Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review

Diptiben Ghelani[1]

[1]Department of Computer Engineering, Gujrat Technological College

September 22, 2022

Abstract

There is a wealth of information security guidance available in academic and practitioner literature. Although other tactics such as deterrence, deception, detection, and reaction are possible, most of the research focuses on how to prevent security threats using technological countermeasures. The findings of a qualitative study conducted in Korea to determine how businesses use security techniques to protect their information systems are presented in this article. The results show a deeply ingrained preventative mindset, driven by a desire to ensure the availability of technology and services and a general lack of awareness of enterprise security concerns. While other tactics were evident, they were also preventative measures. The article lays out a research agenda for deploying multiple strategies across an enterprise, focusing on how to combine, balance, and optimize systems. This research looked at various topics, including information security and areas where security strategy is likely to be discussed, such as military sources. There are nine security strategies identified. A qualitative focus group approach is used to determine how these security strategies are used in organizations. In focus groups, security managers from eight organizations were asked to discuss their organizations' security strategies. According to the findings, many organizations use a preventive approach to keep technology services available. Some of the other identified methods were used to support the prevention strategy on an operational level.

American Journal of Science, Engineering and Technology
2022; X(X): XX-XX
http://www.sciencepublishinggroup.com/j/ajset
doi: 10.11648/j.XXXX.2022XXXX.XX
ISSN: 2578-8345 (Print); ISSN: 2578-8353 (Online)

Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review

Diptiben Ghelani

Department of Computer Engineering, Gujrat Technological College, Ahmedabad, India

Email address:
Shezi1131@gmail.com

To cite this article:
Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*. Vol. 3, No. 6, 2022, pp. 12-19

Received: May, 09, 2022; **Accepted**: July, 04, 2022; **Published**: August, 05, 2022

Abstract: There is a wealth of information security guidance available in academic and practitioner literature. Although other tactics such as deterrence, deception, detection, and reaction are possible, most of the research focuses on how to prevent security threats using technological countermeasures. The findings of a qualitative study conducted in Korea to determine how businesses use security techniques to protect their information systems are presented in this article. The results show a deeply ingrained preventative mindset, driven by a desire to ensure the availability of technology and services and a general lack of awareness of enterprise security concerns. While other tactics were evident, they were also preventative measures. The article lays out a research agenda for deploying multiple strategies across an enterprise, focusing on how to combine, balance, and optimize systems. This research looked at various topics, including information security and areas where security strategy is likely to be discussed, such as military sources. There are nine security strategies identified. A qualitative focus group approach is used to determine how these security strategies are used in organizations. In focus groups, security managers from eight organizations were asked to discuss their organizations' security strategies. According to the findings, many organizations use a preventive approach to keep technology services available. Some of the other identified methods were used to support the prevention strategy on an operational level.

Keywords: Cyber Security, Cyber Threats, web 3.0, Implications

1. Introduction

Organizations are becoming more aware of information and related technologies in almost every function, particularly in driving innovation and generating competitive advantage. Corporate information and technology services are vulnerable to various security risks in today's information environment, including the leakage of sensitive data and prolonged disruptions in email and internet access, all of which significantly impact business continuity. An organization must implement an information security strategy by establishing a comprehensive framework that allows for the development, institutionalization, assessment, and improvement of an information security program to address these security risks. The information security strategy, in particular, must support the overall strategic plans of the organization, with its content traceable to these higher-level sources [1]. Even though most organizations use "baseline" security measures, the number of security incidents rises. According to research, over 60% of businesses use technical information security countermeasures such as antivirus software, firewalls, anti-spyware software, virtual private networks (VPNs), vulnerability/patch management, and data encryption in transit, and intrusion detection systems. These reports also point out that organizations have been continuously subjected to targeted attacks. These same studies also show that security risk rises due to increased internal and external threats. As a result, security is becoming more challenging to manage. Businesses must use strategies to direct their security efforts and make the most of their limited resources in this environment. However, one system may not be sufficient [1]. Argue that to ensure the effectiveness of security measures and to maintain security policies; businesses should employ multiple information security strategies.. Much of the literature focuses on the operational aspects of information security, particularly security controls and their implementation to 'prevent' security attacks on businesses. However, in addition to

