Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 5641-5647
P-ISSN: 2963-9298, e-ISSN: 2963-914X

The Role of Secretaries in Addressing Cyber Security Challenges in the Modern Workplace (Literature Study)

Reza Feris Perdana
Sekolah Tinggi Manajemen Pariwisata dan Logistik Lentera Mondial
rezaferisperdana@lemondial.ac.id

Abstract

The development of information technology has changed the way organizations work, shifting towards a modern, digitally-based work environment. This change has placed secretaries in a strategic position as managers of organizational information and communication, as well as guardians of data confidentiality. However, the increased use of digital technology has also been accompanied by an increase in cyber security threats such as phishing, malware, data leaks, and social engineering. This study aims to analyze the role of secretaries in facing cyber security challenges in modern work environments based on a literature review. The research method used is a qualitative approach with a literature study of scientific journals, academic books, and official reports from institutions related to information security and the secretarial profession. The results of the study show that secretaries have an important role in the organization's information security system because they are directly involved in the management of digital documents and leadership communication. The main challenges faced include limited digital security literacy, high workloads, and a lack of structured information security policies. Therefore, it is necessary to improve the competence of secretaries through cybersecurity training, the implementation of information security standard operating procedures, and the strengthening of a digital security culture within organizations. This research is expected to provide theoretical and practical contributions to the development of the secretarial profession in the digital era and serve as a reference for organizations in improving human resource-based information security systems.

Keywords: Secretary, Cyber Security, Modern Work Environment, Information Security, Literature Studies.

1. Introduction

The development of information and communication technology has accelerated digital transformation across public and private organizations. Administrative activities that were previously carried out manually such as document recording, correspondence, archiving, and scheduling are now predominantly conducted through digital platforms. The integration of computers, cloud-based storage, enterprise resource planning systems, and real-time communication tools has reshaped how information is created, processed, stored, and distributed within organizations. This transformation is intended to increase efficiency, reduce operational delays, enhance transparency, and improve decision-making accuracy.

However, the expansion of digital systems has also introduced new vulnerabilities. Organizational data is no longer confined to physical archives but is stored in interconnected networks that can be accessed remotely. This condition expands the attack surface for cyber threats. Phishing emails, ransomware attacks, malware infiltration, business email compromise, and unauthorized access attempts are now frequent risks faced by institutions worldwide. Cybersecurity is therefore no longer a technical issue limited to IT departments but a multidimensional organizational challenge.

Recent global security reports indicate that human error remains a dominant contributing factor in cybersecurity incidents (Verizon, 2023). Mistakenly clicking malicious links, using weak passwords, failing to verify suspicious requests, or neglecting data protection procedures can lead to significant financial and reputational losses. These findings highlight that information security depends not only on technological infrastructure but also on the behavior and awareness of individuals who interact with organizational systems.

The information security framework developed by the National Institute of Standards and Technology (NIST) emphasizes that effective cybersecurity management requires the integration of people, processes, and technology.

Human resources operating information systems must possess adequate knowledge and awareness of digital risks. Similarly, the international standard International Organization for Standardization through ISO/IEC 27001 underscores that information security awareness and competency development are integral components of an organization's management system. These frameworks reinforce the view that cybersecurity is a shared responsibility across organizational roles.

Within this broader context, the position of secretaries deserves particular attention. Secretaries are central actors in the administrative structure of organizations. Their responsibilities extend beyond routine clerical tasks and include managing executive communication, organizing confidential documents, coordinating meetings, handling digital correspondence, and maintaining electronic records. As organizations adopt digital systems, these responsibilities increasingly involve interaction with sensitive data in electronic formats.

From a structural standpoint, secretaries often function as information gatekeepers. They regulate access to executive schedules, screen incoming communication, and manage document circulation. Because of this role, secretaries frequently serve as intermediaries between internal management and external stakeholders. This position, while strategic, simultaneously exposes them to cyber risks such as phishing attempts disguised as executive requests, fraudulent financial instructions, or malware embedded in email attachments.

Despite this strategic positioning, cybersecurity discourse tends to focus predominantly on technical personnel, system architecture, or software defenses. Administrative roles are rarely examined in depth within cybersecurity studies, even though they hold continuous access to organizational information flows. This imbalance creates a gap between the importance of administrative functions and the level of cybersecurity preparedness provided to them.

In addition, the evolving nature of office work requires a redefinition of secretarial competencies. Traditional competencies such as communication skills, organizational ability, and document management remain important. However, modern administrative professionals must also demonstrate digital literacy, data protection awareness, and basic cybersecurity understanding. The ability to identify suspicious digital behavior, verify electronic requests, apply secure document handling practices, and adhere to information security procedures has become increasingly relevant.

