Journal of Borneo-Kalimantan

UNIMAS
UNIVERSITI MALAYSIA SARAWAK
INSTITUTE OF BORNEO STUDIES

RESEARCH NOTE

Enhancing Cybersecurity Compliance: A Multi-Dimensional Analysis of Sarawak Security and Enforcement Unit (SSEU)

Zaihidin Abdul Rahman,[1*] Halikul bin Lenando[1] & Ani Hafiffy Anil Yakin[1]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300, Kota Samarahan, Sarawak

**Corresponding author: zaihidinar@sarawak.gov.my*

Received Date: 30 May 2026 Accepted Date: 24 June 2026 Publish Date: 29 June 2026

ABSTRACT

The increasing digitalization of governmental operations has heightened cybersecurity risks, emphasizing the need for robust compliance frameworks to protect sensitive information. While the Sarawak Government ICT Security Policy (Dasar Keselamatan ICT Kerajaan Negeri Sarawak Bil. 1/2012) addresses these challenges, significant compliance disparities persist across hierarchical levels within the Sarawak Security and Enforcement Unit (SSEU). This study evaluates cybersecurity compliance levels, identifies barriers and proposes hierarchical-level-specific strategies to address gaps in cybersecurity compliance within the SSEU. Using a quantitative research design and stratified random sampling, data was collected from SSEU employees across four hierarchical levels via structured digital questionnaires were evaluated using descriptive and inferential statistical approaches including ANOVA and regression analysis. Results revealed that top management exhibited the highest compliance levels due to greater awareness and training, whereas operational groups (AKP1 and AKP2) faced challenges such as insufficient training, weak enforcement mechanisms and time constraints that highlighting systemic gaps in resource allocation and policy dissemination. Addressing these gaps requires targeted training programs, stronger enforcement mechanisms and strategic leadership support to enhance cybersecurity practices across all organizational levels. Future work should include qualitative exploration of employee behavior and organizational culture, as well as the development of advanced diagnostic tools for real-time compliance monitoring.

Keywords— Cybersecurity compliance; Sarawak ICT Security Policy; organizational hierarchies; cybersecurity awareness; policy enforcement

INTRODUCTION

Background Study

The increasing reliance on digital technologies in governmental operations has heightened the need for strong cybersecurity safeguards to safeguard sensitive data and maintain operational continuity. As governmental agencies adopt advanced information and communication technologies (ICT) to enhance efficiency and service delivery, they become increasingly vulnerable to evolving cyber threats. Cybersecurity breaches can compromise the confidentiality, integrity and availability of critical data, resulting in severe consequences for public safety and service reliability. Effective cybersecurity strategies must be innovative and adaptable to evolving threats, utilizing the latest technologies and fostering cross-sector collaboration. This underscores the critical need for comprehensive cybersecurity policies that are not only well-designed but also effectively implemented. Effective cybersecurity strategies must be innovative and adaptable to evolving threats, utilizing the latest technologies and fostering cross-sector collaboration (Sendjaja *et al.*, 2024). Public organizations should enhance cybersecurity awareness across all functional areas, ensuring that tactical and operational teams are well-prepared to implement security measures (Domínguez-Dorado *et al.*, 2023).Cybersecurity, therefore, emerges as a fundamental component in protecting critical information systems against unauthorized access, breaches, and cyberattacks.

The state of Sarawak, Malaysia has recognized the importance of cybersecurity in safeguarding its digital infrastructure. In response, the Sarawak Government introduced *Dasar Keselamatan ICT Kerajaan Negeri Sarawak Bil. 1/2012* (Sarawak Government ICT Security Policy). This policy is a strategic guideline designed to address cybersecurity risks by providing a comprehensive framework for ensuring the secure use of information and communication technologies (ICT) within state agencies. It outlines key principles, including user responsibilities, system security requirements and mechanisms for monitoring compliance to mitigate cybersecurity risks. Establishing robust legal frameworks is essential for protecting the information sphere from cyberattacks, aligning national legislation with international standards (Skrypniuk *et al.*, 2024).

Despite the existence of this policy, challenges persist in ensuring that all personnel across different hierarchical levels fully understand and adhere to the prescribed standards. Many personnel lack a comprehensive understanding of cybersecurity policies, which can lead to unintentional breaches (Sarmoen *et al.*, 2019). The Sarawak Security and Enforcement Unit (SSEU) serves as a vital arm of the state government, tasked with maintaining public safety and enforcing regulatory compliance. Given its role, SSEU relies heavily on ICT systems to manage operations and coordinate activities efficiently. This dependence underscores the importance of strict adherence to cybersecurity policies to protect sensitive data and ensure uninterrupted functionality. However, the multi-tiered structure of SSEU with roles ranging from strategic oversight at the top to hands-on operational implementation creates potential disparities in compliance levels. SSEU, a key government agency tasked with maintaining public safety and regulatory enforcement exemplifies these challenges. While top management demonstrates alignment with strategic compliance objectives, operational groups often face barriers such as limited awareness, insufficient training, and resource constraints, resulting in varying levels of adherence.

