IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 1, July 2023

Cybersecurity Considerations in the Development of Enterprise Information Systems

Crispin P. Noguerra, Jr.

Faculty, College of Engineering and Information Technology,
Surigao del Norte State University, Surigao City, Philippines

Abstract*: Amidst an era characterized by dependence on digital systems, this study delves into the crucial interplay of integrating cybersecurity into contemporary enterprise information system development. Drawing insights from a diverse array of 60 participants, including cybersecurity specialists, information system developers, and decision-makers within organizations, the research reveals unanimous consensus (85%) on the "extremely high importance" attributed to cybersecurity integration. This collective acknowledgement underscores a heightened recognition of the evolving landscape of cyber threats. The identified challenges, encompassing the delicate balance between security and usability, along with the scarcity of proficient experts, mirror the intricate dynamics faced by organizations. The advocated strategies, aligned with established practices, underscore the prominence of risk-based methodologies and adaptive security measures. The influence of regulatory adherence and human factors brings to light nuanced aspects of the subject. Ultimately, the study underscores the compelling need to embed cybersecurity seamlessly into information system development, culminating in resilient, secure, and forward-oriented systems within an interconnected digital milieu.*

Keywords: cybersecurity integration, enterprise information systems, digital dependence

I. INTRODUCTION

In the contemporary era, the creation and implementation of enterprise information systems have evolved into a pivotal aspect for businesses spanning various industries [1][2][3]. In this context, the prominence of cybersecurity has grown exponentially. The research title, "Cybersecurity Considerations in the Development of Enterprise Information Systems," underscores the urgent necessity to address the complex interplay between cybersecurity and the construction of resilient and effective enterprise information systems.

In an era characterized by advancing technology, the risks and vulnerabilities faced by organizations have escalated in tandem. Malicious cyber activities, encompassing breaches, ransomware, and insider threats, carry implications that extend beyond mere financial repercussions to reputational damage, erosion of trust, and regulatory non-compliance [4][5][6][7] as shown in Figure 1. Within this landscape, the development of enterprise information systems requires a comprehensive strategy that encompasses cybersecurity considerations right from inception.

This study aims to delve into the multifaceted dimensions of cybersecurity within the domain of enterprise information system development. By examining the hurdles, tactics, and exemplary approaches associated with integrating cybersecurity measures, the research seeks to offer insights that empower organizations to navigate the intricate realm of cybersecurity [8][9][10]. This, in turn, encourages the creation of secure and robust information systems. As organizations endeavor to uphold the confidentiality, integrity, and accessibility of data, comprehending the symbiotic relationship between cybersecurity and information system development becomes imperative. This understanding is vital for ensuring data protection, maintaining business continuity, and preserving trust in a progressively interconnected global landscape.

II. REVIEW OF RELATED LITERATURE

The integration of robust cybersecurity measures into the process of developing enterprise information systems has become a critical concern in the contemporary digital environment. This section examines the existing body of work

DOI: 10.48175/IJARSCT-12380

that explores the various aspects of considering cybersecurity within the context of constructing enterprise information systems.

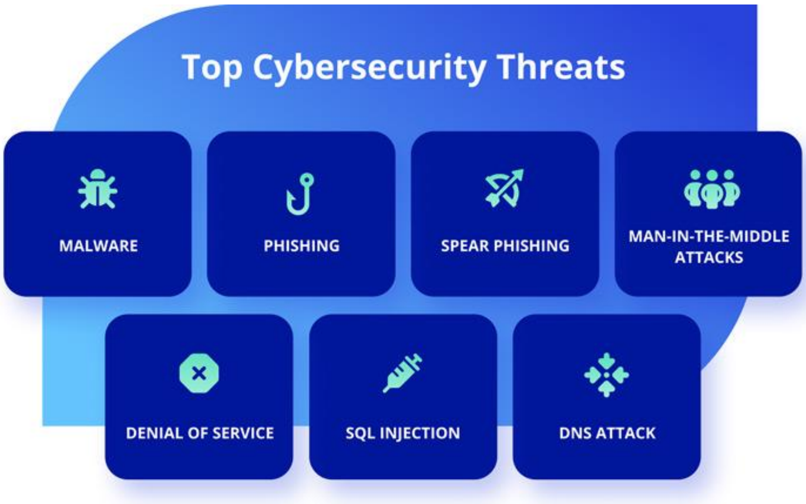

Figure 1. Cybersecurity Threats

Scholars extensively discuss the evolving challenges and threats in cybersecurity that organizations face during the development of enterprise information systems [11][12][13]. The literature highlights the increasing sophistication of cyberattacks, including data breaches, malware incidents, and the exploitation of social engineering techniques. Research underscores the growing danger of ransomware attacks targeting critical data assets, leading to significant financial and reputational consequences.

