An Interpretive Analysis on Security Measures and its Deployment in Web Based Applications

Aditya Mahto,Saloni Manhas

Department of Computer Applications

Chandigarh School of Business

Chandigarh Group of Colleges, Jhanjeri, Mohali, India

Aditykr14324@gmail.com,salonithakur786@gmail.com

Abstract:

Extensive literature from academic and industry sources offers valuable insights into the realm of information security. Despite the availability of various tactics such as deterrence, deception, detection, and response, the majority of research concentrates on technological solutions aimed at thwarting threats. This article discusses the outcomes of a qualitative study conducted in Korea that investigates the security practices adopted by businesses to protect their information systems. The study highlights a predominant focus on preventive measures, driven by the objective of sustaining the availability of technology and services, alongside a limited awareness of enterprise security challenges. While alternative strategies were acknowledged, they mainly functioned as supplementary preventive measures. The article introduces a research blueprint for integrating diverse security strategies across organizations, stressing the importance of harmonizing and optimizing security mechanisms. The investigation delved into various aspects of information security, encompassing deliberations on security tactics in domains like military contexts. Nine unique security methodologies were pinpointed, and a qualitative focus group approach was utilized to probe their deployment within organizations. Participants, comprising security managers from eight organizations, indicated a prevalent inclination towards preventive measures to uphold continuous technology services. The identified strategies, beyond prevention, were principally leveraged to bolster the primary preventive approach at an operational scale.

Keywords: Information Security, Cyber
Threats, Web 3.0, Implications

1. Introduction

In today's rapidly evolving business landscape, organizations are

increasingly recognizing the significance of information and technology across various functions, especially in fostering innovation and gaining a competitive edge. However, corporate information and technology infrastructures are susceptible to a myriad of security threats in the current digital era, ranging from data breaches to prolonged interruptions in essential services like email and internet access, which can severely disrupt business operations. To mitigate these risks, organizations need to formulate a robust information security strategy that encompasses a comprehensive framework for developing, institutionalizing, evaluating, and enhancing their information security programs. This strategy should align with the organization's overarching strategic objectives, ensuring its relevance and traceability to higher-level directives [1]. Despite the prevalent use of basic security measures by many organizations, there is a rising trend in security incidents. Research indicates that over 60% of businesses employ technical security countermeasures, such as antivirus solutions, firewalls, anti-spyware tools, VPNs, vulnerability management, data encryption, and intrusion detection systems. Moreover, these studies highlight the persistent nature of targeted attacks against organizations and the escalating security risks stemming from both internal and external threats, making security management increasingly complex. In this challenging landscape, businesses need to strategically allocate their security resources to maximize effectiveness. However, relying solely on a single security system may not suffice [1]. Therefore, to enhance the efficacy of security measures and uphold security policies, organizations should adopt a multifaceted approach to information security. While existing literature predominantly emphasizes the operational facets of information security, focusing on preventive controls and their implementation, it also introduces alternative security strategies, including detection, deterrence, and deception. Nevertheless, empirical research examining the adoption and implementation of these security strategies by organizations remains limited [2]. Often, business security risks are overlooked, with security managers frequently adopting ad hoc approaches rather than adopting a systematic and planned risk management strategy [3, 4].

2. Literature Review

Strategy is often conceptualized as the process of determining the means to be employed, how to leverage them effectively, and their application in specific contexts, such as military

operations. Beckman and Rosenfield (2008) define strategy as the act of "deciding the direction in which a business aims to progress and identifying the means to achieve this goal." These conceptualizations can be adapted to formulate an information security strategy. In line with these perspectives, Perk et al. define information security strategy as the "skillful selection and deployment of appropriate defensive technologies and measures in a coordinated manner to safeguard an organization's information infrastructure against both internal and external threats, ensuring confidentiality, integrity, and availability while optimizing efforts and costs." Various methods such as deterrence, prevention, surveillance, detection, response, deception, perimeter defense, compartmentalization, and layering have been identified through research [1-5].

From the literature review, two fundamental elements of strategies emerge: timing and spatial considerations. Strategies can be implemented proactively, before an incident occurs, or reactively, in response to an attack. The spatial configuration of the 'battlefield' environment is crucial, emphasizing the importance of spatial segmentation to distinguish between trusted and untrusted computing systems. For instance, segmenting the battlefield into distinct zones can prevent unauthorized access from untrusted systems into secure areas. Additionally, the selection of specific attack and response strategies significantly influences decision-making in strategy formulation. Subsequent sections will further elucidate this literature-based approach [1, 2, 6, 7].