Another important aspect concerns organizational culture and leadership commitment. Even when security policies exist formally, their effectiveness depends on internalization and consistent implementation. Employees who are not adequately informed about cybersecurity procedures may unintentionally compromise organizational security. Therefore, strengthening the cybersecurity role of secretaries cannot rely solely on individual initiative but must be supported by structured training programs, clear standard operating procedures, and institutional reinforcement mechanisms.

From an academic perspective, studies examining human factors in cybersecurity have expanded significantly in recent years. Nevertheless, specific analysis focusing on the secretarial profession remains limited. Most research addresses general employee behavior, compliance with security policies, or technical defense strategies. There is still limited discussion on how administrative professionals, particularly secretaries, experience cybersecurity challenges in their daily operational responsibilities. This gap justifies the need for focused examination.

Based on these considerations, this study aims to analyze the role of secretaries in addressing cybersecurity challenges within modern work environments. Using a literature review approach, this research seeks to synthesize theoretical perspectives on human-centric cybersecurity, information security governance, and digital workplace transformation. The objective is not merely to describe cyber threats but to conceptually position secretaries as part of the organization's non-technical defense layer.

By exploring existing scholarly findings, this study contributes to two main areas. First, it enriches the discourse on cybersecurity by incorporating the administrative dimension into the discussion of human-based security mechanisms. Second, it provides practical insights for organizations in strengthening information security systems through competency development among secretarial professionals. In doing so, this research supports the broader understanding that sustainable cybersecurity resilience requires alignment between technological safeguards and human capability development.

DOI: https://doi.org/10.31004/riggs.v5i1.6818

2. Research Methods

This study employs a qualitative approach using a literature review method to examine the role of secretaries in addressing cybersecurity challenges in modern work environments. The qualitative design was chosen to enable an in-depth exploration of concepts, theoretical perspectives, and findings from previous studies related to human factors in cybersecurity and organizational information security governance. The literature was collected from national and international scientific journals, academic books, and institutional reports discussing cybersecurity practices and digital workplace transformation. To ensure relevance to current technological developments, priority was given to publications from the last ten years, while several foundational works were included to strengthen the theoretical framework.

The data collection process was conducted through academic databases such as Google Scholar, ScienceDirect, and SpringerLink using keywords including "cybersecurity," "information security in office environments," "human factors in cybersecurity," and "security awareness." The selected sources were then analyzed using content analysis techniques to identify key themes related to the strategic role of secretaries, types of cyber threats in organizational settings, behavioral risk factors, and recommended mitigation strategies. The findings from these sources were compared and synthesized into a structured descriptive narrative to answer the research objectives and provide a conceptual understanding of how secretaries can function as part of the organization's human-based defense layer against cyber threats.

3. Results and Discussions

3.1 Mapping of Relevant Literature

The literature used in this study was examined and grouped according to its main discussion and its relevance to the research focus. Each source was reviewed to identify key ideas related to human factors in cybersecurity, organizational information security policies, and the development of secretarial roles in digital work settings. This grouping helps clarify the position of previous studies within the context of this research.

Through this process, the relationship between cybersecurity issues and the responsibilities of secretaries becomes more visible. Although many studies discuss information security and employee behavior, only a limited number explicitly connect these discussions to administrative roles. The summary of the reviewed literature is presented in Table 3.1.

Table 3.1 Summary of Literature Related to Secretaries and Cyber Security

Author(s)	Focus of Study	Key Findings	Relevance to This Study
Ahmad et al. (2021)	Human-centric cybersecurity	Employees are central to information security protection	Supports the role of secretaries as part of the human security layer
Bada & Nurse (2020)	Psychological aspects of cyber-attacks	Human error and stress increase vulnerability	Explains risk exposure in administrative roles
Hadnagy (2018)	Social engineering	Cyberattacks exploit trust and authority	Relevant to phishing risks targeting secretaries
Mitnick & Simon (2011)	Human manipulation in security breaches	Deception is a major cause of data breaches	Strengthens human-factor argument
ISO/IEC 27001 (2013)	Information security management	Security governance involves all personnel	Justifies inclusion of secretaries in SOPs
Haryono (2017)	Secretarial profession in the digital era	Secretaries manage digital documents and confidential communication	Establishes strategic administrative role
Stallings & Brown (2018)	Computer security principles	Human behavior is a major vulnerability	Supports non-technical defense perspective
Westerman et al. (2014)	Digital transformation	Technology adoption requires human capability alignment	Explains need for competency improvement

DOI: https://doi.org/10.31004/riggs.v5i1.6818

3.2 The Strategic Role of Secretaries in Information Security

The rapid integration of digital technologies into organizational systems has reshaped the structure of administrative work. Electronic correspondence, cloud-based document storage, digital scheduling systems, and integrated management platforms have become routine components of office operations. In this context, secretaries function not only as administrative coordinators but also as information intermediaries who regulate access, distribution, and documentation of organizational data (Haryono, 2017). Their daily activities place them in direct contact with confidential files, executive decisions, financial records, and external stakeholder communications.

