Journal of KIIT. Vol. 22, No. 8, pp. 177-188, Aug. 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.8.177

Adopting vCISOs: A Solution for SME Cybersecurity

Dong-Hyuk Shin*

Abstract

This study aims to examine the strategic integration of Chief Information Security Officers(CISOs) and Virtual CISOs(vCISOs) in Small and Medium-sized Enterprises(SMEs) to enhance cybersecurity frameworks. Using advanced international case studies such as Howard county and Forenzy Networks, the research compares the advantages and disadvantages of vCISOs, providing specific strategies based on the current security systems of typical SMEs. Implementing a vCISO requires budget considerations, addressing gaps in in-house expertise, and ensuring compliance with cybersecurity regulations. Organizations must choose a vCISO with relevant experience, industry knowledge, and effective communication skills to align security strategies with business goals. The findings offer practical and strategic guidance, demonstrating how vCISO adoption can mitigate cyber threats and align security strategies with business goals. The conclusions contribute to both theoretical understanding and practical applications, highlighting the importance of strategic leadership in SME cybersecurity.

요 약

본 연구는 중소기업 내에서 최고 정보 보안 책임자(CISO)와 가상 최고 정보 보안 책임자(vCISO)의 전략적 통합에 관해 제시한다. 최근 사이버 위협 사례가 증가함에 따라 정보 자산을 보호하기 위한 CISO의 역할도 함께 강조되었다. 본 연구는 중소기업의 사이버 보안 체계를 고도화를 위한 vCISO의 기능과 역할을 고찰하고 논의한다. 구체적으로, 본 연구는 해외 선진 사례를 고찰하여 시사점을 도출하고 중소기업을 위한 실용적이고 전략적인 지침을 제공한다. 분석 결과, 성공적인 보안 실현을 위해서는, vCISO를 위한 특정 예산을 수립하고, 사내 전문성의 격차를 해소해야 할 필요가 있다. 조직은 보안 전략을 비즈니스 목표에 맞게 조정하기 위해 관련 경험, 업계 지식, 효과적인 커뮤니케이션 기술을 갖춘 vCISO를 선택해야 한다. 본 연구의 제언 및 결론은 중소기업의 사이버 보안 수준을 강화하는데에 있어서 유용한 시사점이 될 것이다.

Keywords
cybersecurity; SMEs, CISO, vCISO, information security

Ⅰ. Introduction

In the contemporary digital landscape, Small and Medium-sized Enterprises(SMEs) face a myriad of cybersecurity threats that jeopardize their operational integrity and data security. The role of Chief Information Security Officers(CISOs) has emerged as crucial in fortifying organizational defenses against these threats. Research indicates that while large corporations have long integrated CISOs into their

* SECUFIND Co.,Ltd. CEO
- ORCID: https://orcid.org/0009-0006-8642-3769

· Received: Jul. 08, 2024, Revised: Aug. 05, 2024, Accepted: Aug. 08, 2024
· Author: Dong-Hyuk Shin
Dept. of Headoffce
Tel.: +82-2-1660-2079, Email: sonoktnd@gmail.com

executive teams, SMEs often struggle with this integration due to limited resources and expertise[1]. Despite their crucial economic contributions, SMEs typically lack the robust cybersecurity infrastructures seen in larger enterprises, making them particularly vulnerable to cyber-attacks.

Existing literature on information security management in SMEs highlights significant gaps. While the importance of cybersecurity is well-documented, there is a paucity of research focusing on the strategic integration of CISOs within SMEs, particularly in the context of South Korea. Previous studies have primarily explored the operational aspects of cybersecurity, often neglecting the strategic roles that CISOs play in aligning security measures with business objectives[2]-[4]. Moreover, the evolving nature of cyber threats necessitates continuous adaptation of security strategies, which SMEs are often ill-prepared to manage without dedicated leadership.

The lack of focused research on the strategic role of CISOs in SMEs is concerning, given the increasing complexity and frequency of cyber threats. SMEs are often seen as easy targets by cybercriminals due to their typically weaker security measures and lack of specialized security personnel[5]. The implications of a cyber-attack on an SME can be devastating, including financial losses, reputational damage, and operational disruptions. As regulatory requirements become more stringent globally, SMEs must not only defend against cyber threats but also comply with complex legal frameworks. Understanding how SMEs can effectively integrate CISOs to manage these challenges is thus of paramount importance.

