Power System Protection and Control
ISSN:1674-3415

# ENHANCING ORGANIZATIONAL RESILIENCE: INTEGRATING CYBERSECURITY RISK MANAGEMENT INTO INFORMATION SYSTEMS GOVERNANCE

**Syed Nazmul Hasan[1], Partha Chakraborty*[2], Md Talha Bin Ansar[3], Abdullah Al Zaiem[4], Niropam Das[5], Ahmed Shan-A-Alahi[6], Jobanpreet kaur[7]**

[1]College of Technology & Engineering, Westcliff University, Irvine, CA 92614, USA
Email: s.hasan.104@westcliff.edu
ORCID ID: https://orcid.org/0009-0008-0977-595X
[2]School of Business, International American University, Los Angeles, CA 90010, USA
Email: parthachk64@gmail.com
ORCID ID: https://orcid.org/0009-0006-3203-8902
[3]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
[4]Department of Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: zaiemab@gmail.com
ORCID ID: https://orcid.org/0009-0006-9442-7647
[5]School of Business, International American University, Los Angeles, CA 90010, USA
Email: niropomdas124@gmail.com
ORCID ID: https://orcid.org/0009-0004-6107-7025
[6]Department of Technology and Computer Science, University of The Potomac, Washington DC, USA
Email: ahmed.shanaalahi@student.potomac.edu
ORCID ID: https://orcid.org/0009-0007-6079-4999
[7]College of Technology & Engineering, Westcliff University, Irvine, CA 92614, USA
Email: j.kaur.244@westcliff.edu
ORCID ID: https://orcid.org/0009-0008-0083-8205

***Corresponding author**: Partha Chakraborty

**Recevied**:18 October 2024 **Revised**: 25 November 2024 **Accepted**: 12 December 2024

***ABSTRACT***

This article examines the enhancement of organizational resilience through the integration of cybersecurity risk management into Information Systems (IS) governance. Organizations are finding it harder to keep their operations safe as technology grows more important and cyber threats get more complicated. This study employs systems theory to offer a comprehensive framework that integrates business objectives with IT strategy, highlighting the necessity of a robust and flexible cybersecurity posture. The research utilizes an extensive analysis of contemporary cybersecurity literature, established frameworks, and industry practices, providing a pragmatic guidance for enterprises to efficiently mitigate cyber threats. The suggested Cybersecurity Resilience Framework combines governance principles, ongoing monitoring, stakeholder involvement, and human behavior variables to create a complete solution. The findings of this study reveal that firms employing automated detection systems have an average response time of 20 minutes, in contrast to 31 minutes for those utilizing manual detection methods. Additionally, businesses with automated systems had less downtime (4 hours instead of 6 hours) and less of an effect on their finances ($150,000 instead of $250,000). The study also found that companies that followed recognized frameworks like NIST and ISO were better at finding threats (more than 80% of the time) and lost less money (around 20% of the time). The Return on Security Investment (ROSI) analysis showed that companies that made smart investments in cybersecurity saved a lot of money, with ROSI percentages between 28% and 61%. Also, firms showed that they were better at finding and responding to threats, as shown by their Cybersecurity Effectiveness Scores (CES), which showed that they were ready to do business. In general, this framework gives businesses a strong plan for dealing with the ever-changing world of cybersecurity while keeping their operations running.


**DOI:** 10.46121/pspc.52.4.4

Power System Protection and Control
ISSN:1674-3415

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

## INTRODUCTION

The fast advancement of digital technology has changed the way businesses manage their information systems, but it has also exposed them to new cybersecurity concerns. As enterprises rely more on interconnected systems and cloud services, the attack surface for possible cyber threats expands, increasing their vulnerability to breaches, ransomware, and data theft [1, 2]. Traditionally, cybersecurity risk management was viewed as a separate job, only concerned with protecting the firm from assaults. However, the changing threat landscape means that cybersecurity risk management needs to be a part of information systems (IS) governance to make sure that systems are not only safe but also able to handle disruptions [3, 4]. Effective IS governance is critical for aligning IT strategy with overall business goals, ensuring that technology is a business enabler rather than a burden [5, 6]. Incorporating cybersecurity risk management into this governance framework enables firms to take a proactive approach to cyber threats, minimizing risks while preserving business continuity [7, 8]. By incorporating cybersecurity into the broader governance paradigm, firms can better foresee, plan for, and respond to future cyber incidents [9]. As the digital landscape evolves, organizations must navigate unprecedented obstacles in maintaining their cybersecurity posture while pursuing innovation and growth. The increase of advanced persistent threats (APTs), malware, and phishing scams shows that hackers are becoming cleverer, focusing on not only financial data but also intellectual property and vital infrastructure [3, 5]. This changing threat has made it evident that cybersecurity cannot be viewed as a technical issue to be handled alone by IT teams. Instead, it necessitates an integrated governance model that encompasses all parts of the company, including leadership, human resources, and operations [9-10]. Organizations can reduce the likelihood of attackers exploiting human error by developing a culture of cybersecurity knowledge among employees at all levels [6].

