International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-08, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

Adopting Security Operation Center: Insights from the Indonesian Financial Sector

Ken Basari[1], Leo Aldianto[2]
[1,2] Faculty of Entrepreneurship and Technology Management, Bandung Institute of Technology, Bandung

ABSTRACT: The rising cybersecurity threats have made Security Operation Centers (SOCs) essential for Indonesian finance companies to protect sensitive data and ensure regulatory compliance. This study explores factors influencing SOC adoption, implementation challenges, and strategies to improve adoption rates. Using a mixed-method approach, it combines survey data and interviews with cybersecurity professionals. Findings reveal that subjective norms and top management support are key drivers, while budget constraints and a lack of skilled personnel pose significant challenges. Recommendations include strengthening management support, leveraging norms, investing in training, and optimizing vendor selection. The study offers practical and theoretical insights for enhancing cybersecurity resilience, with future research suggesting longitudinal studies, cross-sector analysis, and regulatory compliance exploration.

KEYWORDS: Cybersecurity, Security Operations Center (SOC), Technology Adoption, Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB)

INTRODUCTION

Cyberattacks have surged worldwide, posing significant threats to individuals, businesses, and governments. From ransomware to data breaches, these malicious incursions expose critical vulnerabilities in our digital ecosystem. As cybercriminals refine their methods, global organizations must strengthen their defenses. The escalating frequency and severity of attacks demand comprehensive strategies to safeguard sensitive data and protect digital infrastructures.

During 2021 and 2022, the Asia-Pacific region experienced the highest level of cyber-attacks, with Europe coming in second (IBM Security, 2024). As a result of this attack, companies can experience several negative impacts. First, financial losses may occur due to system recovery costs, lost revenue, or potential legal claims. Second, reputational damage is likely as public and customer trust declines. Additionally, legal and regulatory issues can arise if data protection laws are breached. From an operational standpoint, disruptions to systems and business processes can hamper daily activities. Finally, the loss of critical data not only hinders ongoing work but can also create long-term challenges for a company’s future.

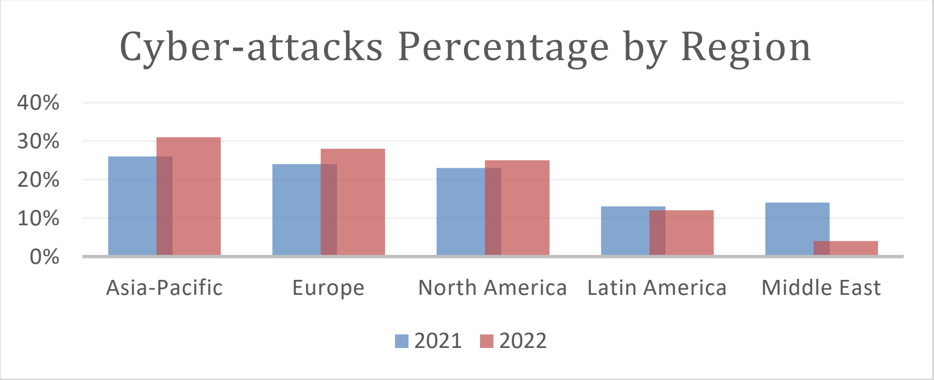

Figure 1. Cyber-attacks Percentage by Region

Lockbit 3.0 ransomware was recently used in an attack on Indonesia’s National Data Center, disrupting critical government services such as immigration and airport operations. The attackers demanded an $8 million ransom, but the government declined to pay (BBC

News Indonesia, 2024). Bank Syariah Indonesia (BSI), the country's largest Islamic bank, was also targeted by the Lockbit group. This incident caused days-long service interruptions and resulted in the theft of 1.5 terabytes of sensitive customer information. Despite a $20 million ransom demand, BSI refused to comply, leading to the data being released on the dark web (Kompas, 2023). Given the growing prevalence of these threats, strong cybersecurity measures are essential. Establishing a Security Operation Center is one approach that can help organizations quickly identify and respond to cyberattacks.

A Security Operations Center (SOC) is a specialized unit focused on protecting an organization's digital infrastructure. It continuously monitors networks, systems, and endpoints through tools such as Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS). By analyzing data for suspicious activity, the SOC quickly detects, contains, and resolves cyber threats. This centralized incident management approach helps organizations minimize damage, maintain business continuity, and strengthen overall cyber resilience. Additionally, an SOC strives to refine overall information security incident management by learning from breaches and establishing preventive measures (Miloslavskaya, 2016).

In Indonesia, the significance of an SOC is further emphasized by Bank Indonesia Regulation Number 2 of 2024, titled Information System Security and Cyber Resilience for Payment System Operators, Money Market and Foreign Exchange Market Participants, and Other Parties Regulated and Supervised by Bank Indonesia (Peraturan Bank Indonesia Nomor 2 Tahun 2024, 2024). This regulation offers a comprehensive framework that governs SOC operations in financial institutions. Under these guidelines, an SOC is responsible for detecting, analyzing, and responding to cyber incidents in compliance with regulatory requirements. By effectively implementing the regulation's provisions, organizations can quickly recover from cyber incidents, uphold business continuity, and minimize the impact on their operations.

Given the importance of SOCs in protecting organizations from cyber threats, along with the regulatory framework provided by Bank Indonesia, it becomes essential to explore how these centers are being adopted within the Indonesian financial sector. The main objective of this study is to thoroughly examine various elements that can impact the adoption of Security Operations Centers (SOC) inside the Indonesian financial sector, to identify the challenges involved in implementing SOCs, and to determine effective strategies for boosting their adoption rates.