2.1. Prevention (PREV)

The primary goal of prevention is to prevent unauthorized access, modification, destruction, or disclosure of information assets. A prevention-centric information security approach adopts a strict zerotolerance stance towards compromises, necessitating the implementation of strong countermeasures to fend off potential threats. Measures like enforcing a clean desk policy through regular inspections for misplaced or confidential documents can help reduce the risks of information leakage. Proactive technological safeguards can be implemented around vital assets. Authentication protocols, restricting access to authorized users, represent commonly used preventive strategies. Utilizing software to control user interactions with information assets, encrypting data during transit to safeguard against unauthorized exposure even in compromised environments, deploying firewalls to screen network traffic, and utilizing intrusion detection systems employing both anomaly and signature-based detection to identify potential threats are additional preventive tactics.

Regular vulnerability assessments and prompt remediation further bolster preventive measures [8, 9].

2.2. Deterrence (DETER)

Deterrence employs disciplinary measures to shape human behavior and attitudes towards adhering to security protocols. The efficacy of deterrence within organizational settings depends on two critical elements: the certainty and severity of consequences. The transparency of repercussions and the capability of enforcement entities to detect and address breaches determine the certainty of sanctions. The variety of available sanctions affects the severity of penalties imposed. Deterrence strategies often target employees who breach security protocols. Implementing educational and training initiatives to acquaint employees with organizational policies and norms can amplify the impact of information security efforts, as advocated by Straub and Welke (1998). Research by Straub (1990) suggests that deterrence approaches, encompassing strict penalties, awareness of deterrence mechanisms, and the presence of security personnel, contribute to diminishing computer misuse. Conversely, findings from Kankanhalli et al. (2003) imply that the severity of penalties exerts limited influence on deterrence effectiveness. In contrast, D'Arcy et al. (2009) observed a notable impact of sanctions severity on deterrence efficacy. Organizations should prioritize compliance training and strict enforcement of security policies to discourage policy breaches [7].

2.3. Surveillance (SURV)

Surveillance entails ongoing monitoring of the security environment to develop situational awareness and respond swiftly to emerging threats and situations. Situational awareness enables security decision-makers to adeptly tackle data security issues and devise robust protective measures.

Monitoring an organization's security status across both physical and digital realms using a blend of technological and procedural strategies presents challenges. Monitoring access to restricted physical and logical zones housing both hardcopy and digital data constitutes a vital component of overseeing interactions with information systems. Surveillance often leverages data gathered by strategically deployed "sensors" and visualization tools to provide security managers with enhanced situational insights. Data sources for surveillance typically include systems and application software, such as intrusion detection systems, offering detailed information on attack frequency, scale, and characteristics [6].

2.4. Detection (DETECT)

Detection serves as an operational technique focused on identifying

specific security incidents promptly. The primary objective of detection is to enable targeted responses to security incidents. Unlike surveillance, which aims for a holistic understanding of the security landscape, detection zeroes in on individual events. Examples of detection include recognizing abnormal or suspicious behaviors, identifying intrusions or misuse, and pinpointing specific attacks targeting web servers. Detection can also serve to gather evidence of suspicious activities and identify perpetrators [15]. Security technologies employed in the detection approach encompass dedicated intrusion detection systems for computers and networks, network and system scanners, anomaly and abuse detectors, content filtering and antivirus solutions, as well as audit tools. Since the advent of information and communication technology, businesses have undergone a transformation, shifting their focus from tangible assets and monetary resources to intellectual capital [1]. This shift has given rise to what Kuehl (2009) refers to as the "first man-made domain." Businesses now leverage the cyber domain's unique attributes, such as reduced time and geographical constraints, to enable innovative business models. However, this increased reliance on the cyber domain also exposes organizations to escalating cyber risks, jeopardizing their security, stability, and long-term viability by undermining the confidentiality, integrity, and availability of their informational and structural assets [6].

The potential impact of cyber risks ranges from disrupting organizational operations to incapacitating national infrastructures. Organizations, being both creators and users of technology, often position themselves as central players in cybersecurity discussions, even when addressing broader societal cybersecurity impacts. Despite the critical role of cybersecurity in safeguarding intellectual assets and operational continuity, it is often perceived as a secondary concern due to its limited potential for direct monetization. The nature of cybersecurity is inherently continuous and complex, representing an ongoing "war" rather than a series of isolated "battles" that can be definitively won. Consequently, cybersecurity presents an enduring challenge that requires continuous management and adaptation [4, 10-12].