Cybersecurity compliance does not serve as a universal solution; instead, it requires tailored approaches that account for varying roles, responsibilities and technical proficiencies

within an organization. Operational teams often face budgetary and resource limitations, hindering their ability to implement necessary security measures (Sarmoen *et al.*, 2019). For example, senior management may focus on strategic decision-making without delving into the operational intricacies of cybersecurity, whereas frontline staff might lack the resources or training needed to implement secure practices effectively. Effective management principles are crucial for implementing internal social policies within organizations. A structured approach to management can enhance policy enforcement by ensuring that all levels of the organization are aligned with the policy objectives.

Globally, similar trends have been observed, where gaps in cybersecurity compliance arise due to a lack of alignment between policy frameworks and the realities of organizational practices. These gaps often stem from factors such as limited training, insufficient enforcement or a lack of resources dedicated to cybersecurity initiatives. Regular training programs are crucial; without them, employees may not recognize the importance of compliance (Sarmoen *et al.*, 2019)(Ali, Dominic and Ali, 2020). In the context of Sarawak, it is crucial to examine how such factors play out within SSEU and to identify ways to bridge these compliance gaps effectively. The fidelity of policy implementation is often compromised due to a lack of coherence and support from management. The adaptation of policies at lower levels can lead to discrepancies between intended and actual outcomes, highlighting the need for strong management support to bridge these gaps (Mitra, 2022). Information and analytical support play a vital role in the management of socio-economic and law enforcement activities. A comprehensive diagnostic approach can help identify issues and improve policy enforcement by providing a framework for effective decision-making (Zakhozhai, 2023).

Additionally, the advent of increasingly sophisticated cyber threats amplifies the need for proactive cybersecurity measures. Cybercriminals now employ advanced tactics, ranging from phishing and ransomware to state-sponsored cyberattacks, targeting governmental agencies for espionage or disruption. The evolving threat landscape makes it imperative for agencies like SSEU to not only comply with existing policies but to continuously adapt and enhance their cybersecurity practices. This study delves into the underlying factors that influence cybersecurity compliance within SSEU. By adopting a multi-dimensional perspective, it aims to capture the complexity of compliance dynamics and provide actionable insights. The study acknowledges that cybersecurity is more than just a technological problem but also a human and organizational one requiring a holistic approach to identify and address vulnerabilities effectively.

Problem Statement

Within the Sarawak State Enforcement Unit (SSEU), varying levels of compliance with the Sarawak Government ICT Security Policy (Dasar Keselamatan ICT Kerajaan Negeri Sarawak Bil. 1/2012) have been observed. These differences stem from disparities in roles, responsibilities, and access to resources across hierarchical levels. While top management tends to align with strategic cybersecurity requirements, operational groups encounter significant challenges. These include limited awareness, insufficient training, and inconsistent policy enforcement, which collectively compromise the agency's overall cybersecurity posture. Systemic issues further exacerbate these challenges, such as outdated technological infrastructure, inadequate resource allocation, and a lack of tailored strategies that address the unique needs of different organizational roles. These factors contribute to disparities in adherence to cybersecurity policies, increasing the vulnerability

of critical ICT systems to potential threats and weakening the resilience of governmental operations.

At present, there is no established framework capable of systematically identifying the root causes of cybersecurity compliance gaps within the Sarawak State Enforcement Unit (SSEU). While existing policies outline general requirements, they lack a structured approach to diagnose specific challenges faced by various organizational levels. This absence of a comprehensive framework hinders the ability to pinpoint factors such as resource disparities, role-based inconsistencies, and enforcement deficiencies that contribute to non-compliance. Without such a mechanism, efforts to address these issues remain fragmented and reactive, leaving critical ICT systems vulnerable to threats. Developing a robust diagnostic tool is therefore essential for improving compliance.

Investigating cybersecurity compliance within the Sarawak State Enforcement Unit (SSEU) is crucial to address existing challenges and improve the agency's overall cybersecurity posture. By understanding the root causes of compliance gaps, targeted strategies can be developed to address key issues, such as resource disparities, inadequate training, and inconsistent enforcement. This investigation will enable the design of tailored approaches that consider the unique roles and responsibilities within the organization, fostering a more cohesive and resilient cybersecurity framework. Ultimately, this effort will enhance the implementation of cybersecurity measures, reduce vulnerabilities, and strengthen the agency's ability to safeguard critical ICT systems.

LITERATURE REVIEW

Overview of Cybersecurity Compliance

Cybersecurity compliance has emerged as a pivotal element in ensuring organizational resilience, particularly within governmental frameworks where the security of critical information systems is paramount. Compliance entails adherence to established standards, regulations, and best practices designed to safeguard information and communication technologies (ICT) from a growing array of cyber threats. Compliance not only ensures regulatory adherence but also enhances an organization's capacity to address threats and rebound from security breaches. However, it presents challenges, including resource demands and the need for continuous updates to address evolving threats (Adebola Folorunso *et al.*, 2024a)(Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu and Adefolake Olachi Adewusi, 2024). The significance of cybersecurity compliance becomes even more pronounced in the context of public sector entities like the Sarawak Security and Enforcement Unit (SSEU), given their role in maintaining public trust and service continuity. While cybersecurity compliance is essential for protecting organizational assets, it is often perceived as a "check-the-box" activity, which may not fully address actual security needs. This perception can lead to gaps between regulatory adherence and effective security measures, emphasizing the importance of taking a proactive approach, risk-based approach to compliance management (Adebola Folorunso *et al.*, 2024a).