Across the globe, cyber threats continue to grow in sophistication, making it crucial for organizations to adopt robust security measures. In Indonesia, setting up a Security Operations Center (SOC) represents a proactive strategy to address these risks, functioning as a "nerve center" by continuously monitoring and analyzing an organization's security posture. However, deciding to implement an SOC involves numerous considerations and can be quite complex.

This study will explore what motivates Indonesian financial companies to establish a Security Operations Center (SOC), examine the challenges they encounter during adoption, and identify practical ways to overcome these hurdles to encourage broader implementation. It employs a mixed-methods approach—combining quantitative and qualitative methods—to investigate factors influencing SOC adoption, key challenges, and strategies to boost adoption rates within Indonesia's finance sector. Structured surveys will be distributed to cybersecurity staff, measuring variables such as perceived usefulness, ease of use, and top management support, and the resulting data will be analyzed to determine the most impactful factors and validate hypotheses. Interviews with cybersecurity employees will further uncover obstacles to SOC adoption, and the combined insights from surveys and interviews will guide recommendations aimed at enhancing SOC implementation.

LITERATURE REVIEW

According to Shankar, cybersecurity involves defending complex data and IT systems from attacks, unauthorized access, and misuse (Shankar Bhosale, 2021). It also encompasses practical measures that shield networks, information, and devices from both internal and external threats (Y. Li & Liu, 2021). As noted by Lloyd, implementing effective cybersecurity strategies can help businesses lower their exposure to threats such as data breaches and ransomware, stimulate growth, retain customers by building trust, and unlock new market opportunities (Lloyd, 2020). Given the increasing frequency and impact of cyberattacks, treating cybersecurity as a core business priority is now more critical than ever.

As mentioned before, a Security Operations Center (SOC) is a specialized unit tasked with managing information security incidents through continuous monitoring (Miloslavskaya, 2016). It uses various protection tools and skilled personnel to detect, report, assess, and respond to threats—particularly within Internet of Things (IoT) ecosystems. According to Alharbi, an SOC has three core elements: Analysts, Processes, and Technology. Analysts must understand the organization's mission, network, and policies, possess strong IT skills, and establish credibility to effectively distinguish real attacks from false alarms and coordinate the appropriate response. Processes must be consistent yet adaptable, with clearly defined roles and responsibilities ("swim lanes") and sufficient authority to handle threats. Technology underpins these efforts by providing the tools necessary to monitor and analyze security events in real time (Alharbi, 2020).

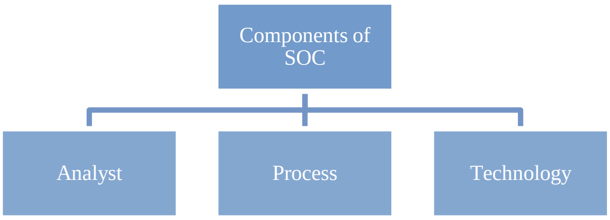

Figure 2. Components of Security Operation Center

Organizations can operate an SOC internally or outsource it to a third party, depending on their resources and expertise. Because SOC functions involve complex technicalities, support from top management is crucial (Atmojo et al., 2019; Furnell et al., 2009). When executives endorse a strong security culture and allocate adequate resources, SOC teams can more effectively reduce cyber risks and bolster overall information security performance.

Table 1. Related Works

Title	Success Factors for Cyber Security Operation Center (SOC) Establishment	Improving Information Security Performance: The Role of Management Support and Security Operation Center	Security Operations Centers – A Business Perspective
Objective	Identifies critical elements that contribute to the successful implementation of an SOC by reviewing past literature and focusing on human, process, and technology factors.	Empirically examines how management backing and the presence of an SOC affect information security performance, particularly in the banking sector.	Takes a business-oriented look at SOCs, examining their value and impact on organizations.
Methodology	Literature review of 10 previous SOC studies.	Uses a questionnaire-based approach analyzed with SEM-PLS.	Literature review drawing on publicly available databases.
Results	Uncovers 10 key success factors, including top management support, financial strategy, human resources, processes, technology, environment, analysis/reporting, physical space, and continuous	Confirms that both management support and having an SOC in place significantly enhance information security outcomes.	Concludes that SOCs offer several corporate advantages, such as preserving market valuation, cutting costs, strengthening brand reputation, and boosting investor confidence.

	improvement—emphasizing their interdependence.		
Strength	Thoroughly synthesizes multiple SOC-related papers.	Employs SEM-PLS effectively to meet its research aims.	Provides a detailed and thorough analysis of public data sources.
Weakness	Relies solely on secondary data, with no validation through surveys or interviews.	Lacks an in-depth critique of the literature and omits the actual survey instrument.	Could offer a more comprehensive discussion of the Technological Frames of Reference (TFR) theory.

In “Success Factors for Cyber Security Operation Center (SOC) Establishment,” Majid and Ariffi review ten prior SOC studies to identify key elements for successful implementation, emphasizing “Top Management Support” (Majid & Ariffi, 2019). In “Improving Information Security Performance: The Role of Management Support and Security Operation Center,**”** Atmojo survey employees in Malaysian finance companies and find that both management backing and having an SOC significantly enhance information security in the banking sector (Atmojo et al., 2019). Lastly, “Security Operation Centers – A Business Perspective,” by Michail, draws on publicly available data to show that SOCs offer substantial corporate benefits, including market valuation preservation, cost avoidance, brand and reputation protection, and higher investor confidence (Michail, 2015).