Intellectual capital, cybersecurity expertise, and knowledge management are integral components of successful businesses. The concept of "knowledge" permeates both cybersecurity and organizational risk discussions. Neef (2005) argues that an organization's ability to manage risk effectively is contingent on its competence in handling relevant knowledge. Tisdale (2015) emphasizes the importance of multidimensional approaches to cybersecurity that transcend traditional technical viewpoints, focusing instead on system

complexity and knowledge management. The ability to address threats to
"the creation and deployment of organizational knowledge" is crucial in an Information Security (IS) context. Julisch (2013) identifies a correlation between knowledge limitations and ineffective cybersecurity strategies, characterized by excessive reliance on intuition, lack of foundational security principles, inadequate governance, or reliance on static and generic knowledge.

In a broader context, knowledge management practices inherently constrain the generation of organizational value based on intellectual capital. Corporate cybersecurity management, aiming to protect intellectual assets and enable operational continuity, serves as a mediator in the value creation process, intersecting with knowledge management [4, 13]. These studies exhibit significant epistemic diversity, reflecting their distinct disciplinary backgrounds, while sharing a consistent, complementary message. This diversity may obscure the collective narrative but does not necessarily diminish the value of individual contributions. A lack of uniform interpretation restricts the consistency of insights and prescriptive value that a phenomenon-focused approach could potentially achieve over a discipline-centric approach. The former allows for a comprehensive examination of organizational cybersecurity, emphasizing technology, human factors, and processes, focusing on competitiveness, intellectual capital, and long-term value creation. Although intellectual capital is a wellestablished research area, it continues to evolve in response to shifts in social, economic, and technological landscapes [1-6, 8, 11].

According to the definition, intellectual capital represents "the collective knowledge possessed by an organization that provides it with a competitive edge." Most experts acknowledge the importance of intellectual capital in value creation, defining it as "intellectual material, knowledge, expertise, intellectual property, and information that can be leveraged to generate value." This perspective necessitates a broader view of intellectual capital research, extending beyond individual organizations to encompass the broader ecosystem in which knowledge and value are generated. Cybersecurity threats emerge from the complex interplay of factors shaping organizational ecosystems, such as internal processes, competitive dynamics, and value creation mechanisms. Consequently, a simplistic technical perspective on cybersecurity falls short, failing to consider emergent socio-technical organizational mechanisms and processes that encompass the organization's human, relational, and

structural capital, which support value creation. Therefore, we argue that a knowledge-centric approach to cybersecurity and its management can directly influence intellectual capital management by shaping the dynamics of human, relational, structural, renewal, and trust capital [9, 10].

3. Knowledge, Strategy, and Cybersecurity

Over the past three decades, various interpretations of knowledge have underpinned several key streams within strategic management and organizational theory. Notable concepts include the knowledge-based view of the firm, dynamic capabilities, and knowledge management.

However, the effectiveness of these approaches has been subject to scrutiny due to several factors, including ambiguous or contested definitions of knowledge, varying perceived practical applicability, fragmented themes that dilute the original progressive vision, and an inherent difficulty in avoiding oversimplification.

When examining the application of "knowledge" within an epistemic framework for organizational cybersecurity strategy, this historical context of utilizing knowledge as an explanatory or prescriptive tool unveils consistent patterns. Identifying the elements that define an "effective" or enduring epistemic foundation for concepts in organizational theory is a complex theoretical pursuit. Nonetheless, the extensive body of literature on this topic offers insights into critical characteristics that contextualize individual conceptualizations within a broader framework.

The epistemological stance, which dictates the source of knowledge (i.e., the knower), its form or manifestation (the known), and the nature, function, and attainability of truth, are intrinsically linked. Additionally, we recognize the contextual relevance of the relational positioning of uncertainty [5, 8].

4. Pragmatism in Epistemology

In the realm of strategy, truths are seldom absolute or definitive, and our desires cannot alter this fundamental reality. This unyielding aspect must be integrated into any philosophical foundation upon which a system is constructed, whether it leans towards pragmatism or otherwise. The evolving discourse positions our understanding of knowledge at the intersection of pragmatism and critical realism. Given its pronounced evolutionary and competitive orientation, the epistemological importance of action and utility, and the focal point and

entity of knowledge, we characterize this viewpoint as "bottom-up" pragmatism. Unlike scientific inquiry, organizational knowledge is adaptive, serving to enhance and sustain value creation. This adaptability is particularly pertinent to cybersecurity, a service that typically lacks direct monetization potential but safeguards Intellectual Capital and operationalization processes. Consequently, concepts like certainty, confidence, and truth are reframed. Knowledge is seen as emerging from the dynamic interplay between the subject and the object under scrutiny, shifting the emphasis from an abstract, conventional understanding of reality to a more dynamic, evolutionary perspective [1, 12, 14].

