, M. N., Al-Shaer, E. and Husari, G. (2017) ROI-Driven Cyber Risk Mitigation Using Host Compliance and Network Configuration. *Journal of network and systems management*. 25(4), pp. 759–783. doi: 10.1007/s10922-017-9428-x
4. Broquist, M., Kratzert, T. and Mosquera, C. O. (2021) *Creating a competitive advantage with cybersecurity*. Available at: https://www.kearney.com/industry/telecommunications/article/-/insights/creating-a-competitive-advantage-with-cybersecurity (Accessed: 17 November 2024).
5. Cambridge University Press & Assessment (2024a) *Cambridge Dictionary*. Available at: https://dictionary.cambridge.org/dictionary/english/centric#google_vignette (Accessed: 31 October 2024).
6. Cambridge University Press & Assessment (2024b) *Cambridge Dictionary*. Available at https://dictionary.cambridge.org/dictionary/english/value (Accessed: 17 November 2024).
7. Carson, J. (2023) *Is Cybersecurity Finally Becoming a Business Enabler?* Available at: https://www.comparethecloud.net/articles/is-cybersecurity-finally-becoming-a-business-enabler/ (Accessed 13 November 2024).
8. DNV (n.d.a) *ISO/IEC 27001 Certification: ISMS.* Available at: https://www.dnv.com/services/iso-iec-27001-information-security-management-system-3327/ (Accessed: 11 November 2024).
9. DNV (n.d.b) *TISAX® - Automotive sector information security*. Available at: https://www.dnv.com/services/tisax-r-automotive-sector-information-security-185873/ (Accessed 11 November 2024).
10. Grobler, M., Gaire, R. and Nepal, S. (2021) User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in big data*. 4. pp. 1-18. doi: 10.3389/fdata.2021.583723
11. Holley, K. (2024) *The Cybersecurity Imperative: Unlocking Business Value* Available at: https://www.linkedin.com/pulse/cybersecurity-imperative-unlocking-business-value-kenneth-holley-6vfmc/ (Accessed: 8 November 2024).
12. IT Governance (2022) *Cyber Security and Business Resilience – Thinking strategically.* Available at: https://www.itgovernance.co.uk/green-papers/cyber-security-and-business-resilience-thinking-strategically (Accessed: 11 November 2024).
13. IT Governance (2024) *Cyber Essentials vs ISO 27001: Key Differences*. Available at: https://www.itgovernance.co.uk/blog/expert-insight-cyber-essentials-vs-iso-27001 (Accessed: 11 November 2024).
14. IT Governance (n.d.) *The Cyber Essentials Scheme.* Available at: https://www.itgovernance.co.uk/cyber-essentials-scheme (Accessed: 11 November 2024).
15. Kamil, Y., Lund, S. and Islam, M. S. (2023) Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information systems and e-business management.* 21(3), pp. 699–722. doi: 10.1007/s10257-023-00646-y
16. Kosel, N., Schumm, J. and Kosel, P. (2024) *How can we build high performance teams (HPTs) in cyber security and support their successful development through exceptional leadership?* Available at: https://cyberunity.io/en/how-can-we-build-high-performance-

teams-hpts-in-cyber-security-and-support-their-successful-development-through-exceptional-leadership/ (Accessed: 12 November 2024).
17. Kosutic, D. and Pigni, F. (2022) Cybersecurity: investing for competitive outcomes. *The Journal of business strategy*. 34(1), pp. 28–36. doi: 10.1108/JBS-06-2020-0116
18. Leedy, P. D. and Ormrod, J. E. (2021) *Practical research: planning and design*. 12th ed. Harlow: Pearson Education.
19. Lustenberger, F. (2015) From product to business-centric organizational structures. *IEEE engineering management review*. 43(4), pp. 10–12. doi: 10.1109/EMR.2015.7433678
20. Malliouris, D. D. and Simpson, A. C. (2019). The Stock Market Impact of Information Security Investments: The Case of Security Standards, *Workshop on the Economics of Information Security*. Boston, 3.-4. June, 2019. Oxford: Oxford University Research Archive, pp. 1-32.
21. National Institute of Standards and Technology (NIST) (no date) *Glossary*. Available at: https://csrc.nist.gov/glossary/term/cyber_security (Accessed: 04 November 2024).
22. Norsk Regnskapsstiftelse (2022) *Norsk RegnskapsStandard 19: Immaterielle eiendeler*. Available at: https://www.regnskapsstiftelsen.no/wp-content/uploads/2023/01/2022-NRS-19-Immaterielle-eiendeler-2022-desember.pdf (Accessed: 17 November 2024).
23. Regnskapsloven (1998) *Lov om årsregnskap m.v.* Available at: https://lovdata.no/dokument/NL/lov/1998-07-17-56/KAPITTEL_6#KAPITTEL_6 (Accessed: 17 November 2024).
24. Sjödin, D. et al. (2020) Value Creation and Value Capture Alignment in Business Model Innovation: A Process View on Outcome-Based Business Models. *The Journal of product innovation management*, 37(2), pp. 158–183. doi: 10.1111/jpim.12516
25. Stahl, O. et al. (2021) *Cybersecurity as a Matter of Competitive Advantage: Understanding cybersecurity as more than the sole fulfillment of regulatory requirements*. Available at: https://www.porsche-consulting.com/sites/default/files/2023-04/cybersecurity_c_2021_porsche_consulting_.pdf (Accessed 18 November 2024).
26. Teece, D. J. (2010) Business Models, Business Strategy and Innovation. *Long range planning*. 43(2), pp. 172–194. doi: 10.1016/j.lrp.2009.07.003
27. Westeren, K. I. (2013) *Kunnskap og konkurranseevne*. Bergen: Fagbokforlaget.
28. Whitman, M. E. and Mattord, H. J. (2019) *Management of information security*. 6th ed. Boston Massachusetts: Cengage Learning.
29. Zachar, M. (2022) *Security as a business enabler: Building trust and empowering users*. Available at: https://kontent.ai/blog/security-as-a-business-enabler/ (Accessed: 18 November 2024).

Chapter 6

Emerging trends in modern cybersecurity

Christin Y. Emanuelsen (10048)

1 Norwegian University of Science and Technology, Gjøvik, Norway

Abstract: This chapter examines the evolving role of cybersecurity, transitioning from a reactive IT function to a strategic business enabler in response to the growing adoption of technologies such as AI, IoT, and cloud computing. As these innovations introduce new and complex risks, traditional defensive strategies are no longer sufficient. A proactive cybersecurity approach, centered on threat intelligence, vulnerability management, and simulated attack exercises, allows organizations to identify and mitigate potential threats before they disrupt operations. This shift not only protects critical systems and sensitive data but also ensures business continuity in the face of evolving cyber threats.

Integrating cybersecurity into business strategy fosters trust with stakeholders, enhances organizational resilience, and drives innovation. By aligning security efforts with broader business goals, companies can confidently embrace digital transformation while protecting their data and infrastructure. This strategic alignment not only secures a competitive edge but also supports long-term growth and operational continuity. Ultimately, proactive cybersecurity enables businesses to navigate emerging challenges, adapt to new risks, and maintain stakeholder confidence in an increasingly interconnected and dynamic digital landscape.

Keywords: Proactive security, threat intelligence, digital transformation, data protection, competitive advantage

1 Introduction:

"Why are these new trends better today, and how do these trends help to position cyber security right?"

Cybersecurity has evolved significantly over recent years, transitioning from a technical issue handled solely by IT departments to a central element of an or-

ganizations overall strategy [5]. In the past cybersecurity was typically treated as a reactive, defensive function aimed at preventing breaches after they occurred. Today it is viewed as a strategic asset that plays a critical role in safeguarding a companys reputation, promoting growth, and providing a competitive advantage [6]. This shift in perspective has been driven by the growing complexity of cyber threats, the increasing number of regulatory requirements, and the fast paced digital transformation of businesses [10]. In todays interconnected world companies are not only concerned with defending their systems from cyberattacks, but also with maintaining the trust of customers, investors, and other stakeholders. The evolving role of cybersecurity reflects its importance not just as a safeguard against threats, but as a crucial element that helps to drive innovation and secure longterm business success.

2 Cybersecurity as a strategic asset

With the rise of sophisticated cyber threats, tighter regulatory demands, and the growing value of data, businesses must view cybersecurity as an essential driver of success [11]. A strong cybersecurity posture not only protects against potential breaches but also enhances trust with customers, investors, and partners. This providing a competitive edge. This chapter explores how cybersecurity has evolved into a strategic asset, essential for safeguarding reputation, fostering growth, and ensuring longterm business durability.

2.1 Proactive security: A new standard

One of the most significant changes in modern cybersecurity strategies is the emphasis on a proactive approach [10]. Unlike traditional methods, which often respond to incidents after they have occurred, proactive security focuses on identifying potential threats before they materialize and addressing vulnerabilities before they are exploited. This approach allows organizations to prevent breaches before they happen and reduce the risk to their operations and reputation.

Proactive cybersecurity relies on continuous monitoring and threat intelligence [10]. It also uses vulnerability scanning to anticipate and counteract cybercriminal activities. By anticipating and mitigating risks in advance, companies can ensure business continuity and maintain customer and stakeholder trust [11]. This shift from reactive to proactive security is essential in todays quick evolving threat landscape, where new vulnerabilities emerge regularly, and attacks become more sophisticated.

2.2 Cybersecurity as a competitive advantage

As businesses continue to digitalize their operations, the importance of robust cybersecurity only increases [6]. The adoption of new technologies, while driving growth and innovation, introduces new security risks that could potentially harm the organization. Embedding cybersecurity into the companys core strategy is not just a necessity for risk management, it also provides a competitive advantage [10]. A business that demonstrates a strong commitment to protecting sensitive data is more likely to attract customers, investors, and partners who prioritize security and trust.

A well established cybersecurity framework not only protects against data breaches but signals to stakeholders that the company is responsible, reliable and trustworthy [6]. This proactive approach helps build stronger relationships with customers and investors by showcasing the companys dedication to safeguarding both its own digital assets and the sensitive information entrusted to it by clients and partners .

2.3 Aligning cybersecurity with business goals

Modern cybersecurity trends highlight the importance of aligning security initiatives with overarching business goals, positioning cybersecurity as a driver of innovation rather than a barrier [8]. Integrating security measures throughout all organizational functions, from product development to customer engagement, helps protect operations while stimulating business growth [10]. This integration allows businesses to manage risks effectively, ensuring that security supports key initiatives rather than slowing them down. When cybersecurity is strategically embedded within organizational planning, companies can innovate confidently [8]. Knowing that a robust security framework supports their initiatives, they can focus on growth without fear of compromising sensitive data or systems. This alignment also strengthens resilience, helping businesses adapt to changing conditions and maintain continuity in the face of evolving threats.

Managing cybersecurity today also requires looking beyond technical risks to address broader operational and strategic risks [2]. Cyber incidents can disrupt business processes, affect decision making, and weaken overall productivity. A proactive holistic approach to risk management ensures that security is woven into every level of the organization, safeguarding against both external threats and internal vulnerabilities. By addressing these risks comprehensively, businesses can protect their operations, uphold customer trust and maintain a competitive edge. Secure systems and protocols help prevent disruptions. This ensures that services can be delivered seamlessly, even in the event of a cyberattack. This strategy not only reduces immediate threats but also positions cybersecurity as a key driver of business success.

Ultimately, integrating cybersecurity with business objectives and managing holistic risks strengthens an organizations resilience [2]. This approach empowers companies to adapt, innovate and thrive in an increasingly complex digital landscape, ensuring long term growth and stability.

3 Proactive cybersecurity in support of digital transformation

In todays fast changing business landscape, digital transformation has become a crucial driver of growth, operational efficiency, and innovation [9]. It is no longer a mere choice for organizations but a necessary strategy to stay competitive and meet evolving customer demands. Businesses are increasingly turning to technologies like artificial intelligence (AI), the Internet of Things (IoT), and cloud computing to enhance their capabilities and reach broader markets.

These technologies enable businesses to enhance customer experiences, foster innovation in products, and secure a competitive advantage in the fast paced digital marketplace [9]. By streamlining operations and unlocking new possibilities, companies can meet evolving customer demands and differentiate themselves in a crowded industry landscape. Along with these significant advantages come new and complex cybersecurity risks that organizations must manage effectively.

3.1 Cloud and IoT security challenges

As organizations adopt digital transformation strategies, they often overlook the implications these technologies have on security [9]. Cloud computing provides the scalability and flexibility businesses need to store and process vast amounts of data. It also creates vulnerabilities due to the distributed nature of cloud infrastructures, where sensitive information is stored across multiple locations and accessible through a variety of devices. Without sufficient protections like encryption, multi-factor authentication, and stringent access control, businesses significantly increase their risk of data breaches and unauthorized access. These vulnerabilities can expose sensitive information to cybercriminals, leading to potential data theft, financial losses and damage to an organizations reputation. While the cloud offers many benefits it also requires careful security planning to ensure the protection of data and business operations.

Similarly, the widespread adoption of IoT devices across various industries creates new security vulnerabilities [9]. Examples like connected medical devices or smart meters in utilities are increasingly embedded into core operational systems [3] . These devices, while offering significant operational benefits, also

expose organizations to new cybersecurity risks. Many of these IoT devices lack robust protection mechanisms, leaving the critical infrastructure vulnerable to cyberattacks. Many IoT devices have limited built-in security features. This makes them susceptible to exploitation if not properly configured. The challenge lies in securing an evergrowing network of connected devices, as these devices often require consistent updates and patches to address emerging vulnerabilities. Failing to do so can leave critical infrastructure exposed to risks that could disrupt operations and threaten sensitive data. The lack of standardized IoT security complicates the issue, as devices may offer varying levels of protection. This inconsistency in security standards adds considerable strain on cybersecurity teams, hence demanding more time and resources to protect connected systems.

Given the complexity and scale of these cybersecurity challenges, a reactive approach to security is no longer sufficient anymore [3].Traditional methods of responding to threats after they occur, such as patching systems post-breach or addressing incidents as they unfold, leave organizations vulnerable to severe damage. Instead, businesses must adopt a proactive cybersecurity strategy, one that anticipates risks and addresses vulnerabilities before they lead any harm to the company. Proactive security involves continuously monitoring systems, assessing potential risks, and employing predictive tools to identify emerging threats. By identifying vulnerabilities before they can be exploited, organizations can stop cyberattacks from disrupting their operations. This proactive approach helps companies strengthen their security and avoid significant damage from potential breaches [10].

A proactive approach is not limited to technical defenses but also encompasses a shift in organizational mindset. Security must be embedded into the broader business strategy to ensure that digital transformation efforts do not compromise business operations [2]. This holistic approach to cybersecurity not only protects sensitive data and infrastructure but also enables organizations to move forward confidently with new technology initiatives. By integrating cybersecurity into their digital transformation efforts, businesses can ensure that they are innovating and scaling while maintaining a strong security posture. Proactive cybersecurity enhances organizational resilience by enabling quick adaptation to emerging cyber threats [3]. As businesses integrate new technologies, maintaining a proactive security strategy ensures they are prepared to address and recover from potential incidents swiftly, reducing operational disruptions and reputational risks. By securing their digital systems, businesses can innovate with confidence, building trust with customers, investors, and partners who depend on the company to protect sensitive information. This security reassures stakeholders that the business is committed to maintaining a safe and reliable environment.

4 Threat intelligence and vulnerability scanning

A central element of proactive security is threat intelligence, which involves collecting and analyzing data about potential risks before they evolve into actual attacks [10] This intelligence can help organizations recognize emerging trends and tactics used by cybercriminals, enabling them to preemptively shore up weaknesses.