prevention, several security strategies have been conceptualized in the literature, including detection, deterrence, and deception. There has been little field research to determine which security strategies organizations use to address various security risks and how they are implemented [2]. Business security risks were ignored mainly by security managers. In general, plans were implemented ad hoc rather than as part of a planned and systematic approach to risk management [3, 4].

2. Literature review

It is best defined as determining what means to employ, how to utilize it, and how to apply it in a military situation. Beckman and Rosenfield (2008) describe strategy as "deciding where your business wants to go and finding out how to get there." These definitions can be used to build an information security strategy. According to these viewpoints, Information security strategy, according to Perk et al., is the "art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defense organization's information infrastructure(s) against internal and external threats by offering confidentiality, integrity, and availability at the expense of least efforts and costs while remaining effective." Deterrence, prevention, Surveillance, detection response, deception, perimeter defense, compartmentalization, and layering are all methods uncovered via research [1-5]. Two key elements of strategies emerged from the literature review: time and space. Strategies might be implemented before an assault or after one has occurred. The way the 'battlefield' environment is designed is essential from a spatial (space) standpoint. Breaking up the battlefield into zones to divide trustworthy and untrusted computing systems, for example, can prevent an untrusted computing system from infiltrating a trusted area. Finally, choosing specific assault and reaction strategies impacts strategy from a decision-making standpoint. The sections that follow define and describe the literature-based approach [1, 2, 6, 7].

2.1. Prevention (PREV)

Preventing illegal access, alteration, destruction, or disclosure of information assets is the goal of prevention. When approaching information security policy from a purely preventative perspective, it suggests that the company has minimal tolerance for any effect; as a result, countermeasures must be deployed to prevent all assaults on the organization. Information leaking can be avoided via prevention techniques. A clean desk policy, for example, enforced by periodic inspections for missing or confidential documents, might be beneficial. Barriers can be erected around important assets before an attack from a technological standpoint. Authentication is a popular preventative measure that seeks to limit access to authorized users. Use software that regulates user interaction with information assets encrypt information flowing over networks to prevent leakage—even if the network is compromised, uses firewalls to filter network traffic, and uses intrusion detection systems that use anomaly and signature detection paradigms to identify suspicious data are all additional prevention techniques. The significance of scanning systems for vulnerabilities and then repairing them [8, 9].

2.2. Deterrence (DETER)

Discipline is used in deterrence to impact human behavior and attitudes. The efficacy of deterrence in organizations is determined by two critical factors: the certainty of consequences and the severity of sanctions. The amount of knowledge about the type of punishment and the competence of enforcing organizations to identify infringing conduct determines the certainty of sanctions (i.e., the likelihood of getting caught). The spectrum of sanctions that can be applied influences the severity of punishments. Deterrence has been used to describe the discipline of workers who fail to comply with policy statements in security policy, which is one of the critical emphases of deterrence. Organizations should operate an education and training program to teach employees about organizational policy and standards, according to Straub and Welke (1998), to make information security activities more successful. Deterrence tactics, such as the severity of penalties, knowledge of deterrence activities, and the number of security workers, have also proven beneficial in reducing computer misuse, according to Straub (1990). Others have discovered that deterrent tactics improve information security, although the harshness of penalties has little effect on efficacy (Kankanhalli et al., 2003). More recently, D'Arcy et al. (2009) discovered that the severity of the sentence had a substantial impact on the quantity of abuse, contrary to Kankanhalli et al. (2003) 's findings. Organizations should strengthen security policy compliance training and emphasis policing policy violations [7].