Table 2. Comparing Technology Adoption Theories

Theory	Strength	Weaknesses
Diffusion of Innovations (DIT)	Well-established for explaining how innovations spread.	May not capture individual-level decision factors.
Technology Readiness	Categorizes readiness into distinct segments.	General groupings may fail to reflect specific behaviors.
Task-Technology Fit	Highlights the importance of individual performance and impact.	May overlook initial adoption decisions.
Theory of Reasonable Action	Straightforward and widely used; emphasizes attitudes and norms.	Omits perceived control as a component.
Theory of Planned Behavior	More comprehensive by incorporating perceived behavioral control.	Can be complex and may overlap with other theories.
Decomposed Theory of Planned Behavior	Offers detailed factors for understanding behavioral intentions.	Complexity often requires large amounts of data.
Technology Acceptance Model (TAM)	Well-validated and easy to apply to IT adoption scenarios.	Does not factor in the influence of social norms.
Technology Acceptance Model 2 (TAM2)	Includes additional determinants and remains effective over time.	Primarily focuses on perceived usefulness and intended usage.
Technology Acceptance Model 3 (TAM3)	Provides a thorough framework for understanding technology adoption.	Does not account for direct effects.
Unified Theory of Acceptance and Use of Technology (UTAUT)	Offers strong explanatory capabilities with key moderating factors.	Excludes direct effects and incorporates social influence, which might not apply universally.

These models each present unique strengths and limitations when examining how users adopt new technologies (Lai, 2017). The Technology Acceptance Model (TAM) is often praised for its simplicity and predictive power, making it a popular choice in IT adoption studies. However, the Theory of Planned Behavior (TPB) offers a more inclusive framework by adding elements of perceived control and social influence, which is especially valuable in situations where these aspects heavily impact user behavior.

In a recent study exploring the application of the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB) to evaluate students' intentions to use a wiki for group work and their actual behaviors, Cheng combined these two theories into a single framework (Cheng, 2019).

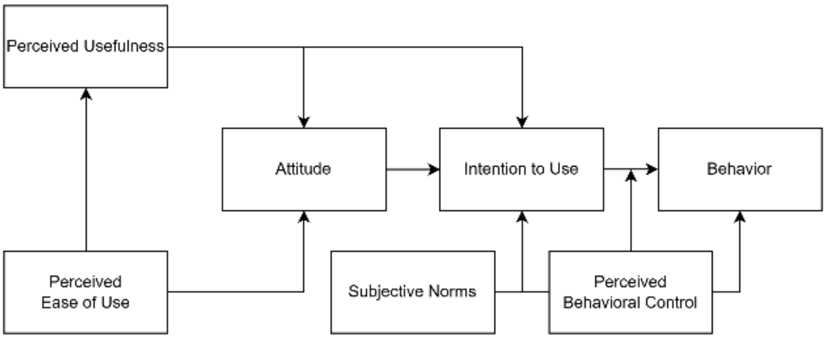

Figure 3. TAM and TPB Framework

The integration of TAM and TPB offers several advantages, as each theory has unique strengths. This combined model creates a more adaptable and comprehensive framework, encompassing both internal factors (such as attitudes and perceptions) and external factors (like subjective norms and behavioral control) that influence technology adoption.

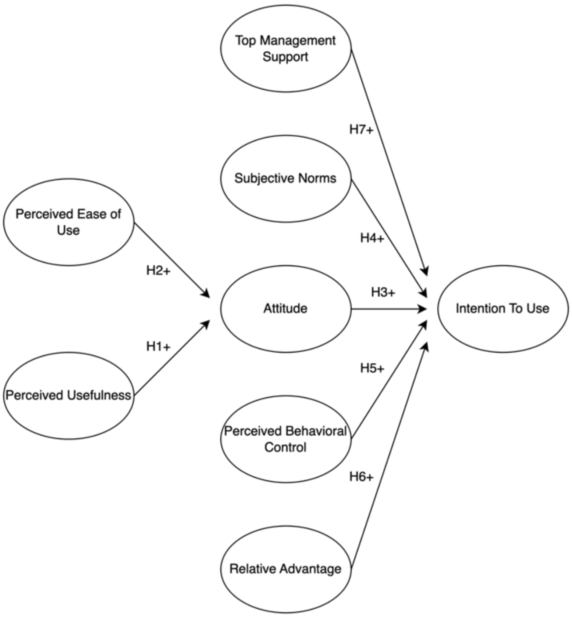

Figure 4. Conceptual Model

In addition to the variables from TAM and TPB, Relative Advantage and Top Management Support are two other factors that can drive businesses to adopt technology. Relative Advantage is taken from a paper that is researching about solar energy technology in Sri Lanka that said that relative advantage influences the intention to use solar energy there (Bandara & Amarasena, 2018). Top Management Support is taken from a paper that is researching about the intention to use cloud computing, where top management support is a key role in supporting the intention to use (Yigitbasioglu, 2015). To introduce innovation in the implementation of Security Operation Centers (SOC) within businesses, these variables have been incorporated into the TAM and TPB framework. The main goal is to create a comprehensive model that provides insight into how businesses can effectively adopt SOC. This model aims to identify the key factors influencing the adoption of SOC in organizations.

From the conceptual framework above, hypothesis is being made:
H1: Perceived usefulness positively influences the attitude towards implementing SOC
H2: Perceived ease of use positively influences the attitude towards implementing SOC
H3: Attitude towards SOC implementation positively influences intention to use SOC
H4: Subjective norms positively influence the intention to use SOC.
H5: Perceived behavioral control positively influences the intention to use SOC
H6: Relative advantage positively influences the intention to use SOC
H7: Top management support positively influences the intention to use SOC

RESEARCH METHODOLOGY

All the data is collected from Cyber Security employee in Indonesian finance companies, both for quantitative and qualitative data. Using Cochran formula, a purposive sampling method will be used to ensure the study is relevant and get the accurate information, which approximately 95 respondents will be gathered to be the main source of the quantitative data. Using Likert scale, eight construct of the framework will be made a questionnaire, each with their own several questions.