Definition and Importance of Cybersecurity Compliance in Governmental Organizations: In the realm of governmental operations, cybersecurity compliance can be defined as the structured adherence to specific policies, standards and frameworks designed to mitigate risks linked to data breaches, unauthorized access and various cyberattacks(Adebola Folorunso *et al.*,

2024a). Governments hold extensive sensitive data, encompassing personal citizen information, critical infrastructure blueprints and intelligence materials. In governmental organizations, compliance involves aligning with international standards like ISO/IEC 27001 and NIST, which provide a structured approach to managing information security (Magnusson, Dalipi and Elm, 2023). While cybersecurity compliance is essential for governmental organizations, it is not a panacea for all cybersecurity challenges. Compliance alone does not guarantee robust security, as it often focuses on meeting minimum standards rather than addressing all potential vulnerabilities. Organizations must adopt a proactive security strategy that goes beyond compliance to effectively counter the evolving threat landscape. This includes integrating risk-based approaches and leveraging automation to enhance compliance management and overall cybersecurity posture (Adebola Folorunso *et al.*, 2024a)(Madnick *et al.*, 2019).

A lack of compliance increases the risk of data breaches, undermines public confidence, and disrupts essential public services. As such, robust compliance mechanisms ensure operational integrity, resilience against cyber incidents and adherence to legal and ethical obligations. Effective cybersecurity compliance frameworks typically emphasize risk management, incident response planning and employee awareness to counter evolving threats (Adebola Folorunso *et al.*, 2024a)(Harris and Martin, 2019). By prioritizing compliance, governments also create a culture of proactive defence, ensuring their systems remain secure and resilient in the face of persistent cyber threats. For government agencies, compliance is crucial in establishing a resilient cybersecurity posture to protect public data and services from cyberattacks(Magnusson, Dalipi and Elm, 2023). Governmental organizations often face challenges in implementing cybersecurity measures due to complex bureaucratic processes and the need to align with various stakeholders (Alam, Ibrahim and Karas, 2024). Employee behaviour and awareness significantly impact compliance. Government social media (GSM) and organizational policies play a role in enhancing cybersecurity awareness and protective behaviours among employees (Tran *et al.*, 2024)(Tran *et al.*, 2024).

Global Context: Cybersecurity Compliance in Protecting Governmental Operations: On a global scale, cybersecurity compliance is widely acknowledged as a critical measure for securing governmental systems and operations. Modern governments are increasingly reliant on interconnected ICT infrastructures to deliver public services, ranging from healthcare and education to law enforcement and transportation. These systems, while enabling efficiency, are vulnerable to cyberattacks aimed at disrupting national security, stealing sensitive information or causing public disorder.

Sarawak Context: The Role of the Sarawak Government ICT Security Policy: The Sarawak Government ICT Security Policy plays a crucial role in safeguarding the state's digital infrastructure and ensuring the secure transition towards a digital economy. This policy is integral to the broader digital transformation efforts in Sarawak, which aim to enhance economic growth, improve governance and address urbanization challenges through technology. The policy's implementation is essential for protecting sensitive information and maintaining the integrity of digital services, which are vital for the state's socio-economic development. In Sarawak, Malaysia, cybersecurity compliance is anchored in the Sarawak Government ICT Security Policy (Dasar Keselamatan ICT Kerajaan Negeri Sarawak Bil. 1/2012). National Cyber Security Policy (NCSP) provides a framework for safeguarding critical national information infrastructure, which is relevant to Sarawak's efforts to secure its digital assets

(Fazlan, Nadia and Zahri, 2018). These policies serve as a comprehensive guide for public sector organizations, including the Sarawak Security and Enforcement Unit (SSEU) to secure their ICT infrastructures against a dynamic threat landscape.

The policy outlines structured guidelines addressing key areas such as access control, data protection, network security and incident response. Sarawak is undergoing a significant digital transformation, marked by initiatives like the Sarawak Digital Economy Strategy 2018–2022, which aims to modernize the state's economy and governance through technology (Goi, 2022). By aligning with these standards, public agencies in Sarawak can mitigate risks associated with cyberattacks and unauthorized access to sensitive information. As digital technologies become more prevalent, the risk of cyber threats increases. Effective ICT security policies are necessary to protect against unauthorized access, data breaches and other cyber threats that could disrupt services and harm the economy (Haris@Harib, Sarijan and Hussin, 2017a)(Fazlan, Nadia and Zahri, 2018).