Another key tool in a proactive strategy is vulnerability scanning. This process involves the regular use of specialized software to detect weaknesses in an organization's infrastructure—whether that's in software, networks, or systems [10]. By identifying these vulnerabilities early, businesses can apply patches and make security upgrades before attackers have an opportunity to exploit them. Vulnerbility scanning and threat intelligence not only bolster an organization's defenses but also provide valuable insights that enable teams to anticipate future threats. In essence, these practices ensure that security remains ahead of potential risks, allowing businesses to focus on growth and innovation without constantly reacting to cyber threats.

4.1 Red Teaming and attack simulations

One of the most effective proasctive techniques is Red Teaming, which simulates real-world cyberattacks to assess an organizations readiness [1]. This approach offers a realistic assessment of an organization's vulnerabilities and helps identify potential gaps in its defenses. By simulating actual attack scenarios, businesses can determine how their systems would react under stress and refine their security measures accordingly. Such simulations are crucial because they provide a clearer picture of how attackers might exploit weaknesses that may not be easily detected through routine audits or automated testing. The insights gained from exercises help organizations adjust their security posture and make informed decisions about where to allocate resources for maximum protection. Overall, Red Teaming enhances both technical and organizational preparedness. It provides actionable insights to strengthen security, reduce risks, and ensure that businesses can quickly recover from breaches, maintaining resilience and protecting their reputation.

5 The role of artificial intelligence in enhancing cybersecurity

Artificial Intelligence (AI) is revolutionizing cybersecurity by enabling organizations to detect and respond to threats more effectively than before [10]. With

the growing sophistication of cyberattacks, traditional defenses often struggle to keep pace. AI-driven tools provide a strong solution by taking over difficult tasks and quickly examining large amounts of data to find possible dangers.

5.1 AI-powered threat detection

AI plays a transformative role in cybersecurity by identifying threats that traditional systems might miss [10]. Its foundation lies in machine learning, which analyzes vast datasets, studying patterns in data movement, user behavior, and system performance. By spotting unusual activities, such as a sudden spike in network traffic or unexpected access attempts, AI can detect potential threats quickly and with precision. For instance, it identifies new malware not by recognizing its signature, like older systems, but by observing its behavior. This capability is vital in combating "zero-day exploits," where attackers target vulnerabilities that developers have not yet patched, making it a game-changer in cybersecurity [4].

One of AI's most practical advantages is its ability to minimize false alarms[1]. Cybersecurity systems often flag benign activities as threats, wasting time and resources. AI reduces these false positives by analyzing context and patterns, allowing security teams to focus on real dangers. This efficiency is critical in large organizations that manage massive data flows daily. AI can handle vast amounts of information at speeds unattainable by humans, providing faster responses to emerging threats. AI also adapts continuously, learning from new data and evolving threats [1]. This adaptability ensures that defenses remain effective against the fast changing attack methods. The combination of precision, speed, and adaptability makes AI a cornerstone of modern cybersecurity, offering robust protection while enabling businesses to operate with confidence in a digital world.

5.2 Automating incident response

AI not only detects cyberthreats but also enables rapid and efficient responses [9]. Automation handles repetitive tasks like isolating infected systems, blocking harmful IP addresses, and resetting compromised accounts. These actions can be carried out within seconds, reducing the impact of an attack and minimizing downtime. AI systems can automatically quarantine a compromised endpoint to stop threats from spreading within the network [2]. Automated tools can also apply patches or adjust firewall settings in real-time to close vulnerabilities before attackers can exploit them. This level of automation is especially beneficial for large organizations where security teams often face heavy work-

loads. By managing routine tasks, AI allows human resources to focus on more strategic efforts, such as strengthening defenses and planning for future risks.

6 Workforce training and organizational culture in cybersecurity

Cybersecurity is not only about technology. It is also about people [**?**]. Many cyberattacks happen because of mistakes made by people, not because the technology is broken. This means companies must focus on training their employees and raising awareness about cybersecurity. A good cybersecurity plan needs both strong technology and workers who help keep the company safe. Training teaches workers how to spot and deal with cyber threats. Many cyber problems happen because people make mistakes, like clicking on fake emails, misusing sensitive information, or using weak passwords. Training should focus on the newest threats, like phishing, ransomware, and tricks used by hackers. This training should create a culture of cybersecurity awareness is essential for every employee in a company. Training should not be limited to just the IT department; it should be extended to everyone [**?**]. This ensures that all employees, from newcomers to top executives, understand how to protect the company's information and what steps they should take if they spot something suspicious. Effective training teaches employees to recognize potential threats like suspicious email attachments, unusual login attempts, or unsafe websites. It also covers how to report possible issues correctly, ensuring that even non-technical employees can take the right action when needed.

Often, training includes practical exercises such as simulated phishing emails, helping employees practice identifying threats and highlighting areas that need more attention [**?**]. Additionally, showing employees the personal consequences of cyberattacks, like identity theft or financial loss, makes the training more relatable. By linking cybersecurity to their personal well-being, employees are more likely to stay engaged. When security is a priority for everyone, it strengthens the company's defense against cyber threats.

6.1 The importance of cybersecurity awareness

Creating a culture of cybersecurity awareness is essential for every employee in a company [5]. This ensures that all employees, from newcomers to top executives, understand how to protect the company's information and what steps they should take if they spot something suspicious. Effective training teaches employees to recognize potential threats like suspicious email attachments, unusual login attempts, or unsafe websites. It also covers how to report possible issues correctly, ensuring that even non-technical employees can take the right action when needed.

Often, training includes practical exercises such as simulated phishing emails, helping employees practice identifying threats and highlighting areas that need more attention [7]. Additionally, showing employees the personal consequences of cyberattacks, like identity theft or financial loss, makes the training more relatable. By connecting cybersecurity to their personal well-being, employees are more likely to remain engaged and take the training seriously. Understanding how cyberattacks can directly impact their personal lives, such as through identity theft or financial loss, helps them see the importance of cybersecurity beyond just their job roles. When security becomes a priority for everyone in the organization, it significantly enhances the company's overall defense against cyber-threats.

6.2 Building a culture of accountability

Accountability is crucial in building a strong cybersecurity culture within a company [7]. When employees understand that they all have a part in protecting the organization, they are more likely to take ownership of their actions. Leaders play a key role in setting the right example by adhering to best practices and maintaining open communication about potential risks. Encouraging a culture of openness allows employees to feel comfortable discussing cybersecurity issues, making it easier to spot and address vulnerabilities promptly. For instance, if an employee accidentally clicks on a phishing link, they should feel confident reporting the mistake without fear of punishment. This approach fosters trust and enables the organization to act quickly to mitigate any potential threats. Additionally, having clear policies and guidelines in place ensures that everyone knows their responsibilities when it comes to safeguarding company data. Regular audits and reviews further reinforce the importance of following security protocols, helping employees stay mindful of their role in maintaining cybersecurity.

7 Conclusion

In conclusion, the evolving landscape of cybersecurity is shifting from a technical requirement to a core element of business strategy. As organizations embrace advanced technologies like AI, IoT, and cloud computing, cybersecurity becomes more than just a protective measure; it becomes a driver of success and innovation. With the rise of sophisticated cyber threats, businesses must adopt a proactive approach to cybersecurity, identifying and addressing vulnerabilities before they can be exploited. This proactive mindset is essential not only for protecting assets but also for building trust with stakeholders and maintaining a competitive advantage. Moreover, integrating cybersecurity with business goals ensures that security measures support growth and innovation, rather than

hindering them.

The role of cybersecurity in modern businesses extends far beyond defense, it is now an enabler of digital transformation and long-term business resilience. By leveraging tools such as threat intelligence, vulnerability scanning, and AI-powered systems, companies can anticipate risks, strengthen their defenses, and respond quickly to emerging threats. This strategic alignment of cybersecurity with business objectives allows organizations to innovate confidently, knowing their sensitive data and systems are secure. As the digital landscape continues to evolve, a comprehensive and proactive cybersecurity approach will be critical for safeguarding business continuity, driving growth, and fostering trust in a rapidly changing world.

References

[1] E. Anderson, J. Holdsworth, and M. Kosinski. What is red teaming? https://www.ibm.com/think/topics/red-teaming, November 2024.

[2] J. Boehm, P. Merath, T. Poppensieker, R. Riemenschnitter, and T. Stähle. Cyber risk measurement and the holistic cybersecurity approach, 2024. McKinsey & Company.

[3] Alan Calder and Steve Perring. *The Cyber Security Handbook: Prepare for, Respond to and Recover from Cyber Attacks*. IT Governance Ltd, 1st edition, 2020.

[4] National Cyber Security Centre. Uk allies warn shift in cyber attackers exploiting zero-day vulnerabilities. https://www.ncsc.gov.uk/news/uk-allies-warn-shift-in-cyber-attackers-exploiting-zero-day-vulnerabilities, 2024. Accessed: 2024-12-11.

[5] G. James. Making the case for business-focused application management – case closed!, 2021. Capgemini Insights.

[6] Dejan Kosutic and Federico Pigni. Cybersecurity: Investing for competitive outcomes. *The Journal of Business Strategy*, 43(1):28–36, 2020.

[7] Burcu Kör and Bilgin Metin. Understanding human aspects for an effective information security management implementation. *International Journal of Information Security Science*, 10(2):125–137, 2021.

[8] Javaad Malik. How aligning cybersecurity with strategic objectives can protect your business, June 2022.

[9] D. Rupanetti and N. Kaabouch. Combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities. *Applied Sciences*, 14(16):7104, 2024.

[10] M.E. Whitman and H.J. Mattord. *Principles of Information Security*. Cengage, Boston, 7th edition, 2021.

[11] World Economic Forum. Global cybersecurity outlook 2022, January 2022.

Chapter 7

Risk management approach – A competitive advantage?

Julian Berg (10034)

Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This chapter will delve into the importance of risk management approaches, cultural engagement, security convergence, it will also look at information security from a business perspective and explore the possible risks and threats businesses could encounter. This will highlight how security approaches can help with strategic planning, reducing the impact of attacks and knowing what to prioritize. With these stages the paper aims to see if it's worth the investment and if it can potentially lower the chances of the business losing customers or capital. The holistic security approach that will be explained in this chapter is the ESRM. By going through this approach, it should provide knowledge on how it can benefit organizations and why it should be valued in terms of the impact it can have.

Keywords: Information security, cyber security, risk management, ESRM, holistic approach, cultural engagement, security convergence.

1 Introduction

This chapter will present and go through some of the aspects of the enterprise security risk management approach while also focusing on the business and organizational elements within information and cyber security. The emphasis on this paper will be to get a clearer understanding on how organizations can benefit from investing in information and cyber security. In business it's often an emphasis on finding "low-cost" solutions, rather than investing in competent security workers and full-established security approaches, this can have detrimental impact on the company (Whitman and Mattord, 2022). Whitman and Mattord (2022, p. 110) states that *"the cost of information security should be considered a part of the cost of doing business, much like the cost of computers, networks, and voice communications systems"*.

2 Investing in information security

While information or cyber security might not directly contribute to profit growth it can help earn the organization better reputation and build trust to potential clients. It's also important for successful management that security is being considered, since it can impact both organizational changes and development (Whitman and Mattord, 2022). Other benefactors of preventing cyber security attacks are being able to mitigate or prevent data breaches or system shutdowns (Whitman and Mattord, 2022). There are multiple reports of this happening to different businesses around the world today. One paper that researched these kinds of incidents is a study written by Dinger & Wade (2019) that focuses on "the strategic problem with information security and data breaches". This study discusses 17 incidents of breaches over four years and identifies the strategic security decisions made by the managers. It's stated that the average cost of security breaches to businesses is around $3,9 million (Ponemon, 2015, 2018 as cited Dinger & Wade, 2019. p.1). One of these incidents happened in 2016 when a hospital in California became victim to a ransomware attack were all the employees got locked out of their computers, and the perpetrators demanded 9,000 bitcoins to unlock all the computers (Purba, 2016). Another incident happened with the Norwegian company Hydro which lost over $71 million in a cyber-attack that occurred because of an opened an infected e-mail opened by an employee that contained a virus which implanted itself into the system (Briggs, 2019) .

During the rise of information technology, the demand has gone up for cyber security competence and professionals working the field. Organizations have had to pay excessive cost for these services because of the high demand and low supply especially in the US (Whitman and Mattord, 2022). In isc2 newest report they estimated that the global cybersecurity workforce should increase by 440, 000 thousand new jobs (ISC2, 2023). Organizations have different kind of requirements depending on their business. In the current market a valuable skill is being able to have both an organizational and technical understanding of cybersecurity. Even though a technical background is important there is now a high demand in security professionals that have competence in how to manage people and maintaining the current risk management system within the organization (Whitman and Mattord, 2022).

3 Strategic planning

Strategic planning is an important part in information security leadership, this involves how the organization evaluates the decisions and resources used to achieve the set goals in the future (Whitman and Mattord, 2022). The strategy plan should also consider the different sectors of the organization, and the efforts needed before implementation (Allen and Loyear, 2018). Whitman and Mattord (2022, p. 84) mention in terms of strategic planning that "GRC" is known as one of the most known holistic approaches that focuses on governance, risk management and compliance. The corporate governance is the responsibilities and guidelines the business follows and make sure that it complies with the goals and directions managed within the organization (Whitman and Mattord, 2022). In terms of the organizations stakeholders well estab-

lished communication is an important part of the security governance. This includes "development of constructive relationships, a common language, and a commitment to the objectives of the organization" (Whitman and Mattord, 2022, p. 86). In short the security governance is being able to allocate the right resources by using information security knowledge while having the organizational objectives in mind (Whitman and Mattord, 2022).

Risk management and compliance both revolve around accessing risk and able to follow the necessary guidelines and protocols to ensure proper information security. GRC is also there to contribute to technical implementations within the IT department, in this cases there need for an evaluation of the risks to minimize the chance of failure. When the organization have structured the strategic planning within every sector, the next phase is to render them into definite objectives (Whitman and Mattord, 2022). The "strategic plans are used to create tactical plans, which in turn are used to developed operational plans" (Whitman and Mattord, 2022). Tactical planning is used to split the strategic goals and focusing on how the resources should be allocated and assessing the project plans, so they know what to expect and what to work towards within a set date. It will also get converted to operational planning which will be used by the employees and managers to organize and help with daily tasks (Whitman and Mattord, 2022). The operational planning should also represent the structure of the organization, and the different sectors involved (Whitman and Mattord, 2022). If well-established communication is apparent between all the involved parties the operational planning has increased chance of succeeding (Whitman and Mattord, 2022).

4 Implementation of information security systems

Implementing information security systems is something every organization should consider when trying to adapt to the current digital environment and prepare for the risk of an attack. Since almost all organizations today are moving towards having data stored in the cloud its needed to emphasize security even more (Whitman and Mattord, 2022). Research also indicates that organizations benefit greatly from having information security system management in place. Dhillon and Backhouse (2000) mentions that businesses often implement IT without thinking about the security concerns. Another factor as stated earlier is the that the technical side of security is not enough, and that the managers responsible needs to be able to consider the whole infrastructure within the organization (Dhillon and Backhouse, 2000). This will reduce the chances of "fraud, corruption or loss of data, and the improper use of information systems that could affect the privacy and well-being of all concerned" (Dhillon and Backhouse, 2000, p. 126). In terms of how fast-changing technology is today, businesses must be able to adapt, which also impacts security within the business environment and its competitiveness in their current market (Whitman and Mattord, 2022). Ernest Chang and Ho (2006, p. 357) concludes that being able to manage information security "can serve as a powerful weapon to survive highly competitive environment".

Organizations in the first stages of implementing a security system need to consider their goals and user needs then decide what kind of system that will reflect these in the most optimal way. Whitman and Mattord (2022, p. 418) mention that there are different traditional software options to choose from, "including Rad, Jad Agile and one of the newest approaches, DevOPS". Plant, Van Hillegersberg and Aldea (2021) states that DevOps teams can give businesses a competitive advantage by being a dynamic feature that can highlight threats and give more opportunities which in turn can transform their assets. Whitman and Mattord (2022) describes DevOps as an approach that can continuously help improving the system functionality and updates the teams in terms of improving security. Even if the implementation of security systems is successful it depends on how big of an effect it really has on the organization. Hagen, Albrechtsen and Hovden (2008, p. 394) found that "awareness-creation measures are assessed to be very effective compared to the basic formal security systems". Furthermore, for security systems to effectively benefit the organization there needs to be a collective combination of different approaches that are reliant on each other, which in turn will reduce the risk and continuously improve development of the security culture (Hagen, Albrechtsen and Hovden, 2008).