2.3. Surveillance (SURV)

Surveillance is the process of continuously monitoring the security environment to build situational awareness and respond to rapidly changing conditions and threats. Situational awareness allows security decision-makers to effectively deal with data security problems and design more effective defenses. Monitoring an organization's information security environment in the physical and digital realms using technological and non-technical techniques is difficult. Logging access to limited physical and logical places where hardcopy and softcopy information is held is one component of monitoring an individual's interaction with news and information systems. Surveillance often employs data gathered by strategically placed "sensors" and visualization tools to help security managers better grasp the situation. Surveillance data is usually collected through systems and applications software, such as intrusion detection systems that report on the number of assaults, the degree of attack propagation, and the kind of attack [6].

2.4. Detection (DETECT)

Detection is a low-level operational method for detecting specific security activity. The goal of detection is for the organization to be able to react in a targeted manner. On the other hand, Surveillance tries to gain a comprehensive understanding of the situation. As a result, detection concentrates on a single occurrence, whereas Surveillance monitors the overall situation. Identification of harmful or bizarre behavior, intrusion or misuse, and particular assaults against web servers are all examples of detection. Detection can also be used to collect evidence of misuse of suspicious activities and the identification of culprits [15]. Dedicated computer and network intrusion detection devices, network scanners, system scanners, abuse and anomaly detectors, content filtering and antivirus software, and audit programs are the security technologies utilized in the detection approach. Since its inception, information and communication technology has revolutionized economic value creation by allowing firms to shift their reliance on tangible assets and money to intellectual capital [1]. As a result, most markets now rely on what Kuehl (2009) refers to as the "first man-made domain." The unprecedented capacity of companies to harness the cyber domain's relative lack of time and geographical restrictions as a facilitator of unique business models is one of the benefits of leveraging the cyber domain. However, the scale of the vulnerability that this dependency involves is becoming an increasingly significant side consequence. Cyber risks can compromise an organization's security, stability, and long-term viability by compromising informational and structural capital's confidentiality, integrity, and availability [6]. Organizational collapse to the incapacitation of nation-state infrastructures are examples of this potential for disruption and its externalities. Given their dual function as technology makers and facilitators of its usage, organizations continue to depict themselves as the critical vectors of action even while discussing the societal impacts of cybersecurity. Surprisingly, most business models see cybersecurity as a secondary responsibility since it offers little potential for monetization and value generation - the organization's raison d'être. Cybersecurity strategy is based on a symbolic self-perpetual "war" scenario, which, unlike individual "battles," cannot be conclusively won. In other words, cybersecurity is not an issue that can be "solved." Furthermore, cybersecurity management reveals an epistemic core much like other strategic efforts [4, 10-12].