One of the most important parts of this integrated approach is keeping an eye on and evaluating possible hazards all the time [7, 11]. Cybersecurity risks are not fixed; they evolve continuously with the advent of new technology and the innovation of attack strategies by adversaries. Because of this, companies need to use a dynamic risk management framework that adapts as things occur. Organizations can find and deal with problems in real time thanks to continuous monitoring, which stops damage from getting worse before it turns into a full-blown catastrophe [12]. Also, adding cybersecurity risk management to IS governance makes sure that risk assessment and mitigation plans are looked at and updated on a regular basis to make sure they are in line with the organization's business goals, regulatory requirements, and changes in operations [8, 10]. The increasing complexity of cyber threats underscores the necessity for coordination among internal and external parties. Cross-functional teams made up of IT specialists, risk managers, and senior executives should work together to find weaknesses and come up with complete plans to fix them [5, 13]. Organizations should work with other businesses in their field, government agencies, and cybersecurity professionals to share information about threats and best practices [14]. Organizations may make their defenses stronger and be more resilient against complex cyberattacks that target the global supply chain and interconnected digital ecosystems by taking a communal approach to cybersecurity governance [11].

In this case, organizational resilience isn't only about being able to defend itself; it's also about being able to bounce back swiftly from problems. Cyber events can lead to major operational downtimes and financial losses, but a strong business can adapt and keep running even when things go wrong [10, 11]. This necessitates a governance framework that incorporates ongoing risk evaluation, oversight, and a response strategy that is congruent with both business and IT goals [12]. Recent major hacks have shown how important it is to include cybersecurity in governance frameworks [13, 14]. The attacks on international organizations have shown that IT security solutions that only work in one place are no longer enough. Cybersecurity needs to be a part of IS governance so that it covers all parts of the organization, including technology, people, and business processes [15]. Additionally, regulatory demands from frameworks like the General Data Protection Regulation (GDPR), ISO/IEC 27001, and the NIST Cybersecurity Framework compel enterprises to implement risk-based cybersecurity governance approaches [16]. These standards stress the importance of ongoing risk assessment,

 **DOI:** 10.46121/pspc.52.4.4

proactive threat management, and making sure that cybersecurity plans fit with business goals [17]. Organizations that do not include cybersecurity in their governance structures run the danger of not following the rules, which can lead to large fines and damage to their reputation [18]. This study provides a complete framework that incorporates cybersecurity risk management into information systems governance to improve organizational resilience. The framework's goal is to help businesses make sure that their cybersecurity efforts are in line with their larger business goals, so that they can stay safe and thrive even as cyber dangers develop [19].

## LITERATURE REVIEW

The incorporation of cybersecurity risk management into information systems governance has been the subject of extensive research, categorized into three primary domains: (1) Security risk management methodologies for cyber-physical systems (CPS); (2) Cybersecurity in smart grids; and (3) Security risk management frameworks, standards, and guidelines. This review delineates significant studies in each category, emphasizing their role in augmenting organizational resilience.

Cyber-physical systems (CPS) are essential infrastructures that integrate physical systems with digital control, encountering distinct security vulnerabilities. The Risk Breakdown Structure (RBS) methodology has been extensively utilized to evaluate and mitigate these risks. Cherdantseva et al. (2016) examined cybersecurity risk assessment methodologies for SCADA systems and emphasized the necessity for a holistic approach encompassing all phases of the risk management process [20]. Patel et al. (2008) presented a quantitative assessment of cyber-vulnerability indices, offering enterprises critical insights into their existing security weaknesses and improving their ability to recognize hazards [21]. Hahn et al. (2013) established a cyber-physical security testbed for smart grids, illustrating the significance of anomaly detection and real-time monitoring for security maintenance [22]. These investigations underscore the imperative for a cohesive and adaptive strategy for CPS security, in light of the escalating interconnectedness and intricacy of these systems. Smart grids, which amalgamate power systems with digital communication networks, are vulnerable to advanced cyber-attacks. Gai et al. (2017) introduced a distributed power consumption model to counteract spoofing and jamming attacks on smart grids [23]. The experimental outcomes of the study were encouraging; however, the model necessitates additional testing in practical settings. Ray et al. (2010) created a comprehensive risk management strategy designed for the unique requirements of smart grids, emphasizing threat and vulnerability modeling [24]. Yadav and Mahajan (2015) underscored the necessity of an all-encompassing cybersecurity solution for smart grids, incorporating stakeholder involvement and ongoing risk evaluation [25]. These studies underscore the dynamic nature of smart grid vulnerabilities and the urgent requirement for resilient, flexible cybersecurity solutions.