This study proposes to address these gaps by investigating how SMEs can better integrate the functions of CISOs and virtual CISOs(vCISOs) to enhance their cybersecurity frameworks. vCISOs offer part-time, flexible, and cost-effective cybersecurity leadership, making them particularly beneficial for SMEs with limited resources. By examining advanced case studies and real-world examples, this research aims to provide practical insights and strategic guidance for SMEs. The study will explore various engagement models for CISOs and vCISOs, assessing their effectiveness in different organizational contexts. It will also analyze the communication dynamics between CISOs, vCISOs, and other executive roles, aiming to understand how these interactions can facilitate better cybersecurity practices[6][7].

This research makes several significant contributions to the field of cybersecurity management in SMEs. Firstly, it provides a detailed examination of the strategic integration of vCISOs, which is currently underexplored in existing literature. By focusing on SMEs, the study adds a regional perspective that is often overlooked in global cybersecurity research. Secondly, the study offers practical recommendations for SMEs to enhance their cybersecurity posture through effective CISO engagement. These recommendations are grounded in empirical evidence from case studies, making them highly relevant for practitioners. Lastly, the study aims to contribute to the broader discourse on organizational cybersecurity by highlighting the critical role of strategic leadership in managing cyber threats and compliance requirements[8][9].

II. Literature Review

2.1 Chief Privacy Officer(CPO) and CISO

The roles of CPO and CISO are critical in contemporary organizations, especially given the increasing importance of data privacy and cybersecurity. While both roles focus on protecting information, they differ significantly in their areas of responsibility and expertise. This literature review examines the definitions, roles, responsibilities, and integration of CPOs and CISOs within organizations, highlighting their unique contributions and the interplay between these two positions.

The CPO is primarily responsible for overseeing an

organization's data privacy strategy and ensuring compliance with relevant laws and regulations. The role of the CPO has gained prominence with the advent of stringent data protection regulations such as the General Data Protection Regulation(GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States[10]. CPOs ensure that personal data is collected, stored, and processed in a manner that respects individuals' privacy rights and complies with legal requirements. CPOs also play a crucial role in risk management by identifying potential privacy risks and implementing measures to mitigate them[8]. They work closely with various departments within an organization to develop privacy policies and procedures, conduct privacy impact assessments, and train employees on data privacy best practices[11]. Moreover, CPOs often serve as the point of contact for data protection authorities and manage responses to data breaches and privacy-related incidents[9].

The CISO is responsible for an organization's overall information security strategy. This role encompasses protecting the organization's information assets from cyber threats and ensuring the confidentiality, integrity, and availability of data[12]. CISOs develop and implement comprehensive security policies, conduct regular security assessments, and lead incident response efforts in the event of a cyber attack [13]. CISOs must stay abreast of the latest cybersecurity trends and threats, adapting the organization's security posture accordingly. They are responsible for implementing technical controls such as firewalls, encryption, and intrusion detection systems, as well as promoting a security-conscious culture within the organization[5]. Additionally, CISOs often liaise with other executives to align the cybersecurity strategy with the organization's overall business objectives[14].

While the roles of CPOs and CISOs are distinct, their collaboration is essential for a holistic approach to data protection and cybersecurity. Effective communication and coordination between these officers can enhance an organization's ability to protect sensitive data and comply with legal requirements[6]. For instance, during a data breach, the CISO focuses on mitigating the threat and securing the network, while the CPO handles legal compliance and communication with stakeholders[7].

The literature underscores the importance of both CPOs and CISOs in safeguarding an organization's information assets. While their responsibilities differ, their collaboration is crucial for achieving comprehensive data protection and cybersecurity. Future research could explore the evolving dynamics between these roles as regulatory landscapes and cyber threats continue to evolve. This study focuses on CISOs due to the growing complexity of cyber threats and the critical role CISOs play in developing and implementing robust cybersecurity strategies, ensuring the protection of organizational data and systems.

2.2 Information security in SMEs in South Korea

Small and Medium-sized Enterprises(SMEs) in South Korea play a crucial role in the country's economy. However, these enterprises face significant challenges in managing information security due to limited resources and expertise. SMEs in South Korea often struggle with implementing effective information security measures due to constrained budgets and lack of specialized knowledge. Many SMEs do not have dedicated Information Technology(IT) security personnel, leading to inadequate protection against cyber threats[15]. This vulnerability is exacerbated by the increasing sophistication of cyber-attacks targeting these enterprises.

