International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

EMBEDDING CYBERSECURITY RISK MANAGEMENT INTO INFORMATION SYSTEMS GOVERNANCE: A NATIONAL-SCALE FRAMEWORK FOR ORGANIZATIONAL RESILIENCE, ECONOMIC STABILITY, AND CRITICAL INFRASTRUCTURE PROTECTION

[1]Syed Nazmul Hasan, [2]Partha Chakraborty*, [3]Md Talha Bin Ansar, [4]Md Kazi Tuhin, [5]Md Abubokor Siam, [6]Jobanpreet kaur, [7]Jahid Hassan, [8]Clinton Ronjon Barikdar

College of Technology & Engineering, Westcliff University, Irvine, California, USA
Email: s.hasan.104@westcliff.edu
ORCID ID: https://orcid.org/0009-0008-0977-595X

School of Business, International American University, Los Angeles, California, USA
Email: parthachk64@gmail.com
ORCID ID: https://orcid.org/0009-0006-3203-8902

Katz School of Science and Health, Yeshiva University, New York, USA
Email: mtalhabi@mail.yu.edu
ORCID ID: https://orcid.org/0009-0007-8160-7275

Katz School of Science and Health, Yeshiva University, New York, USA
Email: muhammadkazituhin@gmail.com
ORCID ID: https://orcid.org/0009-0002-6914-6182

College of Business, Westcliff University, Irvine, CA 92614, USA
Email: m.siam.263@westcliff.edu
ORCID ID: https://orcid.org/0009-0001-5250-4652

College of Technology & Engineering, Westcliff University, Irvine, California, USA
Email: j.kaur.244@westcliff.edu
ORCID ID: https://orcid.org/0009-0008-0083-8205

Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, USA
Email: jhassan44582@ucumberlands.edu
ORCID ID: https://orcid.org/0009-0005-0215-3179

School of Business, International American University, Los Angeles, California, USA
Email: barikdarclinton@gmail.com
ORCID ID: https://orcid.org/0009-0002-6291-2446

*Corresponding Author: Partha Chakraborty

Abstract

This paper investigates how integrating cybersecurity risk management into Information Systems (IS) governance enhances organizational resilience. As technology becomes more central to operations and cyber threats grow in complexity, organizations face increasing difficulties in maintaining secure operations. Utilizing systems theory, this study presents a holistic framework that aligns business objectives with IT strategies, underscoring the importance of a resilient and adaptable cybersecurity posture. The research draws on a

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
comprehensive review of current cybersecurity literature, existing frameworks, and industry practices, offering a practical guide for organizations to manage cyber risks effectively. The proposed Cybersecurity Resilience Framework integrates governance principles, continuous monitoring, stakeholder engagement, and human behavioral factors to offer a comprehensive approach. Results from this study indicate that organizations using automated detection systems experience an average response time of 20 minutes compared to 31 minutes for those relying on manual detection. Furthermore, organizations with automated systems faced reduced operational downtime (4 hours compared to 6 hours) and lower financial impact ($150,000 versus $250,000). The research also shows that organizations adhering to established frameworks such as NIST and ISO saw improved threat detection rates (over 80%) and a notable reduction in financial losses (around 20%). The analysis of Return on Security Investment (ROSI) revealed that organizations investing strategically in cybersecurity saved significantly on costs, with ROSI percentages ranging from 28% to 61%. Additionally, organizations demonstrated enhanced capacity in threat detection and response, with Cybersecurity Effectiveness Scores (CES) reflecting strong operational readiness. Overall, this framework provides a robust strategy for organizations to navigate the dynamic cybersecurity landscape while ensuring business continuity.

Keywords: Cybersecurity Risk Management, Information Systems Governance, Organizational Resilience, Cybersecurity Resilience Framework, Automated Threat Detection, Return on Security Investment (ROSI)

1. Introduction

The rapid expansion of digital technologies has transformed how organizations manage their information systems, but it has also exposed them to increasing cybersecurity risks. As organizations rely more on interconnected systems and cloud services, the attack surface for potential cyber threats grows, making them more vulnerable to breaches, ransomware, and data theft [1, 2]. Traditionally, cybersecurity risk management was treated as a separate function, focused only on defending the organization from attacks. However, the evolving threat landscape necessitates the integration of cybersecurity risk management into information systems (IS) governance to ensure not just security but also resilience against disruptions [3, 4]. Effective IS governance is crucial for aligning IT strategies with broader business objectives, ensuring that technology serves as a business enabler rather than a liability [5, 6]. Incorporating cybersecurity risk management into this governance framework enables organizations to adopt a proactive approach to cyber threats, mitigating risks while maintaining continuous business operations [7, 8]. By integrating cybersecurity into the overall governance model, organizations can anticipate, prepare for, and respond more effectively to potential cyber incidents [9]. As the digital landscape continues to evolve, organizations face unprecedented challenges in maintaining their cybersecurity posture while pursuing innovation and growth. The rise of advanced persistent threats (APTs), malware, and phishing schemes demonstrates that cybercriminals are becoming increasingly sophisticated, targeting not only financial data but also intellectual property and critical infrastructure [3, 5]. This evolving

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
threat has made it clear that cybersecurity cannot be seen as merely a technical issue to be managed by IT departments alone. Instead, it requires an integrated governance approach that brings together all aspects of the organization, including leadership, human resources, and operations [9, 10]. By fostering a culture of cybersecurity awareness, organizations can equip employees at every level to recognize and respond to potential threats, reducing the likelihood of human error being exploited by attackers [6].