Cybersecurity, expertise, and intellectual capital are essential components of a successful business. In various ways, the concept of "knowledge" pervades cybersecurity and organizational risk narratives. Neef (2005) contends that an organization's capacity to manage risk successfully is based on its ability to handle relevant knowledge. In terms of cybersecurity, Tisdale (2015) emphasizes the necessity for multi-dimensional methods that go beyond the "traditional" technical perspective and instead focus on systems/complexity and knowledge management. Show how accounting for threats to "the creation and deployment of organizational knowledge" is critical in an Information Security (IS) setting. Julisch (2013) identifies a link between knowledge constraints and the ineffectiveness of a cybersecurity strategy, as indicated by an overreliance on intuition, the absence of security foundations, poor governance, or reliance on static/generic "knowledge" about the context. In a larger sense, they argue that knowledge management approaches naturally limit the production of organizational value based on intellectual capital. Because corporate cybersecurity management strives to secure intellectual assets and operationalization, it acts as a moderator for the value creation process, overlapping with knowledge management [4, 13]. These works display substantial epistemic heterogeneity, reflecting the main topics of their respective disciplinary settings, aside from their generally constant, complimentary message. This makes the shared narrative less clear, but not necessarily the individual pieces. The lack of a uniform interpretation of information restricts the homogeneity of insight and prescriptive value that a phenomenon-driven rather than a discipline-driven approach may accomplish. The former allows researchers to look at organizational cybersecurity as a combination of technology, people, and processes, emphasizing competitiveness, intellectual capital, and long-term value generation. Even though intellectual capital is a well-established and thriving study topic, it is still seen as one that evolves through time in response to changes in the social, economic, and technical environment [1-6, 8, 11]. "The sum of all that everyone in an organization knows that offers it a competitive advantage," according to the definition. Most experts recognize the significance of intellectual capital in value creation as "intellectual material, knowledge, expertise, intellectual property, and information that may be used to produce value." This necessitates a shift in intellectual capital research from the organization to the larger ecosystem in which knowledge and value are produced. Surprisingly, cybersecurity threats arise as a result of – among other things – the systemic interplay of those aspects that make up organizational ecosystems and shape them, such as internal processes and forms of competition and value capture. As a result, a simple technical perspective on cybersecurity as a function is shortsighted, failing to account for emergent socio-technical organizational mechanisms and processes involving the organization's human, relational, and structural capital, supporting value development. As a result, we believe that a knowledge-based approach to cybersecurity and its management would directly impact intellectual capital management by influencing the dynamics of human, relational, structural, renewal, and trust capital [9, 10].

3. Knowledge, strategy, and cybersecurity

A hypothetical forerunner Interpretations of knowledge as

a construct has supported numerous main strands of strategic management and organizational theory during the last three decades. The knowledge-based vision of the company, dynamic capabilities, and knowledge management are some examples. However, the efficacy of such efforts has been questioned for various reasons, including an ambiguous or contested interpretation of knowledge, varying degrees of perceived practical utility, overly divided themes that dilute the original vision of progress, and, ultimately, an inability to avoid Occam's razor. When applied to an epistemic approach to organizational cybersecurity strategy, this history of using "knowledge" as an explanatory or prescriptive concept reveals regularities worth noting. Identifying what constitutes an "effective," or at the very least, the long-lasting epistemic basis of concepts in organizational theory is a theoretical endeavor. The substantial amount of literature on the subject, on the other hand, provides a pattern of crucial characteristics that place individual conceptualizations in a larger framework. The epistemological position, which informs the locus of knowledge (i.e., the knower), its manifestation/form (the known), and the function, nature, and attainability of truth, are all interrelated. We also believe in the contextual relevance of the relational placement of uncertainty [5, 8].

4. Pragmatism in epistemology

Truths are neither specific nor definitive in strategy, and our wishes will not change. This brutal reality must undoubtedly be included in whatever philosophical underpinnings a system may be built on - pragmatist or else. The emergent narrative situates our knowledge interpretation at the crossroads of pragmatism and critical realism. Due to the significant evolutionary/competitive orientation, the epistemological significance of action and utility, and the locus and unit of knowledge, we portray this perspective as "bottom-up" pragmatism. Unlike other epistemic processes such as scientific inquiry, organizational knowledge is adaptive to the extent that it aids in better enabling/sustaining value production. This is especially true for cybersecurity, which is a service that cannot be monetized in most business models but protects Intellectual Capital and the process of operationalization. As a result, concepts like certainty, confidence, and truth are shaped. It also views knowledge as arising through the interplay of the subject and the object of investigation. The emphasis on an abstract, conventional understanding of reality is replaced with a more dynamic, evolutionary approach [1, 12, 14].

The industrial industry in developed nations is becoming increasingly reliant on digital networks and services. The reliance will not decrease; instead, it will expand. Cyber security is a crucial facilitator of digitization, but if it is improperly managed, it may undermine all benefits. Companies' cyber security should be proactive: the harm has already been done following a major cyberattack. If, for example, a facility is already at a standstill or essential information has been stolen, reactive upgrades are too late. The manufacturing industry is becoming increasingly global. Companies in the sector are expanding their operations and stakeholders throughout the world, and the evolving global operating environment will present both possibilities and problems in the future. Cyber security management and contingency planning for future cyber attacks are two significant challenges. Cyber security is no longer only the domain of IT departments; its relevance has been recognized in corporate boardrooms, and executives' attention is expected to grow [6, 10].