One critical issue is the lack of awareness and training regarding cybersecurity among employees. Many security breaches in South Korean SMEs result from human error, highlighting the need for comprehensive cybersecurity education and training

programs[16]. Research emphasize the importance of regular training sessions to keep employees informed about the latest security practices and potential threats. Compliance with regulatory requirements is another challenge for South Korean SMEs. The Personal Information Protection Act(PIPA) mandates stringent data protection measures[17], which many SMEs find difficult to implement fully due to resource constraints. Non-compliance can result in hefty fines and damage to the company's reputation, making it imperative for SMEs to prioritize regulatory adherence.

Despite these challenges, innovative technological strategies can offer substantial assistance. This study focuses on the role of vCISOs for SMEs. Given the increasing complexity of cyber threats and the critical role of CISOs in safeguarding information assets, this research aims to explore how SMEs can better integrate CISO functions to enhance their cybersecurity framework by investigating advanced case studies.

III. vCISO Case Study

3.1 Information Systems Audit and Control Association of America(ISACA)

The ISACA defines a vCISO as an independent security professional offering "CISO-as-a-Service" solutions. This role is becoming increasingly popular among Small and Medium-sized Businesses(SMBs) due to its cost-effectiveness and flexibility compared to hiring a full-time CISO[18][19]. Table 1 provides a detailed overview of the roles, definitions, and hiring types associated with vCISOs, highlighting their typical responsibilities and how they differ from traditional CISOs. It also emphasizes the qualifications and scope of services that vCISOs offer to organizations.

vCISOs typically offer remote and part-time services to multiple clients simultaneously, providing strategic guidance and support in cybersecurity. Their roles are similar to those of traditional CISOs, focusing on strategizing, advising, coordinating, and managing information security. However, unlike full-time CISOs, vCISOs do not perform hands-on implementation tasks such as firewall installation[19].

Organizations can procure vCISO services through various methods, including retainers, project-specific engagements, or on an as-needed basis. This flexibility allows businesses to address immediate security needs without committing to long-term employment contracts. Effective communication is a critical skill for vCISOs, as they need to translate complex security terminology into business language that executives and board members can understand[20]. This ensures that security strategies are aligned with the organization's business goals and that all stakeholders are informed about the company's security posture.

Table 1. Overview of vCISO roles and characteristics

Category	Details
Definition	vCISOs are independent security professionals who provide "CISO as a Service" solutions.
Roles	vCISOs typically provide remote and part-time services to clients, often working with multiple clients simultaneously.
Hire type	Temporary or part-time
CISO difference	CISOs and vCISOs typically have similar qualifications, experience, roles, and responsibilities.
Example	The roles and responsibilities of a vCISO and a CISO include strategizing, advising, coordinating, and managing information security. However, they do not implement firewalls themselves.
Qualification	vCISOs are independent security professionals who provide "CISO as a Service" solutions.

The ISACA highlights the growing importance and utility of vCISOs in the current cybersecurity landscape. By providing a cost-effective, flexible, and expert-driven approach to managing information security, vCISOs are becoming a vital resource for SMBs looking to enhance their cybersecurity strategies without the overhead costs associated with a full-time CISO.

3.2 Howard county, USA vCISO program

The Howard County, Maryland, USA vCISO Program is a pioneering initiative designed to support SMBs that may not have the resources to hire a full-time CISO. Launched by the Howard County Economic Development Authority(HCEDA) in collaboration with the Maryland Center for Entrepreneurship(MCE), this program aims to provide critical cybersecurity leadership and expertise to member companies of the Howard Tech Council (HTC) who lack their own CISOs[21]. The Howard County vCISO Program offers free vCISO services to eligible organizations within the HTC. These services are delivered by experienced security professionals from renowned organizations such as AT&T and the U.S. Department of the Interior. The program ensures that participating companies receive the strategic and advisory support necessary to strengthen their cybersecurity posture without the significant financial burden of a full-time hire. The Howard County vCISO Program provides vCISOs on a part-time basis, enabling organizations to utilize their services as needed. This model not only saves costs but also ensures that security expertise is available without the need for a long-term commitment. Companies can engage vCISOs for specific projects, interim roles, or continuous advisory services.

Several organizations within the Howard Tech Council have benefited from the vCISO program. For example, businesses that participated in the program reported improved cybersecurity strategies and better alignment of security measures with their business objectives[22]. The expertise brought by vCISOs has helped these companies navigate complex regulatory requirements and enhance their overall security posture.