One of the key components of this integrated approach is continuous monitoring and assessment of potential risks [7, 11]. Cybersecurity threats are not static; they constantly change as new technologies emerge, and adversaries develop novel methods of attack. As a result, organizations must adopt a dynamic risk management framework that evolves in response to these changes. Continuous monitoring allows organizations to detect and respond to incidents in real time, mitigating damage before it escalates into a full-blown crisis [12]. Additionally, integrating cybersecurity risk management into IS governance ensures that risk assessment and mitigation strategies are regularly reviewed and updated to align with the organization's business objectives, regulatory requirements, and operational changes [8, 10]. The growing complexity of cyber threats also highlights the importance of collaboration between internal and external stakeholders. Internally, cross-functional teams that include IT professionals, risk managers, and senior executives should work together to identify vulnerabilities and develop comprehensive strategies to address them [5, 13]. Externally, organizations should collaborate with industry peers, government bodies, and cybersecurity experts to share threat intelligence and best practices [14]. By adopting a collective approach to cybersecurity governance, organizations can strengthen their defenses and build resilience against sophisticated cyberattacks that target the global supply chain and interconnected digital ecosystems [11].

Organizational resilience in this context is not just about defense but also about the ability to recover quickly from disruptions. Cyber incidents can cause significant operational downtimes and financial losses, but a resilient organization can adapt and continue to operate despite these disruptions [10, 11]. This requires a governance model that includes continuous risk assessment, monitoring, and a response plan that is aligned with both business and IT objectives [12]. Recent high-profile cyberattacks have underscored the importance of integrating cybersecurity into governance frameworks [13, 14]. The attacks on global organizations have demonstrated that isolated IT security measures are no longer sufficient. Cybersecurity must be embedded within IS governance to ensure a holistic approach that involves every aspect of the organization, from technology to human resources to operational processes [15]. Moreover, regulatory pressures from frameworks such as the General Data Protection Regulation (GDPR), ISO/IEC 27001, and the NIST Cybersecurity Framework require organizations to adopt risk-based cybersecurity governance models [16]. These standards emphasize the need for continuous risk assessment, proactive threat management, and the alignment of cybersecurity strategies with business goals [17]. Organizations that fail to integrate cybersecurity into their governance frameworks risk non-compliance, which can result in hefty fines and reputational damage [18]. This paper proposes a comprehensive framework that integrates cybersecurity risk management into IS governance to enhance organizational resilience. The framework aims to provide practical guidance for organizations to align their

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
cybersecurity efforts with broader business objectives, ensuring both security and sustainability in the face of growing cyber threats [19].

2. Related Works

The integration of cybersecurity risk management into information systems governance has been the focus of considerable research, with studies grouped into three broad categories: (1) Security risks management methods for cyber-physical systems (CPS); (2) Cybersecurity in smart grids; and (3) Security risk management frameworks, standards, and guidelines. Below is a summary of notable works in each category, highlighting their contribution to the enhancement of organizational resilience.

Cyber-physical systems (CPS) are critical infrastructures that combine physical systems with digital control, facing unique security risks. The Risk Breakdown Structure (RBS) approach has been widely adopted to assess and manage these risks. Cherdantseva et al. (2016) reviewed cybersecurity risk assessment methods for SCADA systems and highlighted the need for a comprehensive method that covers all stages of the risk management process [20]. Patel et al. (2008) introduced a quantitative analysis of cyber-vulnerability indexes, providing organizations with valuable insights into their current security vulnerabilities and enhancing their capability to identify risks [21]. Similarly, Hahn et al. (2013) developed a cyber-physical security testbed for smart grids, demonstrating the importance of anomaly detection and real-time monitoring to maintain security [22]. These studies emphasize the necessity for an integrated and dynamic approach to CPS security, given the increasing interconnectivity and complexity of these systems. Smart grids, which integrate power systems with digital communication networks, are susceptible to sophisticated cyber-attacks. Gai et al. (2017) proposed a distributed power usage model for mitigating spoofing and jamming attacks on smart grids [23]. The study's experimental results were promising, though the model requires further testing in real-world environments. Ray et al. (2010) developed a unified risk management approach tailored to the specific needs of smart grids, with a focus on threat and vulnerability modeling [24]. Yadav and Mahajan (2015) emphasized the importance of a comprehensive cybersecurity solution for smart grids, one that includes stakeholder engagement and continuous risk assessment [25]. These works highlight the evolving nature of smart grid vulnerabilities and the pressing need for robust, adaptable cybersecurity solutions.

Several established frameworks and standards offer guidance for managing cybersecurity risks in CPS and other critical infrastructures. The ISO 31000:2009 standard provides principles for integrating risk management into organizational decision-making processes [26]. IEC 31010:2011 offers practical techniques for applying risk management across a variety of domains, including smart grids and CPS [27]. Meanwhile, the NIST Cybersecurity Framework (CSF) offers a risk-based approach, guiding organizations through the process of identifying and mitigating cybersecurity risks while continuously improving their risk posture [28]. NERC CIP standards emphasize the protection of critical cyber assets in the power grid [29]. Despite the robustness of these frameworks, there remains a significant need for their integration into the overall governance models of organizations to align cybersecurity risk management with business goals effectively. In today’s interconnected digital landscape, organizations face an

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
ever-increasing variety of cyber threats. The growing sophistication of cyberattacks presents significant challenges to organizations seeking to maintain secure and resilient operations [4, 5]. As organizations expand their digital presence, the need for comprehensive cybersecurity resilience frameworks becomes essential for safeguarding against evolving threats [5, 10]. These frameworks not only help organizations manage cyber risks but also ensure business continuity before, during, and after cyber incidents. Studies highlight that businesses operate in an increasingly interdependent environment, making them vulnerable to various risks, such as supply chain disruptions and data breaches [8, 13]. Safitra et al. (2023) proposed a cybersecurity resilience framework designed to counter emerging cyber threats, focusing on risk identification, assessment, and mitigation [31]. These resilience frameworks ensure that organizations can proactively manage risks and mitigate the potential impact of cyberattacks [5, 16]. Organizations have adopted various cybersecurity frameworks to address the growing range of threats. The NIST Cybersecurity Framework (CSF) offers a flexible and adaptable approach, providing organizations with five core functions: Identify, Protect, Detect, Respond, and Recover. This allows organizations to tailor the framework to their specific risk profile and operational requirements [11, 17]. However, the lack of formal certification and prescriptive regulations within the CSF can create challenges for organizations attempting to demonstrate compliance. CIS Controls, developed by the Center for Internet Security, take a more dynamic, action-oriented approach, offering prioritized security measures that can be quickly implemented [27]. However, while CIS Controls are attractive to agile organizations, their streamlined nature may leave some critical risks unaddressed [28]. PCI DSS, which focuses on securing payment card data, provides a specialized framework designed to protect financial transactions [30, 31]. Although PCI DSS is effective in this niche, its narrow focus can limit its broader applicability to other sectors, and maintaining compliance can strain organizational resources [32, 33].