New technologies in industrial environments introduce new cyber dangers, as hackers discover new methods to exploit known and undisclosed weaknesses in older systems, technologies, and processes. According to the Finnish national cyber security policy, preventing cyber security risks necessitates proactive operations and planning. The new operating environment demands knowledge and the capacity to react quickly and consistently. To achieve proactive cyber security, not just businesses but the entire society requires high-quality research on the future of cybersecurity from all industries' viewpoints. In this study, the prospects of cyber security were examined from the perspective of Finnish manufacturing organizations: priorities in 2021, what will be less critical in 2021, and the significant targets shortly? The study used a time range of 4-5 years as a standard for strategic planning. For organizations, ignoring cyber security may be pretty costly. A data security breach costs a victim firm $473 million. A breach's consequences and repercussions are complex and long-term. According to the findings of this study, security experts are fully aware of the possible costs of security breaches. For example, in the next five years, the manufacturing industry will face significant hurdles from more linked equipment and digitalization and the issues of managing who utilizes organizational networks. The results of a literature review that served as the foundation for the Delphi study are described in the next section, followed by the Delphi study's conclusions [2, 8, 10].

The report concludes with implications of the study findings for the manufacturing industry in particular and the cyber security community in general. The panelists were asked to define cyber security from their perspective in the first round. As predicted, the responses were quite diverse. They might, however, be combined into a single definition: Cyber security is primarily a new phrase on top of information security, and the prefix 'cyber' broadens its scope to include IoT and industrial contexts, for example. The panel agreed with this definition in the second round. In the first round, several experts stated that cyber security consists of three components: processes, people, and technology. Some of the panelists also mentioned how cyber security issues now extend to the actual world: for example, it would be conceivable to endanger human lives by targeting major systems in factories [9].

American Journal of Science, Engineering and Technology
2022; X(X): XX-XX
http://www.sciencepublishinggroup.com/j/ajset
doi: 10.11648/j.XXXX.2022XXXX.XX
ISSN: 2578-8345 (Print); ISSN: 2578-8353 (Online)