5 Enterprise Security Risk management (ESRM)

The risk management approach that will be explored in this paper is the Enterprise security risk management (ESRM). This security approach look at the "fundamental risk principles to manage all security risks – whether related to information, cyber physical security, asset management, or business continuity – in a comprehensive holistic all-encompassing approach" (Allen and Loyear, 2018, p. 4). ESRM was developed by ASIS international, which is a security company that delivers guidelines, standards and issues certifications for organizations (Feeney, 2019). The company was founded in 1955 and is stated on their website as a global community of security practitioners with members virtually represented in every business today (ASIS, 2024). The way ESRM differs from other risk/threat models is how the "cycle requires a security practioner to manage security risks both proactively and reactively" (Allen and Loyear, 2018. p. 73). This is also backed up by two different papers from CSO roundtable group that describes ESRM as proactive in the way it assesses the full extent of security related risks and focuses on reducing the impact while also learning how it can affect the risk assessment process (CSO roundtable, 2015, as cited in Allen and Loyear, 2018 p. 73).

ESRM have been explained in this paper as an approach that covers security in its full extent. Understanding how this approach can be effective in reducing breaches, maintaining stakeholder relationships and minimizing cost is through the "The ESRM Life Cycle" (Allen and Loyear, 2018, p. 70). The life cycle illustrates the process of implementing an ESRM program into an organization as an ongoing commitment both structurally and on an individual level (Allen and Loyear, 2018).

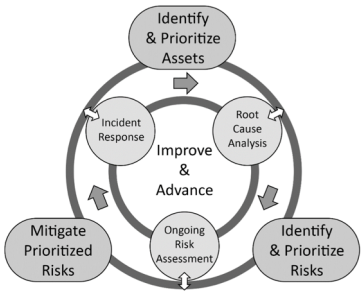

Figure 5-1. The ESRM Life Cycle

Fig 1. The ESRM Life-Cycle (Allen and Loyear, 2018, p. 70)

The phases shown in this model recognizes the risks and security as a process that keeps continuing. Allen and Loyear (2018, p. 70) states that to achieve the benefits of complete risk-based management all the steps must be followed rather than singling out the different tasks. Comparing the model to similar risk management models like "NIST" and "COBIT" the ESRM differ by having been used over many years in different security industries and is more likely to succussed in a more comprehensive management of enterprise security risk (Allan and Loyear, 2018). The ESRM is also referred to as an approach that have a larger emphasis on the business perspective and heavily consider the stakeholders and different partners involved in the security enterprise (Allen and Loyear, 2018).

5.1 Identify and prioritize assets

This is the first step in the ESRM cycle, it involves identifying what assets are connected to the organization and how to accurately secure them. It's also a part of seeing how these assets are valuable in strategic planning and the impact it has on business goals (Allen and Loyear, 2018). Placing the stakeholders and ranking the assets based on their influencing power is fundamental to the organization in this stage. Prioritizing assets can help in understanding what level of security is required and can provide information on the decisions taken during security management planning. This includes allocating the right resources to the different assets and stakeholders, which in turn can create a more resilient risk framework for the organization (Allen and Loyear, 2018). Zarinjooei et al., (2025, p. 156) research about the effectiveness of ESRM implementation suggest that "companies should take a broader perspective and make decisions based on firms financial risks instead of paying attention to the companies profitability and stock price changes".

5.2 Identify and prioritize risks

Next stage is about identifying and prioritizing the risks for the prioritized assets from the last stage. This step focuses on establishing what kind of risks the assets are vulnerable to, and create an overview of the risk landscape the organization is facing. This is done by first resolving the difference between risks and threats, then creating a

structured risk assessment which should prove beneficial in developing proper risk management. Allen and Loyear (2018, p. 99) highlight “the risk triangle” model as an is important benefactor for identifying the different risk to the assets. The threats are “something that could potentially cause harm to the asset”, examples of this are “Theft, cyber-attack, vandalism, fire, flood and data breaches” (Allen and Loyear, 2018, p. 99). The next part of the triangle is exposure, this considers the probability of the threats potentially having an affect on the organization’s assets. Impact is the last factor that looks at the potential damage a threat could do if it were to happen, examples of these kinds of occurring impacts are to financial, operational or even reputable damage (Allen and Loyear, 2018, p. 99).

5.3 Mitigate and prioritized risks

The step mitigates and prioritized risks focus on providing a structural basis where every sector involved in the security process have the necessary leadership needed for reducing the possible risks (Allen and Loyear, 2018). Together with the last step, by identifying the possible risks, threats and impacts its now possible to start mitigating and go through with further planning. Allen and Loyear (2018) mention that this step clearly highlights the difference between ESRM and traditional security measures, mainly because of the focus on the holistic security measurements rather than only functional security. Some of the processes involved in “risk mitigation plans are: Use and manage passwords, maintain access, install network firewalls, post guards, use and manage passwords, plan for crisis management and response, conduct investigations and monitor facilities with closed circuit video” (Allen and Loyear, 2018, p. 116). Following these activities will contribute to showing the connected stakeholders that the risks are being handled. The risk mitigation can also be applied to a lot of different types of organizations, it does not require to be a specific standard every time, rather it can be adapted to the security risks of the chosen sector (Allen and Loyear, 2018). The main point that is recognized within the ESRM approach is that it will have some kind of reaction or response to handle the risk (Allen and Loyear, 2018).

5.4 Improve and advance

For all these steps to be applicable to the risk management life cycle, it’s important to follow the final phase which is to improve and advance. This part involves reassessing if an incident were to happen and trying to figure out the main cause. Reason for this is to be able to analyze what can be done differently the next time and trying to improve the security by looking at potential new or former risks (Allen and Loyear, 2018). This last step also mentioned to be the core of the cycle, which has three factors: Incident response, root cause and security investigations and ongoing security risk assessment (Allen and Loyear, 2018).

The incident response is either a reactive response or a proactive response. (Allen and Loyear, 2018). In a reactive response a solution must occur fast, and it must be dealt with immediately, in the proactive response there will be information first on potential harm that could happen if not dealt with and its usually time to identify it

and try to mitigate it (Allen and Loyear, 2018). Ahmad et al., (2020) found in their study benefits of using organizational learning when developing a strong incident response could help reducing security flaws and heighten the security response of the enterprise. The risks to consider differ from either unknown or residual. Unknown risk will have a high chance of happening and would possible be something that was not noticed earlier in the identification process. Residual risk is the impact from an expected risk which means it will be mitigated, even though it can be reoccurring and still must be considered for the defense team (Allen and Loyear, 2018).

Investigations and security analysis are central to the improve and advance step and consistent of trying to find the main causes of the incident occurring. The investigations will be done by going through two different types of investigations, this is either reactive or proactive (Allen and Loyear, 2018). The reactive investigation engages the facts revolving the incident and follow the different clues and factors connected to the suspicion. A proactive investigation targets the environment in both external and internal, this includes scanning the vulnerabilities in the organization and learning how different type of hacks could affect the business (Allen and Loyear, 2018). These two both have as main goal to supply the organization with enough information that could potentially improve the security and reduce future incidents from occurring. Root cause analysis is aimed to get an overview of the root cause of the incident with asking questions specifically towards helping prevent incidents from reoccurring. These questions can be “how did it happen” or “what vulnerabilities were exploited” (Allen and Loyear, 2018, p. 131). When the analysis is finished the people responsible need to establish a report which is supposed to provide information to the current stakeholders and improve further strategic planning. Having this kind of report will present the risks to everyone involved and be able to support in handling or accessing the unknown risks (Allen and Loyear, 2018). Wangen et al., (2017) concludes that doing a root cause analysis is a costly and resource heavy task that can be justified if there is proper evaluation before going through with it.

Ongoing security risk assessment is the final part of the improvement step and focuses on always having an overview and accessing the organizations risks. This part follows risk procedure of identifying and reassessing the risks, impacts, threats and assets, furthermore, finding out what the actual risk is and hand it over to the risk stakeholders for final decision making (Allen and Loyear, 2018). Organizations can benefit from having ongoing risk assessment since it reduces the time doing every step from the start, since it’s a constant process (Allen and Loyear, 2018). Other ways the enterprise can find risks are highlighting to employees the importance of awareness. With mandatory reporting there could be an influx of reports that could strengthen the security knowledge, potential downside of this is false reports and time consumption in analyzing all the information brought forward (Allen and Loyear, 2018). Every organization must evaluate their own risks and the process of implementation depending on the structure and different variations within. Allen and Loyear (2018, p. 76) states that the most detrimental part of the ESRM life cycle is having a step-by-step process with every step having an influence on each step that follows. By following this process, it should be beneficial in helping both small and larger security problems a business could be encountering (Allen and Loyear, 2018).

6 Cultural engagement in information security

The holistic approach is meant to cover a range of areas. In an organization there is different kind of sections that all can have an impact on the security, and this is one of the main reasons for having a holistic risk management approach (Whitman and Mattord, 2022). In terms of what security elements an organization should engage, differs depending on their specific goals and their available resources. One factor that could have a big impact on improving the security is cultural engagement and employee training (Whitman and Mattord, 2022). Temitayo Oluwaseun Abrahams et al., (2024 p. 113) found that a combination of "engagement strategies, continuous learning, leadership and clear communication" will show a noticeable effect on the awareness and education programs within the organization. There should be room for a dynamic workplace where there is endorsement of employees interacting and getting the necessary competence about the threat landscape. This will benefit both the organization and management with a stronger and more proactive cybersecurity position (Temitayo Oluwaseun Abrahams et al., 2024). Implementing security education in the organization does not always need specific formal requirements or be related to a degree to be an effective tool to improve security. With a program called SETA which stands for security, education, training and awareness the organization can train employees in information security and reduce potential incidents. Whitman and Mattord (2022, p. 104) mention that employee errors are the leading threat to information assets. The SETA program is supposed to give employers the necessary knowledge about information security, so they know when to avoid for example phishing e-mails or other malware. This program should be part of the implementation in the life cycle and can be a key benefactor in enhancing security (Whitman and Mattord, 2022). Sikolia et al., (2023, p. 5) found that SETA programs reduce phishing suspect vulnerability by 50 % and increase knowledge level by 12 % to 17 %. Furthermore, the research displayed that the program helped short term, but could potentially not be as effective in the long term (Sikolia et al., 2023).

In the beginning phase of implementing security training within the organization there is some factors which should be considered. With a holistic security approach everything related to security will occur under one approach, its therefore useful to focus on providing the employees with proper training and awareness to prevent mixed messages from different groups (Allen and Loyear, 2018). Whitman and Mattord (2022) mention that it can be beneficial for the organization with security programs that new personnel get immediate training, so they understand early what to be aware off. Zhang et al., (2021) states that workers often are the major cause of cybersecurity incidents and that there should be incentive to invest in cybersecurity awareness training programs. The challenges with introducing and implementing a program can be the cost and having to frequently adapt to the constant changes within cybersecurity, it can therefore be favorable to include it as part of their strategic planning (Zhang et al., 2021). Other challenges with culture can occur between the employees who are familiar with information technology and those who are not, this can potentially lead to divisiveness between the two or even management (Allen and Loyear, 2018, p. 380)

7 Security convergence

Convergence is a practice that is used to convert all security under one reporting structure with only one executive in charge. Advantages with using this kind of structure is to potentially reduce the enterprise risks and strengthen the risk mitigation (Allen and Loyear, 2018). Convergency of technology has become normalized in most companies' security solutions, this includes having security alarms, surveillance cameras and other equipment on the same network (Allen and Loyear, 2018). The convergency has also now started to move into risk management with multiple cases of how risks affect our daily technology usage. There is now different skillsets and tools being used to tackle different issues and becoming more intervened with each other (Allen and Loyear, 2018). Organization convergence is as stated earlier as having all the different workers and tasks under a single reporting structure and usually having a chosen CISO in charge. With the ESRM approach there is not a requirement implementing this kind of convergence, but the organization should consider the convergence of philosophy. This tackles how employees' decisions related to risk management should be made by the business and managed by the leader and security team (Allen and Loyear, 2018 p. 373). The security goals and philosophy should therefore align with the business, and this means that all parties involved are responsible to follow the same approach.

Introducing a converged structure should be favorable in terms of minimizing confusion and give clear instructions on how to react or who to contact if an incident were to happen (Allen and Loyear, 2018). If there are too many steps for the employee to consider when needing to report a security issue, it lowers the chance of the incident being reported at all. Including all security in one single construct can help the employees feel less confused about what steps to go through (Allen and Loyear, 2018). This can be a helpful in terms of simplifying the reporting process which can lead to higher percentage of employees actually following through with the incident report. Moore, Dynes and Chang (2015) found that most CISO value security management frameworks when making decisions regarding investment or when having to define the risks related to the business. It was presented that data breaches from employees and other risks could potentially give reputational and financial damage, which made investing in cybersecurity a priority for most companies (Moore, Dynes and Chang, 2015). Whether the organization should consider a converged security program depends on different factors and if it can respond to everything being controlled under one single structure. If they choose to go forward with this change there needs to be transparent communication so both employee and the different sectors are prepared on how it will affect future reporting and decision making tied to security (Allen and Loyear, 2018). Mattord et al., (2024) found an increase in organizations that were willing to try security convergence in aim to better their security. Furthermore, it was beneficial for organizations which considered it, since it helped identifying issues and provided a clearer overview over the whole security operations (Mattord, et al., 2024). In relation to ESRM security program there is a potential for the organization to advantage from implementing such a program, but it depends if the management see the value and effort in restructuring. It could therefore be necessary to do a full analyze of the whole organizational structure before going through with this kind of change (Allen and Loyear, 2018).

8 Methodology and limitations

This paper uses sources from research papers, books and articles. There is not any new research presented by either qualitative or quantitative methods, information found is based on existing literature. The literature method of finding research and articles in this paper were trough Google scholar, NIST, Oria and science.gov. Limitations to consider are the lack of actual findings and if the literature presented is actually transferable to real-life practice. Various factors can also influence if organizations can use information in this paper to consider implementing a risk management approach and whether doing so is cost-effective.

9 Conclusion

This paper aimed to provide understanding of the components tied to risk management approaches and the factors involved in both technical and organizational aspects within information security. Another purpose of this chapter was to find out if what kind of value the business could get by investing in risk management approaches. Based on the research provided it indicated potential benefits, but organizations should consider analyzing their whole structure before choosing a security approach, since it increases the chance of succeeding with the implementation. ESRM was found to be advantageous for organizations who wants to have a comprehensive framework were all security is being addressed in one holistic approach. Cultural engagement was beneficial when trying to reduce employee errors and reducing the overall risk to the company. Implementing a security program could help both new and old employees understanding the importance of security and what steps to take regarding reports and handling incidents. Research also found that it gave positive results and reduced the number of incidents occurring. Security convergence is something each organization have to consider depending on their own structure and resources available for restructuring.

References

1. Allen, B.J. and Loyear, R. (2018) Enterprise Security Risk Management. First edition. Brooksfield, CT: Rothstein Publishing.

2. ASIS (2024) About ASIS. Available at: http://www.asisonline.org/footer-pages/about-asis/ (Accessed: 18 October 2024).

3. Ahmad, A. et al. (2020) 'How integration of cyber security management and incident response enables organizational learning', Journal of the Association for Information Science and Technology, 71(8), pp. 939–953. Available at: https://doi.org/10.1002/asi.24311.

4. Briggs, B. (2019) Hackers hit Norsk Hydro with ransomware. The company responded with transparency. Available at: https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (Accessed: 1 December 2024).