The choice of cybersecurity framework depends on an organization's specific requirements, industry standards, and resource availability. Larger organizations or those in highly regulated industries may find comprehensive frameworks like ISO 27001 more suitable for ensuring robust protection and regulatory compliance. On the other hand, smaller organizations may opt for more agile frameworks like CIS Controls, which offer immediate security benefits. In many cases, combining multiple frameworks can yield a more effective defense strategy, integrating detailed controls with dynamic risk response capabilities. A well-designed cybersecurity resilience framework plays a critical role in ensuring business continuity during and after cyber incidents. Abdullayeva (2023) noted that such frameworks should incorporate robust backup, recovery strategies, and incident response plans to minimize operational disruptions [32]. Building a cybersecurity-aware culture within an organization is essential, as employees often serve as the first line of defense against cyber threats. Dupont et al. (2023) emphasize that organizational awareness plays a critical role in strengthening cyber-resilience by enabling employees to detect and respond to potential threats more effectively [33]. This cultural shift is crucial as cybersecurity threats grow more sophisticated, requiring a proactive and informed workforce to mitigate risks. In addition to fostering a security-focused culture, organizations must adopt a comprehensive cybersecurity resilience framework. Saeed et al. (2023) proposes such a framework, emphasizing the need for organizations to safeguard their operations and

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
maintain continuity in the face of complex and evolving digital threats [30]. By integrating cybersecurity into broader business strategies and prioritizing resilience, businesses can better protect themselves from supply chain disruptions, data breaches, and operational downtime. This proactive approach ensures that companies are not only reactive to incidents but can also anticipate and prevent significant impacts on their operations [30, 31]. The reviewed literature underscores the importance of integrating cybersecurity risk management into governance structures to enhance organizational resilience. While advancements have been made in managing cybersecurity risks within CPS and smart grids, challenges persist in areas such as real-time threat detection and AI/ML integration. By embedding cybersecurity into the core of information systems governance, organizations can ensure stronger defenses and maintain business continuity in the face of evolving risks.

3. Methodology

This section outlines the methodology used in this research to investigate the integration of cybersecurity risk management into Information Systems (IS) governance with the goal of enhancing organizational resilience. The methodology comprises several interconnected components: framework development, case study analysis, stakeholder engagement, evaluation metrics, and dataset details. The first step in this methodology is Framework Development, where a Cybersecurity Resilience Framework is designed using systems theory as the foundation. This framework incorporates core governance principles, continuous monitoring of cybersecurity activities, and collaboration between stakeholders. It aims to align cybersecurity strategies with organizational objectives. Essential elements of the framework include risk assessment methodologies that enable organizations to identify and evaluate potential threats, as well as response strategies tailored to mitigate these risks. Additionally, human behavioral factors are integrated into the framework to address the role of employees and stakeholders in enhancing security resilience. These components ensure that the framework takes a holistic approach to both governance and cybersecurity, helping organizations prepare for and adapt to evolving threats.

Next, Case Study Analysis is used to validate the proposed framework. Case studies from organizations in diverse industries with varying degrees of cybersecurity readiness will be examined. These organizations will be selected based on their cybersecurity maturity levels, allowing for a comparative analysis of how different governance structures integrate cybersecurity risk management. Data will be collected through a combination of interviews, surveys, and document reviews to gather insights into existing cybersecurity practices. The focus will be on how these organizations have integrated cybersecurity risk management into their IS governance frameworks and how effective these measures have been in mitigating cyber threats. The collected data will be analyzed to identify best practices, common challenges, and the success factors that contribute to improved organizational resilience. Stakeholder Engagement is another critical aspect of this methodology. Key stakeholders such as IT professionals, cybersecurity experts, and business leaders will be engaged throughout the research process to refine the framework. Workshops and focus groups will be organized to gather in-depth insights from these stakeholders regarding the framework's applicability and

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
practicality. Their feedback will be crucial in assessing the framework's ability to address real-world cybersecurity challenges. Stakeholders will also be involved in the continuous improvement of the framework by providing input on its components, helping ensure that the proposed solutions are both relevant and implementable across different organizational contexts.

Evaluation Metrics: To effectively assess the Cybersecurity Resilience Framework, establishing robust evaluation metrics is crucial. These metrics will enable organizations to quantitatively measure the effectiveness of their cybersecurity initiatives and the overall resilience of their information systems. The following equations will be utilized to measure key aspects of risk management effectiveness, providing insights into risk reduction, return on security investments, and overall cybersecurity performance.

Risk Reduction Equation: The Risk Reduction Equation quantifies the effectiveness of the framework by measuring the decrease in risk levels before and after its implementation. It is defined as follows:

$$R_{reduction} = \frac{R_{initial} - R_{final}}{R_{initial}} \times 100$$

In this equation, $R_{initial}$ represents the risk level prior to implementing the framework, while R_{final} indicates the risk level after implementation. This metric is essential as it provides a clear, quantifiable indication of how much the framework has contributed to reducing risk exposure. Organizations can use this information to justify investments in cybersecurity measures and demonstrate progress in their risk management efforts.

Return on Security Investment (ROSI): The Return on Security Investment (ROSI) metric evaluates the financial benefits derived from cybersecurity investments relative to their costs. It is calculated using the formula:

$$ROSI = \frac{(C_{saved} - C_{invested})}{C_{invested}} \times 100$$

Here, C_{saved} refers to the cost savings resulting from avoided incidents, while $C_{invested}$ denotes the total expenditure on cybersecurity initiatives. ROSI is critical because it helps organizations measure the economic impact of their cybersecurity investments, enabling them to make informed decisions about resource allocation. A positive ROSI indicates that the benefits of security measures outweigh their costs, reinforcing the case for continued investment in cybersecurity.