The Howard County Virtual CISO Program stands as a model for how local governments and business councils can collaborate to enhance cybersecurity for SMBs. By offering access to seasoned security professionals, the program provides essential support that helps organizations protect their assets and comply with regulatory standards. This initiative not only demonstrates the potential of vCISO services but also highlights the importance of innovative solutions in addressing cybersecurity challenges for smaller enterprises.

3.3 Forenzy networks vCISO

Forenzy Networks, a prominent cybersecurity and computer forensics firm, offers vCISO services that provide strategic guidance and support to organizations on a part-time, as-needed basis[23]. This case study examines how Forenzy's vCISO services effectively enhanced the cybersecurity posture of a global manufacturing firm, showcasing the strategic implementation and operational impact of these services. A global manufacturing firm, hosting sensitive data across its network infrastructure, faced significant cybersecurity challenges. The firm required a comprehensive assessment of their network vulnerabilities to safeguard their critical operations. They contracted Forenzy Networks for a Network Vulnerability Assessment and Penetration Testing (VAPT) to identify and mitigate potential risks within their infrastructure.

Forenzy's vCISO team initiated the engagement with a thorough evaluation of the firm's existing security framework. This included a detailed analysis of network configurations, security policies, and existing vulnerabilities.

The assessment revealed several critical issues, including unauthorized access to sensitive CCTV feeds within the production units, which could potentially lead to significant security breaches. The vCISO team identified vulnerabilities in the firm's infrastructure that allowed access to live streaming of sensitive operations without proper login credentials. This vulnerability posed a significant risk, especially given the nature of the firm's production activities related to defense manufacturing.

Forenzy's vCISO services provided a strategic roadmap to address the identified vulnerabilities. The plan included immediate remediation steps to secure the CCTV feeds and a comprehensive strategy to enhance the overall security posture of the firm. Key actions included. Firstly, the vCISO team worked closely with the firm's IT department to implement robust access controls and secure the identified vulnerabilities. This involved reconfiguring network settings, updating security protocols, and ensuring compliance with industry standards. Secondly, the vCISO helped develop and implement new security policies to prevent future breaches. This included regular security audits, employee training programs on cybersecurity best practices, and continuous monitoring of network activities. Finally, the vCISO team established a risk management framework that prioritized vulnerabilities based on their potential impact and likelihood. This proactive approach enabled the firm to allocate resources efficiently and address the most critical issues promptly.

The intervention by Forenzy's vCISO services resulted in several significant improvements. The firm achieved a more secure network environment with reduced risks of unauthorized access and data breaches. The immediate remediation of critical vulnerabilities fortified the firm's defenses against potential cyber threats. With the implementation of new security policies and regular audits, the firm ensured compliance with relevant industry regulations and standards, thereby minimizing legal and operational risks. The vCISO's strategic guidance helped streamline the firm's cybersecurity operations, allowing internal IT staff to focus on core business activities while maintaining robust security measures.

Forenzy Networks' vCISO services provided the manufacturing firm with expert cybersecurity leadership, enabling them to address critical vulnerabilities and enhance their overall security framework. This case illustrates the effectiveness of vCISO services in delivering high-level strategic support and operational improvements, making it a viable solution for organizations seeking to strengthen their cybersecurity without the overhead costs of a full-time CISO. Table 2 outlines the primary services offered by vCISOs in Forenzy Networks, detailing their roles in developing cybersecurity strategies, managing risks, responding to incidents, providing security training, and ensuring compliance with regulations.

Table 2. Virtual CISO services in forenzy networks

Services offered	Details
Security strategy and planning	Develop and implement a comprehensive cybersecurity strategy that aligns with business goals.
Manage risk	Identify, assess, and mitigate cybersecurity risks across the organization.
Incident response	Provide guidance and support in the event of a cyberattack or data breach.
Security awareness training	Educate employees on cybersecurity best practices and create a culture of security within the organization.
Compliance and governance	Ensure compliance with applicable cybersecurity regulations and industry standards.

IV. Benefits and Drawback of vCISO

4.1 Benefits of vCISO

vCISOs offer numerous advantages, making them an attractive option for many organizations, particularly SMBs.

4.1.1 Cost-effectiveness

One of the primary benefits of vCISOs is their cost-effectiveness. Hiring a vCISO is significantly cheaper than employing a full-time CISO, which is crucial for SMBs with limited budgets. This cost-saving allows organizations to access high-level security expertise without the financial burden of a full-time executive salary[2].