The Sarawak Government ICT Security Policy also emphasizes employee training and awareness, recognizing that human error often serves as a critical vulnerability in cybersecurity breaches. The Sarawak Government ICT Security Policy supports the growth of e-commerce by ensuring a secure environment for online transactions. This is crucial for the adoption of e-commerce services, which are a key component of the state's digital economy strategy (Ahmad *et al.*, 2019)(Serojai, Ujir and Hipiny, 2021). For the SSEU, compliance with this policy ensures not only the security of its operations but also the protection of the public interest it serves. By embedding these measures into its operational framework, the SSEU exemplifies a proactive approach to addressing the region’s cybersecurity challenges, thereby reinforcing trust in Sarawak's digital governance.

Moreover, Sarawak’s commitment to ICT security aligns with Malaysia’s broader vision for digital transformation, as outlined in the Malaysia Cyber Security Strategy 2020-2024, which seeks to enhance the nation's overall cyber resilience. The dynamic nature of cyber threats necessitates ongoing updates and improvements to the ICT security policy to adapt to new challenges and technologies (Haris@Harib, Sarijan and Hussin, 2017b). Regular review and development of cybersecurity policies, along with enforcement mechanisms, are crucial for maintaining compliance (Alam, Ibrahim and Karas, 2024). Addressing the digital divide between urban and rural areas is a challenge that the Sarawak Government ICT Security Policy must consider. Ensuring secure and equitable access to digital resources is essential for inclusive development (Horn and Gifford, 2022). Consequently, the Sarawak Government ICT Security Policy not only serves as a localized compliance framework but also contributes to Malaysia's efforts to address global cybersecurity challenges effectively.

Factors Influencing Cybersecurity Compliance

The successful implementation of cybersecurity compliance measures in organizations is contingent on a range of interrelated factors. These factors can be broadly categorized into individual, organizational and systemic domains. Each of these domains plays a critical role in determining the effectiveness of compliance strategies, particularly in governmental institutions like the SSEU, which operate in a highly regulated and resource-sensitive environment.

Individual Factors: Awareness, Training and Technical Proficiency: At the individual level, the awareness and technical proficiency of employees are fundamental to ensuring adherence to cybersecurity policies. Employees represent the first line of defence against cyber threats and their actions can either fortify or compromise an organization's cybersecurity posture.

Studies have consistently shown that cybersecurity awareness campaigns and regular training sessions significantly reduce incidents of non-compliance and accidental breaches. The intention to comply, influenced by awareness and understanding of security policies plays a crucial role. Security education and awareness programs can improve employees' intention to comply (Chiniah and Ghannoo, 2023)(Ofori *et al.*, 2022). Effective training and awareness programs are essential to improve employee compliance with cybersecurity policies (Thamae, Abdullah and Mujinga, 2024). For example, programs that emphasize phishing detection, safe password practices and secure data handling equip employees with the knowledge to identify and avoid common cyber risks. There is a demand for improved cyber situational awareness (SA) among security practitioners in Malaysia. However, the current capabilities and assessments do not meet this demand. Enhancing SA involves understanding it from the perspective of human operators and developing methods to measure and improve it effectively (Gutzwiller, Dykstra and Payne, 2020). In the context of SSEU, fostering a culture of continuous learning is critical to ensuring that employees understand and internalize the principles outlined in the Sarawak Government ICT Security Policy.

Organizational Factors: Leadership Support, Enforcement Mechanisms, and Resource Allocation: Organizational factors, particularly leadership commitment and resource management, are critical enablers of cybersecurity compliance. Institutions that prioritize cybersecurity at the strategic level tend to demonstrate higher levels of policy adherence and resilience against cyber threats.

Strong leadership and commitment from top management are critical in fostering a culture of compliance. Management's active involvement in promoting security policies can significantly influence employees' compliance behaviour (Assefa and Tensaye, 2021). Leaders who actively endorse and communicate the importance of cybersecurity initiatives signal to employees that compliance is a priority. At SSEU, leadership can drive this agenda by regularly assessing compliance metrics, addressing gaps and reinforcing the significance of complying to ICT security policies. Robust enforcement mechanisms ensure that policies are applied uniformly and deviations are promptly addressed. Mechanisms such as regular audits, incident reporting systems and clear disciplinary procedures for non-compliance are essential. For SSEU, integrating these mechanisms with their operational workflows ensures a structured approach to cybersecurity management. Adequate allocation of financial and human resources is indispensable for maintaining compliance. Implementing cybersecurity measures requires investments in advanced technologies, employee training programs, and expert consultation.

Systemic Factors: Infrastructure Limitations, Technological Advancements and Policy Clarity: The systemic environment in which an organization operates also significantly influences its ability to achieve cybersecurity compliance. These factors are often external to the organization but have a profound impact on its compliance capabilities.

Inadequate infrastructure, such as outdated ICT systems and insufficient network security tools, poses a significant challenge to cybersecurity compliance. For SSEU, ensuring that their ICT infrastructure aligns with the standards set forth in the Sarawak Government ICT Security Policy is a foundational requirement. Upgrading legacy systems, implementing robust firewalls and ensuring secure data storage are crucial steps toward achieving compliance. Developing methods to measure security performance can help organizations assess their ability to protect, discern, react, and recover from cyberattacks (Magnusson, Dalipi and Elm, 2023). While technological advancements can enhance cybersecurity, they also introduce new risks. Emerging advancing technologies such as cloud computing, Internet of Things (IoT) and artificial intelligence (AI) present opportunities for improved security but require updated compliance frameworks. SSEU must remain agile in adapting its policies to accommodate these advancements while mitigating associated risks. The ease of use and accessibility of security tools can affect compliance. Tools that are user-friendly and integrate seamlessly into daily operations encourage adherence to security policies (Abukar Aweis, Isak Abdirahman and Jeilani Mohamud, 2024).