5. Dhillon, G. and Backhouse, J. (2000) 'Technical opinion: Information system security management in the new millennium', Communications of the ACM, 43(7), pp. 125–128. Available at: https://doi.org/10.1145/341852.341877.

6. Ernest Chang, S. and Ho, C.B. (2006) 'Organizational factors to the effectiveness of implementing information security management', Industrial Management & Data Systems, 106(3), pp. 345–361. Available at: https://doi.org/10.1108/02635570610653498.

7. Feeney, D.R. (2019) 'A Brief Guide to ESRM Implementation'. Available at: https://www.asisonline.org/security-management-magazine/articles/2019/11/a-brief-guide-to-esrm-implementation/ (Accessed: 2 December 2024).

8. ISC2. (2023). 'Cybersecurity workforce study '. Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e (Accessed: 2 December 2024)

9. Plant, O.H., Van Hillegersberg, J. and Aldea, A. (2021) 'How DevOps capabilities leverage firm competitive advantage: A systematic review of empirical evidence', in 2021 IEEE 23rd Conference on Business Informatics (CBI). 2021 IEEE 23rd Conference on Business Informatics (CBI), Bolzano, Italy: IEEE, pp. 141–150. Available at: https://doi.org/10.1109/CBI52690.2021.00025.

10. Merete Hagen, J., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and effectiveness of organizational information security measures', Information Management & Computer Security, 16(4), pp. 377–397. Available at: https://doi.org/10.1108/09685220810908796.

11. Mattord, H. et al. (2024) ‘Organizational perspectives on converged security operations’, Information & Computer Security, 32(2), pp. 218–235. Available at: https://doi.org/10.1108/ICS-03-2023-0029.

12. Moore, T., Dynes, S. and Chang, F.R. (2015) ‘Identifying How Firms Manage Cybersecurity Investment’, Darwin Deason Institute for Cyber Security Southern Methodist University Dallas [Preprint]. Available at: https://www.semanticscholar.org/paper/Identifying-How-Firms-Manage-Cybersecurity-Moore-Dynes/5b82ff36401e45c66251bbca25c9680c1dcda971.

13. Purba, N. (2016) US hospital hit with ’random’ ransomware attack. Available at: https://www.welivesecurity.com/2016/02/15/us-hospital-hit-random-ransomware-attack/ (Accessed: 1 December 2024).

14. Sikolia, D. et al. (2023) ‘How Effective are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training’, Journal of Cybersecurity Education Research and Practice, 2023(1). Available at: https://doi.org/10.32727/8.2023.13.

15. Temitayo Oluwaseun Abrahams et al. (2024) ‘cybersecurity awareness and education programs: a review of employee engagement and accountability’, Computer Science & IT Research Journal, 5(1), pp. 100–119. Available at: https://doi.org/10.51594/csitrj.v5i1.708.

16. Wangen, G. et al. (2017) ‘An Empirical Study of Root-Cause Analysis in Information Security Management’, 26-33. Available at: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2484055

17. Whitman, M.E. and Mattord, H.J. (2022) Principles of information security. Seventh edition. Boston, MA: Cengage.

18. Zhang, Z. (Justin) et al. (2021) ‘Cybersecurity awareness training programs: a cost–benefit analysis framework’, Industrial Management & Data Systems, 121(3), pp. 613–636. Available at: https://doi.org/10.1108/IMDS-08-2020-0462.

19. Zarinjooei, K. et al. (2025) ‘Identifying and Prioritizing the Factors Affecting Enterprise Risk Management Implementation’, Iranian Journal of Finance, 9(1), pp. 134–161. Available at: https://doi.org/10.30699/ijf.2024.448623.1463.

Chapter 8

New Cyber Security Trends to Adapt to the Ever-Changing Threat Landscape

Emil Nesheim-Hauge[10066]

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This chapter explores the role of business focused and business centric cybersecurity in the context of an ever-changing threat landscape. By integrating cybersecurity with business goals, organizations can increase their ability to withstand cyberattacks, best allocate resources, and improve decision-making. The chapter also examines how the Factor Analysis of Information Risk model helps quantifying risks and guide strategic investments. Despite challenges in implementation, these trends offer competitive advantages, helping businesses proactively manage risks and protect critical assets in a rapidly changing threat landscape.

Keywords: Risk management, FAIR, Treat landscape.

1 Introduction

With dependence on more digital systems than before and an increasing number of threats, cyber security is becoming an important topic. In this context, new trends such as business focused cybersecurity and business centric cybersecurity have received increased attention. These trends have been thoroughly reviewed in previous chapters, but here is a brief explanation of them. Business focused cybersecurity can be seen as a way of aligning security measures with the overall business goals and outcomes (Cyberunity, 2024). In addition to integrating security into business processes, business centric cybersecurity focuses on security being central to every business decision, thereby making security a core component of the business model (Cyberunity, 2024). We will bring this with us as we will later take a closer look at how these trends or approaches perform in the new threat landscape.

At the same time, organizations face an increasingly challenging threat landscape. The threat landscape is constantly changing, and new cyber threats will appear at regular intervals (Fadziso et al., 2023). Therefor businesses need protection against both current and future threats. Rapid changes make it difficult for organizations to adapt. In addition to the technical challenges, there will also be business-critical risk factors. The new threat landscape will therefor require approaches that combine technical resilience with business-oriented strategies.

To assess how the new trends perform in the new threat landscape, in this chapter we will use the Factor Analysis of Information Risk (FAIR) model. The FAIR-model is a risk management framework which can help organizations understand, analyze and measure information risk (Whitman and Mattord, 2021).

The aim of this chapter is to examine how the new trends work in the face of a constantly changing threat landscape by using the FAIR-model. The chapter is limited to dealing with only one model, which is FAIR. This model is basically a risk model and not directly a threat model but will after clearance be used in this chapter. The chapter will address the new threat landscape, the Factor Analysis of Information risk model, risk models as a competitive advantage, discussion and then conclusion.

2 Development of the threat landscape

First, we will explain what a threat is and what is meant by threat landscape. A threat can be defined as any event or circumstance that has the potential to adversely affect operations and assets (Whitman og Mattord, 2021). According to Marinos and Sfakianakis (2012, as mentioned in Babate et al., 2015), threat landscape can be explained as an overview of threats that contains data about threat risk and attack vectors that can result in the takeover of valuable resources or assets in a computer system when an attacker exploits the systems' weakness. With this understanding, we will further look to address the new threat landscape and what it entails.

The new threat landscape refers to today`s landscape which consists of more advanced threats than before and they change quickly (Fadziso et al., 2023). Cyber threats are becoming more difficult to deal with due to the blending of different types of attack into more damaging forms (Choo, 2011). The fact that threats are constantly changing poses a significant challenge to the cybersecurity (Fadziso et al., 2023). One of the reasons behind the rapidly changing threat landscape is the changes in technology. According to Ballamudi et al. (2022, as mentioned in Fadziso et al., 2023) existing technologies are exploited in novel ways and the new technology leads to new attack vectors become available.

Another point to highlight about the new threat landscape is the rise of supply chain attacks. Third-party packages are frequently used in modern software development which is raising the concern of supply chain attacks (Zahan et al., 2022). Bodepudi et al. (2019, as told in Fadziso et al., 2023) mentions that companies look after and secure their internal systems. This approach has shown weakness in the spike of supply chain attacks (Fadziso et al., 2023).

As mentioned earlier, technological developments affect the development of cyber threats. In this context, artificial intelligence (AI) cannot be ignored. AI provides

benefits, but can be used maliciously, such as for highly targeted and evasive attacks (Kaloudi and Li, 2020). Attack strategies are constantly improved and changed by the threat actors with particular emphasis on the application of AI-driven techniques (Kaloudi and Li, 2020).

As one can see, today`s threat landscape is changing rapidly and consists of both already existing and new threats. The increasing number of attacks on the supply chain and threats based on AI-driven techniques are examples of what the new threat landscape consists of.

3 Factor Analysis of Information Risk

Factor Analysis of Information Risk is a risk management framework as mentioned in the introduction. This model or framework is intended to contribute to more cost-effective information security management (Whitman and Mattord, 2021). Information security will not always be cost-effective as there can be high and unwanted costs to prevent possible losses (Anderson and Choobineh, 2008). So, these are decisions that the management must weigh. Then the costs associated with security must be weighed against the probability and risk of loss. FAIR is not a pure threat model, but as a risk model, it addresses threats as one of several components (Whitman and Mattord, 2021). FAIR consists of four stages, which are identifying scenario components, evaluate loss event frequency, evaluate probable loss magnitude and derive and articulate risk (Whitman and Mattord, 2021). Each of these stages consists of one or more steps (Whitman an Mattord, 2021).

The FAIR model provides a framework for quantifying cybersecurity risks, allowing organizations to assess potential financial impacts of cyber threats (Wang, Neil and Fenton, 2020). A quantitative approach like this helps in prioritizing risks and making informed decisions (Wang, Neil and Fenton, 2020). This model is particularly effective in calculating expected economic losses arising from cybersecurity, which is crucial for organizations (Wang, Neil and Fenton, 2020). By enabling risk managers to prioritize risks, the FAIR model supports strategic decision-making in cybersecurity, and it helps organizations understand the potential consequences of cyber threats (Wang, Neil and Fenton, 2020). It offers a standardized methodology for risk assessment, which can facilitate communication and understanding among stakeholders, including management and technical teams (Wang, Neil and Fenton, 2020). As one can see, this model contributes to a quantitative understanding of cybersecurity risks, which is essential for effective risk management in organizations. Further, we look to get to understand how the FAIR analysis is carried out, and we will briefly go through the different stages and steps. Jones (2006) will be used in reviewing the steps in the different stages.

Before doing the review, it is important to understand some terms we will encounter along the way. Terms that will be defined are risk, asset, vulnerability, threat agent, loss and threat event. Risk can be defined as the probability of an unwanted occurrence, such as an adverse event or loss (Whitman and Mattord, 2021). Asset can be described as the organizational resource that is being protected (Whitman and Mattord, 2021). Vulnerability is according to Whitman and Mattord (2021) a potential weakness in an asset or its defensive control system. Threat agent is the specific component or instance of a threat (Whitman and Mattord, 2021). Loss can be described as a single instance of an information asset suffering destruction or damage, denial of use or unauthorized or unintended disclosure or modification (Whitman and Mattord, 2021). Threat event is an occurrence of an event caused by a threat agent (Whitman and Mattord, 2021). With this understanding of the terms, the review becomes understandable.

In the first part of the FAIR analysis where scenario components are identified, one should identify the asset at risk and identify the threat community (Jones, 2006). Identifying the asset at risk involves determining what specific asset is vulnerable to potential threats (Jones, 2006). In the next step, one wants to define the specific group of potential threat agents that could act against the already identified asset (Jones, 2006). By doing so, one establishes an understanding of what is at risk and who might pose a threat, facilitating a more focused risk assessment.

Further we get to the next part of the FAIR model which is to evaluate loss event frequency (LEF). First step in this part is to estimate the probable threat event frequency (TEF), and this involves assessing how often a threat agent is likely to act against the identified asset within a timeframe (Jones, 2006). This is being categorized based on the expected frequency of potential attacks (Jones, 2006). Next step is to estimate the threat capability (TCap), in which evaluates the level of skill or force that a threat possesses to exploit vulnerabilities in the asset (Jones, 2006). Further, we want to estimate control strength (CS). This step assesses the effectiveness of existing controls in mitigating risks to the asset, and this control strength is rated based on how well they can protect against various levels of threat (Jones, 2006). Derive vulnerability (Vuln) calculate the likelihood that the asset will be unable to withstand the actions of a threat agent based on the previously estimated TCap and CS (Jones, 2006). The last step in this stage is to derive loss event frequency (LEF). This step combines the information from the previous steps to estimate how often a loss event is expected to occur (Jones, 2006). To understand the potential impact of risks on the organization this frequency is crucial (Jones, 2006). These steps help in quantifying the risk associated with specific assets and threats, enabling better risk management decisions.

Stage three which is to evaluate probable loss magnitude (PLM) consists of two steps. The first step is to estimate worst-case loss, which involves determining the maximum potential loss that could occur if a specific set of adverse factors converge (Jones, 2006). The threat action most likely to lead to a worst-case scenario will be identified,

the magnitude of losses associated with various loss forms are estimated, and then the sum of these magnitudes to arrive at a worst-case loss is estimated (Jones, 2006). The second step is to estimate probable loss. Here, it is being estimated the expected or average loss that could occur from a risk event, considering the likelihood of various loss scenarios (Jones, 2006). This involves that the frequency of loss events and their associated magnitudes is being evaluated to derive a more realistic estimate of potential losses that the organization might face under typical circumstances (Jones, 2006). With these steps, one can quantify the financial consequences of risks and inform decision-making about risk management strategies.

Stage four is the last stage in the FAIR analysis. This stage is to derive and articulate risk and consist of only one step which is to derive and articulate risk (Whitman and Mattord, 2021). This step involves combining the estimated loss event frequency and the estimated probable loss magnitude to define the overall risk associated with a particular threat (Jones, 2006). This process provides decision-makers with key information about the likelihood and potential impact of loss events (Jones, 2006). It is important that the information presented is clear and includes the worst-case loss to form a comprehensive picture of the risk landscape (Jones, 2006). The goal is to ensure that decision-makers have a clear understanding of the risks involved, which aids in informed decision-making.

To summarize the FAIR analysis, it involves identifying what is at risk and who could pose a threat, then assessing how often a loss event could occur by looking at threat event frequency, threat capacity, control strength and vulnerability. It then estimates the potential financial losses, both in a worst-case scenario and a more likely scenario, before finally combining the information to articulate the overall risk. In this way, decision makers will have a clear picture of both probability and consequence.

As can be seen from Wang, Neil and Fenton (2020) the FAIR model has several positive aspects, but it also has disadvantages. The model is dependent on certain assumptions, which means that it does not necessarily always reflect real-world scenarios (Wang, Neil and Fenton, 2020). This can lead to inaccurate risk assessments. Furthermore, it can be resource-intensive in that the implementation is complex and requires significant data mining and analysis efforts (Wang, Neil and Fenton, 2020). The FAIR model also has limitations when it comes to extensibility, which makes it difficult to integrate with other advanced risk assessment models (Wang, Neil and Fenton, 2020).

4 Risk models as a competitive advantage

Risk management is an important part of strengthening a company`s economy and competitiveness (Whitman and Mattord, 2021). A conscious attitude to risk will not

necessarily directly be a competitive advantage, but it can ensure that competitive disadvantages are avoided (Whitman and Mattord, 2021). By using risk models, such as FAIR, companies can maintain business operations during unforeseen events (Whitman and Mattord, 2021). This ensures a fast response time and maintains trust with customers, which can be crucial to keeping companies running or achieving set business goals.

Furthermore, it is important to protect business processes. This includes, for example, maintaining the integrity, confidentiality and availability of critical data (Whitman and Mattord, 2021). This could help the organization achieve its long-term goals (Whitman and Mattord, 2021). Such an approach will be valuable, for example in sectors where the loss of data or services can have devastating consequences.

Through cost-benefit relationships, risk models support strategic decision-making (Whitman and Mattord, 2021). This is about having a structured approach to justifying and evaluating investments in security. For example, such analyses can show how investing in preventive measures can reduce the likelihood of financial losses in the event of a security breach (Whitman and Mattord, 2021). Doing so ensures that resources are used where they have the greatest impact, while strengthening the company`s competitiveness (Whitman and Mattord, 2021).

As we understand from this and what is mentioned earlier, risk management has several positive aspects. This is also supported by Saeidi et al. (2019) where several of the same positive aspects are highlighted. According to Saeidi et al. (2019), companies will be able to make more informed decisions, and organizations will be able to anticipate and reduce potential threats. Furthermore, companies will be able to optimize the use of resources and reduce costs related to risk events (Saeidi et al., 2019). In addition, active risk management will often be viewed positively by stakeholders (Saeidi et al., 2019).