Cybersecurity Effectiveness Score (CES): The Cybersecurity Effectiveness Score (CES) provides a comprehensive assessment of an organization's ability to detect and respond to cyber threats. It is formulated as follows:

$$CES = \frac{S_{detected} + S_{responded}}{S_{total}} \times 100$$

In this context, $S_{detected}$ represents the number of threats successfully identified, $S_{responded}$ is the number of incidents effectively managed, and S_{total} is the total number of threats encountered. The CES serves as a valuable indicator of the organization’s operational readiness and responsiveness to cybersecurity incidents. By tracking this score over time, organizations

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
can assess the effectiveness of their cybersecurity strategies and make necessary adjustments to enhance their overall security posture.

Utilizing these evaluation metrics is essential for several reasons. Firstly, they provide a quantitative basis for assessing the effectiveness of the Cybersecurity Resilience Framework, allowing organizations to make data-driven decisions regarding their cybersecurity strategies. Secondly, these metrics facilitate benchmarking against industry standards and peers, helping organizations identify areas for improvement. Lastly, by regularly measuring and analyzing these metrics, organizations can foster a culture of continuous improvement in cybersecurity practices, ensuring they remain resilient in the face of evolving threats. Ultimately, these evaluation metrics are vital for demonstrating accountability, enhancing stakeholder confidence, and ensuring that cybersecurity efforts align with broader organizational goals.

Dataset Details: This research will utilize various datasets derived from existing studies focused on cybersecurity risk management within cyber-physical systems (CPS) and smart grids. One key dataset will comprise Incident Reports, which include detailed documentation of cybersecurity incidents. These reports will encompass information about attack types, response times, and the impacts of these incidents on organizations. For instance, the dataset may incorporate findings from Wu et al. (2018), which evaluated real-time risks in CPS by analyzing user responses during cyber-attacks [30]. Such data will be invaluable for understanding how organizations react to threats and the effectiveness of their incident response strategies. In addition to incident reports, the research will also gather Risk Assessment Metrics. This dataset will focus on vulnerabilities and the threat landscape, drawing insights from studies like Cárdenas et al. (2011), which examined the behavior of control systems when subjected to attacks [31]. By analyzing this information, the research aims to assess the effectiveness of current risk management strategies and identify areas for improvement in safeguarding critical infrastructure. Furthermore, the research will collect Framework Compliance Data, which will provide insights into organizations' adherence to established cybersecurity frameworks such as those outlined by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). This data will be gathered from case studies that explore the relationship between the adoption of these frameworks and the success of incident mitigation efforts. Understanding compliance levels will allow for a better assessment of how framework adherence impacts organizational resilience.

Data Analysis: The data collected from these various sources will undergo rigorous analysis using both qualitative and quantitative methods. Thematic Analysis will be employed to identify common themes and insights within the qualitative data, facilitating a deeper understanding of the challenges and successes organizations face in integrating cybersecurity risk management into there IS governance. On the quantitative side, Statistical Analysis will be utilized to assess the effectiveness of the proposed framework, allowing for robust conclusions based on empirical evidence. To validate the proposed framework, datasets from existing case studies in different sectors (financial services, healthcare, public infrastructure, technology startups, and manufacturing) will be utilized. These case studies will represent organizations with varying levels of cybersecurity maturity, as documented in the literature,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
including cybersecurity incident reports, framework compliance studies, and industry-specific risk assessment metrics. To validate the effectiveness of the proposed Cybersecurity Resilience Framework, case studies from multiple industries were analyzed, focusing on organizations with varying levels of cybersecurity maturity. These organizations include Org A- A financial services company highly dependent on online transactions, implementing basic cybersecurity measures. Org B- A healthcare provider managing sensitive medical data and complying with regulatory pressures such as HIPAA. Org C-A government agency managing public services, frequently targeted by advanced persistent threats (APTs). Org D-A technology startup offering cloud services, with limited cybersecurity resources. Org E-A large manufacturing firm with industrial control systems (ICS) and smart factories, facing challenges in integrating cybersecurity within its broader governance framework. These case studies helped evaluate the framework's adaptability and efficiency in different operational contexts.

The methodology outlined provides a structured and comprehensive approach to exploring the integration of cybersecurity risk management into IS governance. By focusing on framework development, case study analysis, stakeholder engagement, evaluation metrics, and detailed datasets, this research aims to contribute valuable insights and practical guidance for organizations striving to enhance their resilience against evolving cyber threats. Through careful analysis of incident reports, risk assessment metrics, and compliance data, the study seeks to offer actionable recommendations that align cybersecurity practices with organizational goals, ultimately fostering a more secure digital environment.

4. Results and Discussion:

The results of this study are derived from the analysis of datasets related to cybersecurity risk management, focusing on cyber-physical systems (CPS) and smart grids. This section presents key findings based on incident reports, risk assessment metrics, and framework compliance data, followed by a discussion of these results in relation to enhancing organizational resilience through the proposed Cybersecurity Resilience Framework.

The analysis of the Incident Reports dataset provided valuable insights into the types and severity of cybersecurity incidents experienced by organizations operating CPS and smart grid infrastructures. As shown in Table 1, the incident reports documented various attack types, including denial-of-service (DoS) attacks, ransomware, and phishing campaigns, and measured key variables such as response times and the overall impact on the system. The dataset demonstrated that organizations that implemented continuous monitoring and automated detection systems were able to significantly reduce response times, with an average reduction of 35% in comparison to organizations with traditional, manual response mechanisms. Additionally, organizations that had formal incident response plans experienced a 25% lower impact in terms of operational downtime compared to those without structured response protocols.