From the perspective of information security governance, individuals who interact with sensitive data form part of the organizational control environment (ISO/IEC 27001, 2013). This means that secretaries contribute to maintaining the confidentiality, integrity, and availability of information, whether consciously or unconsciously. The human-centric cybersecurity model further emphasizes that security resilience is shaped by user awareness, behavioral patterns, and institutional culture (Ahmad et al., 2021). Therefore, the secretary's role can be understood as a frontline administrative defense layer that operates alongside technical safeguards such as firewalls and encryption systems.

Moreover, digital transformation has reduced hierarchical barriers in communication flows. Executives often rely on secretaries to filter emails, verify meeting requests, and manage external contacts. This gatekeeping function increases their exposure to suspicious messages and potential cyber manipulation. As a result, the strategic importance of secretaries in safeguarding information assets becomes increasingly evident within modern governance structures.

3.3 Cyber Security Threats in Modern Work Environments

The expansion of digital infrastructure has been paralleled by the diversification of cyber threats. Phishing emails disguised as executive instructions, malware hidden in document attachments, ransomware attacks targeting organizational databases, and identity spoofing have become recurring risks in professional settings. Many of these attacks are designed to exploit psychological factors rather than technical vulnerabilities.

Social engineering strategies rely on urgency, authority pressure, and trust manipulation to influence human behavior (Hadnagy, 2018; Mitnick & Simon, 2011). Secretaries, who routinely respond to requests on behalf of leadership, are particularly susceptible to impersonation attempts. Fraudulent emails that mimic executive directives may lead to unauthorized data disclosure or financial transactions if verification mechanisms are not properly followed.

Empirical discussions in information security literature show that human error remains a dominant factor in security incidents (Stallings & Brown, 2018). Heavy workloads, repetitive digital tasks, and time-sensitive administrative responsibilities can reduce attention to detail. Bada and Nurse (2020) highlight that cognitive overload and stress may impair decision-making processes, increasing the likelihood of clicking malicious links or overlooking anomalies. Within high-demand office environments, these risks are intensified by constant multitasking and communication pressure.

These findings indicate that cyber threats in modern offices are not limited to technical system failures. Instead, they often emerge from behavioral gaps, making administrative personnel central actors in organizational vulnerability assessments.

3.4 Key Challenges Faced by Secretaries

The literature review identifies three interconnected challenges that influence the effectiveness of secretaries in maintaining information security.

Limited digital security literacy remains a significant issue. While secretaries are generally proficient in office software and communication tools, not all possess structured knowledge of cyber threat patterns or risk mitigation techniques (Ahmad et al., 2021). The absence of systematic training reduces their ability to distinguish legitimate communication from malicious attempts.

DOI: https://doi.org/10.31004/riggs.v5i1.6818

Intensity and time constraints create operational vulnerabilities. Administrative roles demand responsiveness, coordination, and simultaneous task management. Under such conditions, procedural verification steps may be bypassed to maintain efficiency. As noted by Bada and Nurse (2020), time pressure can weaken critical evaluation processes, especially when digital requests appear urgent or authoritative.

Organizational security policies are not always clearly integrated into administrative workflows. Although ISO/IEC 27001 (2013) emphasizes employee awareness and responsibility, implementation often concentrates on technical departments. Without explicit Standard Operating Procedures (SOPs) tailored to secretarial tasks—such as email verification protocols, document classification guidelines, or access control instructions—administrative staff may lack operational clarity.

These challenges reveal a discrepancy between the strategic exposure of secretaries to sensitive information and the structural support provided by organizations. Strengthening this alignment becomes essential to reducing human-related security risks.

3.5 Strengthening the Role of Secretaries in Organizational Cybersecurity

The literature suggests that improving organizational cybersecurity resilience requires integrating administrative personnel into security governance frameworks. Several strategic measures can be identified.

Structured and continuous cybersecurity training programs are essential. Training should move beyond theoretical explanations and include scenario-based simulations, particularly phishing recognition exercises and incident reporting procedures (Ahmad et al., 2021). Practical exposure enhances pattern recognition and improves response accuracy in real situations.