Numerous defined frameworks and standards provide guidance for the management of cybersecurity risks in cyber-physical systems and other critical infrastructures. The ISO 31000:2009 standard delineates concepts for the incorporation of risk management into corporate decision-making processes. IEC 31010:2011 provides pragmatic methodologies for implementing risk management in diverse fields, such as smart grids and cyber-physical systems [27]. The NIST Cybersecurity Framework (CSF) is a risk-based methodology that assists companies in identifying and mitigating cybersecurity threats while perpetually enhancing their risk posture [28]. The NERC CIP rules prioritize the safeguarding of essential cyber assets inside the power grid. Notwithstanding the strength of these frameworks, a considerable necessity persists for their incorporation into the comprehensive governance structures of businesses to effectively link cybersecurity risk management with business objectives. In the contemporary interconnected digital environment, enterprises encounter a continually expanding array of cyber dangers. The increasing complexity of cyberattacks poses substantial hurdles for businesses striving to uphold secure and resilient operations. As enterprises enhance their digital presence, the necessity for robust cybersecurity resilience frameworks becomes imperative to protect against emerging threats [5, 10]. These frameworks assist firms in managing cyber risks and ensuring business continuity before, during, and after cyber incidents. Research indicates that enterprises function within an increasingly interconnected environment, rendering them susceptible to numerous hazards, including supply chain disruptions and data breaches [8, 13]. Safitra et al. (2023) introduced a cybersecurity resilience architecture aimed at addressing increasing cyber threats, emphasizing risk identification, assessment, and mitigation [31]. These resilience frameworks enable firms to proactively manage risks and limit the potential effects of cyberattacks [5, 16]. Organizations have implemented


**DOI:** 10.46121/pspc.52.4.4

diverse cybersecurity strategies to mitigate the expanding array of threats. The NIST Cybersecurity Framework (CSF) is a versatile and adjustable methodology, encompassing five fundamental functions: Identify, Protect, Detect, Respond, and Recover. This enables enterprises to customize the framework according to their distinct risk profile and operational needs [11, 17]. The absence of formal certification and prescriptive restrictions within the CSF may provide difficulties for firms seeking to verify compliance. CIS Controls, formulated by the Center for Internet Security, adopted a dynamic and action-oriented methodology, providing prioritized security measures that can be rapidly executed. Nevertheless, whereas CIS Controls appeal to dynamic enterprises, their streamlined design may result in certain essential risks remaining unmitigated [28]. The PCI DSS, which emphasizes the security of payment card information, offers a particular framework aimed at safeguarding financial transactions [30, 31]. While PCI DSS is effective within its own domain, its limited scope may restrict its applicability to other industries, and ensuring compliance might burden organizational resources [32, 33].

The selection of a cybersecurity framework is contingent upon an organization's particular needs, industry norms, and resource accessibility. Extensive enterprises or those in heavily regulated sectors may consider comprehensive frameworks such as ISO 27001 more appropriate for guaranteeing strong protection and regulatory adherence. Conversely, smaller firms may choose more agile frameworks such as CIS Controls, which provide prompt security advantages. In several instances, amalgamating various frameworks can produce a more efficacious security strategy, merging comprehensive controls with adaptive danger response capabilities. An effectively constructed cybersecurity resilience strategy is essential for maintaining company continuity during and following cyber catastrophes. Abdullayeva (2023) emphasized that such frameworks must integrate comprehensive backup, recovery procedures, and incident response plans to mitigate operational disruptions [32]. Establishing a cybersecurity-conscious culture within an organization is crucial, as employees frequently act as the initial line of defense against cyber threats. Dupont et al. (2023) assert that corporate knowledge is crucial in enhancing cyber-resilience by equipping staff to identify and address potential risks more efficiently [33]. This cultural transformation is essential as cybersecurity threats become increasingly sophisticated, necessitating a proactive and knowledgeable workforce to alleviate risks. Organizations must implement a complete cybersecurity resilience strategy alongside cultivating a security-oriented culture. Saeed et al. (2023) provides a paradigm that underscores the necessity for enterprises to protect their operations and ensure continuity against intricate and growing digital threats [30]. By incorporating cybersecurity into comprehensive business strategies and emphasizing resilience, organizations can enhance their protection against supply chain disruptions, data breaches, and operational outages. This proactive strategy guarantees that organizations are not merely reactive to disasters but can also foresee and avert substantial effects on their operations [30, 31]. The examined literature highlights the necessity of incorporating cybersecurity risk management into governance frameworks to improve organizational resilience. Despite progress in mitigating cybersecurity threats in CPS and smart grids, issues remain in real-time threat detection and the integration of AI and machine learning. Integrating cybersecurity into the fundamental framework of information systems governance enables firms to fortify defenses and sustain business continuity amidst increasing threats.

## METHODOLOGY

The approach taken in this study to examine how cybersecurity risk management might be included in Information Systems (IS) governance in order to improve organizational resilience is described in this section. Framework development, case study analysis, stakeholder interaction, evaluation measures, and dataset details are some of the interrelated elements that make up the technique. This methodology's initial step, Framework Development, involves using systems theory as the basis for the building of a cybersecurity resilience framework. This approach integrates stakeholder engagement, ongoing cybersecurity activity monitoring, and fundamental governance concepts. It seeks to match organizational goals with cybersecurity strategies. The framework's key components include reaction plans designed to reduce risks and risk assessment techniques that help businesses recognize and analyze possible threats. Furthermore, the framework incorporates human behavioral elements to address the role of stakeholders and employees in improving security resilience. These elements guarantee that the framework approaches cybersecurity and governance holistically, assisting firms in anticipating and responding to changing threats.