4.1.2 Organizational flexibility

vCISOs provide organizational flexibility by offering services on a part-time basis as needed. This flexibility is beneficial for businesses that may not require a full-time CISO but still need expert guidance in their cybersecurity strategy. Organizations can gradually increase the involvement of a vCISO, potentially transitioning them to a full-time role as their security needs grow.

4.1.3 Access to specialized talent

vCISOs bring a wealth of experience and specialized skills to an organization. They are often former executives or seasoned professionals in the field of information security, providing expertise that an SMB's in-house staff may lack. This access to specialized talent helps businesses effectively manage and enhance their cybersecurity posture[23].

4.1.4 Independent and objective problem identification

An external, independent vCISO can provide an objective perspective on an organization's security posture. This independent viewpoint is valuable in identifying blind spots and areas for improvement that internal staff might overlook. The unbiased analysis helps in developing more robust security strategies.

4.1.5 Flexible and scalable security strategy

vCISOs offer a flexible and scalable approach to cybersecurity. They can adapt their services to meet the changing needs of the organization, ensuring that the security strategy evolves in line with business goals and technological advancements. This adaptability is crucial for maintaining effective security measures over time.

In summary, the benefits of vCISOs include cost-effectiveness, organizational flexibility, access to specialized talent, objective problem identification, and a flexible and scalable security strategy. These advantages make vCISOs an essential resource for SMBs looking to enhance their cybersecurity measures without the overhead costs associated with a full-time CISO[19][21][23].

4.2 Drawbacks of vCISO

While vCISOs offer numerous advantages, there are also several drawbacks to consider.

4.2.1 Limited availability

One significant drawback is the limited availability of vCISOs. Since they typically work with multiple clients simultaneously, their time and attention might be divided, leading to potential delays in addressing urgent security issues.

4.2.2 Lack of deep organizational integration

vCISOs might lack deep integration within the organization's culture and processes. This can result in a less thorough understanding of the company's unique challenges and nuances compared to a full-time, in-house CISO.

4.2.3 Potential security risks

The involvement of external consultants can introduce security risks, particularly if the vCISO is not fully aligned with the organization's security protocols and practices. Ensuring secure communication and data sharing can be challenging.

4.2.4 Perceived lack of commitment

There may be a perceived lack of commitment from vCISOs, as they are not permanent employees. This perception can affect their influence and the implementation of their recommendations within the organization.

4.3 Analysis of vCISO Adoption in SMEs

Most SMEs lack a dedicated CISO, with cybersecurity responsibilities often overlapping with other roles. In this context, adopting a vCISO presents distinct advantages and disadvantages. On the positive side, vCISOs provide specialized, strategic oversight without the financial burden of a full-time hire. They offer flexible engagement models, tailored expertise, and real-time threat response. However, drawbacks include limited availability, potential lack of deep organizational integration, and perceived lower commitment compared to in-house CISOs. This analysis highlights the need for SMEs to carefully weigh these factors when considering vCISO adoption.

V. Suggestions for a Successful vCISO

5.1 Prerequisites

Implementing a vCISO requires careful consideration and certain prerequisites to ensure its effectiveness and alignment with organizational goals. These prerequisites include budget considerations, growing cybersecurity requirements, compliance needs, and addressing gaps in in-house expertise. Firstly, organizations with limited budgets might find it challenging to hire a full-time CISO due to the high costs associated with such positions. A vCISO can provide essential cybersecurity expertise at a fraction of the cost, making it a viable option for SMBs looking to enhance their security posture without significant financial strain[19]. Secondly, as an organization expands, its cybersecurity needs often become more complex. A vCISO can help effectively scale the security program to meet these evolving requirements. By offering strategic guidance and support, a vCISO ensures that the organization's cybersecurity measures grow in tandem with its operations, safeguarding against increasingly sophisticated threats. Thirdly, compliance with specific cybersecurity regulations is crucial for many organizations. A vCISO can provide the necessary guidance and support to ensure that the organization adheres to these regulations. This includes developing and implementing policies and procedures that meet compliance standards, conducting regular audits, and staying updated on regulatory changes[3]. Fourthly, many organizations lack the in-house expertise needed to manage comprehensive cybersecurity programs. A vCISO can fill this gap by bringing specialized knowledge and experience. This external expertise is particularly valuable for organizations that do not have dedicated cybersecurity teams, as it ensures that their security strategies are robust and effective. Fifthly, there must be clear and effective communication channels between the vCISO, executive management, and internal IT teams. The vCISO should be able to translate complex security concepts into business language that stakeholders can understand, ensuring alignment between security strategies and business objectives[4]. Lastly, organizational leadership must be committed to the vCISO initiative, providing the necessary support and resources. This includes budget allocation, authority to implement changes, and active participation in security strategy discussions. Without this commitment, the vCISO may struggle to achieve meaningful impact.