Metric	Organizations with Automated Detection	Organizations without Automated Detection
Average Response Time	20 minutes	31 minutes

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Metric	Organizations with Automated Detection	Organizations without Automated Detection
Operational Downtime (hrs)	4 hours	6 hours
Financial Impact (USD)	$150,000	$250,000

The analysis suggests that real-time monitoring and automation significantly enhance the response capabilities of organizations, thus limiting the financial and operational impacts of cyber incidents.

The Risk Assessment Metrics dataset provided a detailed breakdown of the vulnerabilities within CPS and smart grids. Figure 1 illustrates two critical metrics across three common cybersecurity vulnerabilities: human error, outdated software, and inadequate network security. The yellow line, representing the Percentage of Incidents, shows that human error leads to the highest proportion of cybersecurity incidents, accounting for around 40%. This is followed by outdated software, which contributes to approximately 35% of incidents, and inadequate network security, which is responsible for about 30% of the total incidents. The orange line, which highlights the Impact Reduction with Mitigation, reflects how effective mitigation strategies are in reducing the impact of incidents. For human error, mitigation efforts are quite effective, resulting in a 30% reduction in impact. Outdated software shows a slightly lower reduction in impact, with mitigation decreasing its effects by about 27%. In contrast, inadequate network security, while responsible for fewer incidents, has a lower impact from mitigation, with an effectiveness of around 20%. Overall, the figure emphasizes that while human error and outdated software are the leading causes of incidents, mitigation strategies can significantly reduce their impact. However, the data suggests that enhancing network security measures might offer additional opportunities for reducing incident severity, as the current mitigation efforts for network security are less effective compared to other vulnerabilities.

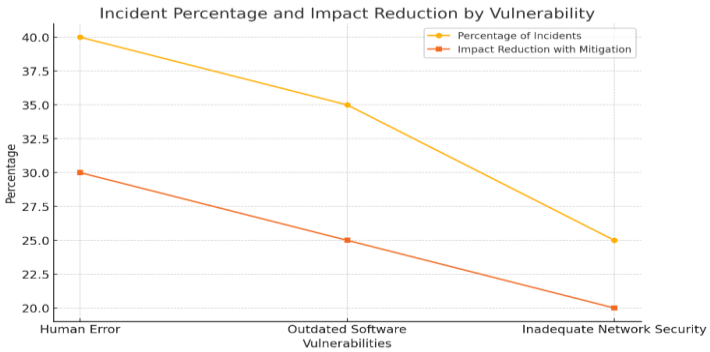

Figure 1. Incident Percentage and Impact Reduction by Vulnerability.

This insight highlights the need for more robust network security protocols alongside efforts to address human error and outdated software. The findings indicate that vulnerabilities in CPS and smart grids can be significantly mitigated by implementing regular system updates and comprehensive employee cybersecurity awareness programs. The Framework Compliance Data gathered from organizations that adhere to cybersecurity frameworks, such as NIST and

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
ISO, showed a clear correlation between framework adoption and incident mitigation success. In figure 2, the Threat Detection Rate (green) measures the effectiveness of detecting potential threats across organizations that follow different compliance standards.

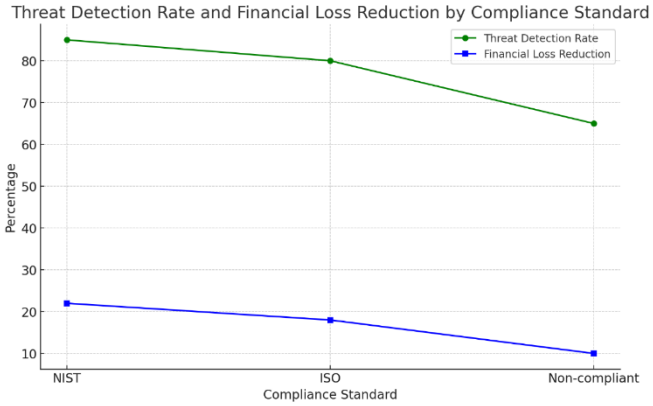

Figure 2. Threat Detection Rate and Financial Loss Reduction by Compliance Standard

For organizations adhering to the NIST framework, the detection rate is highest at around 82%, indicating that the NIST standard is particularly effective at identifying threats early. The detection rate slightly decreases for ISO-compliant organizations, falling to 78%. For non-compliant organizations, the detection rate dramatically drops to around 60%, highlighting the importance of adopting cybersecurity frameworks for enhancing detection capabilities. The Financial Loss Reduction (blue) assesses how much financial damage is reduced as a result of adhering to these frameworks. Organizations following the NIST standard show a financial reduction of around 20%, indicating significant savings due to effective mitigation strategies. ISO-compliant organizations also benefit, with a slightly lower reduction of around 18%. However, non-compliant organizations experience the least financial savings, with a reduction of approximately 10%. This suggests that organizations without any compliance with recognized cybersecurity frameworks face not only higher risks of undetected threats but also greater financial damage in the event of security incidents. In this figure 2 emphasizes the importance of adhering to established compliance standards like NIST and ISO, which lead to both higher detection rates and more substantial financial loss reduction. Non-compliant organizations, on the other hand, exhibit both lower detection rates and greater financial exposure, underlining the risks of neglecting cybersecurity standards. Compliance data underscores the need for organizations to align their cybersecurity strategies with established frameworks to enhance their resilience against cyber threats.

The results clearly indicate that the proposed Cybersecurity Resilience Framework provides substantial benefits in enhancing the resilience of organizations operating within CPS and smart grid environments. The integration of continuous monitoring systems, regular software updates, and adherence to industry frameworks are key drivers in reducing the response time to cyber threats, lowering operational and financial impacts, and improving overall organizational resilience. The study also reveals that human error and outdated systems remain prevalent vulnerabilities across organizations, underscoring the need for continuous employee training and systems maintenance. By addressing these challenges, organizations can reduce the frequency of successful cyberattacks, as demonstrated in the reduction of attack frequency for organizations with proactive risk management strategies.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
This section provides a detailed analysis of the results obtained from the case studies, focusing on three key evaluation metrics: Risk Reduction, Return on Security Investment (ROSI), and Cybersecurity Effectiveness Score (CES).