So far, we have looked at how the threat landscape is constantly changing, what the FAIR model entails and how a FAIR analysis is carried out, and how risk models and risk management affect companies. We will take this into our discussion where we will discuss whether the new trends provide a competitive advantage, how the new trends perform in the new threat landscape, and whether the FAIR model contributes to increased security and a possible competitive advantage.

5 Discussion

5.1 Can the new trends provide a competitive advantage and ensure success?

With business focused and business centric cybersecurity, one ensures that cybersecurity becomes an integrated part of the company`s overall strategy and avoid

cybersecurity becoming a separate part. Such an approach can help build a solid defense against cyber threats that are directly linked to the business-critical goals the organization has set. As we have seen from earlier, companies that link cybersecurity measures to their business goals will be better able to allocate resources in a way that provides the greatest benefit to the company. This can in turn lead to better decision-making and increased efficiency. As an example, a company with well-implemented security measures will be able to experience increased trust from its customers. In this way, it can provide a competitive advantage. From another perspective, integrating cybersecurity into business objectives could lead to coordination challenges, and this inefficiency could affect the company`s operations.

Cybersecurity can be an important factor in how a company is perceived by customers. Here, companies that work proactively to protect their business will be able to achieve a higher level of trust and thus also a better reputation. When security is closely linked to the business strategy, it becomes the basis for an organizational culture that prioritizes security and trust. This trust that can be achieved is a form of competitive advantage. Although it has its positive aspects, it will not necessarily be easy to implement in practice. One challenge may be to get the management to join in on this. Security has traditionally been seen as a cost, and this mindset can be difficult to change, especially regarding linking cybersecurity directly to the company`s overall goals. If the management is interested in short-term gains, it will be difficult as cybersecurity can often mean long-term gains that cannot necessarily be quantified.

Furthermore, there may also be challenges related to financial performance goals. Competition is becoming increasingly fierce, and organizations are working to reduce costs and maximize revenues. This can be a challenge for business focused cybersecurity, as it can lead to security not receiving sufficient attention, which can thus make the organization more vulnerable to threats. If you turn the mindset around, business focused cybersecurity will, as mentioned, lead to better resource allocation. Businesses will be able to implement targeted security measures and thus make it cost-effective instead of several general measures without the same benefit. This reduces costs somewhat, while maximizing the return on the investments made in cybersecurity. In risk assessments where the organization wants to map vulnerable areas, models such as FAIR can be used.

5.2 How are the new trends performing in the new threat landscape?

A major advantage of business focused and business centric cybersecurity in today`s threat landscape is that they are flexible approaches, in addition to being adapted to the rapid evolution of the threat landscape. As we have seen earlier, attack methods are developing rapidly, and it is crucial for organizations to adapt quickly. In this development, the traditional approach to cybersecurity, where it is seen as a technical problem, can be too rigid in the face of new threats such as AI-driven threats or supply chain attacks. At the same time, one can also imagine that costs and resource use can be a challenge in this. That implementing this cybersecurity requires a lot of

resources has already been mentioned. Linking cybersecurity and business processes together requires a thorough understanding of both the technical and business aspects. This can lead to investments related to technology and training. The rapidly changing threat landscape makes it difficult for organizations to keep up in terms of investments and updates to security measures.

Another challenge we see here will be complexity, as we have also mentioned. Cybersecurity integrated into business strategies can lead to complexity around how risk is managed and assessed. For organizations, it can be challenging to balance security with business objectives. This can then become a challenge in managing different types of risk effectively. Looking at it from the other side, business focused cybersecurity will be well equipped to handle threats that can both affect technological infrastructure and business processes. Examples of such threats could be AI-driven attacks that can be technically advanced, but also affect the operations of the organization identify how the technology can be protected, in addition to how potentially exposed business processes and critical data can be affected. In this way, it will contribute to the threat.

Business centric cybersecurity is an important step towards a proactive approach to risk assessment and making security a continuous part of business processes. In this way, companies can anticipate threats before they occur, instead of reacting when a situation arises. In the rapidly changing threat landscape, it will not necessarily be sufficient to wait for an attack to occur and the react reactively to the incident. By linking security and business, companies can better manage risk and make necessary changes before a potential attack causes damage. An example of this could be if a company is exposed to an AI-driven phising attack targeting employees. In this case, a proactive approach would be useful by identifying vulnerabilities in communication systems or training employees to identify such attacks. By doing so, the company will be more resilient, and it could reduce the size of potential losses. A negative side of this form of security integration is that it can lead to underestimating security needs. It can happen that decision-makers emphasize financial goals rather than necessary security measures. This will weaken protection against threats.

5.3 How does the FAIR-model affect cybersecurity and a possible competitive advantage?

One of the biggest advantages of the FAIR model is that it allows for the quantification of risk. The fact that the FAIR model provides a quantitative approach makes it easier for decision-makers to understand the scope and potential for financial losses, as they will not have to rely on qualitative assessments or assumptions. By linking risk to specific financial consequences, management will have a better basis for prioritizing investments in cybersecurity based on what affects the organization most financially. However, as we know, this model also has some negative sides. Something that is common when we look at business focused and business centric

cybersecurity through models such as FAIR is the complexity and the demand for resources. It takes time and resources to obtain accurate data and build a realistic model that can quantify the risk. This will be challenging for companies that do not have a good enough foundation in risk management or the necessary tools in place to collect and analyze the data.

The FAIR model is good in that it is a common framework for both those with technical expertise and managers, which means that risk can be communicated in an understandable way to non-technical decision-makers. This means that the collaboration between a typical IT department and a management team will be improved. By quantifying the risk, there will be a financial basis for making decisions and the management will be able to more easily understand the importance of investing in cybersecurity. With these advantages, it is obvious that the company should use a risk model like FAIR. However, it can be challenging. You may encounter resistance from parts of the organization, such as management. This may be due to a lack of understanding of risk or the benefit of quantifying potential losses in financial terms. Another reason may be that businesses are used to a qualitative approach to cybersecurity and therefore do not want a data-driven model like FAIR.
Using the FAIR model also provides a long-term approach to risk management. Organizations can plan for risk over time and continually adjust their security measures to meet new threats by understanding the financial consequences of potential losses and threats. In this way, they will maintain a cost-effective security strategy that both addresses current threats and improves the organization`s risk tolerance in the future.

6 Conclusion

This chapter has looked at how the new trends of business-focused and business-centric cybersecurity are performing in the rapidly evolving threat landscape. Cybersecurity has evolved from being a separate function to being integrated into the overall business strategy, which may be due to organization`s increasing awareness of cybersecurity and their reliance on digital systems. This transition is making cybersecurity a core component of business operations. These trends have the potential to provide competitive advantage by strengthening customer trust, improving decision-making, and optimizing resource allocation. However, this integration of cybersecurity is not without challenges. It can present challenges related to management resistance and coordination complexity.

The chapter also discusses the Factor Analysis of Information Risk (FAIR) model, which provides a quantitative approach to managing and assessing cybersecurity risk. By linking risk assessments to financial consequences, the FAIR model helps organizations prioritize security measures based on potential financial impact,

ensuring that resources are allocated to the areas of greatest concern. Communication risk in financial terms facilitates collaboration between those with technical expertise and management, helping non-technical decision-makers understand the importance of investing in cybersecurity.

Implementing business-centric cybersecurity and using risk models like FAIR will be resource-intensive and may encounter internal resistance, especially if the organization is inexperienced with quantitative risk models. Furthermore, the complexity can lead to security needs being underestimated if financial goals overshadow the importance of active risk management. Although this approach to cybersecurity meets these challenges, it can provide strategic benefits. Businesses will then be able to proactively manage risk, protect critical assets, and maintain resilience in the face of evolving cyber threats over the long term.

Ultimately, implementing business-focused cybersecurity and risk models such as FAIR presents both opportunities and challenges. Such an approach strengthens organization's ability to manage risk effectively. Organizations that adopt this approach to cybersecurity will also be better equipped to face the new threat landscape and could contribute to long-term improved competitiveness.

References

1. Anderson, E. E. and Choobineh, J. (2008) Enterprise information security strategies, Computers & security, 27(1-2), s. 22-29. doi: https://doi.org/10.1016/j.cose.2008.03.002
2. Babate, A. et al. (2015) State of cyber security: emerging threats landscape, International Journal of Advanced Research in Computer Science & Technology, 3(1), s. 113-119.
3. Choo, K.-K. R. (2011) The cyber threat landscape: Challenges and future research directions, Computers & security, 30(8), s. 719-731. doi: https://doi.org/10.1016/j.cose.2011.08.004
4. Cyberunity (2024) Cyber Security Competitve Advantage. Unpublished.
5. Fadziso, T. et al. (2023) Evolution of the cyber security threat: an overview of the scale of cyber threat, Digitalization & Sustainability Review, 3(1), s. 1-12. doi: https://doi.org/10.6084/m9.figshare.24189921.v1
6. Jones, J. A. (2006) An Introduction to Factor Analysis of Information Risk (FAIR), Norwich University Journal of Information Assurance (NUJIA), 2(1).
7. Kaloudi, N. and Li, J. (2020) The ai-based cyber threat landscape: A survey, ACM Computing Surveys (CSUR), 53(1), s. 1-34. doi: https://doi.org/10.1145/3372823
8. Saeidi, P. et al. (2019) The impact of enterprise risk management on competitive advantage by moderating role of information technology, Computer standards & interfaces, 63, s. 67-82. doi: https://doi.org/10.1016/j.csi.2018.11.009
9. Wang, J., Neil, M. and Fenton, N. (2020) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model, Computers & security, 89, s. 101659. doi: https://doi.org/10.1016/j.cose.2019.101659
10. Whitman, M. E. and Mattord, H. J. (2021) Principles of Information Security 7th ed. Boston: Cengage Technology Inc.
11. Zahan, N. et al. (2022) What are weak links in the npm supply chain?, i Proceedings of the 44th International Conference on Software Engineering: Software Engineering in Practice. s. 331-340.

Chapter 9

New technology in cybersecurity

Hilde Rangnes (10086)

[1] Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This paper examines emerging technologies within cybersecurity, focusing on artificial intelligence and cloud computing, within the context of two business approaches: business-focused and business-centric. The business-focused approach prioritizes compliance and risk management, while the business-centric approach emphasizes flexibility and adaptation. By understanding the risks and opportunities associated with AI and cloud computing, businesses can develop robust cybersecurity strategies. The paper explores potential benefits and challenges of adopting these technologies within each approach.

1 Introduction

The digital revolution has transformed the business landscape, creating new possibilities and challenges. While businesses take advantage of new technologies for growth and innovation, they also face a complex and evolving threat landscape. Cybersecurity has become critical for business, and needs to be integrated into the business strategy (Blum, D., 2020)

This paper aims to explore the intersection of cybersecurity and emerging technologies, focusing on artificial intelligence (AI) and cloud solutions. And how these technologies can contribute to security within a business context. I will look at two approaches to cyber security, business-focused and business-centric. And analyze how these approaches can adopt the new technology. By understanding the risks and opportunities with AI and cloud solutions, businesses can develop cybersecurity strategies that are robust.

2 Overview of business focused- and business centered trends

To understand how business-centric and business-focused approaches can be effectively implemented, it's essential to have a fundamental understanding of key concepts of cybersecurity. This chapter will therefore give a short introduction to essential frameworks within cybersecurity, furthermore it will give an overview of new business trends within cybersecurity.

Established frameworks such as the NIST Cybersecurity Framework and ISO 27001 provide guidance to best practice for managing cyber risks. The National Institute of Standards and Technology, NIST, has made a cybersecurity framework which seeks to help organizations to understand and improve their management towards this topic (NIST, n.d). “The framework describes how organizations can proceed to frame risk decisions, assess risk, respond to risk when identified and monitor risk for ingoing effectiveness and continuous improvement” (Whitman, et.al., 2021, p.167). ISO is another framework, which almost everyone has heard of in some sense. This is a standardization framework made by The International Organization for Standardization. ISO 27001 consists of the requirements towards security management systems (Brenner, J. (2007). ISO 27001 sets a baseline for robust IT governance. This standard includes several key components necessary for achieving compliance (Brenner, J., 2007. Importantly, ISO 27001 certification can help organizations meet the requirements of various regulatory standards, such as the General Data Protection Regulation (GDPR).

These frameworks can be utilized in both business-centric and business-focused approaches, but with different emphases. A business-centric approach will often place more emphasis on flexibility and adaptability, while a business-focused approach will prioritize compliance with standards and regulations. Regardless of the approach, it is essential to have a comprehensive cybersecurity strategy that is rooted in business objectives.

With this foundation in cybersecurity principles we can now take a further look at the new business trends, the business-centric and business-focused approach.

The digital revolution has not only transformed how business operates, but also reshaped the landscape of cybersecurity. This aligns with the rise of the internet and digitalization, which has fundamentally transformed business models, leading to increased complexity. Whereas the increased complexity with interconnected systems, cloud computing and the Internet of Things. This chapter explores two emerging paradigms within cybersecurity: the business-centric approach and the business-focused approach.

Traditionally, cybersecurity has been viewed as an expense, a necessary evil to protect organizations from digital threats. As Lustenberger (2015) highlights, this perception of cybersecurity often stems from siloed organizational structures, where departments operate independently with limited communication and collaboration. By adopting a business-centric approach, the organization prioritizes business processes rather than focusing on individual tasks. Embracing this approach requires a shift in mindset, as the ability for adaptation to the complexities of the modern business world is crucial (Lustenberger, 2015).

While also empathizing with alignment with business goals, the business-focused approach is often more targeted. As this approach focuses on specific security

measures to protect critical assets and ensure compliance. The business focused approach towards cybersecurity, is not just about implementing individual security measures, it's about making security a part of how the organization operates and achieves its goals. This approach focuses on identifying and addressing cyber risks to protect important assets and ensure that the organization is uninterrupted. To accomplish this, organizations need to incorporate security measures into their everyday work, stay compliant with regulations, and adapt as new threats emerge. This approach can contribute to the strengthening of security measures within the organization, which will result in higher trust amongst customers as a competitive advantage (Blum, 2020).

While both approaches seeks to strengthen cybersecurity, there is a fundamental difference in how the different approaches prioritize and implement security measures. The business-focused approach might be categorized as reactive and compliance-driven (Blum, 2020). With a focus on identifying and reducing risk to meet regulatory requirements. The business-centric approach, on the other hand, is more proactive and integrated with a focus on building security into the business core (Lustenberger, 2015). By doing this, the business can support innovation, flexibility and growth. The choice of approach relies on the organization's specific needs, risk profile and strategic objectives.

3 New Technologies within cybersecurity

With an understanding of the different business approaches to cybersecurity, we can now take a closer look at new technologies within cybersecurity. The cybersecurity landscape is driven by rapid technological advancements and the evolving tactics of cybercriminals (Garnter, 2024c). New technologies offer the potential to enhance security within the organization but also introduce new challenges and complexities. This chapter explores some of the new technologies in cybersecurity, such as artificial intelligence and cloud computing.

3.1 Status quo with Gartner

The Gartner Security & Risk Management Summit is the premier conference for exploring new technologies in cybersecurity. As a leading event in the field, they offer valuable insight into the latest trends and challenges. At this year's Security and Risk Management Summit 2024, VP Analyst Christopher Mixter and Dennis Xu made the opening statement about the need for augmented cybersecurity. Whereas they described an increase in cyberattacks alongside what is becoming a more complex threat environment (Mixter & Xu, 2024). Furthermore, they encouraged organizations to build a fault-tolerant infrastructure and improve response and recovery capabilities. To achieve this, there must be a change within the mindset of the organization. From a zero-tolerance-for-failure perspective to an elevated response and recovery mindset (Mixter & Xu, 20204).