Organizations need to formalize security responsibilities within secretarial job descriptions. The implementation of SOPs aligned with ISO/IEC 27001 (2013) can provide clear guidance on data classification, password management, document sharing restrictions, and communication verification processes. Clear procedural standards reduce ambiguity and strengthen accountability.

Cultivating a digital security culture requires leadership involvement. Westerman et al. (2014) argue that successful digital transformation depends on managerial commitment and cultural alignment. When executives demonstrate compliance with security protocols and emphasize shared responsibility, administrative personnel are more likely to adopt protective behaviors. Through these integrated efforts, secretaries can transition from being perceived as potential security weaknesses to functioning as proactive contributors within the organization's human-based defense system. Strengthening their competence and institutional support ultimately reinforces the broader information security architecture in modern work environments.

3.6 Disucussion

The findings of this study demonstrate that secretaries occupy a structurally strategic yet frequently underestimated role within organizational cybersecurity systems. As digital transformation reshapes administrative workflows, secretaries are increasingly responsible for managing electronic correspondence, digital archives, and executive communication. This proximity to sensitive information situates them within the organization's information security ecosystem rather than merely in an operational support function.

Cybersecurity research consistently highlights that technological safeguards alone are insufficient to prevent security incidents. Human-related factors remain among the dominant causes of data breaches (Verizon, 2023). Similarly, Ahmad et al. (2021) emphasize that protecting organizational information requires a human-centric cybersecurity approach in which employees are viewed as active components of security defense rather than passive users of technology. In this regard, secretaries represent a critical human layer within organizational protection systems.

Social engineering presents a particular concern for administrative roles. As explained by Hadnagy (2018) and Mitnick and Simon (2011), cyber attackers frequently exploit authority, urgency, and trust to manipulate victims. Because secretaries routinely handle executive instructions and external communications, they may become

DOI: https://doi.org/10.31004/riggs.v5i1.6818

primary targets of impersonation or phishing schemes. These risks are not necessarily due to negligence but are rooted in the structural communication patterns inherent in administrative work.

Moreover, empirical studies confirm that employee security behavior is influenced by psychological and contextual factors. Bada and Nurse (2020) note that stress and cognitive overload reduce individuals' capacity to detect malicious intent in digital communication. Administrative roles, which often involve multitasking and time-sensitive responsibilities, may therefore face heightened exposure to cyber threats. Supporting this perspective, Yildirim et al. (2021) identify awareness level, organizational climate, and perceived responsibility as significant predictors of secure employee behavior.

Beyond individual awareness, compliance with information security policies is strongly shaped by organizational governance mechanisms. D'Arcy and Herath (2011) demonstrate that deterrence mechanisms and policy enforcement influence employees' adherence to security procedures. Likewise, Ifinedo (2023) finds that leadership commitment and security-oriented organizational culture significantly enhance information security policy compliance. These findings reinforce the argument that strengthening the cybersecurity competence of secretaries requires institutional commitment rather than relying solely on individual initiative.

Training interventions also play a decisive role in reducing cyber risk. Research by Puhakainen and Siponen (2010) indicates that structured information security training programs improve employee compliance behavior. More recent findings by Parsons et al. (2022) show that phishing simulation exercises significantly enhance employees' detection accuracy and reporting rates. Complementing this, Alshaikh (2022) highlights that cultivating a cybersecurity culture through continuous education positively influences employee vigilance and accountability.

From a governance perspective, ISO/IEC 27001 establishes that information security responsibilities must be distributed across organizational roles rather than centralized solely within IT departments. However, in practice, administrative personnel are not always systematically included in formal security capacity-building initiatives. This creates a misalignment between access authority and protection capability.

Furthermore, digital transformation literature underscores that technological advancement must be accompanied by human capability development to achieve sustainable organizational performance (Westerman et al., 2014). Investment in digital infrastructure without strengthening employee competence may generate vulnerabilities rather than resilience. Secretaries, as key actors in daily information exchange, therefore require continuous professional development aligned with cybersecurity governance principles.

Overall, the integration of human-centric security theory (Ahmad et al., 2021), behavioral compliance research (D'Arcy & Herath, 2011; Yildirim et al., 2021), security culture studies (Alshaikh, 2022; Ifinedo, 2023), and practical training evidence (Parsons et al., 2022; Puhakainen & Siponen, 2010) demonstrates that empowering secretaries in cybersecurity practices is a strategic organizational imperative. Rather than being positioned as potential vulnerabilities, secretaries should be recognized as essential contributors to organizational cyber resilience in the digital era.