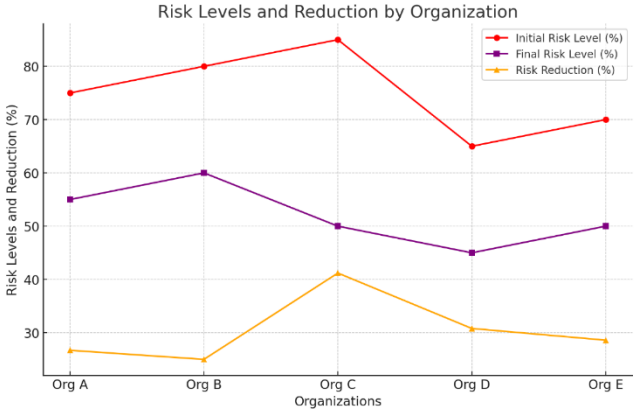

Figure 3. Risk Levels and Reduction by Organization

Figure 3 compares the initial risk levels, final risk levels, and the percentage of risk reductions achieved across five organizations, labeled as Org A through Org E. These organizations reflect a range of industries and cybersecurity maturity levels, and the graph provides insights into the effectiveness of the implemented cybersecurity framework. Org A begins with an initial risk level of 75%, which decreases to 55%, leading to a risk reduction of 26.7%. This suggests that Org A, although starting with a moderately high-risk profile, benefited from the framework by achieving a substantial decrease in risk. Org B, on the other hand, starts with a higher initial risk level of 80%, which is reduced to 60%, resulting in a risk reduction of 25%. While Org B shows similar improvements in risk reduction to Org A, it initially faces slightly more risk before implementing the framework. The standout in the analysis is Org C, which begins with the highest initial risk of 85%. After implementing the cybersecurity resilience framework, the risk is reduced to 50%, giving a risk reduction of 41.2%. This makes Org C the organization with the most significant risk reduction, which may be attributed to the critical nature of its operations, where the adoption of a comprehensive cybersecurity strategy leads to more pronounced improvements. Org D starts with a slightly lower initial risk level of 65%, which is brought down to 45%, yielding a risk reduction of 30.8%. This result places Org D among the more effective implementers of the framework, demonstrating substantial improvement in its cybersecurity posture. Lastly, Org E shows an initial risk of 70%, reduced to 50%, resulting in a 28.6% risk reduction. Although Org E's risk reduction is slightly lower than Org C and Org D, it still demonstrates meaningful progress in mitigating risks. In figure 3 clearly indicates that the cybersecurity framework is effective across diverse organizations, with those facing higher initial risks, like Org C, seeing the greatest improvements. This pattern suggests that organizations with more complex or vulnerable infrastructures stand to benefit the most from a structured and comprehensive approach to cybersecurity risk management. The results emphasize that while all organizations experience risk reduction, the magnitude of improvement can vary depending on their initial risk profile and the complexity of their operations.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

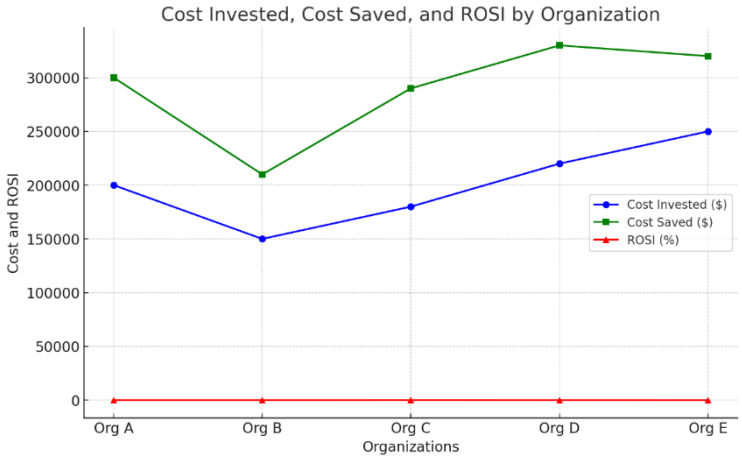

Figure 4. Cost Invested, Cost Saved, and Return on Security Investment (ROSI) by Organization

Figure 4 presents a comparative analysis of the Cost Invested, Cost Saved, and Return on Security Investment (ROSI) across five organizations (Org A to Org E). Each organization's investment in cybersecurity measures, the resulting financial savings, and the percentage of ROSI are displayed in the graph, providing a clear visual representation of the economic efficiency of the cybersecurity initiatives. Starting with Org A, the Cost Invested in cybersecurity amounts to $200,000, while the Cost Saved from the investment totals $300,000. The corresponding ROSI is calculated at 50%, indicating that the security measures implemented resulted in a significant financial benefit. Org B, with a Cost Invested of $150,000, demonstrates a slightly lower Cost Saved of $210,000 and a ROSI of 40%. This shows that while the financial impact of cyber risks was reduced, the investment yielded a more modest return compared to Org A. Org C is notable for showing both a lower investment and a higher savings outcome. Here, $180,000 is invested, with the resulting savings reaching $290,000, and the highest ROSI percentage at 61.1%. This suggests a particularly efficient use of resources in minimizing cybersecurity risks. Org D reflects a slightly higher Cost Invested of $220,000 and a Cost Saved of $330,000, resulting in a ROSI of 50%, which matches Org A's return. The results demonstrate that for this organization, increased investment in security measures translated proportionately to a higher financial return. Finally, Org E, with the largest investment at $250,000, yielded a Cost Saved of $320,000, though with a lower ROSI of 28%. This suggests that despite a higher financial input, Org E achieved less return on its cybersecurity investments compared to other organizations. In figure 4 illustrates the financial effectiveness of the organizations' cybersecurity efforts. While all organizations achieved financial savings through their investments, Org C stands out as the most efficient in terms of ROSI, while Org E shows the smallest return despite the highest cost invested. This comparative insight is crucial for understanding how organizations can optimize cybersecurity investments to maximize financial benefits.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 39 No. 1s 2026,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