Another key takeaway from this year's conference was the session regarding whether AI would save or ruin cybersecurity. VP Analyst Jeremy D'Hoinne emphasized the importance of building a strong foundation for integrating AI into security practices. To achieve this, he recommended organizations to develop a roadmap that outlined clear policies, risk mitigation strategies and focused on upskilling employees to work alongside AI (Garner, 2024b).

In addition to the Security and Risk Management Summit, Gartner has published a report forecasting the ten most significant technological trends for 2025. These trends were organized into three themes: AI imperatives and risks, human-machine synergy and new frontiers of computing. Gartner (2024a) predicts a significant increase in adoption of AI platforms across various sectors. However, the report also highlights potential challenges, such as difficulties in establishing standardized guidelines due to varying use cases across industries. Given the challenge within Gartner's report, establishing standardized guidelines for AI makes it crucial to understand the hype cycle. As this can be used by organizations to navigate the complexities of technology.

3.2 The hype cycle model

The hype cycle was first introduced in 1995 by Gartner Inc. The model illustrates the typical path technology follows in terms of expectations and visibility over time. The y-axis represents the expectations and perceived value of technology, while the x-axis represents time (Dedehavir, O. & Steinert, M., 2016). The bell-shaped curve of the hype cycle reflects the initial, often overly optimistic and irrational reaction to a new technology. Dedehavir and Steinert highlight previous research by Fenn and Rasko, who identified three phenomena that contribute to the curve's shape. This consists of attraction to novelty, social contagion and heuristic attitude in decision-making (Dedehavir, O. & Steinert, M., 2016). These phenomena contribute to overenthusiasm towards new technologies. In addition, the media focus on exiting stories which also leads to collective hype amongst people. Once technology gains hype, decision-makers within organizations may follow the trend without critically assessing its potential. This kind of decision-making strategy can be risky. The initial enthusiasm surrounding new technologies often gives way to disappointment when they fail to meet inflated expectations. This disappointment can lead to wasted resources, missed opportunities and security vulnerabilities if the technology is not properly assessed (Dedehavir, O. & Steinert, M., 2016).

To better understand the implications of these phenomena, we'll examine the five phases of the hype cycle. The Innovation Trigger, represents the initial introduction of a new technology, often accompanied by media attention. The Peak of Inflated Expectations, is characterized by overenthusiasm and unrealistic expectations. The Trough of Disillusionment follows as technology fails to meet these expectations,

leading to disappointment. The Slope of Enlightenment represents a period of gradual understanding and realistic assessment of the technology's capabilities. Finally, the Plateau of Productivity marks the stage where the technology reaches mainstream adoption and delivers tangible benefits (Dedehavir, O. & Steinert, M., 2016) (Gartner, 2024c).

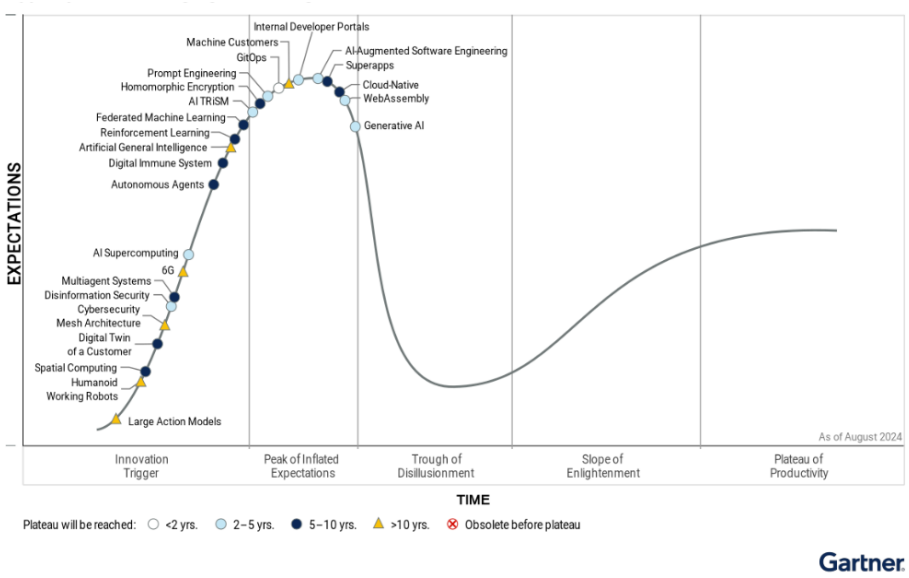

FIG
Currently, artificial intelligence in cybersecurity appears to be approaching the peak of inflated expectations. While the potential benefits of artificial intelligence are significant, it's crucial to maintain realistic expectations and acknowledge potential limitations (Gartner, 2024c).

4 Identified risks and opportunities with new technologies

Having examined the hype cycle and its potential impact on decision-making, we can now dive into the specific risks and opportunities associated with new technologies in cybersecurity. To narrow the scope of this paper, I will focus on the use of AI and machine learning for threat identification and the application of cloud solutions in cybersecurity.

4.1 AI, machine learning, for threat identification

Despite the hype towards AI, its value in cybersecurity is already evident. For instance, machine learning algorithms are used to detect and identify malicious patterns in network traffic (Immastephy, A. J. A. et al. (2024). This is also known as an intrusion detection system, or IDSs. The system can detect different kinds of malicious network communications (Tsai et al., 2009). The reason for this system, is based on

the assumption that intruders behave differently than legitimate users (Stallings (2006). There are two categories of IDSs, anomaly and misuse detection. Tsai (2009) describes anomaly detection as an approach that seeks to determine deviation from the normal usage pattern. Misuse detection on the other hand uses already well-known patterns for attacks (Tsai et al, 2009).

Furthermore, this paper will look at the anomaly approach. As mentioned, this approach seeks to determine deviation from the normal pattern. Anomaly-based IDS monitors network to discover irregularities that can indicate a security breach. Further, the monitoring will analyse based on employees heuristics or applied rules to categorize the irregularities as normal or anomalous. Possible challenges for this approach include designing a set of rules to identify unique assaults. And it's here the power of AI comes thru!

Machine learning is a branch of artificial intelligence, AI, that focuses on developing algorithms that can classify and predict outcomes based on data (Immastephy, A. J. A. et al. (2024). Machine learning is often useful for finding existing data patterns, as the employee might not be able to. Within machine learning there is two subcategories, supervised learning and unsupervised learning. To make supervised learning function efficiently, labeled data with relevant information is required. Classification is one of the most common tasks in supervised learning, and this also applies to IDSs. However, manual labeling of data is time-consuming and expensive. This leads to a lack of sufficient data, which is also the main challenge for supervised learning. Unsupervised learning, on the other hand, is easier to implement as it can extract relevant information from unlabeled data (Immastephy, A. J. A. et al. (2024). Nevertheless, supervised learning often exceeds unsupervised learning because of the detection efficiency.

However, Immastephy (2024) have argued that most of machine learning approaches are shallow learning. Due to this, the detection method has a limited capacity for learning and will weaken as the network complexity increases. Because of this weakness, researchers have turned to deep learning approaches. There are some advantages, and disadvantages with this approach, but nevertheless deep learning is considered an intriguing technology. With further research in this area, it will be possible to reveal even more possibilities, but also challenges, in relation to intrusion detection (Immastephy, A. J. A. et al. (2024).

4.2 Cloud computing in cybersecurity

The term cloud computing became a new buzzword after Web 2.0 and refers to the delivery of computing services over the internet (Verma, A. & Kaushal, S. (2011). This phenomenon changed the way IT services are invented, updated and paid for. Key components to cloud computing are delivering all the existing information technology and reducing costs (Verma, A. & Kaushal, S. (2011).

There are various definitions to cloud computing, therefore there will be provided a definition, to set common ground. The National Institute of Standards and Technology (NIST) have defined cloud computing like this:

"*Cloud computing is a model for enabling convinitent, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*

Alongside the definition of cloud computing, NIST has defined five main characteristics of cloud computing. First, cloud computing offers on-demand self-service, allowing consumers to provision computing capabilities like server time and network storage as needed without human interaction. Second, ubiquitous network access ensures accessibility through standard mechanisms on various devices. Third, location-independent resource pooling enables providers to serve all consumers using a multi-tenant model, dynamically assigning resources according to demand. Fourth, rapid elasticity allows for quick scaling of resources up or down. Finally, measured service derived form business model properties, means that providers control and optimize resource use through automated tools. These characteristics collectively define the core nature of cloud computing (Verma, A. & Kaushal, S. (2011). These findings also sums up the advantages of cloud computing, but there are some disadvantages.

Cloud computing requires a shared responsibility between provider and customer. Verma and Kaushal (2011) argue that security issues in cloud computing fall into two categories: those faced by the provider and those faced by the customer. Providers are responsible for securing their infrastructure and protecting customer data and applications. This includes measures like defending against cyberattacks and ensuring data is encrypted and stored securely. Customers on the other hand, are responsible for choosing a provider with robust security measuers and following best practices for cloud security. This includes using strong passwords, enabling multi-factor authentication and staying informed about potential threats. By understanding these distinct responsibilities, both providers and customers can contribute to a more secure cloud environment (Verma, A. & Kaushal, S. (2011)

Another security challenge related to cloud computing is accessibility, as it's possible to reach data from anywhere with an internet connection. Due to this, cloud computing needs robust security measures to verify users' identities to protect sensitive information. This is where Identity Management (IDM) systems come into play. IDM refers to the processes and technologies used to manage digital identities. (Verma, A. & Kaushal, S. (2011). An effective IDM system authenticates users based on their credentials and characteristics, granting them access to resources while safeguarding private information. By implementing a robust IDM system organization can ensure secure access to cloud service (Verma, A. & Kaushal, S. (2011).

As seen, cloud services offer both opportunities and challenges in terms of cybersecurity. To ensure that the benefits of cloud services are fully realized, it's crucial to address the security and privacy concerns that still exist. This requires more development and improvement of existing solutions. Verma and Kaushal argue that cloud services are still in their infancy, and how security landscape changes will have a major impact on whether cloud services are successfully adopted (Verma, A. & Kaushal, S. (2011).

5 AI and cloud computing in new business approaches

With a solid understanding of the core technologies and emerging business approaches, we can now examine how AI and cloud computing can be applied in practice to enhance cybersecurity.

5.1 New technology within business-focused approaches

In the digital age, the amount of data generated has increased. This can make it difficult for organizations to operate their in-house servers. Cloud computing on the other hand, are allowing large storage capacity in the "cloud", while delivering the same functionality as prior in-house servers (Avram, M.G., 2014). This technology would be interesting for organizations with a business-focused approach, because of the cost reduction and ability to access and manage data from anywhere. With centralized management, organizations can strengthen their security with the use of cloud computing (Google Cloud, n.d)

On the other hand, there are some barriers to adopting cloud computing regarding security and privacy. With the use of cloud computing, there is some uncertainty regarding how all security levels can be achieved. Because of this, there have been some information executives questioning whether cloud computing can provide good enough protection of business information (Avram, M.G., 2014).

Another challenge regarding cloud computing is the reliability of technology. If the technology were to failure, organizations are dependent on available support operations (Avram, M. G., 2014). In context of the business-focused approach, it would be important to negotiate aspects of reliability as a part in the SLA. Avram (2014) highlights the additional cost of higher level of reliability. While businesses can take steps to minimize risks, the cannot eliminate them entirely, and the cost of failure can still be significant (Avram, M. G., 2014). Taking this into account, is it possible that cloud computing is echoing the dot-com craze of the 1990's? It's not easy to determine, but the advantages of cloud computing might overcome the disadvantages.

5.2 New technology within business-centric approaches

The business-centric approach differs from business-focused approaches, as it seeks to seamlessly integrate cybersecurity measures within the business core. Adaptions of AI technology within intrusion detection systems might be a suitable for the business-centric approach as it might unlock innovation advantages.

As previously mentioned, the anomaly approach towards intrusion detection has both advantages and disadvantages. Some of the disadvantages consist of adaptation to new technology such as AI (Dash, B., 2022). Organizations might find it hard to adapt to new technologies because of the uncertainty regarding use. This can be defined as the early stages of the hype cycle by Garnter. Another barrier towards adaptation relies in the investment cost. Even though the business-centric approach seeks to leverage new technologies like AI to achieve business goals, the organization still need to maintain realistic expectations and acknowledge potential limitations (Gartner, 2024c).

While AI has its limitations and challenges, it remains a valuable technology for cybersecurity defense (Dash, B., 2022). Reports indicate that AI-powered systems have successfully prevented attacks from various threat actors. Dash (2022) also argues that some of the challenges mentioned above could be resolved by increasing awareness of the new technology.

6 Conclusion

This paper has explored the evolving landscape of cybersecurity in the digital age, focusing on AI within intrusion detection and cloud computing. Within the new business approaches, business-focused and business-centric. We have been highlighting that AI offers significant potential for enhancing security through threat identification. As AI in cybersecurity approaches the peak of inflated expectations, it is crucial for organizations to maintain a balanced perspective. While AI offers significant potential for improving security, it is important to avoid overhyping its capabilities and to acknowledge its limitations. Because of this, organizations should carefully evaluate AI solutions and ensure they align with their specific needs and risk appetite.

Within cloud computing, we have explored how it can provide scalability, flexibility and cost-effectiveness towards the business. But it also introduced new challenges related to data security and privacy.

Ultimately, the success of adapting new technologies like AI and cloud computing in cybersecurity depends on a balanced perspective. Furthermore, a clear understanding of risks and opportunities associated with each technology. By aligning these technologies with specific business objectives and risk appetite, organizations can develop

robust cybersecurity strategies. Finally, this could enhance resilience and competitive advantage in the face of evolving threats.

References

Avram, M.G. (2014) 'Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective', *Procedia Technology*, 12, s. 529-534. doi:10.1016/j.protcy.2013.12.525.

Blum, D. (2020) *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. 1. utg. Springer Nature. doi:10.1007/978-1-4842-5952-8.

Brenner, J. (2007) *ISO 27001 Risk Management and Compliance*. Vol. 54. New York: Sabinet Online.

Dash, B., Ansari, M.F., Sharma, P. og Ali, A. (2022) 'Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review', *International Journal of Software Engineering & Applications (IJSEA)*, 13(5). From: https://ssrn.com/abstract=4323258 (Accessed at 9. December 2024).

Dedehayir, O. og Steinert, M. (2016) 'The Hype Cycle Model: A Review and Future Directions', *Technological Forecasting & Social Change*,. Tilgjengelig fra: https://doi.org/10.1016/j.techfore.2016.04.005. (Accessed at 3. December 2024).

Gartner (2024a) 'Technology for Trends 2025: Gartner Top 10 Strategic Technology Trends', (online). Stamford, CT: Gartner. From: https://www.gartner.com/en/documents/786816/technology-for-trends-2025-gartner-top-10-strategic-t (Accessed at 20. november 2024).

Gartner (2024b) 'Gartner Security & Risk Management Summit 2024 Executive Summary', (online). Stamford, CT: Gartner. From: gartner-na-executivesummary-2024.pdf (Accessed at 21. November 2024).

Gartner (2024c) 'Gartner 2024 Hype Cycle for Emerging Technologies Highlights Developer Productivity, Total Experience, AI and Security', (online).

Google Cloud (n.d.) 'Advantages Of Cloud Computing', (online). Tilgjengelig fra: https://cloud.google.com/learn/advantages-of-cloud-computing (Accessed at 9. December 2024).

Immastephy, A.J.A. et al. (2024) 'A Systematic Review on Network Intrusion Detection System Based on Machine Learning and Deep Learning Approach', *E3S Web of Conferences*, (online). Accessed at : http://dx.doi.org/10.1051/e3sconf/202454014006 (Accessed 3. December 2024).

Lustenberger, F. (2015) 'From Product to Business-Centric Organizational Structures', *IEEE Engineering Management Review*, 43(4), s. 10-12. doi:10.1109/EMR.2015.7433678.

Malatji, M. og Tolah, A. (2024) 'Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI', *AI Ethics*. doi:10.1007/s43681-024-00427-4.