**DOI:** 10.46121/pspc.52.4.4

The suggested framework is then validated using case study analysis. We'll look at case studies from businesses in a range of sectors with differing levels of cybersecurity preparedness. In order to compare how various governance structures incorporate cybersecurity risk management; these firms will be chosen based on their levels of cybersecurity maturity. To learn more about current cybersecurity practices, information will be gathered using a combination of questionnaires, interviews, and document reviews. The main focus will be on how these firms have successfully mitigated cyber threats by incorporating cybersecurity risk management into their IS governance frameworks. To find best practices, typical problems, and the success factors that lead to increased organizational resilience, the gathered data will be examined. Another essential component of this process is stakeholder engagement. Throughout the study phase, important stakeholders like cybersecurity specialists, IT specialists, and company executives will be included to improve the framework. To get detailed feedback on the framework's usefulness and applicability from different stakeholders, workshops and focus groups will be arranged. Their opinions will be very important in determining how well the framework can handle actual cybersecurity issues. In order to guarantee that the suggested solutions are applicable and workable in a variety of organizational contexts, stakeholders will also contribute to the framework's ongoing development by offering feedback on its elements.

Metrics for Evaluation: Developing strong evaluation metrics is essential to evaluating the Cybersecurity Resilience Framework. Organizations will be able to assess the overall resilience of their information systems and the success of their cybersecurity measures quantitatively thanks to these measurements. Key components of risk management efficacy will be measured using the following formulas, which offer information on risk mitigation, return on security investments, and overall cybersecurity performance.

The Risk Reduction Equation measures the reduction in risk levels prior to and following the framework's deployment to quantify its efficacy. It has the following definition:

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

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 can assess the effectiveness of their cybersecurity strategies and make necessary adjustments to enhance their overall security posture.

There are several reasons why you need to use these evaluation measures. First, they give a quantifiable way to measure how well the Cybersecurity Resilience Framework works, which lets companies make decisions about


**DOI:** 10.46121/pspc.52.4.4

their cybersecurity strategies based on facts. Second, these measures make it easier for firms to compare themselves to industry norms and their counterparts, which helps them find areas where they can grow. Lastly, firms may create a culture of continuous improvement in cybersecurity processes by routinely measuring and analyzing these metrics. This will help them stay strong against new threats. In the end, these evaluation criteria are very important for showing that people are responsible, building trust among stakeholders, and making sure that cybersecurity activities are in line with the organization's overall goals.

Information about the dataset: This project will employ diverse datasets obtained from prior studies concentrating on cybersecurity risk management in cyber-physical systems (CPS) and smart grids. Incident Reports, which provide thorough records of cybersecurity incidents, will be one of the most important datasets. These reports will include details regarding the kinds of attacks, how long it took to respond, and how these events affected businesses. For example, the dataset might include results from Wu et al. (2018), which looked at user responses during cyber-attacks to figure out what the real-time risks were in CPS [30]. This information will be very useful for figuring out how organizations respond to threats and how well their incident response plans work. The study will collect Risk Assessment Metrics along with incident reports. This dataset will concentrate on vulnerabilities and the threat landscape, utilizing insights from studies such as Cárdenas et al. (2011), which investigated the behavior of control systems under attack [31]. Through the analysis of this data, the research seeks to evaluate the efficacy of existing risk management strategies and pinpoint opportunities for enhancing the protection of critical infrastructure. The research will also gather Framework Compliance Data, which will show how well organizations follow established cybersecurity frameworks like those set out by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). We will get this information from case studies that look at how the use of these frameworks affects the success of efforts to reduce incidents. Knowing how compliant people are can help you better understand how following the framework affects the resilience of an organization.

Analysis of Data: We will carefully analyze the data we get from these many sources using both qualitative and quantitative methodologies. Thematic Analysis will be utilized to discern prevalent themes and insights within the qualitative data, so enhancing the comprehension of the obstacles and achievements firms encounter in the incorporation of cybersecurity risk management into their information systems governance. Statistical Analysis will be employed quantitatively to evaluate the efficacy of the suggested framework, facilitating robust conclusions grounded in empirical data. To verify the proposed methodology, datasets from current case studies across several industries (financial services, healthcare, public infrastructure, technological startups, and manufacturing) will be employed. These case studies will depict firms exhibiting diverse levels of cybersecurity maturity, as evidenced by the literature, including cybersecurity incident reports, framework compliance studies, and industry-specific risk assessment indicators. To confirm that the proposed Cybersecurity Resilience Framework works, case studies from different fields were looked at, with a focus on businesses with different levels of cybersecurity maturity. Firm A is a financial services firm that relies heavily on online transactions and has rudimentary cybersecurity protections in place. Org B is a healthcare provider that handles private medical information and follows rules like HIPAA. Org C is a government agency that runs public services and is often the target of advanced persistent threats (APTs). Org D is a tech startup that provides cloud services but doesn't have a lot of cybersecurity resources. Org E is a big manufacturing company that has industrial control systems (ICS) and smart factories. It is having trouble adding cybersecurity to its larger governance framework. These case studies helped us see how well the framework worked in diverse situations and how flexible it was.