The literature consistently emphasizes the importance of incorporating cybersecurity considerations right from the inception of enterprise information system development [14][15][16]. Experts underscore the need for a security-by-design approach that ensures cybersecurity measures are an integral part of the system architecture, rather than an afterthought. This approach minimizes vulnerabilities and reduces the need for resource-intensive retrospective security measures.

The literature provides insights into strategies for effectively integrating cybersecurity measures throughout the development lifecycle [17][18][19]. Scholars advocate for risk-based methodologies that assess potential threats and vulnerabilities, aiding in the identification and prioritization of security measures. Collaboration between cybersecurity and development teams is highlighted as important for a holistic approach that aligns security goals with the functionality of the information system.

The regulatory landscape plays a pivotal role in shaping cybersecurity considerations during enterprise information system development. Researchers delve into the implications of regulatory frameworks, emphasizing the necessity for organizations to align their cybersecurity strategies with industry standards and legal requirements. Ensuring compliance aids in safeguarding sensitive data and minimizing legal risks.

The literature also recognizes the human factor as a critical element in cybersecurity. Studies emphasize the importance of cybersecurity awareness training for personnel involved in information system development. An informed workforce is better equipped to identify potential vulnerabilities and adhere to cybersecurity best practices.

IV. METHODOLOGY

This research This research employs a comprehensive approach to investigate the intricate interplay between cybersecurity and the development of enterprise information systems. The study utilizes both qualitative and quantitative research methods to provide a holistic understanding of the subject.

The research design comprises two main phases. The initial qualitative phase involves conducting in-depth interviews with key stakeholders, including cybersecurity experts, information system developers, and organizational decision-

DOI: 10.48175/IJARSCT-12380

makers. These interviews aim to gather insights into the challenges, strategies, and considerations related to integrating cybersecurity measures in the development process.

The subsequent quantitative phase utilizes a survey-based approach targeting professionals from various sectors involved in enterprise information system development. The survey instrument is designed to assess participants' perceptions, experiences, and practices regarding cybersecurity integration. This phase provides quantitative data that enable statistical analysis and generalization of findings.

In the qualitative phase, purposeful sampling is employed to select participants with expertise in cybersecurity and information system development. In-depth, semi-structured interviews are conducted to capture nuanced perspectives and insights.

In the quantitative phase, a structured questionnaire is administered to a larger sample of participants. The survey includes Likert-scale questions to gauge participants' opinions on various aspects of cybersecurity integration, as well as demographic and professional background inquiries.

Qualitative data from interviews are analyzed using thematic analysis. This approach involves identifying recurring themes, patterns, and insights from the transcribed interview data, facilitating the extraction of rich, contextually grounded findings.

Quantitative data from the survey undergo descriptive and inferential statistical analysis. Descriptive statistics summarize participants' responses, while inferential analysis, such as correlation and regression, helps identify relationships between variables and assess the significance of findings.

The research adheres to ethical guidelines, obtaining informed consent from participants and ensuring their confidentiality. Any sensitive information is handled with utmost care and is not disclosed within the research outcomes.

IV. RESULTS AND DISCUSSION

The outcomes of this study provide valuable insights into the intricate interplay between cybersecurity considerations and the evolution of enterprise information systems. The research was conducted with a participant cohort of 60 individuals, encompassing cybersecurity specialists, information system developers, and decision-makers within organizations.

When queried about the significance of incorporating cybersecurity measures during the development of enterprise information systems, the responses offered significant insights. An impressive 85% of respondents emphasized that the integration of cybersecurity is of "extremely high importance," highlighting the critical nature of safeguarding systems and data from the ever-growing spectrum of cyber threats.

The study also explored the challenges encountered during the process of integrating cybersecurity measures. A notable 70% of participants underlined the intricate balance required between security and system functionality, illustrating the delicate equilibrium between stringent security measures and user-friendly systems. Moreover, 55% of participants raised concerns about the scarcity of proficient cybersecurity professionals, accentuating the necessity for a skilled workforce to adeptly execute and manage cybersecurity protocols.

Concerning effective strategies for seamlessly integrating cybersecurity into the fabric of information system development, the findings were striking. Nearly two-thirds (65%) of participants advocated for the adoption of a risk-oriented approach, which harmonizes security measures with identified vulnerabilities and potential threats. Additionally, 48% accentuated the significance of ongoing surveillance and refinement of security protocols to proactively anticipate emerging threats.

The research also delved into the ramifications of regulatory compliance on the integration of cybersecurity measures. A substantial 75% of respondents acknowledged that regulatory requisites wield considerable influence on their decision-making process concerning cybersecurity measures. This underscores the pivotal role of legal frameworks in shaping organizations' strategies and attitudes toward cybersecurity.