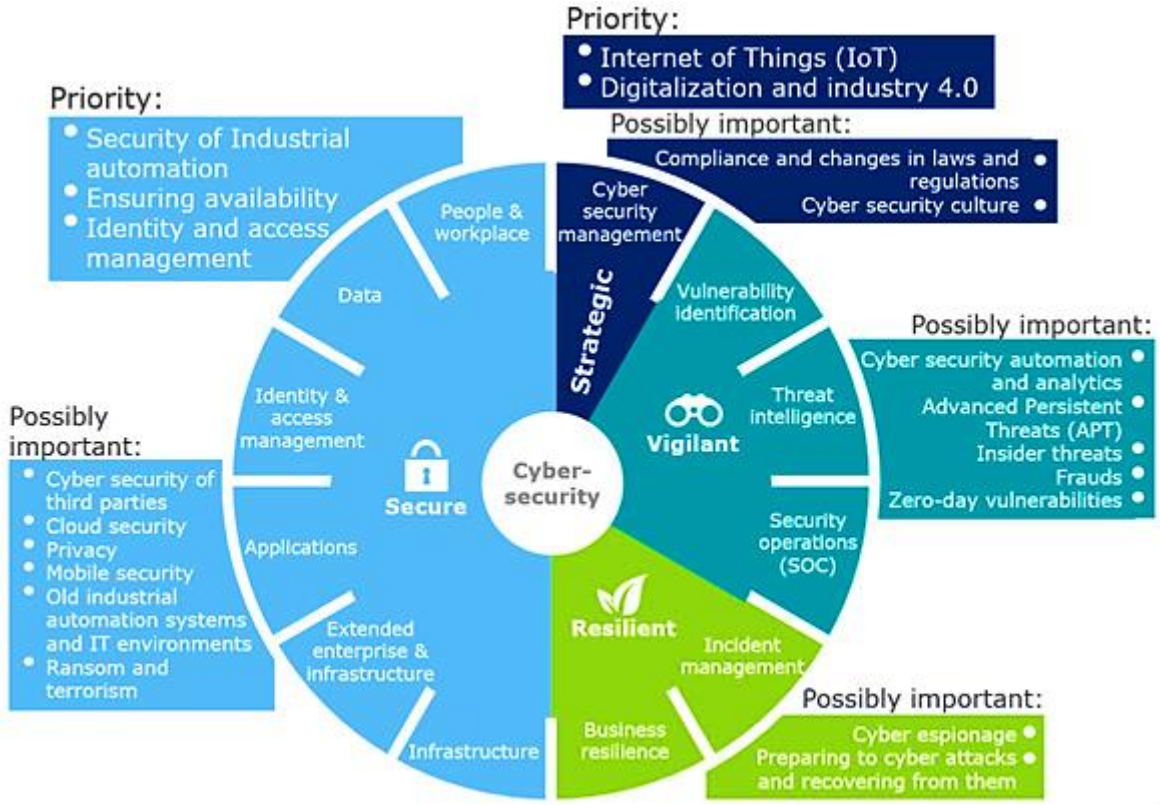

Figure 1. *Priorities of cyber security in manufacturing [12].*

Less significant cyber security related areas in this study that the manufacturing industry will not focus on as much in the future include at least executive commitment, reputation risk management, obstacles in cooperating with authorities, and cybersecurity measurement. Many of these items were deemed in good working order by the panel in 2021, and the work and costs associated with them are primarily maintenance-related. As a result, according to the panel, manufacturers will allocate resources and invest in additional cyber security problems in 2021.

Even though the experts had many of the same viewpoints as the literature, they did not choose some of the book's subjects as manufacturing priority for 2021. IoT, digitalization, and industry 4.0, for example, will be major drivers for cyber security in manufacturing in 2021, according to both literature and panelists [1].

Security of industry automation (ICS), identity and access management, and assuring availability were also listed as key problems. The Cyber Security Framework's Secure and Strategic categories covered the majority of these concerns. However, the Vigilant and Resilient categories included potentially critical concerns that both the panel and the literature study thought noteworthy. Increased usage of cyber security analytics and automation is an excellent illustration of this. Networking numerous self-governed microgrids (MGs) is emerging as one of the greatest options for improving power system resiliency and dependability. It has the ability to offer appropriate electric infrastructure to enable the use of cost-effective and environmentally-friendly electric power generated by distributed energy resources (DERs). MGs are entities that are meant to combine clusters of renewable and non-renewable distributed generation (DG) to provide loads within a set electrical border. In grid-connected mode, these MGs may sell their excess power to the distribution grid, or they can function autonomously in islanded mode. Solar photovoltaics (PV) panels and wind turbines (WTs) are examples of renewable DGs, whereas diesel engines (DEs), micro-turbines (MTs), fuel cells (FCs), and combined heat and power (CHP) plants are examples of non-renewable DGs [6, 10, 15]. Advanced control and communication technologies allow several MGs to work together with the distribution system (DS) to efficiently meet the day-to-day expanding electrical energy demand. Multiple MGs linked to the grid or to another grid-connected or isolated MG can provide more dependable and cost-effective electricity to users. It may also open up the possibility of a competitive auxiliary sector. During crises, the coordinated operation of numerous MGs can help restore power supply to the main grid by providing black-start support to conventional power plants, allowing essential loads to be supplied for extended periods of time [16]. Because multiple sources of uncertainty, such as load fluctuation, wind, and solar power generation variation, are included in the evaluation, energy management and coordination across MGs