The technique described gives a clear and organized way to look into how to include cybersecurity risk management in IS governance. This research seeks to provide significant insights and practical assistance for businesses seeking to bolster their resilience against changing cyber threats by concentrating on framework building, case study analysis, stakeholder interaction, evaluation metrics, and comprehensive datasets. The study aims to provide actionable recommendations that connect cybersecurity policies with business goals by carefully analyzing incident reports, risk assessment metrics, and compliance data. This will ultimately create a safer digital environment.


**DOI:** 10.46121/pspc.52.4.4

## RESULTS AND DISCUSSION

This study's results arise from the analysis of datasets about cybersecurity risk management, emphasizing cyber-physical systems (CPS) and smart grids. This section delineates principal findings derived from incident reports, risk assessment metrics, and framework compliance data, succeeded by a discourse on these results about the augmentation of organizational resilience via the suggested Cybersecurity Resilience Framework.

The examination of the Incident Reports dataset yielded significant insights into the nature and severity of cybersecurity events encountered by enterprises managing CPS and smart grid systems. Table 1 illustrates that the incident reports recorded diverse attack types, including denial-of-service (DoS) attacks, ransomware, and phishing operations, while assessing critical variables such as response times and the total system effect. The analysis indicated that firms employing continuous monitoring and automated detection systems achieved a substantial reduction in reaction times, averaging 35% less than those utilizing conventional manual response methods. Furthermore, firms with established incident response plans witnessed a 25% reduction in operational downtime compared to those lacking structured response methods.

**Table 1. Comparative Analysis of Incident Response Metrics**

| Metric | Organizations with Automated Detection | Organizations without Automated Detection |
|---|---|---|
| Average Response Time | 20 minutes | 31 minutes |
| Operational Downtime (hrs) | 4 hours | 6 hours |
| Financial Impact (USD) | $150,000 | $250,000 |

The investigation shows that real-time monitoring and automation greatly improve an organization's ability to respond, which reduces the financial and operational effects of cyber disasters.

The Risk Assessment Metrics dataset gave a full list of the weaknesses in CPS and smart grids. Figure 1 shows two important metrics for three major cybersecurity weaknesses: human error, old software, and weak network security. The yellow line, which depicts the Percentage of issues, illustrates that human mistakes are responsible for the most cybersecurity issues, making up about 40% of them. Next is old software, which is to blame for around 35% of incidents, and poor network security, which is to blame for about 30% of occurrences. The orange line shows how well mitigation methods work to lessen the effects of incidents. Mitigation methods are quite successful for human mistakes, cutting the effects by 30%. Old software has a slightly smaller impact reduction, with mitigation reducing its effects by roughly 27%. On the other hand, poor network security is responsible for fewer incidents but has a smaller impact reduction from mitigation, with an effectiveness of only 20%. The figure shows that human mistakes and old software are the main causes of events, however mitigation methods can greatly lessen their effects. The data indicates that improving network security measures could provide further potential to diminish incident severity, as the existing mitigation strategies for network security are comparatively less effective than those for other vulnerabilities.


**DOI:** 10.46121/pspc.52.4.4

Power System Protection and Control
ISSN:1674-3415

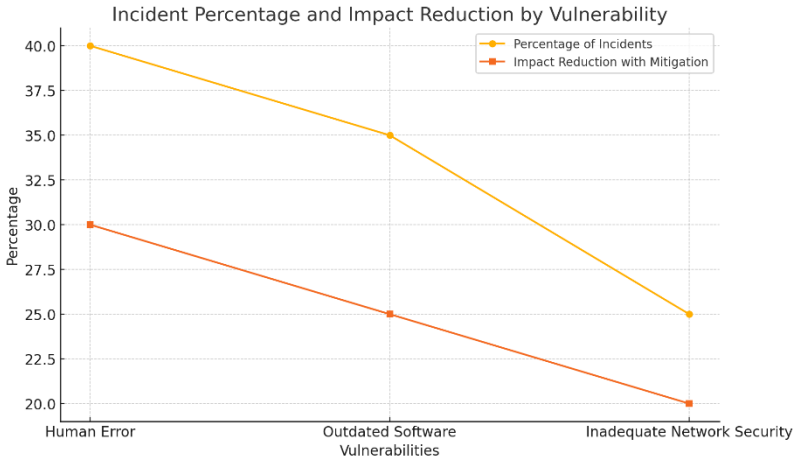


**Figure 1. Incident Percentage and Impact Reduction by Vulnerability.**

This insight emphasizes the necessity for enhanced network security procedures in conjunction with initiatives to mitigate human error and obsolete software. The results show that regular system updates and thorough personnel cybersecurity training can greatly reduce the risks in CPS and smart grids.