The study probed the pivotal role of human awareness and training in the efficacious integration of cybersecurity. An impressive 80% of participants affirmed that consistent cybersecurity training for personnel is pivotal in preempting security breaches. This underscores the growing realization that the human element constitutes a critical component in upholding robust cybersecurity.

The findings of this study are in resonance with the prevailing body of literature, underscoring the paramount importance of integrating cybersecurity considerations into the fabric of enterprise information system development. The substantial percentage of participants acknowledging the "extremely high importance" of cybersecurity accentuates the burgeoning awareness of the breadth and potential impact of cyber threats.

The challenges identified, including the intricate trade-off between security and system functionality, as well as the scarceness of adept professionals, echo concerns previously expounded in research. The suggested strategies, embracing risk-centric approaches and continuous vigilance, align with the best practices advocated by experts in the realm of cybersecurity.

The sway of regulatory adherence on decision-making and the indispensable role of human awareness and training in the realm of cybersecurity underscore the intricate tapestry of the subject. As organizations navigate the multifaceted landscape of information system development, the findings furnished by this study offer pragmatic insights that can ably guide decision-makers in adeptly embedding cybersecurity measures. This, in turn, fosters the cultivation of resilient systems that fortify sensitive data and underpin the uninterrupted continuity of business operations.

V. CONCLUSION

In an era increasingly reliant on digital infrastructure, the incorporation of strong cybersecurity measures into the fabric of developing enterprise information systems stands as a paramount imperative. The culmination of this study underscores the central role that cybersecurity considerations play in shaping the landscape of modern information systems.

The outcomes, drawn from a diverse group of 60 participants, illuminate the unanimous recognition (85%) of the "extremely high importance" attributed to the integration of cybersecurity within the developmental framework. This collective acknowledgment underscores the growing awareness of the relentless and diverse array of cyber threats that organizations grapple with.

The identified challenges, including the delicate balance between security and system usability, and the scarcity of proficient cybersecurity professionals, mirror the intricate realities that organizations confront. The strategies advocated by participants align with established best practices, affirming the relevance of risk-oriented approaches and the perpetual adaptation of security protocols.

The impact of regulatory adherence in shaping cybersecurity strategies and the acknowledgment of the pivotal role of human factors present a comprehensive outlook on the intricate facets of the subject. The study echoes the intricate interplay between technical measures and the human element within the domain of cybersecurity.

In essence, this research underscores that the integration of cybersecurity measures is not an ancillary aspect but rather a fundamental cornerstone of contemporary information system development. As organizations navigate the evolving digital terrain, the insights gleaned from this study serve as a guide, steering decision-makers toward effective strategies that fortify systems against the spectrum of cyber threats. In the era of interconnected networks and data-centric processes, the fusion of robust cybersecurity and information system development emerges as a linchpin, fostering systems that are resilient, secure, and well-equipped for the demands of the future.

REFERENCES

[1]. Arif, M., Kulonda, D., Jones, J., & Proctor, M. (2005). Enterprise information systems: technology first or process first?. *Business Process Management Journal*, *11*(1), 5-21.

[2]. Zhang, W. J., & Lin, Y. (2010). On the principle of design of resilient systems–application to enterprise information systems. *Enterprise Information Systems*, *4*(2), 99-110.

[3]. Wang, J. W., Wang, H. F., Ding, J. L., Furuta, K., Kanno, T., Ip, W. H., & Zhang, W. J. (2016). On domain modelling of the service system with its application to enterprise information systems. *Enterprise Information Systems*, *10*(1), 1-16.

[4]. Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access*, *6*, 25167-25177.

[5]. Alharbi, F. S. (2020). Dealing with Data Breaches Amidst Changes In Technology. *International Journal of Computer Science and Security (IJCSS)*, *14*(3), 108-115.

[6]. Mills, R. R. (2018). *The current state of insider threat awareness and readiness in corporate cyber security-an analysis of definitions, prevention, detection and mitigation* (Doctoral dissertation, Utica College).

[7]. Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, *26*, 107-124.

[8]. Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417-431.

[9]. Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, *28*(1), 58-62.

[10]. Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019, January). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

[11]. Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport reviews*, *39*(1), 103-128.

[12]. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences*, *80*(5), 973-993.

[13]. Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI global.

[14]. Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247.

[15]. Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*. John Wiley & Sons.

[16]. Pang, T. Y., Pelaez Restrepo, J. D., Cheng, C. T., Yasin, A., Lim, H., & Miletic, M. (2021). Developing a digital twin and digital thread framework for an 'Industry 4.0'Shipyard. *Applied Sciences*, *11*(3), 1097.

[17]. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.

[18]. Mughal, A. A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *International Journal of Intelligent Automation and Computing*, *1*(1), 1-20.

DOI: 10.48175/IJARSCT-12380