Table 3. Survey Questions

Construct	Question	Reference
Perceived Ease of Use	1. Learning how the Security Operations Center (SOC) works would be easy for my company 2. It is easy for my company to become skillful at using the Security Operations Center (SOC) 3. Overall, adopting the Security Operations Center (SOC) is easy for my company.	(Hasan et al., 2023)
Perceived Usefulness	1. Adopting the Security Operations Center (SOC) enhances my company’s security effectiveness. 2. Adopting the Security Operations Center (SOC) makes it easier for my company to respond cyber threat and incident 3. Overall, adopting the Security Operations Center (SOC) is useful for my company	(Hasan et al., 2023)
Attitude	1. Our company believes that implementing SOC is valuable 2. Our company supports the adoption of SOC. 3. Our company believes that establishing a strong SOC enhances our security posture and brand reputation.	(X. Li et al., 2023)

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-08, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

	4. SOC implementation would make our business more attractive to potential partners and investors	
Subjective Norms	1. Regulatory policies mandate the implementation of an SOC in our company 2. Cybersecurity policies are strict in our company 3. Our clients and partners prefer to work with companies that have a robust SOC in place 4. Media reports highlight the importance of SOC in preventing and mitigating security incidents	(X. Li et al., 2023)
Perceived Behavioral Control	1. Our company has sufficient budget and financial resources for SOC implementation 2. Our company has sufficient skilled personnel to operate and manage an SOC 3. I believe that implementing a SOC in our business is within our control 4. Our company has access to sufficient external expertise and consultants to assist with SOC implementation	(X. Li et al., 2023)
Intention to Use	1. I would like my company to adopt the Security Operations Center (SOC) 2. Implementing a SOC in our company is a priority 3. Our company is ready to adopt SOC practices in the future 4. Our company is ready to integrate SOC operations with our existing IT systems	(X. Li et al., 2023) (Hasan et al., 2023)
Relative Advantage	1. Adopting an SOC benefits the company significantly 2. The use of a SOC can lead to improved operational efficiency, setting us apart from competitors 3. Adopting an SOC will decrease security breaches 4. Adopting an SOC will offer competitive benefits to the company	(Alam, 2012)
Top Management Support	1. The management of our company believes that SOC has the potential to provide significant business benefits	(Yigitbasioglu, 2015)

	2. The management of our company believes that SOC will create a significant competitive 3. The management of our company promotes the use of SOC 4. Our management provides financial banking for acquiring and implementing advanced security technologies 5. Investment in information security infrastructure, such as SOC, is strongly supported by management.	

The questionnaire data will be analyzed using R statistical software to ensure accuracy and reliability. The analysis includes Descriptive Analysis to summarize the data, Correlation Analysis to examine relationships between variables, Regression Analysis to assess the impact of independent variables on the dependent variable, and Hypothesis Testing to validate the conceptual framework. The results will inform interview questions addressing challenges in implementing SOCs in finance companies.

Interview data will be analyzed to identify common challenges, assess their significance, gather insights, and develop recommendations to enhance SOC adoption in finance companies. Transcribed survey data will undergo thematic analysis to uncover key themes representing challenges. Based on these findings, actionable recommendations will be formulated.

RESULT AND ANALYSIS

The first result that will be analyzed is the survey result. There are a total of 112 respondents for the survey, each with their different answers. The first analysis is the years of experience in IT security, availability of SOC in companies, and range of time of SOC operational.

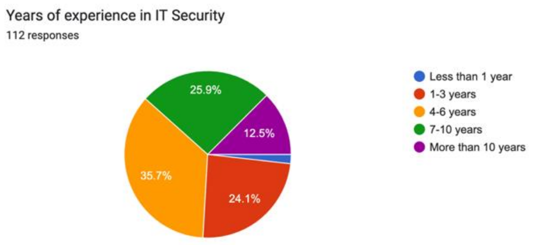

Figure 5. Years of Experience Chart

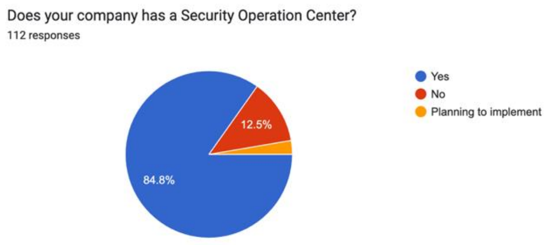

Figure 6. SOC Availability Chart

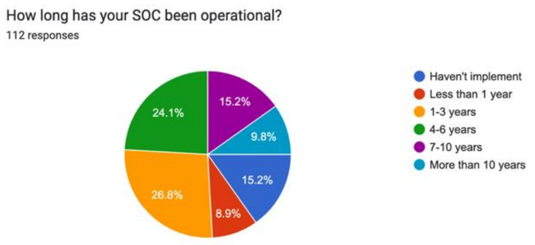

Figure 7. SOC Sustainability Chart

From the three diagram that are shown above, we can conclude that IT security field is relatively young but growing rapidly, with most professionals having 1–10 years of experience and a smaller number possessing over a decade of expertise, reflecting the field's developmental stage. A significant number of companies have recognized the importance of Security Operation Centers (SOCs), with the majority already implementing them, while a few are either planning or yet to establish one. SOC maturity varies, with many companies implementing SOCs within the last 1–6 years, suggesting a growing awareness and effort toward strengthening cybersecurity. Additionally, the presence of long-established SOCs in some organizations highlights a proactive approach to cybersecurity, contributing to a more secure corporate landscape in Indonesia.