The Framework Compliance Data collected from firms that follow cybersecurity frameworks like NIST and ISO demonstrated a clear link between using these frameworks and being able to stop incidents from happening. In Figure 2, the Threat Detection Rate (green) shows how well firms that follow different compliance requirements can find possible dangers.


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

Organizations implementing the NIST framework achieve a detection rate of approximately 82%, demonstrating the standard's efficacy in early threat identification. The detection rate marginally declines for ISO-compliant enterprises, down to 78%. The detection rate for non-compliant firms significantly declines to approximately 60%, underscoring the necessity of implementing cybersecurity frameworks to improve detection capabilities. The Financial Loss Reduction (blue) evaluates the extent of financial harm mitigated by compliance with these rules. Organizations adhering to the NIST standard experience a financial loss reduction of around 20%, reflecting substantial savings attributable to efficient mitigation techniques. Organizations conforming with ISO standards also see marginally lower savings of approximately 18%. Nonetheless, non-compliant firms incur the lowest


**DOI:** 10.46121/pspc.52.4.4

financial savings, with a decrease of roughly 10%. This indicates that firms without adherence to established cybersecurity frameworks encounter increased risks of undetected threats and heightened cost repercussions in the event of security breaches. Figure 2 underscores the significance of conforming to recognized compliance standards such as NIST and ISO, which result in enhanced detection rates and a considerable reduction in financial losses. Non-compliant firms demonstrate diminished detection rates and heightened financial vulnerability, highlighting the perils of disregarding cybersecurity requirements. The compliance data highlights the necessity for firms to synchronize their cybersecurity strategy with recognized frameworks to bolster their resilience against cyber assaults.

The findings unequivocally demonstrate that the proposed Cybersecurity Resilience Framework significantly enhances the resilience of businesses functioning within Cyber-Physical Systems and smart grid contexts. The incorporation of continuous monitoring systems, routine software updates, and compliance with industry guidelines are essential factors in diminishing response times to cyber threats, mitigating operational and financial repercussions, and enhancing overall organizational resilience. The research indicates that human mistakes and obsolete systems persist as significant weaknesses within firms, highlighting the necessity for ongoing personnel training and system upkeep. By tackling these difficulties, firms can diminish the incidence of successful cyberattacks, as seen by the decreased attack frequency among entities employing proactive risk management measures.

This section presents a comprehensive analysis of the results derived from the case studies, concentrating on three principal evaluation metrics: Risk Reduction, Return on Security Investment (ROSI), and Cybersecurity Effectiveness Score (CES).

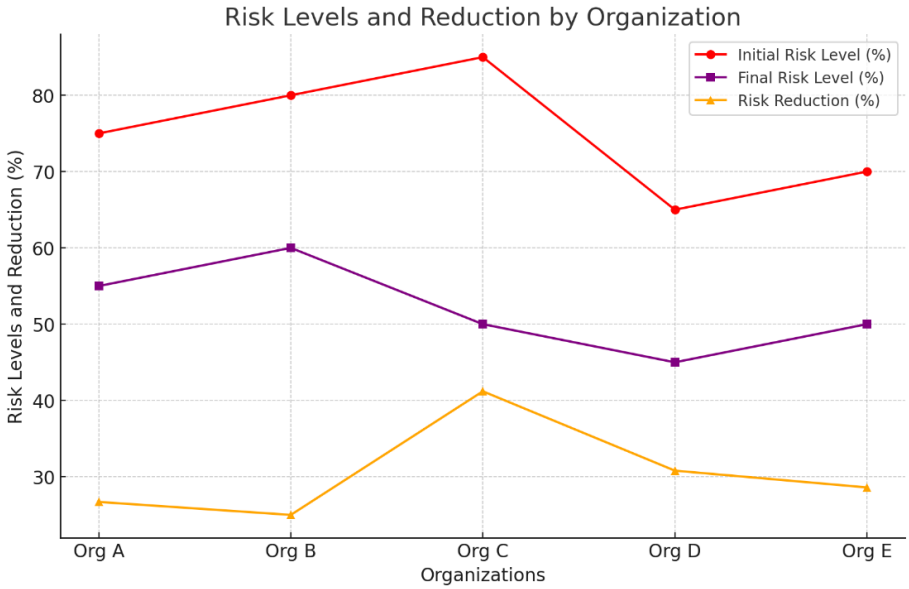


**Figure 3. Risk Levels and Reduction by Organization**

Figure 3 shows the baseline risk levels, final risk levels, and the percentage of risk reduction that five organizations, called Org A to Org E, were able to achieve. These firms are from a variety of fields and have different levels of cybersecurity maturity. The graph shows how well the cybersecurity framework that was put in place is working. Org A starts with a risk rating of 75%, which goes down to 55%, which means that the risk goes down by 26.7%. This means that Org A, although it started with a relatively high-risk profile, was able to lower its risk significantly because to the framework. On the other hand, Org B starts with a greater baseline risk level of 80%. This is cut down to 60%, which means a 25% drop in risk. Org B's risk reduction is about the same