While these factors provide a comprehensive view of the influences on cybersecurity compliance, it is important to consider the dynamic nature of the cybersecurity landscape. As threats evolve, organizations must continuously adapt their compliance strategies to address new challenges. Additionally, the balance between regulatory compliance and proactive security measures remains a critical consideration, as organizations strive to protect against emerging threats while meeting existing standards (Adebola Folorunso *et al.*, 2024c).The interplay between individual, organizational and systemic factors highlights the multifaceted nature of cybersecurity compliance. For entities like SSEU, addressing these factors requires a holistic approach that combines employee training, strategic leadership, resource investment and policy refinement. By aligning efforts across these dimensions, SSEU can strengthen its cybersecurity posture and ensure sustained adherence to the Sarawak Government ICT Security Policy.

The digital divide in Sarawak, particularly between urban and rural areas, exacerbates cybersecurity challenges. Many remote villages in Sarawak lack basic infrastructure such as paved roads and grid electricity, which hampers the deployment of digital technologies. Although mobile phone and internet access have been introduced under Malaysia's Universal Service Provision, the quality and speed of these services remain inadequate for many users (Horn and Rennie, 2018). In rural areas, the use of smartphones for information search is prevalent, but the effectiveness is limited by low-speed internet and limited digital literacy. A strong connection exists between the perceived usefulness of smartphones and their actual use, indicating a need for improved digital literacy training (Sandun, Alan and Mat Jusoh, 2023). Rural agencies often lack access to advanced technologies and sufficient training resources, making compliance more difficult compared to their urban counterparts. While significant progress has been made in addressing the digital divide in Sarawak, the issue remains complex and multifaceted. The digital divide is not only about access to technology but also involves the skills and cultural relevance of digital content. Efforts to bridge this divide must consider the unique needs and contexts of rural communities, ensuring that technology is both accessible and meaningful. Additionally, the role of alternative media and digital platforms in shaping political and social landscapes in Sarawak highlights the broader implications of digital access beyond mere connectivity(Fernandez, Pandian and Abu Bakar, 2014).

The integration of advanced technologies, such as those used in automotive systems, presents cybersecurity challenges. The adoption of standards like ISO/SAE 21434 is necessary to

manage cybersecurity risks effectively. This standard provides a framework for identifying, assessing and mitigating risks throughout the lifecycle of automotive systems (Siddiqui *et al.*, 2023). The use of machine learning in cybersecurity is still in its nascent stages in Malaysia. While it offers potential for addressing complex cyber threats, further research and development are needed to mature these technologies and integrate them effectively into existing cybersecurity frameworks (Rananga and Venter, 2024).

While these gaps highlight significant challenges, they also present opportunities for growth and improvement. By addressing these issues, Malaysia can enhance its cybersecurity resilience and competitiveness on a global scale. Moreover, the development of national standards harmonized with international guidelines, such as ISO 27032, can provide a structured approach to improving cybersecurity practices across various sectors (Markov and Tsirlov, 2014). However, the rapid evolution of cyber threats necessitates continuous adaptation and innovation in cybersecurity strategies to stay ahead of potential risks.

The existing literature on cybersecurity compliance reveals notable inconsistencies and gaps that hinder the development of effective, multi-dimensional strategies. These challenges are especially pertinent in the Sarawak and Malaysian contexts, where unique regional and cultural factors shape the cybersecurity landscape. Addressing these gaps requires a shift toward more inclusive research methodologies that integrate technical, human, organizational, and systemic dimensions. For SSEU and similar agencies, localized and context-specific analyses are essential to bridge the gap between policy and practice, ensuring sustainable compliance in an era of evolving cyber threats.

RESEARCH METHODOLOGY

Research Design

This study adopts a quantitative research design to assess cybersecurity compliance within the Sarawak Security and Enforcement Unit (SSEU). A multidimensional framework is employed to investigate the influence of individual, organizational, and systemic factors on adherence to the Sarawak Government ICT Security Policy (Dasar Keselamatan ICT Kerajaan Negeri Sarawak Bil. 1/2012). This design facilitates a holistic evaluation of compliance gaps across multiple hierarchical levels within the SSEU, ensuring a comprehensive understanding of the challenges and enabling the development of targeted, evidence-based strategies to address them effectively. Compliance frameworks ensure consistent security measures and foster a security-first culture across all organizational levels(Adebola Folorunso *et al.*, 2024d). The study also applies PMT and TAM to guide the survey design and data analysis where PMT constructs include Threat Appraisal which assesses employees perceptions of the severity of cybersecurity threats and their vulnerability to such threats and Coping Appraisal, which measures self-efficacy (confidence in following policies), response efficacy (belief in the effectiveness of measures) and response costs (effort required to comply). TAM constructs include Perceived Usefulness, which explores whether employees believe cybersecurity tools enhance their work efficiency and Perceived Ease of Use,which evaluates whether employees find these tools intuitive and user-friendly.