Table 4. Descriptive Analysis Result

Code	Construct	Mean	SD
1Z	Perceived Ease of Use	4.078	0.789
2Z	Perceived Usefulness	4.339	0.669
3Z	Attitude	4.328	0.661
4Z	Subjective Norms	4.201	0.699
5Z	Perceived Behavioural Control	4.252	0.713
6Z	Intention to Use	4.270	0.692
7Z	Relative Advantage	4.302	0.663
8Z	Top Management Support	4.241	0.668

The result of the descriptive analysis comes with the Mean and Standard Deviation (SD) for each construct in the framework. The table indicates that all constructs positively influence user perceptions, as shown by mean scores above 4.0, with low standard deviations reflecting consistent responses.

Table 5. Correlation Analysis Result

Code	Construct	Correlation
1Z	PU - AT	0.524
2Z	PEOU - AT	0.091
3Z	AT - INT	0.029
4Z	SN - INT	0.392
5Z	PBC - INT	0.330
6Z	RA - INT	0.352
7Z	TMS - INT	0.426

The result of the correlation analysis indicates that Top Management Support, Subjective Norms, and Relative Advantage are influential factors driving Intention to Use, underlining the importance of organizational backing, perceived benefits, and social influences.

Table 6. Regression Analysis Result

	Unstandardized Coeff.	Std. Error	T	Sig.
(Intercept)	1.405802	0.517478	2.717	0.0077
Attitude	0.003501	0.103568	0.034	0.9731
Subjective Norms	0.209691	0.103455	2.027	0.0452
Perceived Behavioural Control	0.027962	0.103923	0.269	0.7884
Relative Advantage	0.145612	0.102321	1.423	0.1576
Top Management Support	0.288374	0.119963	2.404	0.0180

The result of the regression analysis indicates that Top Management Support and Subjective Norms, once again, is the most influential factors driving Intention to Use. On the other hand, Attitude and Perceived Behavioral Control show negligible effects and are not statistically significant. Relative Advantage shows some influence but is not strong enough to be conclusive.

From the three analyses, which is descriptive analysis, correlation analysis, and regression analysis, the analysis highlights the critical role of Top Management Support and Subjective Norms in driving system adoption. While Perceived Usefulness strongly shapes attitudes, it indirectly contributes to adoption intentions by reinforcing positive perceptions. Conversely, Attitude and Ease of Use play relatively minor roles in influencing adoption, indicating that users prioritize external influences and perceived benefits over personal perceptions or usability. For successful system adoption, organizations should focus on leadership advocacy, fostering a supportive social environment, and emphasizing the system's practical advantages while addressing usability concerns as a secondary priority.

For the hypothesis testing, the researcher uses data from all the analysis and combine it into a conclusion:

H1: Perceived usefulness positively influences the attitude towards implementing SOC
Perceived Usefulness has a strong positive influence on Attitude towards implementing SOCs, with a high overall mean, moderate positive correlation, and significant positive impact.
H2: Perceived ease of use positively influences the attitude towards implementing SOC
Perceived Ease of Use has a weak and insignificant relationship with Attitude, with positive mean score, weak and insignificant correlation, and no significant impact, but still a positive influence.
H3: Attitude towards SOC implementation positively influences intention to use SOC
Attitude has a weak and insignificant direct effect on Intention to Use SOC, with strong positive mean, weak but significant positive relationship, and insignificant direct effect, but still a positive influence.
H4: Subjective norms positively influence the intention to use SOC.
Subjective Norms significantly influence Intention to Use SOC, with high mean score, moderate positive relationship, and significant positive impact.
H5: Perceived behavioral control positively influences the intention to use SOC
Perceived Behavioral Control positively influences Intention but is not significant in regression, with high mean score, moderate positive relationship, and insignificant regression score.
H6: Relative advantage positively influences the intention to use SOC
Relative Advantage has a positive influence but is not significant in regression, with high mean score, moderate positive relationship, and insignificant regression score.
H7: Top management support positively influences the intention to use SOC
Top Management Support significantly influences Intention to Use SOC, with high mean score, moderate to strong relationship, and significant positive impact.

For the qualitative analysis, which is interviews with 5 respondents, aimed to explore and validating the data from the survey above. The interviews conducted with that is related to cyber security in finance industries, each with their various experiences.

The first interview is with a SOC Leader from Company A. The interview highlighted the critical role of SOCs in Indonesian finance companies for monitoring threats, responding to incidents, and analyzing risks through Security Information and Event Management (SIEM) systems, as required by OJK regulations to protect customer data. However, she identified key challenges, including a lack of skilled personnel, budget constraints, and the need for strong management support. While no law mandates SOC implementation, firms face pressure to safeguard data and address cybersecurity risks. To overcome these challenges, she suggested increasing management awareness through clear proposals and regular updates to secure their commitment and demonstrate SOCs' importance in protecting company assets.

The second interview is with a Network Management Service Engineer from Company B. He emphasized SOC's critical role as the frontline defense against cyber threats, protecting sensitive financial transactions and customer data. In his organization, SOC implementation is relatively new and outsourced to an external vendor, with the supporting tasks like analysis and system hardening.