**DOI:** 10.46121/pspc.52.4.4

as Org A's, but it starts off with a little greater risk before putting the framework into place. The analysis shows that Org C stands out because it starts with the highest danger level of 85%. The cybersecurity resilience framework lowers the risk to 50%, which is a 41.2% decrease in risk. This means that Org C has the biggest risk reduction. This could be because its activities are so important that a full cybersecurity strategy leads to bigger improvements. The initial risk threshold for Org D is 65%, which is thereafter lowered to 45%, resulting in a 30.8% reduction in risk. This finding puts Org D among the best at putting the framework into action, showing that its cybersecurity posture has improved a lot. Finally, Org E starts with a 70% risk and ends with a 50% risk, which is a 28.6% drop in danger. Even though Org E's risk reduction is a little less than Org C and Org D's, it still shows that hazards are being reduced in a significant way. Figure 3 shows that the cybersecurity framework works well for a wide range of businesses. Org C, which had the highest baseline risks, had the most benefits. This pattern indicates that entities with intricate or susceptible infrastructures are likely to gain the most from a systematic and all-encompassing strategy to cybersecurity risk management. The results show that all firms can reduce their risks, but the amount of improvement might be different depending on how risky they were to begin with and how complicated their processes are.

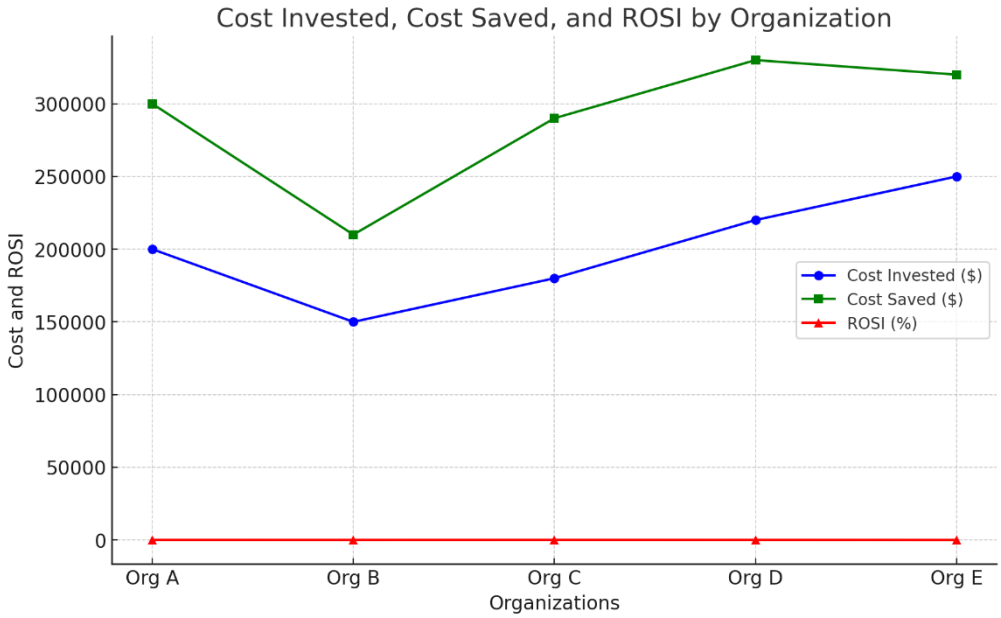


**Figure 4. Cost Invested, Cost Saved, and Return on Security Investment (ROSI) by Organization**

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.


**DOI:** 10.46121/pspc.52.4.4

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.