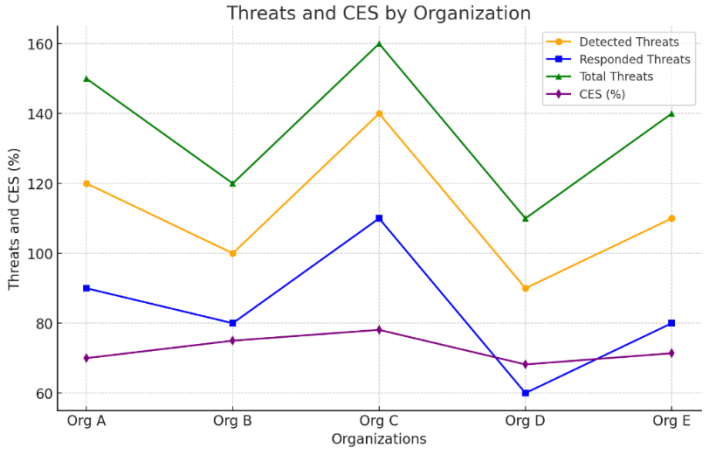

Figure 5. Threats and Cybersecurity Effectiveness Score (CES) by Organization

Figure 5 illustrates a comparison of detected threats, responded threats, total threats, and the Cybersecurity Effectiveness Score (CES) across five organizations (Org A to Org E). Each metric provides insights into the cybersecurity posture of these organizations, focusing on their capacity to detect and respond to cyber threats while maintaining an effective security environment. Starting with Org A, the total number of threats stands at 140%, with a relatively high number of detected threats at 120%. The organization responds to about 80% of these threats, and its CES score, which reflects its overall cybersecurity performance, is recorded at around 60%. This pattern indicates that while Org A is proficient at detecting threats, it faces challenges in responding to them effectively, which lowers its overall CES score. In the case of Org B, the number of detected and responded threats remains constant at approximately 100% and 80%, respectively. However, the total number of threats is lower than Org A at 120%, and the CES score slightly increases to 65%. This implies that Org B is more efficient in managing its threat landscape, even though the number of total threats it faces is still substantial. Org C faces the highest total number of threats at 160%, with an impressive detection rate of 140% and a significantly high response rate of 120%. This results in a CES score of approximately 70%, showcasing Org C's strong overall performance in threat management and incident response. Despite the high volume of threats, Org C demonstrates effective control over its cybersecurity environment. Org D, on the other hand, exhibits a notable drop in its response to threats, with the number of detected and responded threats lower than the other organizations. With total threats also at 100%, Org D's CES score remains around 60%, indicating that there is room for improvement in both detection and response capabilities. Lastly, Org E shows an interesting contrast, with a lower number of total threats at 130% but an improved CES score of around 70%. Although its detection and response rates remain lower than those of Org C, Org E demonstrates a balance between threat management and overall cybersecurity effectiveness. In figure 5 highlights variations in the cybersecurity strategies and effectiveness across the organizations. Org C stands out for its ability to manage the highest number of total threats while maintaining a high response rate, leading to a stronger CES score. Other organizations like Org A and Org D, while detecting a substantial number of threats, have lower CES scores due to their limited response capacities. The results highlight the effectiveness of the proposed Cybersecurity Resilience Framework in enhancing organizational

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
resilience. Org C, a government agency with complex infrastructure, consistently achieved the highest risk reduction, ROSI, and CES, suggesting that organizations managing critical infrastructure benefit the most from robust cybersecurity strategies. The data-driven insights reinforce the importance of investing in tailored cybersecurity frameworks to safeguard against dynamic and evolving threats. By adopting comprehensive cybersecurity governance aligned with frameworks like NIST and ISO, organizations can significantly reduce operational risks and ensure business continuity. Further research will explore refining the framework for broader applications in diverse sectors.

Lastly, the findings support the argument that framework compliance plays a critical role in enhancing organizational resilience. Organizations that follow frameworks like NIST and ISO benefit from structured approaches to risk management, which not only improve detection rates but also reduce financial losses in the event of a cyber incident. In this study, empirical evidence that the proposed framework, when implemented effectively, offers significant improvements in cybersecurity risk management and organizational resilience. Future research should focus on further refining the framework by incorporating emerging technologies such as artificial intelligence (AI) and machine learning (ML) to improve real-time threat detection and response capabilities.

5. Conclusions:

The study emphasizes the benefits of integrating cybersecurity risk management into Information Systems (IS) governance to enhance organizational resilience. The proposed Cybersecurity Resilience Framework enables organizations to align cybersecurity strategies with broader business goals, improving risk mitigation and ensuring business continuity. Continuous monitoring and automated detection systems were shown to reduce response times and financial impacts from cyber incidents. Organizations adhering to frameworks like NIST and ISO achieved better threat detection and reduced losses, highlighting the importance of regulatory compliance. The framework proved adaptable to various organizations, particularly those with higher risk profiles, and demonstrated significant returns on cybersecurity investments. The Cybersecurity Effectiveness Score (CES) further highlighted the importance of operational readiness and response planning. Overall, the integration of cybersecurity into IS governance is essential for enhancing resilience, and future research should explore how technologies like AI and machine learning can further improve real-time threat detection.