He identified budget constraints and a lack of skilled personnel as major challenges, noting the high costs of technology and qualified cybersecurity professionals. He highlighted the importance of top management support, as companies often prioritize SOC implementation only after recognizing potential financial and reputational risks. To address these issues, he recommended investing in employees with cybersecurity certifications, viewing SOC tools as essential assets, and outsourcing SOC services as a cost-effective alternative, though he noted internal SOCs are more effective for monitoring critical assets. Lastly, he stressed SOC's role in defending against ransomware, advocating for at least outsourced 24/7 monitoring to protect corporate assets.

The third interview is with a VP Cyber Security Risk and Data Protection from Company C. He shared his experience in building a Security Operations Center (SOC) for a financial institution, transitioning from office hours to 24/7 operations between 2016 and 2019 to combat the growing sophistication of cyberattacks. He highlighted SOC's critical role in real-time threat monitoring, incident response, and vulnerability testing through blue and red team operations. He emphasized the importance of top management support in driving SOC implementation, noting that proactive leadership and awareness of cybercrime risks were pivotal, even before regulatory mandates. However, establishing a SOC posed challenges, including substantial investment in technology like SIEM systems, assembling a skilled cybersecurity team, and retaining talent in a competitive field. While he acknowledged that external SOC services could reduce costs, he stressed the advantages of internal teams for better control over sensitive data. He also underlined SOC's essential role in mitigating ransomware threats by continuously monitoring vulnerabilities, working with IT to patch security gaps, and creating policies to prevent ransomware infiltration. Without SOC, he warned, organizations face significant financial and reputational risks that far outweigh the initial investment.

The fourth interview is with a Security Assessment from Company D. He described SOC as a critical hub for detecting, analyzing, and responding to cybersecurity incidents, essential for safeguarding financial institutions from significant financial and reputational risks. SOC helps protect customer trust and mitigate threats like ransomware, which can severely damage a company's reputation. He highlighted three key considerations for SOC implementation: aligning the SOC's scale with organizational needs, leveraging the latest technology, and ensuring skilled personnel to manage operations. He emphasized the importance of top management support, noting that his company's leadership mandates security checks for all new applications and aligns with regulations such as the ITE Law, which indirectly encourages SOC adoption. While acknowledging cost as a major challenge, he argued that the risks of not having a SOC outweigh the investment, suggesting that data-driven proposals demonstrating the financial impact of threats can help secure resources. He also noted that external SOC services can complement internal operations by addressing external threats, but a balance between internal and external resources is ideal. Lastly, he emphasized SOC's role in mitigating ransomware through continuous monitoring, fast detection, and the use of AI technology to automate responses and protect critical systems effectively.

The fifth interview is with a Information Security from Company E. She highlighted SOC's importance in protecting sensitive customer data and internal information, emphasizing its role in real-time threat detection and proactive risk mitigation to prevent significant damage from breaches. He noted that SOC enhances overall risk management and ensures compliance with OJK and Bank Indonesia regulations, aligning the company with cybersecurity standards. Challenges in establishing SOC included a lack of internal expertise, requiring training and new SOP development, as well as resistance from some departments to the increased governance SOC entails. Despite these hurdles, top management support, driven by awareness of global cybersecurity incidents, was critical in securing resources and advancing the SOC project. She also acknowledged that regulatory pressure and industry norms influenced the decision to localize SOC operations. Before SOC implementation, the company relied on AWS tools, vulnerability assessments, and penetration testing to manage threats effectively.

Table 7. Interview Key Insights

Themes	Explanation	Key Insights
	In all interviews, top management support emerged as a key factor in SOC adoption. Without active involvement from senior leadership, SOC initiatives often struggle to secure the necessary resources and prioritization. Interviewees noted that management typically becomes	Awareness among management of the financial and reputational risks posed by cyber threats drives the adoption of SOC.

Top Management Support	invested once they fully grasp the potential risks posed by cybersecurity threats. This support plays a critical role in budget allocation and the alignment of security initiatives. Ultimately, successful SOC implementation depends on management's acknowledgment of cybersecurity as a fundamental business priority.	
Subjective Norms (Regulatory, Industry, Reputation, and Peer Pressures)	Regulatory and industry pressures significantly drive SOC adoption, with companies motivated by compliance requirements from authorities like OJK and BI and the need to align with industry standards. Interviews highlighted the role of external factors, such as competitor behavior and evolving cybersecurity regulations, in influencing adoption decisions. Additionally, reputation and peer pressure play a role, as companies tighten cybersecurity measures to avoid incidents like those affecting competitors. Internal advocacy from knowledgeable employees or management further reinforces the importance of SOC for ensuring business continuity.	SOC adoption is influenced by compliance requirements, competitive pressures, and peer behaviors. Organizations often align with industry norms and peer practices to stay competitive and showcase their commitment to robust security standards. The fear of lagging behind industry leaders or being seen as weak in cybersecurity further heightens the impact of peer pressure on SOC implementation decisions.
Budget Constraint	Budget constraints pose a major challenge to SOC adoption, especially for smaller financial institutions with limited resources. Larger organizations can more easily invest in SOC technology and talent, while smaller firms often find the costs difficult to justify. However, interviewees emphasized that the potential consequences of not implementing an SOC, such as data breaches or reputational harm, outweigh the initial investment. To address this, some companies opt for outsourced SOC services, though internal SOCs are preferred for greater control over sensitive data.	While the high cost of SOC implementation can be a deterrent, interviewees emphasized that the potential consequences of not having an SOC, such as data breaches, far exceed the initial investment.
Skilled Personnel Shortage	A common challenge highlighted in the interviews was the shortage of skilled personnel required for SOC implementation. Recruiting and retaining cybersecurity talent is difficult, often resulting in overburdened teams and reduced SOC effectiveness. Proposed solutions include upskilling internal staff and leveraging external vendors, though continuous investment in cybersecurity training remains essential for companies aiming to develop robust internal SOC capabilities.	The absence of internal cybersecurity expertise affects SOC performance. Suggested solutions include training existing employees or outsourcing SOC operations to third-party providers.
Vendor and Tool Selection	Choosing the right vendor and tools is a crucial step in SOC implementation, with many companies reviewing the solutions used by peers to guide their decisions. The success of SOC heavily depends on selecting vendors whose tools align with the organization's specific security needs, as mismatched solutions can result in inefficiencies or vulnerabilities. Companies often	The selection of a vendor significantly affects SOC efficiency, prompting many companies to study peer practices to guide their decision-making.