Mixter, C. og Xu, D. (2024) *Augmented Cybersecurity*. Presentasjon på Gartner Security and Risk Management Summit 2024, National Harbor, MD, 10.-13. juni.

The National Institute of Standards and Technology (n.d.) 'Cybersecurity Framework', (online). Tilgjengelig fra: https://www.nist.gov/cyberframework (Accessed at 3. December 2024).

Stallings, W. (2006) *Cryptography and Network Security: Principles and Practices*. USA: Prentice Hall.

Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y. og Lin, W.-Y. (2009) 'Intrusion Detection by Machine Learning: A Review', *Expert Systems with Applications*, 36(10), s. 11994-12000. doi:10.1016/j.eswa.2009.05.029.

Verma, A. og Kaushal, S. (2011) 'Cloud Computing Security Issues and Challenges: A Survey', i *Advances in Computing and Communications*, 193, s. 445-454. doi:10.1007/978-3-642-22726-4_46.

Whitman, M. E. and Mattord, H. J. (2019) Management of information security. 6th ed. Boston Massachusetts: Cengage Learning.

Chapter 10

Cybersecurity in Industry 4.0: Integrating Strategic Measures to Enhance Resilience and Performance

Guro Skari Berger [10058]

1 Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. This chapter reviews key cybersecurity challenges in Industry 4.0 manufacturing and how emerging cybersecurity trends address these issues. By integrating cybersecurity with business objectives, organizations can enhance resilience and performance. However, the complexity and interconnectedness of Industry 4.0 systems increase vulnerability, necessitating robust, adaptive security strategies. The study underscores the need for proactive measures and strategic alignment to safeguard against evolving cyber threats.

Keywords: Industry 4.0, Hyperconnectivity, Cybersecurity.

1 Introduction

The realm of Industry 4.0 emerging technologies like Cyber-Physical Systems (CPS), Industrial Internet of Things (IIoT), and Artificial Intelligence (AI) technologies has revolutionized the manufacturing sector. This transformation has enabled the creation of smart factories and highly automated production processes, enhancing efficiency, flexibility and customization. However, the hyperconnectivity inherent in these advanced systems has also introduced a number of new cybersecurity challenges. As manufacturing companies are targeted by cybercriminals, taking on a substantial share of global cyber-attacks, it is imperative to address these vulnerabilities to safeguard business performance and competitiveness. Drawing on the theory of normal accidents, which suggests that failures are inevitable in complex, tightly coupled systems, it can be argued that there is a need for robust cybersecurity measures in the interconnected and automated environments of Industry 4.0. This chapter aims to identify the key cybersecurity challenges in this current technology-driven industrial paradigm and examine how emerging cybersecurity trends are addressing these issues. Through this literature review, this chapter provides insights into the intersection of Industry 4.0 and cybersecurity, highlighting the importance of integrating cybersecurity measures with business objectives to ensure resilience and sustained growth.

2 Research Method and Purpose

This chapter is being written based on a literature review approach, with the aim of identifying key cybersecurity challenges in Industry 4.0 manufacturing and examining how emerging cybersecurity trends perform responding to these issues. The review process involved systematically searching academic databases using relevant keywords

and search terms. This method allowed for the collection and analysis of a wide range of scholarly articles and industry reports, providing a adequate foundation for drawing informed conclusions about the intersection of Industry 4.0 and cybersecurity. Although the literature review conducted cannot be considered exhaustive, this chapter provides an overview of the topic addressed.

The purpose of this chapter is to elaborate on the following problem statement:

"Do the new cybersecurity trends perform better in the automated infrastructures?"

In this chapter the notion of automated infrastructures is tied to Industry 4.0 technologies, as they are increasingly present in these environments. Narrowing down the focus to the manufacturing industry, one can identify specific cybersecurity challenges with highly interconnected and automated systems, which is relevant for sufficiently addressing the problem statement. By researching whether emerging cybersecurity trends manage to successfully respond to the identified challenges in these highly automated environments, the chapter aims to determine whether these measures can adequately protect against possible cyber attacks.

3 Overview of the Current Cybersecurity Trends

The principle of cybersecurity revolves around three core dimensions: confidentiality, integrity, and availability (known as the CIA-triad), of which needs to be maintained to ensure cyber security. Confidentiality ensures that sensitive information is accessible only to authorized individuals, protecting data from unauthorized access and breaches (Whitman and Mattord, 2021). Integrity involves maintaining the accuracy and completeness of data, ensuring that information is not altered or tampered with by unauthorized entities (Aslan *et al.*, 2023). Availability are concerned with information and resources being accessible to authorized users when needed, preventing disruptions in service due to cyberattacks or system failures (Whitman and Mattord, 2021). Effective cybersecurity measures addresses all three dimensions, in order to protect operations and maintain trust in digital infrastructures (Lezzi *et al*., 2018; Pochmara and Swietlicka, 2024). This is fundamental to cybersecurity as it addresses the core objectives of protecting information systems.

In the evolving landscape of cybersecurity, there is an increasing need to incorporate cybersecurity measures into business functions and align security measures with business goals to support long-term growth and competitiveness (Kosutic and Pigni, 2022; Hasani, *et al.,* 2023). Unlike previous approaches that primarily viewed cybersecurity as a technical and defensive measure aimed at protecting data and systems from external threats (Whitman and Mattord, 2021), modern strategies emphasize the integration of cybersecurity with business objectives. By integrating cybersecurity into business functions, organizations can protect their critical assets, ensure compliance with regulations, and foster trust among stakeholders, thereby supporting overall business goals

(Mmango and Gundu, 2024). As a result, cybersecurity measures are increasingly implemented as a strategic component with potential to enhance organizational performance and competitive advantage (Hasani, *et al.,* 2023).

Through strategic alignment, cybersecurity measures should be integrated into core business processes to ensure that they support overall goals and enhance organizational resilience (Hasani, *et al*., 2023). Organizations must prioritize their cybersecurity efforts based on potential business impact, ensuring critical assets are protected, in order to sustain organizational success and resilience (Zimmerman, 2024). Compliance with regulatory requirements and industry standards, such as the General Data Protection Regulation (GDPR) and ISO/IEC 27001, is essential for maintaining transparency and accountability, thereby building trust with shareholders, regulators, and customers (Mmango and Gundu, 2024). By aligning cybersecurity measures with strategic business priorities, organizations can therefore effectively mitigate risks, safeguard their interests, and demonstrate the value of cybersecurity investments to stakeholders (Folorunso, *et al.,* 2024).

It is increasingly understood that cybersecurity needs to be addressed through organizational measures in addition to technical measures (Reegård, Blackett and Katta, 2019). As one of the biggest threats to an organization's information security is its own employees (Whitman and Mattord, 2021), increasing cybersecurity awareness can be beneficial. Creating a culture of security awareness through fostering collaboration between departments, increased monitoring and sufficient training programs, is essential for mitigating human-related cybersecurity risks. It can be argued that creating a good security culture relies on top management support, clear and accessible policies and procedures and maintaining training and awareness programs (Uchendu, *et al.,* 2021). Through embedding security practices into the organizational culture, employees become more vigilant and proactive in identifying and responding to potential threats. In addition to a likelihood of security breaches, this cultural shift can enhance the organization's resilience against cyberattacks (Willie, 2023).

Through emphasizing integrating security measures with business objectives, organizations benefit from the ability to protect their assets and prevent losses (Kosutic and Pigni, 2022), as well as also leverage cybersecurity as a business enabler. By staying compliant with regulatory standards and introducing efforts to align security measures with overall strategic goals to ensure that cybersecurity efforts support the overall vision, organizations take on a business focus approach to cybersecurity. This approach introduces the transitioned view on cybersecurity as a critical business concern that demands attention from all levels of the organization (Zimmerman, D., 2024). However, it can be identified that only by staying compliant with regulations and industry standards, organizations can miss out on emerging cyber threats (Folorunso, *et al*., 2024). By adopting a more proactive cybersecurity strategy, organizations aiming to thrive in today's dynamic and interconnected environment can actively contribute to business performance and value creation, making cybersecurity measures a vital element of their strategy. This holistic approach can be identified as a business centric

approach, ensuring that cybersecurity is not just a technical necessity but a strategic asset that supports and enhances business objectives (Mmango and Gundu, 2024).

4 What are Automated Infrastructures?

Industry 4.0, also known as the fourth industrial revolution, is the current phase of industrialization largely driven by disruptive trends within connectivity, advanced analytics, automation and advanced-manufacturing technology (McKinsey & Company, 2022). Modern machinery in manufacturing facilities is equipped with various smart devices all connected to networks, as well as other machines and data processing systems, often communicating over private industrial networks (Corallo, Lazoi and Lezzi, 2019). As these disruptive technologies are incorporated into hyperconnected systems, the manufacturing landscape has changed (Dawson, 2018). The implementation of Industry 4.0 technologies enhances efficiency, flexibility, and customization in production, addressing the growing demands of a dynamically ever-changing global market (Yang and Gu, 2021).

In this paradigm shift, manufacturers strive towards creating smart factories, where machines and systems are interconnected, enabling real-time data exchange and autonomous decision-making (Elnadi and Abdallah, 2023). This smart production environment requires integration of new and disruptive technologies facilitating communication between all industrial devices and the Internet (Mullet, Sondi and Remat, 2021). The industry 4.0 landscape, as visualized in figure 1, can be identified as hyper connected systems employed across production processes to enhance efficiency, flexibility, and sustainability. The benefits manufacturers see can be reduced machine downtime due to predictive maintenance and remote monitoring; increased labor productivity from automation of manual work; reduction of inventories, improvement of service levels, and improved product quality resulting from the possibility to analyze vast amounts of data (Lezzi, *et al.,* 2018).

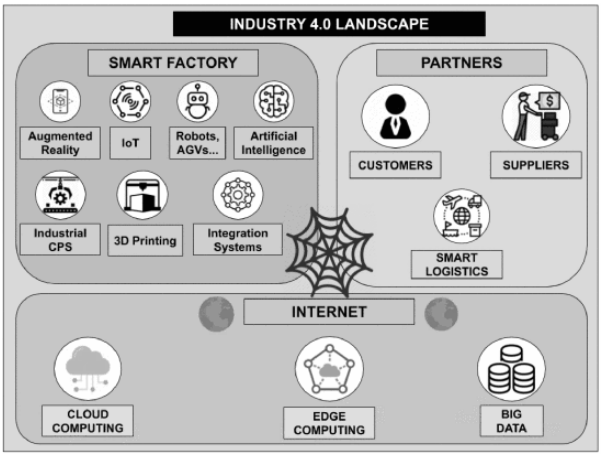

Figure 1: Industry 4.0 Landscape with main technologies (Mullet, Sondi and Remat, 2021)

One of the central technologies present in a smart factory setting is Cyber-Physical Systems (CPS). CPS can be defined as "transformative technologies for managing interconnected systems between its physical assets and computational capabilities" (Lee, Bagheri and Kao, 2014). This technology tightly integrates the Internet with networking, physical processes and embedded computers (Dawson, 2018). CPS are engineered systems that combine physical and cyber components to monitor, control, and optimize physical processes in real-time. These systems operate by leveraging sophisticated algorithms and real-time data analysis in order to enable autonomous decision-making, adaptability and performance optimization (Fortinet, 2024).

Although CPS is an integral to the advancements of Industry 4.0, the technology is often linked with other emerging technologies like the Internet of Things (IoT) and Artificial Intelligence (AI). The IoT is a network of interconnected devices and sensors that collect, exchange, and analyze data in real-time (Lynn, *et al*., 2020), that in industrial setting (referred to as Industrial IoT, IIoT) are applied to improve manufacturing and industrial processes (Radanliev, *et al.,* 2020). IIoT will enhance CPS by enabling more precise monitoring and control of physical systems, which is valuable for enhancing the dynamic and adaptive nature of CPS. Additionally, AI technologies often play a central role in analyzing the vast amounts of data generated by the IoT devices, creating a system of interrelated computing devices capable of operating without human interaction (Radanliev, *et al.,* 2020). As a result, these technologies work synergistically to create intelligent environments where devices and systems can operate autonomously and respond dynamically to changing conditions. For example, in smart manufacturing, IoT technology can be used to monitor the health and performance of equipment, then feeding data into a CPS that can predict maintenance needs or optimize production processes (Klumpp, M. 2018).

5 The theory of Normal Accidents

The theory of Normal Accidents, proposed by sociologist Charles Perrow in his 1984 book *Normal Accidents: Living with High-Risk Technologies,* suggests that in complex and tightly coupled systems, accidents are inevitable and cannot be completely prevented (Gephart, 2004). The dynamics of Normal Accidents are present when systems both have complex interactivity and tightly coupling between system components (Beckman, 2023). Further elaboration of these terms emphasizes system components as not only technical, but also human operators, procedures or administrative services. The level of interaction and interconnectedness between these system components represent the interactive complexities present in the system. Additionally, thigh coupling refers to the interdependency or lack of redundancy within a system, meaning that when a part fails it will be unable to isolate from other functioning parts, and the production will be severely impacted and likely must stop. Perrow (1999) argued that system designs are increasingly getting so complicated that all the possible interactions of inevitable failures cannot be anticipated, in addition to added safety devices being deceived, avoided or defeated by hidden paths in the system. As a result of this Perrow

emphasized the difficulty in analyzing and evaluating how failures in individual components may combine to cause accidents.

The theory of Normal Accidents, as proposed by Charles Perrow, is highly relevant to address cyber security challenges in Industry 4.0 technologies. These technologies significantly impact the cybersecurity of organizations by introducing new challenges and risks. The interconnected nature of technologies like CPS, IoT and AI creates a complex environment where traditional cybersecurity measures may not be sufficient (Toth, 2022). These technologies create environments in which highly complex and tightly coupled systems are present, leading to a setting of which interdependencies between components can lead to cascading failures. For instance, integrating IoT devices in manufacturing processes increases the system's complexity, and therefore also the potential for unforeseen interactions and events. Then adding AI technologies will increase the system's complexity even further. The interconnectedness increases the attack surface, making it difficult to predict and prevent cyber threats (Alani and Alloghani, 2019). As a result, the inherent complexity and thigh coupling in industry 4.0 systems align with Perrow's assertion that accidents, or cyber events, are inevitable in these environments.

6 Identifying the Cybersecurity Challenges in Automated Infrastructures

The integration of CPS, IIoT and AI technologies in industry 4.0 has resulted in a considerable transformation across the manufacturing sector, through enabling smart factories and increasingly automated production processes. However, this hyperconnectivity between systems raises a number of new cybersecurity challenges leaving the industry more vulnerable than before (Dawson, 2018). The past few years manufacturing companies have been the most attacked industry by cybercriminals (Alvarez, 2024; Alger, 2024) accounting for as much as a quarter of the global share of cyber-attacks in 2023 (Petrosyan, 2024). With such a large number of cybersecurity breaches, the possibility of incidents adversely affecting business performance increases. A number of potential negative business impacts resulting from cyber-attacks to manufacturing systems can be identified in the following layers:

> *"(i) sabotage of the entire critical infrastructure or target machines and components, (ii) denial of service of networks and computers, (iii) theft of industrial trade secrets and intellectual property, (iv) violation of regulations in the fields of safety and pollution, (v) until the occurrence of life-threatening situations for workers"*
>
> *(Corallo, Lazoi and Lezzi, 2019, p. 2.)*

It can be emphasized that modern manufacturing infrastructures often suffer from insecure network connections, making systems more vulnerable for cyber-attacks (Corallo, Lazoi and Lezzi, 2019). Some of the vulnerabilities cyber criminals often take

advantage of when hacking industry devices can be identified as devices running for long periods of time without any security updates or antivirus tools; controllers in industrial control systems (ICS) networks being disrupted by malformed network traffic, or even just too high volume of correctly formed traffic; uncontrolled pathways in the network of which cyber-security threats can enter; lacking physical or virtual isolation between unrelated networks, as many ICS networks are implemented as large, flat networks (Benias and Markopoulos, 2017). A common type of vulnerabilities is 'those unknown', like zero-day vulnerabilities, as these can be identified in the interfaces between components exchanging information. These vulnerabilities are particularly concerned with communication infrastructure and network protocols, application server, database server, human machine interfaces, program logic controllers, remote terminal units (Lezzi, *et al*., 2018). Consequently, network vulnerabilities are a critical component of manufacturing systems potentially leading to damaging cyber events, by either natural malfunctioning or system failures, or by being exploited by cyber criminals.