becomes more difficult. Controlling the functioning of many MGs in collaboration with DSO is one of the most difficult tasks since it involves several difficulties with security, privacy, and uncertainty. The functioning of several MGs in a coordinated way is referred to as networked MGs in general. Several effective ways for optimum energy management, operation, and control of networked MGs in collaboration with the sy [4] stem's DSO have been developed. In, a bi-level programming technique based on the leader-follower strategy was presented for energy management of numerous MGs. Each MG in the developed system comprises of DERs and controlled loads at the lower level of the distribution center and high inertia dispatchable DG at the upper level. A cooperative and dynamic power dispatch system has been devised to satisfy load needs efficiently using many MGs inside a DS. In, a dynamic economic dispatch issue with numerous MGs was developed for minimizing PV power curtailment while protecting MG privacy [2].

In comparison to the literature, the panel did not appear to be under any particular pressure from rising real-time requirements. Even though the panelists admitted that in a hurry, the business might forget about cyber security, they seemed to believe that no one would intentionally violate cyber security if the secure habits and actions were made simple enough for them. Robots are cyber-physical systems that, depending on whether they're 'for use in industrial automation applications' or 'perform useful tasks for humans,' combine hardware and software components, network and communication processes, mechanical actuators, controllers, operating systems, and sensors to interact with the physical world [17]. In professional, public, private, or health-care settings, these complex systems are increasingly interacting with humans [19]. Industrial robots, warehouse robots, feeding robots, exoskeletons, assistants, socially interactive robots, robotic wheelchairs, and robotic surgeons are just a few examples [20]. These systems are distinguished by the fact that they create an interconnected structure where the virtual and physical worlds collide. The more interconnected systems and devices there are, the more opportunities for weaknesses to emerge, and the higher the risk of system failures or malicious attacks. Cloud services allow robots to offload heavy computational tasks such as navigation, speech, or object recognition to the cloud, and thus mitigate some of the limitations [18. To date, however, little is known about how an attacker can use a robot's computational parts to manipulate the physical environment in industrial, social, or medical settings , and what that means for the users involved in the interaction. While robotics manufacturers place a high value on safety, development costs, market timing, and customer-oriented features, some authors argue that consumers place a higher value on usability, functionality, and a competitive price [5, 7, 8]. Consumers are willing to prioritize and pay more for higher security when buying connected products, according to research, as long as the security level is communicated in a clear and understandable manner. Furthermore, security flaws in robots are a major source of concern for manufacturers, programmers, and those who interact with them in sensitive applications like healthcare. In a healthcare setting, robots interact with children, older adults, and people with disabilities in close, direct contact, and the target user may not know whether the robot is working properly or is under attack. Attackers can interfere with robot control and disrupt the manufacturing process. In the health sector, an attack on a healthcare robot could have a negative impact on people's health, well-being, and safety, which the Food and Drug Administration (FDA) in the United States has identified as an unresolved, major concern [2, 12, 14]. Outside of factories, interconnected 'things' and robots are relatively new, and safety legislation was mostly designed for things working in isolation, mostly in industrial environments. The revisions of these laws, particularly the General Product Safety Directive, are only planned for 2020. As if policymakers failed to recognize the link between cybersecurity and safety in the case of cyber-physical systems, such as products or medical devices, cybersecurity and safety concerns are frequently addressed in separate pieces of legislation [4, 8].