The industrial sector in developed nations is increasingly dependent on digital networks and services, a trend expected to intensify rather than diminish. While cybersecurity facilitates digitization, inadequate management can negate its benefits entirely. Cybersecurity measures must be proactive; reacting post-cyberattack is too late and may result in irreversible damage. With the manufacturing industry's global expansion, companies face both opportunities and challenges in a continually evolving global landscape. Cybersecurity is no longer confined to IT departments; its importance is acknowledged in corporate boardrooms, with executive attention anticipated to escalate [6, 10].

Emerging technologies in industrial settings introduce new cyber threats, as hackers exploit vulnerabilities in legacy systems, technologies, and processes. Finnish national cybersecurity policy emphasizes the need for proactive operations and planning to mitigate cybersecurity risks. The evolving landscape demands knowledge and swift, consistent responses. Achieving proactive cybersecurity requires high-quality research encompassing perspectives from various industries. This study examines cybersecurity prospects from Finnish manufacturing organizations' standpoint, focusing on 2021 priorities, shifting priorities, and imminent challenges. The study employs a 4-5 year timeframe as a strategic planning benchmark. Ignoring cybersecurity can be financially devastating for organizations, with data breaches costing victim firms an average of $473 million. The repercussions of breaches are multifaceted and long-lasting. Security experts are acutely aware of these potential costs. Over the next five years, the manufacturing industry will grapple with challenges posed by increasingly interconnected equipment, digitalization, and network user management issues. A literature review underpinning the Delphi study's findings is discussed in the subsequent section, followed by conclusions drawn from the Delphi study [2, 8, 10].

The report concludes by highlighting the study's implications for the manufacturing industry and the broader cybersecurity community. Panelists were asked to define cybersecurity from their vantage point in the initial round, yielding a range of responses. These varied perspectives were synthesized into a unified definition: cybersecurity is essentially an extension of information security, with the 'cyber' prefix expanding its scope to encompass IoT and industrial contexts. The panel endorsed this definition in subsequent rounds. Several experts identified three key components of cybersecurity: processes, people, and technology. Some panelists also noted that cybersecurity issues now permeate the physical world, suggesting potential risks to human life through targeting critical industrial systems [9].

5. Conclusion

This study delved into cybersecurity challenges within the framework of Industry 4.0, employing a systematic literature review and qualitative analysis of selected articles. The assessment of the articles focused on four key areas: (1) defining cybersecurity in the context of Industry 4.0/IIoT; (2) identifying industry types and industrial assets most susceptible to cybersecurity threats; (3) outlining system vulnerabilities, cyber threats, risks, and corresponding countermeasures in Industry 4.0 scenarios; and (4) pinpointing guidelines and structured solutions to address cybersecurity challenges.

Consequently, the major components of each area were delineated within a reference framework. This framework consolidates and summarizes the most cited evidence for each investigative area, offering an immediate synthesis that can guide future research and management endeavors. Despite the development of numerous solutions to address cybersecurity challenges in Industry 4.0, none comprehensively consider the three exposure layers of Cyber-Physical Systems (physical, network, and compute) that may be simultaneously exploited by cyberattacks.

Moreover, the reviewed papers predominantly approached cybersecurity from an IT perspective rather than a management standpoint. A managerial perspective could assist businesses in effectively adopting new organizational practices and implementing change management initiatives. Future research can utilize this study as a foundational platform for industry-specific investigations and to advance the current state of knowledge in the field.

6. 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] Manhas, S. (2022). An Interpretive Saga of SQL Injection Attacks. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 1(pp. 3-12). Singapore: Springer Nature Singapore.

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

[6] Manhas, S. (2021, December). Ontology of XSS Vulnerabilities and its Detection using XENOTIX Framework. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 320-323). IEEE.

[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.103119.

[10] Manhas, S., & Taterh, S. (2018). A Comparative Analysis of Various Vulnerabilities Occur in Google Chrome. In Soft Computing: Theories and Applications: Proceedings of SoCTA 2016, Volume 1 (pp. 51-59). Springer Singapore.

[11] International Journal of Cyber Criminology, 2019. 13 (2): p.564-577.

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

[13] 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.

[14] Manhas, S., Taterh, S., & Singh, D. (2020). Deep Q learning-based mitigation of man in the middle attack over secure sockets layer websites. Modern Physics Letters B, 34(32), 2050366.

[15] 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.

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

[17] Manhas, S., Taterh, S., & Singh, D. (2019). A Novel Approachfor Phishing Websites Detection using Decision Tree.

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

[19] 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).

[20] 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.

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

[22] Dr. John Ughulu. The role of Artificial intelligence (AI) inStarting, 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.