	dedicate considerable time to evaluating vendors, carefully balancing cost considerations with the quality of services offered.	

So, with all the quantitative and qualitative data taken, we can answer the research question. The first research question is "What factors influence finance Indonesian companies decision to adopt Security Operation Centers (SOC)?", there are 2 factors that influence finance Indonesian companies decision to adopt SOC, Top Management Support and Subjective Norms. Top management support plays a crucial role in SOC implementation, as leadership commitment ensures cybersecurity becomes a priority. External pressures, such as regulatory requirements from bodies like OJK and BI, industry standards, peer practices, and the need to maintain a strong reputation, further drive companies to adopt SOC.

The second research question is "What are the challenges in adopting Security Operation Centers (SOC) for finance Indonesian companies, and how can these challenges be addressed to increase adoption rates?", there are 2 main challenges and 4 factors that can increase SOC implementation. The 2 main challenge is Budget Constraint and Skilled Personnel Shortage. Budget constraints and a shortage of skilled personnel are major challenges in SOC implementation, particularly for smaller organizations. The high cost of SOC technology, tools, and staffing often forces companies to consider outsourcing as a cost-effective alternative. Similarly, the lack of qualified cybersecurity professionals hampers effective SOC operations, with many relying on third-party vendors temporarily while training internal teams to address the talent gap.

The 4 factors that can increase SOC implementation is Top Management Support, Subjective Norms, Training and Development for Skilled Personnel, and Vendor and Tool Selection. Strong top management support is crucial for overcoming barriers like budget constraints and resistance, ensuring SOC initiatives are prioritized, resourced, and sustained across the organization. Regulatory requirements and industry standards also drive SOC adoption by creating benchmarks that promote compliance and competitiveness. Investing in cybersecurity training helps address the skills gap, builds a capable internal team, and reduces reliance on external vendors, enhancing long-term SOC effectiveness. Additionally, selecting vendors and tools that align with organizational needs minimizes implementation challenges, reduces inefficiencies, and streamlines SOC operations.

CONCLUSION AND RECOMMENDATION

This study examined how Security Operations Centers (SOC) are adopted in Indonesia's financial sector, focusing on influencing factors, challenges, and strategies to boost adoption. The findings highlight:

1. Factors Influencing SOC Adoption
   a. Top Management Support
      Senior leadership's commitment significantly shapes SOC implementation.
   b. Subjective Norms
      Regulatory demands (e.g., OJK, BI) and industry benchmarks pressure organizations to adopt SOC, bolstered by peer practices and reputation concerns.
2. Challenges in SOC Adoption
   a. Budget Constraint
      High costs for technology, tools, and talent pose financial hurdles, especially for smaller firms.
   b. Skilled Personnel Shortage
      Lack of qualified cybersecurity staff complicates SOC operations, often leading to outsourcing or temporary external support.
3. Opportunities to Enhance SOC
   a. Top Management Support
      Strong leadership backing ensures sufficient resources, helps overcome resistance, and sustains SOC programs.
   b. Subjective Norms
      Compliance with regulations and industry standards encourages SOC adoption, maintaining competitiveness and legal alignment.

   c. Training and Development
      Continuous skill-building and professional development address talent gaps and foster internal expertise.
   d. Vendor and Tool Selection
      Choosing solutions that match organizational needs improves cost-effectiveness and operational efficiency, streamlining SOC adoption.

There are 3 implications for this study. It highlights how strong management support, regulatory frameworks, and strategic decision-making collectively enhance cybersecurity resilience in Indonesia's financial sector:

1. Theoretical Implication
   This study integrates the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB), enhanced with constructs like Relative Advantage and Top Management Support. The framework underscores how management backing and subjective norms significantly shape SOC adoption, filling a research gap by examining SOC within Indonesia's unique cultural and regulatory context.
2. Practical Implication
   Early and visible leadership support is crucial for successful SOC implementation, guiding resource allocation and securing employee buy-in. Training initiatives help address skill gaps, easing SOC use and adoption. Policymakers can further encourage SOC integration by offering incentives, mandating usage for certain operations, or setting standardized guidelines on training, technology, and reporting.
3. Global Implication
   Broad SOC adoption in the financial sector bolsters Indonesia's position as a digital economy leader by mitigating cyber threats and protecting both businesses and consumers. Stronger data privacy and security enhance consumer trust, attract foreign investment, and stabilize the nation's digital infrastructure.