5.2 Procedures for choosing the vCISO

Selecting an appropriate vCISO is essential for enhancing an organization's cybersecurity framework. The following factors are crucial in making an informed decision. Firstly, the foremost criterion is the vCISO's experience and expertise in cybersecurity. It is crucial to select a professional with a demonstrated track record and extensive knowledge in areas pertinent to the organization's needs. An experienced vCISO will have a comprehensive understanding of various security threats, mitigation strategies, and

incident response protocols, which are vital for effective cybersecurity management[24]. Secondly, choosing a vCISO who possesses a deep understanding of the specific industry is imperative. Such knowledge ensures that the vCISO is familiar with the unique cybersecurity challenges and compliance requirements pertinent to the sector. An industry-savvy vCISO can provide tailored solutions and ensure adherence to industry-specific standards and regulations, which is essential for maintaining a robust cybersecurity posture. Thirdly, effective communication and collaboration skills are crucial for the successful integration of a vCISO into the organization. The vCISO must be adept at translating complex security concepts into language that is easily understood by non-technical stakeholders, including executives and board members. Additionally, the ability to collaborate effectively with internal IT and security teams is vital for fostering a cooperative and productive working environment[25]. Fourthly, ensuring that the vCISO is available and responsive is critical, particularly during security incidents or when urgent guidance is required. Assess the vCISO's availability during the selection process to confirm that they can meet the organization's needs promptly and without delay. This responsiveness is essential for maintaining the security of the organization's digital assets. Finally, whether the services are required on a retainer basis, for specific projects, or on-demand, flexibility is key to accommodating the organization's dynamic cybersecurity needs. A flexible engagement model allows for the scaling of vCISO involvement based on evolving requirements, ensuring both cost-effectiveness and operational efficiency.

The vCISO model provides a versatile solution to contemporary cybersecurity challenges, enabling organizations to leverage high-level expertise without the overhead costs associated with a full-time CISO. By carefully considering the factors of experience, industry knowledge, communication skills, availability, and flexible engagement options, organizations can significantly strengthen their cybersecurity posture and protect their valuable assets from digital threats.

5.3 Analysis of vCISO adoption in SMEs

Most SMEs lack a dedicated CISO, with cybersecurity responsibilities often overlapping with other roles. In this context, adopting a vCISO presents distinct advantages and disadvantages. On the positive side, vCISOs provide specialized, strategic oversight without the financial burden of a full-time hire. They offer flexible engagement models, tailored expertise, and real-time threat response. However, drawbacks include limited availability, potential lack of deep organizational integration, and perceived lower commitment compared to in-house CISOs. This analysis highlights the need for SMEs to carefully weigh these factors when considering vCISO adoption.

Ⅵ. Conclusion

This study provides significant theoretical contributions by bridging the gap in understanding vCISOs' strategic integration into SMBs, a topic previously underexplored[27][28]. Unlike earlier research focused on operational aspects[25][29], this study emphasizes vCISOs' strategic roles, particularly in translating complex security concepts for non-technical stakeholders, highlighting the importance of effective communication. Findings suggest vCISOs mitigate risks and enhance organizational resilience by fostering a security-aware culture.

These insights offer scholars a new perspective on vCISOs' strategic impact, encouraging further research on their influence on business outcomes and cybersecurity governance. Future studies could extend these results to other areas, such as corporate information security training and personal data protection management[30]-[32].

The findings have significant implications for

practitioners, particularly top managers, CISOs, and cybersecurity providers. SMBs can leverage vCISOs for high-level security expertise without the cost of full-time CISOs, allowing scalability in cybersecurity efforts. vCISOs provide strategic insights, translating complex issues into actionable business strategies, ensuring alignment with organizational goals. During cyberattacks, vCISOs offer immediate response guidance and long-term security improvements. Cybersecurity providers can enhance their services by integrating vCISO solutions, addressing immediate threats while contributing to clients' strategic cybersecurity directions. Practitioners are encouraged to adopt flexible vCISO engagement models to meet specific client needs effectively.