It is important to recognize that all factories and businesses utilizing automation systems can be targeted by cyber criminals, whether it be for ransomware extortion, damaging machinery or production, or generating losses to gain competitive advantage (Pochmara and Swietlicka, 2024). In the industry 4.0 context, some of the potential cyber threats include direct attacks on external accesses; indirect attacks on service provider IT systems; unknown attack vectors exploiting zero-day vulnerabilities; non-targeted malware impairing functionality; and intrusions into neighboring networks or segments (Flatt, et al., 2016). Additionally, the industry has experienced targeted attacks on automation systems, unauthorized access from office to production networks, malicious (re-)configurations via remote access, and disruptions in machine-to-machine communications and internet-based attacks on decentralized control systems (Lezzi, et al., 2018). As the manufacturing sector commonly holds outdated technologies, lack of network segmentation and zero-day vulnerabilities in systems, in addition to increasingly complex integrations and hyperconnected systems (Pochmara and Swietlicka, 2024; Aslan, et al., 2023), it is possible for cyber criminals to keep exploiting these known vulnerabilities.

Previously, manufacturing systems were closed, ensuring security through access control and isolation (Corallo, Lazoi and Lezzi, 2019). Today, the interconnected nature of Industry 4.0 technologies means that a single cyber incident can cascade through the entire system, affecting multiple components and processes simultaneously. According to Corallo, Lazoi, and Lezzi (2019), the complexity and interconnectivity of these systems increase the vulnerability of critical industrial assets. One of the primary issues is therefore the increased attack surface resulting from this extensive connectivity of devices and systems by use of IoT and similar emerging technologies (Cisco, 2022). Through elaborating on existing cyber-attacks, cyber criminals further generate different versions and use new attack variants for these devices (Aslan, et al., 2023). Additionally, the extensive data exchange and automation in a hyperconnected system increases the risk of adverse consequences from cyberattacks (Dawson, 2018). The interconnectedness can lead to a vulnerability in one device or system that can potentially

be exploited to gain access to the entire network, possibly leading to widespread disruptions.

7 Strategic Approaches to Integrating Cybersecurity in Industry 4.0

As discussed in the previous chapter, one can identify many cybersecurity challenges in the smart manufacturing environment of the industry 4.0 paradigm. Considering the manufacturing industry is largely targeted by cybercriminals (Alvarez, 2024; Alger, 2024; Petrosyan, 2024), there is a need to address cybersecurity challenges in the industry to avoid loss of confidentiality, integrity or availability of information, that could potentially have negative effects on business performance.

Within Industry 4.0 contexts, cybersecurity plays a leading role in preventing companies to lose competitiveness (Lezzi *et al*, 2018). Addressing cybersecurity issues in a proactive way is therefore an important driver for companies wanting to preserve their competitive advantage (Cisco, 2016). Lezzi *et al*. (2018) suggests two main causes for lack of sufficient cybersecurity measures in firms: (1) the lack of accurate standards to which companies can refer to, and (2) the lack of managerial and technical skills necessary to implement them. Pochmara and Swietlicka (2024) also highlights the importance of investing in robust cybersecurity measures to protect industrial automation systems, as this can help minimize risks and reduce costs associated with potential incidents. These focuses on industry standards and technical measures align with the business focused cybersecurity approach as identified above. It can be emphasized that through implementing policies, directives and laws, organizations will have to ensure cybersecurity is embedded into systems throughout lifecycle processes (Dawson, 2018). This strategy can prove beneficial to organizations through demanding compliance and setting a cybersecurity focus on the agenda.

However, Aslan *et al.* (2023) identifies that in an ever-changing cybersecurity landscape cyber criminals are continuously finding new ways to exploit vulnerabilities. Further, Dawson (2018) stresses that traditional cybersecurity measures are often insufficient to properly secure these advanced systems, demanding more robust and adaptive security strategies. In addition to increasing the attack surface, the hyperconnectivity inherent in Industry 4.0 also complicates incident detection and response. By fully integrating cybersecurity measures with business objectives, organizations can leverage cybersecurity as a strategic asset that supports and enhances business objectives (Mmango and Gundu, 2024). Corallo, Lazoi and Lezzi (2019) stress that cybersecurity strategies that are fully integrated with both organizational and information technology strategies increase the ability of organizations to proactively face cybersecurity issues. This includes educating employees on cybersecurity and staying up to date with the latest trends and threats in the surrounding landscape (Pochmara and Swietlicka, 2024). Taking into consideration these findings, it could be argued that a business centric cybersecurity approach is largely relevant for managing cybersecurity risks. Through this

approach, organizations can preserve their competitive advantage and increase the performance of their entire manufacturing value chain.

While laws, regulations, and standards can enhance cybersecurity for Industry 4.0 manufacturers, they often lag behind the rapidly evolving threat landscape (Alani and Alloghani, 2019). This delay leaves organizations vulnerable to new cyber threats that emerge faster than regulatory bodies can respond. Therefore, it is crucial for companies to integrate cybersecurity with their business objectives and embed these practices across the organization (Cisco, 2016). However, even the most diligent efforts and up-to-date measures may not suffice. The theory of normal accidents, as discussed by Perrow (1999), suggests that some accidents are inevitable, especially in highly complex and tightly coupled systems, as in present in automated infrastructures. This theory suggests that in complex systems, failures are not only expected but are a normal occurrence due to the intricate interdependencies and interactions within the system. Beckman (2023) further emphasizes that as systems become more interconnected and automated, the likelihood of such accidents increases. This is particularly relevant to Industry 4.0, where the complexity and interconnectivity of systems heighten the risk of cyber incidents.

The interconnectedness of systems can lead to a situation where a vulnerability in one device or system can potentially be exploited to gain access to the entire network, possibly leading to widespread disruptions (Benias and Markopoulos, 2017). This interconnectedness, while beneficial for operational efficiency and data integration, also creates multiple entry points for cyber attackers. Therefore, organizations must not only focus on preventing cyberattacks but also develop robust incident response plans to manage and mitigate the impact of attacks when they occur (Pochmara and Swietlicka, 2024). This approach ensures that companies are prepared to handle incidents effectively, minimizing damage and ensuring continuity of operations. By embedding cybersecurity into the lifecycle processes of systems through policies, directives, and laws, organizations can create a more resilient infrastructure (Dawson, 2018). This strategy can prove beneficial by enhancing protection against cyber threats, reducing downtime, preventing data breaches, and maintaining operational efficiency. Ultimately, this comprehensive approach to cybersecurity helps organizations maintain their competitive edge.

8 Conclusion and Outlook

In conclusion, the integration of CPS, IIoT, and AI technologies in Industry 4.0 has brought about significant advancements in manufacturing, but it has also expanded the attack surface, making cybersecurity a critical concern. While adhering to laws, regulations, and standards can enhance cybersecurity measures, these frameworks often lag behind the rapidly evolving threat landscape. Therefore, it is crucial for organizations to adopt a proactive and strategic approach to cybersecurity, aligning it with business

objectives and embedding it across the entire organization. The theory of normal accidents underscores the inevitability of failures in complex, tightly coupled systems, emphasizing the need for robust incident response plans. By integrating cybersecurity into the lifecycle processes of systems and fostering a culture of security awareness, organizations can enhance their resilience against cyber threats, reduce downtime, prevent data breaches, and maintain operational efficiency. Ultimately, this comprehensive approach to cybersecurity not only protects critical assets but also supports and enhances business performance, ensuring a competitive edge in the dynamic landscape of Industry 4.0.

While this chapter underscores the importance of integrating cybersecurity measures with business objectives in Industry 4.0 manufacturing, further research is needed to empirically assess the impact of this integration on organizational performance. Future studies should explore how aligning cybersecurity strategies with business goals influences competitive advantage of organizations. Additionally, research should investigate the long-term benefits and challenges of this approach across different industry contexts and organizational settings. Examining these aspects can provide deeper insights into the effectiveness of strategic cybersecurity integration and offer practical recommendations for enhancing resilience and performance in the face of evolving cyber threats.

9 References

1. Alani, M. M. and Alloghani, M. (2019) Security Challenges in the Industry 4.0 Era. In: Dastbaz, M. and Cochrane, P. (eds.) *Industry 4.0 and Engineering for Sustainable Future*. Springer: Cham. doi: 10.1007/978-3-030-12953-8_8

2. Alger, J. (2024) *Manufacturing is the most targeted sector by cyber criminals.* Available at: https://www.securitymagazine.com/articles/100966-manufacturing-is-the-most-targeted-sector-by-cyber-criminals (Accessed: 11.10.24)

3. Alvarez, M. (2024) *Manufacturing Is #1 in Cyber Attacks for Third Straight Year. What Can Be Done?* Available at: https://www.industryweek.com/technology-and-iiot/cybersecurity/article/55043740/manufacturing-is-1-in-cyber-attacks-for-third-straight-year-what-can-be-done (Accessed: 11.10.24)

4. Aslan, Ö. *et al*. (2023) A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*. 12(6). doi: 10.3390/electronics12061333

5. Benias, N. and Markopoulos, A. P. (2017) A review on the readiness level and cyber-security challenges in Industry 4.0. *South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Kastoria, Greece, 2017, pp. 1-5, doi: 10.23919/SEEDA-CECNSM.2017.8088234.

6. Beckman, S. (2023) Normal Cyber Accidents, *Journal of Cyber Policy.* 8(1), pp. 114-130. doi: 1080/23738871.2023.2281675

7. Charles Perrow (1999) *Normal Accidents: Living with High Risk Technologies - Updated Edition.* Princeton, New Jersey: Princeton University Press (Princeton Paperbacks).

8. Cisco (2016) *Cybersecurity as a growth advantage.* Available at: https://www.cisco.com/c/dam/assets/offers/pdfs/cybersecurity-growth-advantage.pdf (Accessed: 11.10.24)

9. Cisco (2022) *The shift to a security approach for the full application stack.* Available at: https://www.appdynamics.com/c/dam/r/appdynamics/2023/06-resources/08-ebook/AppDynamics_Application_Security_Report-1.pdf (Accessed: 10.12.24)

10. Corallo, A., Lazoi, M. and Lezzi, M. (2019) Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*. 114. doi: 10.1016/j.compind.2019.103165

11. Dawson, M. (2018) Cyber Security in Industry 4.0: The Pitfalls of Having Hyperconnected Systems. *Journal of Strategic Management Studies.* 10(1). pp. 19-28. doi: 10.24760/iasme.10.1_19

12. Elnadi, M. and Abdallah, Y. O. (2023) Industry 4.0: critical investigations and synthesis of key findings. *Management Review Quarterly.* 74, pp. 711-744. doi: 10.1007/s11301-022-00314-4

13. Flatt, *et al*., (2016) Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements, *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Berlin, Germany, 2016, pp. 1-4, doi: 10.1109/ETFA.2016.7733634.

14. Fortinet (2024) *Cyber-Physical Systems (CPS).* Available at: https://www.fortinet.com/resources/cyberglossary/cyber-physical-systems (Accessed: 6.11.24)

15. Folorunso, A., *et al.* (2024) Security Compliance and Its Implication for Cybersecurity. *World Journal of Advanced Research and Reviews.* 24(1), pp. 2105-2121. doi: 10.30574/wjarr.2024.24.1.3170

16. Gephart, R. P. (2004) NORMAL RISK: Technology, Sense Making, and Environmental Disasters. *Organization & environment.* 17 (1), 20–26. doi: 10.1177/1086026603262030

17. Hasani, T., *et al*. (2023) Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Bus Econ*. 3(97). doi: 10.1007/s43546-023-00477-6

18. Klumpp, M. (2018) Innovation Potentials and Pathways Merging AI, CPS, and IoT. *Applied system Innovation.* 1(1). doi: 10.3390/asi1010005

19. Kosutic, D. and Pigni, F. (2022) Cybersecurity: investing for competitive advantage. *Journal of Business Strategy.* 34(1). pp. 28-36. doi: https://www.emerald.com/insight/content/doi/10.1108/jbs-06-2020-0116/full/pdf?title=cybersecurity-investing-for-competitive-outcomes

20. Lee, J., Bagheri, B. and Kao, H.A. (2014) A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*. 3(2015). pp. 18-23. doi: 10.1016/j.mfglet.2014.12.001

21. Lezzi, M. *et al.* (2018) Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry.* 103. pp. 97-110. doi: 10.1016/j.compind.2018.09.004

22. Lynn, T. *et al*. (2020) The Internet of Things: Definitions, Key Concepts, and Reference Architectures, in Lynn, T. *et al*. (eds) *The Cloud-to-Thing Continuum.* Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham, pp. 1-22. doi: 10.1007/978-3-030-41110-7_1

23. McKinsey & Company (2022) *What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?* Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#/ (Accessed. 11.10.24)

24. Mmango, N., and Gundu, T. (2024) Cybersecurity as a Competitive Advantage for Entrepreneurs, In: Gerber, A. (eds.) South African Computer Science and Information Systems Research Trends. *SAICSIT 2024. Communications in Computer and Information Science*, vol. 2159. Springer, Cham. pp. pp 374-387. doi: 10.1007/978-3-031-64881-6_22

25. Mullet, V., Sondi, P. and Remat, E. (2021) A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0, *IEEE Access,* 9(2021). doi: 10.1109/ACCESS.2021.3056650

26. Petrosyan, A. (2024) *Distribution of ransomware attacks on industrial organizations and infrastructures worldwide in Q4 2023, by region.* Available at: https://www.statista.com/statistics/1372383/industrial-ransomware-share-by-region/ (Accessed: 11.10.24)

27. Pochmara, J. and Swietlicka, A. (2024) Cybersecurity of Industrial Systems - A 2023 Report. *Electronics.* 13(7), doi: 10.3390/electronics13071191

28. Radanliev, P., *et al* (2020) Artificial intelligence in cyber physical systems. *AI & Society.* 36(2021), pp. 783-796. doi: 10.1007/s00146-020-01049-0

29. Reegård, K., Blackett, C. and Katta, V. (2019) The Concept of Cybersecurity Culture. *Proceedings of the 29th European Safety and Reliability Conference.* 22.-26. September, 2019. Hannover: ESREL. pp. 4036-4043. doi: 10.3850/978-981-11-2724-3_0761-cd

30. Toth, P. (2022) *Cybersecurity and Industry 4.0 – What You Need to Know.* Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-and-industry-40-what-you-need-know (Accessed: 11.12.24)

31. Uchendu, B., *et al.* (2021) Developing a cyber security culture: Current practices and future needs. *Computers & Security.* 109(1). doi: 10.1016/j.cose.2021.102387

32. Whitman, M. E. and Mattord, H. J. (2021) *Principles of Information Security*. 7th ed. Boston: Cengage Learning

33. Willie, M. M. (2023) The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. *Journal of Research, Innovation and Technologies.* 2(4), pp. 179-198. doi: 10.57017/jorit.v2.2(4).05

34. Yang, F. and Gu, S. (2021) Industry 4.0, a revolution that requires technology and national strategies. *Complex & Intelligent Systems*. 7, pp. 1311-1325. doi: 10.1007/s40747-020-00267-9

35. Zimmerman, D. (2024) *Cybersecurity in the Digital Age: What Every Business Leader Needs to Know.* Available at: https://www.aspen.edu/altitude/cybersecurity-in-the-digital-age-what-every-business-leader-needs-to-know/ (Accessed: 8.12.24)