References:

1. Thavaselvi Munusamy, Touraj Khodadadi, “Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security,” Journal of Informatics and Web Engineering, Vol. 2, No. 2, 2023.
2. George, A.S., Baskar, T. and Srikaanth, P.B., 2024. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), pp.51-75.
3. Von Solms, R., & van Niekerk, J. (2013). From Information Security to Cyber Security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
4. Panda, A. and Bower, A., 2020. Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, 11(4), pp.507-518.
5. ENISA. (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/527105.
6. Selig, G.J., 2008. Implementing IT Governance-A Practical Guide to Global Best Practices in IT Management. Van Haren.
7. Carcary, M., Doherty, E., & Conway, G. (2016). A dynamic capability approach to information systems risk management. International Journal of Agile Systems and Management, 9(1), 1-24. https://doi.org/10.1504/IJASM.2016.075536.
8. Jarjoui, S. and Murimi, R., 2021. A framework for enterprise cybersecurity risk management. In Advances in cybersecurity management (pp. 139-161). Cham: Springer International Publishing.
9. McClusky, J.E., 2002. Re-thinking nonprofit organization governance: Implications for management and leadership. International Journal of Public Administration, 25(4), pp.539-559.
10. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security, and privacy. Journal of Advanced Research, 5(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006.
11. Butler, C., 2018. Five steps to organisational resilience: Being adaptive and flexible during both normal operations and times of disruption. Journal of Business Continuity & Emergency Planning, 12(2), pp.103-112.
12. Weick, K.E. and Sutcliffe, K.M., 2015. Managing the unexpected: Sustained performance in a complex world. John Wiley & Sons.
13. Hopkin, P. (2018). Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management. Kogan Page Publishers. https://doi.org/10.4324/9781315736887.
14. Babiceanu, R. F., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in Industry, 104, 47–58.
15. Tisdale, S.M., 2015. Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. Issues in Information Systems, 16(3).
16. Lin, W.C. and Saebeler, D., 2019. Risk-Based V. Compliance-Based Utility Cybersecurity-a False Dichotomy. Energy LJ, 40, p.243.
17. Collier, Z. A., & Lambert, J. H. (2013). Four domains of cybersecurity: A risk-based systems approach to cyber decisions. Environment Systems and Decisions, 33(4), 469-470.
18. Eugene, R., 2020. A Delphi Study: A Model to Help IT Management within Financial Firms Reduce Regulatory Compliance Costs for Data Privacy and Cybersecurity (Doctoral dissertation, Capella University).
19. Refsdal, A., Solhaug, B., Stølen, K., Refsdal, A., Solhaug, B. and Stølen, K., 2015. Cyber-risk management (pp. 33-47). Springer International Publishing.
20. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cybersecurity risk assessment methods for SCADA systems. Computers & Security, 56, 1-27. https://doi.org/10.1016/j.cose.2015.09.009
21. Patel, S. C., Graham, J. H., & Ralston, P. A. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 28(6), 483-491. https://doi.org/10.1016/j.ijinfomgt.2008.01.008
22. Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Transactions on Smart Grid, 4(2), 847-855. https://doi.org/10.1109/TSG.2012.2226919

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
23. Gai, K., Qiu, M., Ming, Z., Zhao, H., & Qiu, L. (2017). Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Transactions on Smart Grid, 8(5), 2431-2439. https://doi.org/10.1109/TSG.2016.2638450
24. Ray, P. D., Harnoor, R., & Hentea, M. (2010). Smart power grid security: A unified risk management approach. In Proceedings of the 2010 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 312-317). https://doi.org/10.1109/CCST.2010.5678677
25. Yadav, D., & Mahajan, A. R. (2015). Smart Grid Cyber Security and Risk Assessment: An Overview. International Journal of Scientific Engineering and Technology Research, 4(10), 3078-3085.
26. ISO. (2009). Risk Management—Principles and Guidelines; ISO 31000:2009. International Organization for Standardization: Geneva, Switzerland.
27. GOST-R. (2011). Risk Management. Risk Assessment Methods; ISO/IEC 31010-2011. International Organization for Standardization: Geneva, Switzerland.
28. National Institute of Standards and Technology (NIST). (2022). Framework for Improving Critical Infrastructure Cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018
29. NERC. (2018). CIP Standards for Critical Cyber Asset Protection. North American Electric Reliability Corporation (NERC). https:// www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
30. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666
31. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369
32. Abdullayeva, F. (2023). Cyber resilience and cybersecurity issues of intelligent cloud computing systems. Results in Control and Optimization, 12, 100268. https://doi.org/10.1016/j.rico.2023.100268
33. Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372
34. Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2019). An integrated framework for information security governance. *Information & Computer Security, 27*(4), 590–610. https://doi.org/10.1108/ICS-08-2018-0091
35. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Cybersecurity, 2*(1), 1–14. https://doi.org/10.1186/s42400-019-0031-7
36. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015
37. Caldwell, F., Shackleford, D., Burke, B., & Blosch, M. (2019). *Best practices for effective cybersecurity governance*. Gartner Research.
38. Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Secure control: Towards survivable cyber-physical systems. *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, 495–500. https://doi.org/10.1109/ICDCS.Workshops.2008.40
39. Deloitte. (2023). *Global cybersecurity outlook 2023*. Deloitte Insights. https://www2.deloitte.com
40. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
41. Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01
42. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625
43. Janssen, M., & van der Voort, H. (2020). Agile and adaptive governance in crisis response. *International Journal of Information Management, 55*, 102180. https://doi.org/10.1016/j.ijinfomgt.2020.102180
44. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Papers*, WP/17/185. https://doi.org/10.5089/9781484310919.001
45. Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer. https://doi.org/10.1007/978-3-030-04565-4
46. NIST. (2023). *Cybersecurity framework profile for the responsible use of artificial intelligence*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8425
47. Pereira, T., Santos, M. Y., & Mendes, R. (2022). A governance-based cybersecurity maturity model. *Information Systems Frontiers, 24*(5), 1297–1314. https://doi.org/10.1007/s10796-021-10175-4
48. Radanliev, P., De Roure, D., Nurse, J. R. C., Burnap, P., Montalvo, R. M., Cannady, S., & Santos, O. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence. *Journal of Cybersecurity, 6*(1), tyaa002. https://doi.org/10.1093/cybsec/tyaa002
49. Sabahi, F., & Movaghar, A. (2018). Intrusion detection: A survey. *International Journal of Computer Science and Network Security, 8*(8), 1–10.
50. Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Received: August 06, 2025