While various security solutions such as firewalls, antivirus software, and intrusion detection systems are available to SMEs, these methods alone may not provide comprehensive protection. A vCISO brings strategic oversight, ensuring all security measures are cohesive and aligned with business goals. Unlike generic security solutions, vCISOs offer tailored expertise, ongoing risk assessments, and the ability to respond to evolving threats in real-time. Their role bridges the gap between technical security measures and executive decision-making, providing a holistic approach to cybersecurity that standalone tools cannot achieve.

This study, while comprehensive, has several limitations that open avenues for future research. One limitation is the reliance on case studies from specific industries, which may not be generalizable across all sectors. Future research could address this by including a more diverse range of industries and organizational sizes. Additionally, the study focuses primarily on the strategic role of vCISOs without delving deeply into their operational challenges and day-to-day interactions with in-house teams. Exploring these aspects could provide a more holistic view of the vCISO role. Furthermore, the impact of organizational culture on the effectiveness of vCISOs remains underexplored. Future studies should investigate how different cultural contexts influence the integration and success of vCISO initiatives. Lastly, there is currently a scarcity of literature regarding vCISOs in European or other international contexts. Most available information consists of surface-level case studies evaluated by groups like Gartner, focusing on companies such as SecureWorks and Deloitte[24]. Future research should aim to conduct qualitative studies or investigate more detailed data as it becomes available to better understand the adoption and effectiveness of vCISOs across different regions and organizations.

References

[1] M. Heidt, J. P. Gerlach, and P. Buxmann, "Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments", Information Systems Frontiers, Vol. 21, No. 6, pp. 1285-1305, Dec. 2019. https://10.1007/s10796-019-09959-1.

[2] S. Saxena and T. Nisha, "Augmentation of SECaaS model with eCISO in cloud-based security services: A Comprehensive study", Journal of Physics: Conference Series, Vol. 1964, Jul. 2021. http://dx.doi.org/10.1088/1742-6596/1964/4/042013

[3] M. Bradford, E. Z. Taylor, and M. Seymore, "A view from the CISO: insights from the data classification process", Journal of Information Systems, Vol. 36, No. 1, pp. 201-218, Jul. 2022. http://dx.doi.org/10.2308/ISYS-2020-054.

[4] C. Shayo and F. Lin, "An exploration of the evolving reporting organizational structure for the chief information security officer (ciso) function", Journal of Computer Science, Vol. 7, No. 1, pp. 1-20, Jun. 2019. http://dx.doi.org/10.15640/jcsit.v7n1a1.

[5] L. A. Gordon, M. P. Loeb, and L. Zhou, "The

impact of information security breaches: Has there been a downward shift in costs?", Journal of Computer Security, Vol. 19, No. 1, pp. 33-56, Feb. 2011. http://dx.doi.org/10.3233/JCS-2009-0398.

[6] A. Cavoukian, "Privacy by design: The 7 foundational principles", Information and privacy commissioner of Ontario, Canada, Vol. 5, pp. 12, Jan. 2009.

[7] D. Wright, K. Wadhwa, M. Lagazio, C. Raab, and E. Charikane, "Integrating privacy impact assessment in risk management", International Data Privacy Law, Vol. 4, No. 2, pp. 155-170, May 2014. http://dx.doi.org/10.1093/idpl/ipu001.

[8] K. A. Bamberger and D. K. Mulligan, "Privacy on the ground: driving corporate behavior in the United States and Europe", MIT Press, Oct. 2015. http://dx.doi.org/10.7551/mitpress/9905.001.0001.

[9] D. J. Solove, "The digital person: Technology and privacy in the information age", NyU Press, Vol. 1, Oct. 2004.

[10] J. M. Blanke, "Protection for 'Inferences drawn': A comparison between the general data protection regulation and the california consumer privacy act", Global Privacy Law Review, Vol. 1, No. 2, pp. 81-92, Jun. 2020. http://dx.doi.org/10.54648/GPLR2020080.

[11] F. H. Cate, "The failure of fair information practice principles", Consumer Protection in the Age of the'Information Economy', pp. 341-377, Jan. 2016.

[12] R. V. Solms and J. V. Niekerk, "From information security to cyber security", Computers & Security, Vol. 38, pp. 97-102, Oct. 2013. https://doi.org/10.1016/j.cose.2013.04.004.

[13] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature", Computers & Security, Vol. 45, pp. 42-57, Sep. 2014. http://dx.doi.org/10.1016/j.cose.2014.05.003.

[14] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study", MIS quarterly, Vol. 34, No. 4, pp. 757-778, Dec. 2010. http://dx.doi.org/10.2307/25750704.