Population and Sampling

The importance of selecting appropriate sampling methods is highlighted in quantitative research, where different techniques such as simple random sampling, stratified sampling and convenience sampling are employed based on the research objectives and population characteristics(Hossan, Dato' Mansor and Jaharuddin, 2023). The target population for this study comprises employees of the Sarawak Security and Enforcement Unit (SSEU) across all hierarchical levels, including Top Management, the Management and Professional Group, Implementation Group I and Implementation Group II. A stratified random sampling technique is utilized to ensure proportional representation from each hierarchical group, facilitating the identification of compliance variations across organizational strata. The sample size is determined in accordance with the total population of SSEU employees, ensuring statistical reliability, representativeness and the robustness of the study's findings.

TABLE 1. *Categories of The Employee*

Category	Description
Top Management (TM)	This group includes the highest level of decision-makers and strategic planners within the organization. Their role is crucial in shaping cybersecurity policies and ensuring compliance at an institutional level.
Management and Professional Group (P&P)	This level consists of middle-management personnel and professionals who play a pivotal role in implementing policies, managing resources and overseeing cybersecurity measures.
Implementation Group I (AKP1)	Employees in this category are primarily involved in operational activities and the execution of cybersecurity strategies. Their adherence to policies is key to effective implementation.
Implementation Group II (AKP2)	Representing the frontline workforce, this group is responsible for carrying out routine tasks and interacting directly with technological and operational systems.

Data Collection Methods

TABLE 2. provides a detailed breakdown of the survey questionnaire used for data collection in the study. The questionnaire, consist of a total of 24 questions is divided into five sections, each designed to capture specific dimensions of cybersecurity compliance and practices. The questionnaire's structure ensures a comprehensive evaluation of factors influencing cybersecurity compliance by balancing demographic data, awareness, policy enforcement, risk perception and practical application. The distribution of questions across these categories reflects the multidimensional approach of the study, enabling a nuanced understanding of compliance behaviours within the SSEU.

TABLE 2. *Number of Questionnaire*

Type of questions	Number of questions
Section A: Demographic	6
Section B: Awareness of Cirrcular	5
Section C: Organization's Cyber Security Policies	4
Section D: Cybersecurity Risk	4
Section E: Cybersecurity Practices	5
Total Questions	24

Scope and Limitations

This research is confined to the Sarawak Security and Enforcement Unit (SSEU), with a specific focus on adherence to the Sarawak Government ICT Security Policy. While the findings are intended to address compliance gaps within SSEU, their applicability to other government agencies may be limited. Potential challenges include participant availability and the risk of response bias, which may influence the data collection process. Despite these limitations, the study seeks to generate meaningful insights and actionable recommendations to enhance cybersecurity compliance within the Sarawak public sector.

The study employs a structured and systematic methodology to evaluate cybersecurity compliance within the Sarawak Security and Enforcement Unit (SSEU). By adopting quantitative research design and leveraging a multidimensional framework, the study ensures a comprehensive examination of individual, organizational and systemic factors influencing adherence to the Sarawak Government ICT Security Policy. Through a stratified random sampling approach, proportional representation across hierarchical levels is achieved, enhancing the validity and reliability of the findings. Data collection, facilitated by a structured digital questionnaire, ensures accessibility and high response rates, while rigorous statistical analyses provide meaningful insights into compliance patterns and determinants. Ethical considerations, including informed consent and data confidentiality, are prioritized throughout the process. Despite limitations in generalizability and potential response bias, the methodology is designed to yield robust, actionable insights and recommendations to improve cybersecurity compliance within the Sarawak public sector.

DISCUSSION

The findings of this study highlight critical gaps in cybersecurity compliance across the hierarchical levels of the Sarawak Security and Enforcement Unit (SSEU) with operational groups (AKP1 and AKP2) displaying lower awareness and training levels compared to Top Management and the Professional & Management (P&P) group. This discussion addresses these findings, aligning them with research questions and objectives to provide actionable insights.

Cybersecurity Compliance Levels Across Hierarchical Groups

The study reveals significant disparities in compliance levels, particularly between Top Management and the operational groups. Top Management demonstrates the highest awareness and understanding of the Sarawak Government ICT Security Policy, consistent training exposure and frequent engagement with cybersecurity discussions. In contrast, AKP1 and AKP2 exhibit low mean scores for policy awareness and training participation, reflecting practical barriers to compliance. These gaps are attributed to limited exposure to training programs and inadequate policy dissemination mechanisms.

While the ANCOVA results showed no statistically significant differences in policy understanding across hierarchical groups, practical disparities observed in descriptive statistics underscore the need for targeted training and awareness campaigns for operational groups. This aligns with findings from the literature, which emphasize the critical role of tailored training in bridging compliance gaps at the operational level.