From all the written conclusion, the researcher concludes the recommendation for this study:

1. Financial Institution
   a. Strengthen Top Management Support
      Conduct high-level briefings to highlight the strategic benefits of SOCs, emphasizing them as an investment rather than a cost. Illustrate successful industry examples to demonstrate the positive business impact of SOC adoption.
   b. Leverage Peer Benchmarking
      Compare processes, practices, and performance metrics against industry peers or leaders to pinpoint improvement opportunities.
   c. Enhance Reputation Management
      Proactively safeguard and improve public image, credibility, and stakeholder trust to reinforce institutional resilience.
   d. Develop Cybersecurity Talent
      Form collaborations with universities and training providers to build a skilled SOC workforce. Provide internal training and certifications to upskill current employees.
   e. Optimize Budgets
      Consider hybrid SOCs to lower initial expenses and review existing case studies from other organizations to avoid unnecessary spending.
2. Policymakers and Regulators
   a. Strengthen the Regulatory Framework
      Enforce mandatory SOC adoption for financial institutions while offering a phased rollout to address budget constraints. Develop tailored guidelines to support industry-specific SOC implementation.
   b. Offer Financial Incentives
      Provide tax benefits or subsidies to organizations investing in SOC infrastructure and training, encouraging broader and more rapid SOC adoption.

This study highlights several avenues for further inquiry to build on its findings and address current limitations. These suggestions aim to deepen insights, broaden applicability, and explore new facets of SOC adoption:

1. Broader Sectoral Coverage
   Investigate SOC adoption in other critical industries, such as manufacturing, telecommunications, and healthcare, where security is equally vital. Comparing challenges, drivers, and opportunities across these sectors may reveal both shared patterns and unique elements.
2. Longitudinal Investigations
   Examine the long-term impact of SOC adoption on organizational performance—specifically regarding cybersecurity readiness, operational efficiency, and customer trust.
3. Regulatory and Policy Analyses
   Evaluate how current cybersecurity regulations influence SOC adoption, determining whether mandates and incentives are aligned with organizational capabilities. Comparing SOC-related policies across various countries or regions may uncover best practices that could be adapted for Indonesia.

REFERENCES

1. Alam, S. S. (2012). Intention to Use Renewable Energy: Mediating role of Attitude. *Energy Research Journal*, *3*(2), 37–44. https://doi.org/10.3844/erjsp.2012.37.44
2. Alharbi, S. A. (2020). A qualitative study on security operations centers in saudi arabia: Challenges and research directions. *Journal of Theoretical and Applied Information Technology*, *98*(24), 3972–3982. www.jatit.org
3. Atmojo, T. A., Prabowo, H., So, I. G., & Abdinagoro, S. B. (2019). Improving information security performance: the role of management support and security operation center. *International Journal of Recent Technology and Engineering*, *8*(2), 4880–4886. https://doi.org/10.35940/ijrte.B3653.078219
4. Bandara, U. C., & Amarasena, T. S. M. (2018). Impact of Relative Advantage, Perceived Behavioural Control and Perceived Ease of Use on Intention to Adopt with Solar Energy Technology in Sri Lanka. *Proceedings of the Conference on the Industrial and Commercial Use of Energy, ICUE, 2018-October*. https://doi.org/10.23919/ICUE-GESD.2018.8635706
5. BBC News Indonesia. (2024). *Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber?* https://www.bbc.com/indonesia/articles/cxee2985jrvo
6. Cheng, E. W. L. (2019). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educational Technology Research and Development*, *67*(1), 21–37. https://doi.org/10.1007/s11423-018-9598-6
7. Furnell, S. M., Clarke, N., Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19. https://doi.org/10.1108/09685220910944722
8. Hasan, S., Godhuli, E. R., Rahman, M. S., & Mamun, M. A. Al. (2023). The adoption of conversational assistants in the banking industry: is the perceived risk a moderator? *Heliyon*, *9*(9), e20220. https://doi.org/10.1016/j.heliyon.2023.e20220
9. IBM Security. (2024). *X-Force Threat Intelligence Index 2024*.
10. Kompas. (2023). *Perjalanan Kasus BSI, dari Gangguan Layanan sampai "Hacker" Minta Tebusan*. https://money.kompas.com/read/2023/05/17/072027926/perjalanan-kasus-bsi-dari-gangguan-layanan-sampai-hacker-minta-tebusan?page=all
11. Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21–38. https://doi.org/10.4301/s1807-17752017000100002
12. Li, X., Dai, J., Zhu, X., Li, J., He, J., Huang, Y., Liu, X., & Shen, Q. (2023). Mechanism of attitude, subjective norms, and perceived behavioral control influence the green development behavior of construction enterprises. *Humanities and Social Sciences Communications*, *10*(1), 1–13. https://doi.org/10.1057/s41599-023-01724-9
13. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

14. Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*.
15. Majid, M., & Ariffi, K. (2019). *Success Factors for Cyber Security Operation Center (SOC) Establishment*. https://doi.org/10.4108/eai.18-7-2019.2287841
16. Michail, A. (2015). *Security Operations Centers - A Business Perspective*. 94. http://dspace.library.uu.nl/bitstream/handle/1874/315912/Security Operations Centers - A Business Perspective.pdf
17. Miloslavskaya, N. (2016). Security operations centers for information security incident management. *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, *January*, 131–138. https://doi.org/10.1109/FiCloud.2016.26
18. Peraturan Bank Indonesia Nomor 2 Tahun 2024 (2024). https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_022024.aspx
19. Shankar Bhosale, S. (2021). *Research Paper on Cyber Security*. *June*.
20. Yigitbasioglu, O. M. (2015). The role of institutional pressures and top management support in the intention to adopt cloud computing solutions. *Journal of Enterprise Information Management*, *28*(4), 579–594. https://doi.org/10.1108/JEIM-09-2014-0087