[15] J. Jung, "ICT Adoption and Cyber Security of Korean SMEs", Journal of Korea Safety Management & Science, Vol. 23, No. 2, pp. 53-63, Jun. 2021.

[16] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, "Cyber security incidents analysis and classification in a case study of Korean enterprises", Knowledge and Information Systems, Vol. 62, No. 7, pp. 2917-2935, Jul. 2020. https://10.1007/s10115-020-01452-5.

[17] Personal Information Protection Commission, "Amended Personal Information Protection Act (PIPA) and its Enforcement Decree Become Effective", Sep. 2023. https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2331 [accessed: Jun. 29, 2024]

[18] CISO Global, "Virtual Chief Information Security Officer (vCISO)", 2024. https://www.ciso.inc/capabilities/strategy-risk-solutions/managed-compliance-security-offering/virtual-ciso-vciso-services/ [accessed: Jun. 28, 2024]

[19] ISACA, "Virtual CISOs: Security Leader or Security Risk?", Aug. 2021. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/virtual-cisos-security-leader-or-security-risk [accessed: Jun. 25, 2024]

[20] R. Das, "How to Start Your Own Cybersecurity Consulting Business", First-hand Lessons from a Burned-out Ex-CISO, Auerbach Publications, Aug. 2022.

[21] Howard County Economic Development Authority, "HOCO CISO", Nov. 2017. https://hceda.org/hceda_ip_callouts/hoco-ciso/ [accessed: Jun. 28, 2024]

[22] IANS Faculty, "Benefits of a Virtual CISO", Nov. 2022. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/11/15/benefits-of-a-virtual-ciso [accessed: Jun. 22, 2024]

[23] Forenzy. "Virtual CISO". 2024. https://forenzy.net/services/virtual-ciso/ [accessed: Jun. 27, 2024]

[24] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers", Computers & Security, Vol. 92, No. 101747, Mar. 2020. http://dx.doi.org/10.1016/j.cose.2020.101747.

[25] M. A. S. Canant, "Effective Security Programs Enable Clinical and Business Improvements", Information Security in Healthcare, HIMSS Publishing, pp. 237-246, 2010.

[26] E. Karanja, "The role of the chief information security officer in the management of IT security", Information & Computer Security, Vol. 25, No. 3, pp. 300-329, Jul. 2017. https://doi.org/10.1108/ICS-02-2016-0013.

[27] S. Maynard, M. Onibere, and A. Ahmad, "Defining the strategic role of the chief information security officer", Pacific Asia Journal of the Association for Information Systems, Vol. 10, No. 3, Sep. 2018. http://dx.doi.org/10.17705/1PAIS.10303.

[28] K. Rahul, R. K. Banyal, and N. R. Bhatt, "The Cyber Security Challenges: A Survey of Chief Information Security Officer in Indian Context", ICT for Competitive Strategies, CRC Press, pp. 749-758, 2020.

[29] S.-S. Kim and H. Yoo, "A Study on Technical Protection Measure of Personal Information in Small and Medium-sized Businesses", Journal of KIIT, Vol. 18, No. 1, pp. 157-169, Jan. 2020. http://doi.org/10.14801/jkiit.2020.18.1.157.

[30] S.-Y. Lee, "Analysis of Information Security Training for Business", Journal of KIIT, Vol. 15, No. 9, pp. 125-132, Sep. 2017. https://http://doi.org/10.14801/jkiit.2017.15.9.125.

[31] C. S. Moon and S. H. Kim, "A Study on Advanced Model for Personal Information Security Management", Journal of KIIT, Vol. 13, No. 1, pp. 93-99, Jan. 2015. https://http://doi.org/10.14801/jkiit.2015.13.1.93.

[32] Gartner Peer Insights, "Virtual Chief Information Security Officer Services (vCISO) Alternatives", 2024. https://www.gartner.com/reviews/market/security-consulting-services-worldwide/vendor/lares/product/virtual-chief-information-security-officer-services-vciso/alternatives [accessed: Jan. 31, 2024]

Authors

Dong-Hyuk Shin

2005 : BS degree in Industrial engineeringy, Soong-Sil University

2013 : Master degree in Science in Information Security, Korea University

2017 : Ph.D in Computer Science, Tech University of Korea

2016 ~ Present : ISMS-P Information Security Auditor

Research interests : Virtual CISO, AI, Security Management, Information Security Management System(ISMS), Cloud Security, Platform Satisfaction