5. Conclusion

This study looked at cybersecurity challenges in the context of Industry 4.0, employing a systematic approach to the literature review and a qualitative examination of the contents of the articles that were chosen. The evaluation of the articles concentrated on four areas of examination. These areas include: (1) an examination of cybersecurity and Industry 4.0/IIoT definitions; (2) an examination of industry types and industrial assets most affected by cybersecurity issues; (3) a definition of system vulnerabilities, cyber threats, risks, and countermeasures to be taken in Industry 4.0 scenarios; and (4) the identification of guidelines and more structured solutions to deal with cybersecurity issues. As a consequence, each area's major elements were outlined in a reference framework. The framework gathers and summarizes the most referenced evidence for each area of investigation in order to provide an immediate possibility of synthesis that can be used to guide future research as well as management activities. Although a variety of solutions for dealing with cybersecurity challenges in Industry 4.0 have been created, none of them take into account the three exposure layers of Cyber-Physical Systems (physical, network, and compute) that might be exploited by cyber-attacks at the same time. Furthermore, the papers examined do not approach cybersecurity from a solely management standpoint, but rather from an IT standpoint. A management viewpoint should aid businesses in the proper adoption of new organizational practices and change management activities. Future research can use this study as a platform for addressing industry investigations and expanding the existing state of the art.

References

[1] Mosteanu, N. R., Artificial intelligence and cyber security–face to face with cyber attack–a maltese case of risk management approach. Ecoforum Journal, 2020. 9 (2).

[2] Soni, V. D., Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487, 2020.

[3] Patil, P., Artificial intelligence in cybersecurity. International journal of research in computer applications and robotics, 2016. 4(5): p. 1-5.

[4] Sagar, B., et al. Providing Cyber Security using Artificial Intelligence–A survey. in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019. IEEE.

[5] Sedjelmaci, H., et al., Cyber security based on artificial intelligence for cyber-physical systems. IEEE Network, 2020. 34 (3): p. 6-7.

[6] Mohammed, I. A., ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE. ARTIFICIAL INTELLIGENCE, 2020. 7(9).

[7] Yampolskiy, R. V. and M. Spellchecker, Artificial intelligence safety and cybersecurity: A timeline of AI failures. arXiv preprint arXiv:1610.07997, 2016.

[8] Morel, B. Artificial intelligence and the future of cybersecurity. in Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2011.

[9] Wirkuttis, N. and H. Klein, Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 2017. 1 (1): p. 103-119.

[10] Khisamova, Z. I., I. R. Begishev, and E. L. Sidorenko, Artificial intelligence and problems of ensuring cyber security. International Journal of Cyber Criminology, 2019. 13 (2): p. 564-577.

[11] Li, J.-h., Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 2018. 19 (12): p. 1462-1474.

[12] Taddeo, M., T. McCutcheon, and L. Floridi, Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 2019. 1 (12): p. 557-560.

[13] Zhang, Z., et al., Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 2021: p. 1-25.

[14] Truong, T. C., et al., Artificial intelligence and cybersecurity: Past, presence, and future, in Artificial intelligence and evolutionary computations in engineering systems. 2020, Springer. p. 351-363.

[15] Demertzis, K. and L. Iliadis, A bio-inspired hybrid artificial intelligence framework for cyber security, in Computation, cryptography, and network security. 2015, Springer. p. 161-193.

[16] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, *6*(3), 52-63.

[17] Ghelani, D., Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain.

[18] Oak, R., Du, M., Yan, D., Takawale, H., & Amit, I. (2019, November). Malware detection on highly imbalanced data through sequence modeling. In Proceedings of the 12th ACM Workshop on artificial intelligence and security (pp. 37-48).

[19] Hua, T. K., & Biruk, V. (2021). *Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand*. Partridge Publishing Singapore.

[20] Ughulu, D. (2022). The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs. *ScienceOpen Preprints*.

[21] Ughulu, J. Entrepreneurship as a Major Driver of Wealth Creation.

[22] Dr. John Ughulu. The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs.. *ScienceOpen Preprints.* DOI: 10.14293/S2199-1006.1.SOR-.PP5ZKWJ.v1

[23] Ghelani, D. and T. K. Hua, A Perspective Review on Online Food Shop Management System and Impacts on Business.