Operational and Systemic Challenges in Compliance

The findings identify key barriers to compliance, including insufficient training, weak policy enforcement mechanisms and resource limitations. Operational staff reported time constraints as a significant challenge, indicating that balancing daily tasks with cybersecurity obligations is a recurring issue. Moreover, resource disparities, particularly in AKP2, exacerbate these challenges, leaving frontline employees with inadequate access to the tools and knowledge required for compliance.

Weak enforcement mechanisms, highlighted by employees across all levels, suggest systemic gaps in leadership-driven accountability. Although Top Management displays consistent compliance and training, their role in cascading policies and monitoring adherence at lower levels remains limited. The absence of structured mechanisms for policy enforcement, such as regular audits and performance tracking, undermines the agency's ability to achieve uniform compliance.

Based on the findings, a hierarchical pyramid framework has been developed to align roles, responsibilities and compliance measures across different organizational strata within the SSEU. Fig 6 shows a framework to ensures that interventions address specific challenges faced by Top Management (TM), Professional & Management Group (P&P), Implementation Group I (AKP1) and Implementation Group II (AKP2), fostering a multi-dimensional approach to compliance improvement.

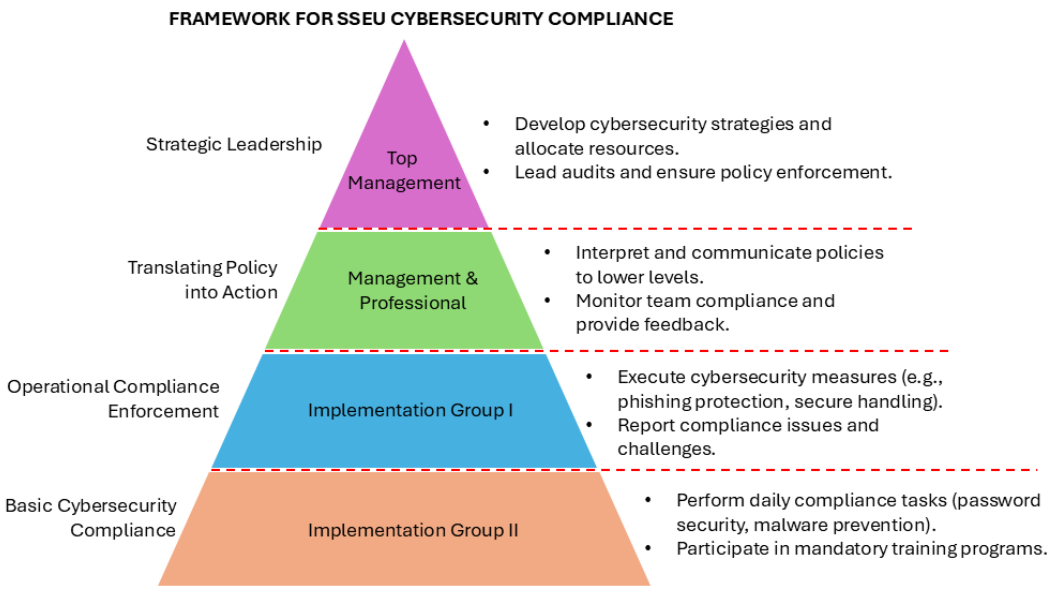

FIGURE 1. *SSEU Hierarchical-Level-Specific Strategies Framework of Cybersecurity Compliance*

This study identified significant disparities in cybersecurity compliance across hierarchical levels within SSEU with Top Management demonstrating stronger alignment with policies while operational groups (AKP1 and AKP2) faced challenges such as insufficient training, resource limitations and weak enforcement mechanisms. To address these gaps, a hierarchical pyramid framework was developed, aligning roles, responsibilities and tailored interventions across four levels which is Top Management, P&P, AKP1 and AKP2. This framework ensures top-down communication of policies, upward reporting for accountability and targeted strategies to improve awareness, training, and resource allocation. By implementing this framework, SSEU can foster a culture of compliance, enhance its cybersecurity posture, and reduce vulnerabilities in line with the Sarawak Government ICT Security Policy.

CONCLUSION

This study provides a detailed evaluation of cybersecurity compliance within the Sarawak Security and Enforcement Unit (SSEU), emphasizing the critical factors influencing adherence to the Sarawak Government ICT Security Policy. The findings highlight significant disparities across hierarchical levels, with operational staff facing greater challenges due to limited awareness, insufficient resources and weak enforcement mechanisms. By adopting a multi-dimensional approach, the study underscores the importance of addressing human, organizational and technological factors to enhance cybersecurity resilience in public administration. The findings underscore the importance of a multi-dimensional approach to advancing cybersecurity compliance in the Sarawak Civil Service and similar public administration systems. Tailored training, resource optimization, leadership advocacy, and cultural transformation are critical to fostering a proactive and resilient cybersecurity environment. Policymakers and practitioners must prioritize these strategies to build trust, engagement, and compliance at all levels. By addressing the challenges identified, public sector organizations can achieve greater cybersecurity resilience and safeguard critical systems in an increasingly complex threat landscape. This study provides a

foundation for enhancing cybersecurity practices and compliance frameworks in public administration paving the way for secure and effective governance.