Another dimension that deserves attention is the relationship between access authority and accountability. Secretaries often possess broad access to calendars, confidential correspondence, financial documentation, and internal reports. However, the scope of this access is not always accompanied by proportional involvement in security planning or risk evaluation processes. When authority and responsibility are not balanced, gaps in oversight may emerge. Strengthening internal coordination between management, IT units, and administrative personnel can reduce such gaps and encourage shared responsibility in safeguarding organizational data.

It is also necessary to consider the ethical dimension of administrative work in digital environments. Secretaries are entrusted with sensitive information that requires discretion, judgment, and professional integrity. In the context of cybersecurity, ethical awareness becomes closely linked to digital conduct, including responsible data sharing, cautious verification of requests, and adherence to confidentiality principles. Embedding cybersecurity awareness within professional ethics frameworks may reinforce internal motivation to comply with security standards, rather than relying solely on external monitoring mechanisms.

Finally, long-term organizational resilience depends on continuous adaptation to evolving threat landscapes. Cyber risks are dynamic, and attack methods continue to develop alongside technological innovation. For this reason,

DOI: https://doi.org/10.31004/riggs.v5i1.6818

strengthening the role of secretaries in cybersecurity should not be approached as a one-time intervention but as an ongoing process. Periodic evaluation of administrative procedures, regular updating of security protocols, and sustained capacity-building initiatives are essential to ensure that secretaries remain prepared to respond to emerging digital threats. Through consistent integration of governance, training, and professional development, administrative roles can contribute meaningfully to sustainable cybersecurity management.

4. Conclusion

Based on the results of the literature review, it can be concluded that secretaries hold a strategic position in maintaining organizational information security within modern digital work environments. The integration of digital technologies into administrative processes has expanded their responsibilities beyond conventional clerical duties. Secretaries are directly involved in managing digital correspondence, confidential documents, and executive communication, which places them within the organization's human-based security layer. The study also confirms that cybersecurity risks are not solely technical issues, but are closely related to human behavior, awareness, and institutional support systems. The findings highlight three primary challenges: limited digital security literacy, high workload and time pressure, and the lack of structured information security policies specifically integrated into administrative functions. These challenges indicate a gap between the strategic exposure of secretaries to sensitive information and the level of cybersecurity preparation provided by organizations. To address this issue, organizations should implement continuous cybersecurity training programs, develop clear Standard Operating Procedures tailored to secretarial tasks, and foster a strong digital security culture supported by leadership commitment. Integrating cybersecurity competencies into professional development programs for secretaries is also recommended to strengthen preventive capacity at the organizational level. This study contributes to the conceptual understanding of secretaries as active participants in organizational cybersecurity governance. However, since this research is based on a literature review, further empirical studies are recommended to examine the practical implementation of cybersecurity awareness among secretaries in various institutional contexts. Future research may also explore the relationship between organizational culture, leadership support, and cybersecurity compliance in administrative roles. Such studies would provide deeper insights and practical evidence to reinforce the strategic role of secretaries in responding to evolving digital security challenges.

Reference

1. Ahmad, A., Bosua, R., & Scheepers, R. (2021). Protecting organizational information: A human-centric approach to cybersecurity. *Computers & Security*, 100, 102084. https://doi.org/10.1016/j.cose.2020.102084
2. Alshaikh, M. (2022). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 112, 102540. https://doi.org/10.1016/j.cose.2021.102540
3. Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks. *Journal of Cybersecurity*, 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005
4. D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643–658. https://doi.org/10.1057/ejis.2011.28
5. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
6. Haryono, S. (2017). *Sekretaris profesional di era digital*. Gramedia.
7. Ifinedo, P. (2023). Information security policy compliance: An empirical study of the role of organizational culture and leadership. *Information & Computer Security*, 31(2), 234–249. https://doi.org/10.1108/ICS-05-2022-0074
8. International Organization for Standardization. (2013). ISO/IEC 27001:2013 *information security management systems — Requirements*. ISO.
9. Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley
10. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2022). The design of phishing simulation training and its impact on user behavior. *Computers & Security*, 118, 102724. https://doi.org/10.1016/j.cose.2022.10272
11. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information security training. MIS Quarterly, 34(4), 757–778. https://doi.org/10.2307/25750705
12. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
13. Verizon. (2023). 2023 data breach investigations report. Verizon Enterprise.
14. Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.
15. Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2021). Factors influencing information security behavior among employees. *Computers & Security*, 104, 102219. https://doi.org/10.1016/j.cose.2021.102219

DOI: https://doi.org/10.31004/riggs.v5i1.6818