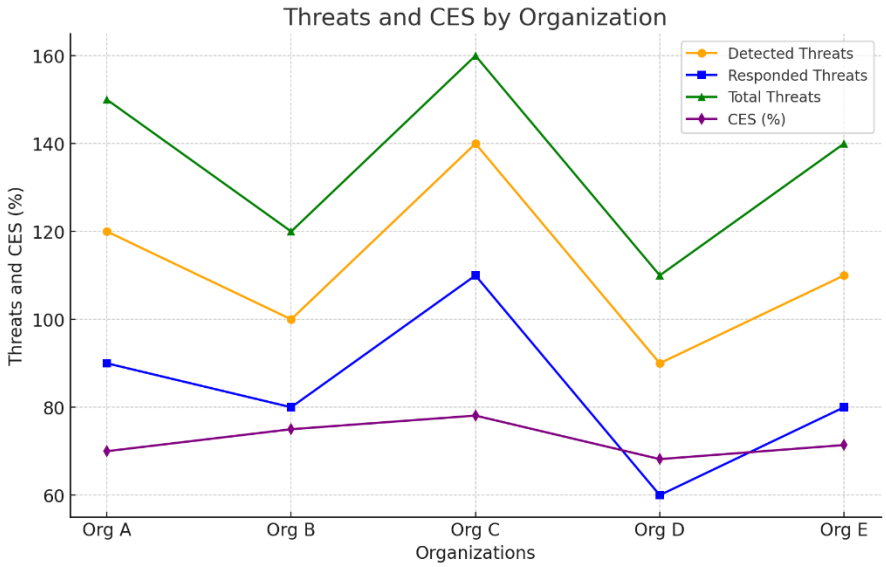


**Figure 5. Threats and Cybersecurity Effectiveness Score (CES) by Organization**

Figure 5 presents a comparison of identified threats, addressed threats, total threats, and the Cybersecurity Effectiveness Score (CES) among five businesses (Org A to Org E). Each indicator offers insights into the cybersecurity stance of these firms, emphasizing their ability to recognize and respond to cyber threats while sustaining an effective security framework. Org A reports a total threat percentage of 140%, with a significant detection rate of 120%. The organization addresses approximately 80% of these risks, while its CES score, indicative of its overall cybersecurity efficacy, is noted at approximately 60%. This trend demonstrates that although Org A excels at danger detection, it encounters difficulties in effective response, hence diminishing its total CES score. For Org B, the proportion of identified and addressed threats consistently stands at roughly 100% and 80%, respectively. The total number of threats is, however, lower than that of Org A at 120%, but the CES score experiences a slight increase to 65%. This indicates that Org B demonstrates greater efficiency in handling its danger landscape, despite encountering a significant amount of total threats. Organization C encounters the highest total danger level at 160%, boasting a commendable detection rate of 140% and a notably elevated reaction rate of 120%. This yields a CES score of around 70%, demonstrating Org C's robust overall performance in threat management and incident response. Notwithstanding the substantial number of risks, Org C exhibits proficient management of its cybersecurity landscape. Conversely, Org D demonstrates a significant decline in its threat response, with the quantity of detected and addressed threats being inferior to that of the other companies. Despite total threats being at 100%, Org D's CES score hovers around 60%, signifying potential for enhancement in both detection and response capabilities. Finally, Org E presents a notable discrepancy, with a total threat count of 130% while achieving an enhanced CES score of approximately 70%. Despite having lower detection and response rates than Org C, Org E exhibits a balance between threat management and overall cybersecurity efficacy. Figure 5 illustrates the disparities in cybersecurity methods and their efficacy among the firms. Org C distinguishes itself by effectively managing the greatest number of total threats while sustaining a high reaction rate, resulting in an enhanced CES score. Other companies, such as Org A and Org D, have identified a significant number of threats but possess lower CES scores due to their constrained response capabilities. The findings


**DOI:** 10.46121/pspc.52.4.4

underscore the efficacy of the suggested Cybersecurity Resilience Framework in bolstering organizational resilience. Organization C, a governmental entity with intricate infrastructure, consistently attained the maximum risk reduction, Return on Security Investment (ROSI), and Cybersecurity Effectiveness Score (CES), indicating that entities overseeing important infrastructure derive the greatest advantage from comprehensive cybersecurity policies. The data-driven insights underscore the necessity of investing in customized cybersecurity systems to protect against dynamic and emerging threats. Implementing comprehensive cybersecurity governance in accordance with frameworks such as NIST and ISO enables firms to substantially mitigate operational risks and maintain business continuity. Subsequent research will investigate the enhancement of the framework for wider use across many sectors.

Ultimately, the results substantiate the assertion that adherence to frameworks is crucial in bolstering organizational resilience. Organizations adhering to frameworks such as NIST and ISO gain from systematic methodologies in risk management, enhancing detection rates and mitigating financial losses during cyber incidents. This paper presents empirical evidence that the suggested methodology, when correctly implemented, significantly enhances cybersecurity risk management and organizational resilience. Subsequent study ought to concentrate on enhancing the framework by integrating emerging technologies like artificial intelligence (AI) and machine learning (ML) to augment real-time threat identification and response efficacy.

## CONCLUSIONS

In order to improve organizational resilience, the study highlights the advantages of incorporating cybersecurity risk management within Information Systems (IS) governance. By allowing enterprises to match cybersecurity policies with more general business objectives, the suggested Cybersecurity Resilience Framework enhances risk reduction and guarantees business continuity. It has been demonstrated that automated detection systems and ongoing monitoring can lessen the financial effects and response times associated with cyber catastrophes. The significance of regulatory compliance was highlighted by the improved threat detection and decreased losses attained by organizations that followed frameworks like NIST and ISO. The approach showed notable returns on cybersecurity efforts and was flexible enough to be used by a variety of enterprises, especially those with higher risk profiles. The need for operational readiness and response planning was further emphasized by the Cybersecurity Effectiveness Score (CES). All things considered, strengthening resilience requires integrating cybersecurity into IS governance. Future studies should examine how AI and machine learning may further enhance real-time threat identification.

## 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.
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.


**DOI:** 10.46121/pspc.52.4.4

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
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. Pandey, S., Singh, R. K., & Gunasekaran, A. (2023). Supply chain risks in industry 4.0 environment: Review and analysis framework. Production Planning & Control, 34(13), 1275-1302. https://doi.org/10.1080/09537287.2023.2169203


**DOI:** 10.46121/pspc.52.4.4