ACKNOWLEDGEMENT

This research would not have been possible without the invaluable support and contributions of various individuals and institutions. First and foremost, I would like to extend my deepest gratitude to Associate Professor Dr. Halikul Bin Lenando, my esteemed supervisor, for his unwavering guidance, insightful feedback, and invaluable support throughout the research process. I also wish to acknowledge the Sarawak Security and Enforcement Unit (SSEU) for their collaboration and for granting access to the necessary data and organizational resources. I further extend my appreciation to the Sarawak Civil Service (SCS) for their commitment to fostering cybersecurity resilience and enhancing policy adherence across public administration.

In addition, I acknowledge the responsible use of artificial intelligence (AI) tools, including Google Gemini, ChatGPT, Microsoft Copilot, and Claude, during the preparation of this thesis. These tools were utilized to support language refinement, improve grammar and writing clarity, assist in summarizing relevant literature, and facilitate brainstorming and idea organization. All AI-generated outputs were carefully reviewed, verified, and revised by the researcher. The interpretation of findings, analysis, conclusions, and the overall intellectual content of this research remain entirely the responsibility of the researcher.

REFERENCES

Abukar Aweis, Z., Isak Abdirahman, M. A., & Jeilani Mohamud, A. (2024). *Factors influencing information security policy compliance behavior: A case study of healthcare workers in a private hospital in Mogadishu, Somalia*. *International Journal of Innovative Science and Research Technology (IJISRT)*, 3425–3436. https://doi.org/10.38124/ijisrt/IJISRT24JUL1238

Adebola Folorunso, et al. (2024). *Security compliance and its implication for cybersecurity*. *World Journal of Advanced Research and Reviews, 24*(1), 2105–2121. https://doi.org/10.30574/wjarr.2024.24.1.3170

Alam, R. G. G., Ibrahim, H., & Karas, I. R. (2024). *Key Issues in Cybersecurity Implementation in Government Agencies: A Case Study in Jakarta Smart City*. https://doi.org/10.1007/978-981-99-9589-9_1

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability, 12*(20), 8576. https://doi.org/10.3390/su12208576

Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: An institutional perspective. *SINET: Ethiopian Journal of Science, 44*(1), 108–118. https://doi.org/10.4314/sinet.v44i1.10

Chiniah, A., & Ghannoo, F. (2023). A multi-theory model to evaluate new factors influencing information security compliance. *International Journal of Security and Networks, 18*(1), 19. https://doi.org/10.1504/IJSN.2023.129949

Domínguez-Dorado, M., et al. (2023). Boosting holistic cybersecurity awareness with outsourced wide-scope CyberSOC. *Information, 14*(11), 586. https://doi.org/10.3390/info14110586

Fazlan, A., Nadia, S. M., & Zahri, Y. (2018). Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. *OIC-CERT Journal of Cyber Security, 1*, 22–31.

Ghasem, Z., Clarke, N., & Furnell, S. (2023). A novel framework to enhance end-user security compliance. *International Journal of Chaotic Computing, 9*(1), 225–237. https://doi.org/10.20533/ijcc.2046.3359.2023.0029

Godwin, O., & Musa, M. O. (2024). Challenges and strategies for enhancing ICT security in public institutions. *International Journal of Innovative Science and Research Technology (IJISRT)*, 2185–2190. https://doi.org/10.38124/ijisrt/IJISRT24JUL1024

Goi, C. L. (2022). The next frontier towards Digital Sarawak. In *Digital Transformation Management* (pp. 247–265). Routledge. https://doi.org/10.4324/9781003224532-14

Gutzwiller, R., Dykstra, J., & Payne, B. (2020). Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats: Research and Practice, 1*(3), 1–6. https://doi.org/10.1145/3384471

Haris@Harib, A. R., Sarijan, S., & Hussin, N. (2017). Information security challenges: A Malaysian context. *International Journal of Academic Research in Business and Social Sciences, 7*(9). https://doi.org/10.6007/IJARBSS/v7-i9/3335

Harris, M. A., & Martin, R. (2019). Promoting cybersecurity compliance. In ... (pp. 54–71). https://doi.org/10.4018/978-1-5225-7847-5.ch004

Horn, C., & Gifford, S. M. (2022). ICT uptake and use and social connectedness in rural and remote communities: A study from Sarawak, Malaysia. *Information Technology for Development, 28*(4), 721–746. https://doi.org/10.1080/02681102.2021.2021844

Madnick, S. E., et al. (2019). *Research plan to analyze the role of compliance in influencing cybersecurity in organizations*. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3567388

Magnusson, L., Dalipi, F., & Elm, P. (2023). Cybersecurity compliance in the public sector: Are the best security practices properly addressed? https://doi.org/10.1007/978-3-031-36001-5_28

Mitra, D. L. (2022). Policy implementation. In *Educational Change and the Political Process* (pp. 207–231). Routledge. https://doi.org/10.4324/9781003212294-15

Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu, & Adefolake Olachi Adewusi. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive, 12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Ofori, K. S., et al. (2022). Factors influencing information security policy compliance behavior. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 213–232). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch010

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803