Eduvest – Journal of Universal Studies
Volume 5 Number 5, May, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

RISK ANALYSIS AND MITIGATION STRATEGIES IN OVERCOMING CYBER ATTACKS IN INFORMATION TECHNOLOGY COMPANIES USING THE OCTAVE FRAMEWORK

Ikbal Danu Setiawan[1], Septi Andryana[2]
Universitas Nasional, Indonesia
Email: ikbaldanusetiawan2017@student.unas.ac.id[1], septi.andryana@civitas.unas.ac.id[2]

ABSTRACT

In the increasingly advanced digital era, information technology companies are the main target of increasingly complex and intense cyberattacks. This study aims to analyze the risk of cyber attacks on information technology companies using the Octave framework. The Octave framework provides systematic and structured risk management guidelines that can be applied to different types of risks, including cyber risks. Based on the results of the risk analysis, priority is given to risks with high severity to obtain appropriate mitigation measures. The proposed risk mitigation strategy includes the implementation of security technologies, the development of security policies and procedures, and the increase in employee awareness and training on cybersecurity practices. In addition, this study emphasizes the importance of continuous monitoring and periodic evaluation of the effectiveness of the mitigation strategies implemented. In an effort to combat cybercrime and protect digital security, this writing uses the Octave framework method. The results of this study show that by using the Octave framework, companies can effectively identify and manage the risk of cyberattacks. The implementation of this framework not only improves information security, but also provides a systematic and structured approach to cyber threats, thereby strengthening the company's resilience to future attacks. After the establishment of the State Cyber and Cryptography Agency (BSSN) in 2017, BSSN Indonesia received many reports related to cyberattacks in both private and government companies. Thus, this research has made an important contribution in the field of cyber risk management and can be a benchmark for information technology companies in developing more reliable security systems.

KEYWORDS *Risk analysis, cyberattacks, information technology companies, octaves, cybersecurity.*

INTRODUCTION

Information technology (IT) is developing very rapidly and bringing many changes in various aspects of life (Brown & Duguid, 2017; Yamin, 2019). On the

How to cite: Setiawan, I. D., & Andryana, S. (2025). Risk Analysis and Mitigation Strategies in Overcoming Cyber Attacks in Information Technology Companies Using the OCTAVE Framework. *Journal Eduvest. 5*(5), 5666-5675
E-ISSN: 2775-3727

one hand, IT offers a variety of opportunities and benefits, such as increased efficiency, ease of access to information, and global connectivity (Atkinson & Castro, 2008; Raja et al., 2013). On the other hand, IT developments also bring various risks that need to be managed effectively. IT risk management is an important part of good IT governance. By identifying, evaluating, and controlling IT risks, organizations and individuals can protect their assets, ensure smooth operations, and take advantage of the opportunities offered by IT. Cybercrime is affected by population growth. By increasing competition in the digital world and personal data theft and cyberattacks, the number of people using the internet and digital technologies and increasing this competition (Sen et al., 2022). The study was conducted by Veronika Asri Tanderirung and Riana T. Mangesa in 2023. Criminals can commit more complex and hard-to-detect crimes thanks to technological advancements such as artificial intelligence, the Internet of Things (IoT), and blockchain. For example, a cyberattack using ransomware or botnets can result in significant losses for the victim (Laksana & Mulyani, 2024). The strengthening of cybersecurity institutions, the absence of a legal basis for cybersecurity, and the lack of professional and domestic and international cooperation are the biggest challenges today. Therefore, governments must strengthen cybersecurity and prepare the people needed in an increasingly digital world (Budi et al., 2021). The protection of personal data typically relies on the context of a country's security of its citizens, but does not take into account the capacity of citizens to protect their personal data on the Internet (Aji, 2023). Security studies in the field of international relations have become an interesting topic. According to Barry Buzan (1989), at the beginning of the Cold War, security studies were limited to political and military issues, but over time security studies began to consider social, economic, and environmental issues (Mahendra & Pinatih, 2023). Over the past few decades, advances in IT and communications have aided global economic growth while increasing competitiveness, productivity, and community participation (Soesanto et al., 2023).

Information technology (IT) companies play an important role in the modern economy, driving innovation and digital transformation in various sectors. However, in the midst of rapid technological developments, cybersecurity threats have also increased significantly. Events such as hacking, malware attacks, and ransomware can not only cause huge financial losses, but can also damage a company's reputation and disrupt business operations. According to a report issued by the State Cyber and Cryptography Agency (BSSN), the number of cyber attacks in Indonesia from the beginning of 2020 to April 12, 2020 reached 88 million cases. Of these, 56% of them were trojan attacks, 43% were intelligence attacks, and 1% were web application attacks (Samudra et al., 2023). The world of the internet, also known as "cyberspace", allows everything to be done, including encouraging human creativity, facilitating access to information, and offering various conveniences and other benefits. However, don't forget that every thing must have its positive and negative sides (Wahib et al., 2022). According to BSSN, there were 190 million attempted cyberattacks in Indonesia from January to August 2020 (Partipilo & Stroppa, 2023). This number has increased more than four times the number of cyberattacks that occurred in the same period in 2019, which was around 39 million (Budi et al., 2021). Cyber risks that can damage an organization's technological systems. Another negative factor is the increase in hacking or

hacking, including data theft, social media accounts, bank accounts, and so on (Fitroh & Sugiantoro, 2023). In addition, the Indonesian government has not provided adequate education on cybersecurity. Although some well-known universities in Indonesia, such as National Universities, have provided adequate knowledge about cybersecurity, there are not many high schools that provide adequate and uniform education on this subject in various regions in Indonesia (Mahendra & Pinatih, 2023). However, as governments, businesses, and communities become more connected in the cyber world, several challenges related to cyber threats have emerged that require the development of stronger cybersecurity (Soesanto et al., 2023). This first version of the OCTAVE method was implemented through various workshops and facilitated by an analysis team formed in an organization or IT department (Deva & Jayadi, 2022). Previous research has shown that risk analysis and information security with the Octave method is focused on risk assessment.

This research aims to analyze and evaluate the application of IT risk management using the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method in the context of cybersecurity threats that are increasingly complex in Indonesia.

The results of this research are expected to provide multiple benefits. For academic purposes, this research contributes to the body of knowledge in the field of cybersecurity and IT governance, particularly in the use of structured frameworks like OCTAVE for risk assessment. For practitioners and IT managers, the study provides practical insights on how to identify, analyze, and mitigate IT risks effectively, which can help protect vital information assets and improve organizational readiness.

RESEARCH METHOD

In this study, the OCTAVE risk assessment method is used because it is able to focus on assessing the risk of information assets according to the scope required by the company (Emmanuel & Maulany, 2023). OCTAVE is an information security risk assessment approach that is comprehensive, systematic, directed, and self-applyable. This approach consists of a set of standards that define the essential components for information security risk evaluation (Widiyasti et al., 2023). The method of controlling and analyzing information technology security risks used is Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Deva & Jayadi, 2022). Previous research has shown that the risk analysis and information security with the OCTAVE method concentrates on assessing the risk of information assets according to the needs of the company (Emmanuel & Maulany, 2023). This approach is structured from a set of standards that define critical components for information security risk assessment (Supradono, 2009).

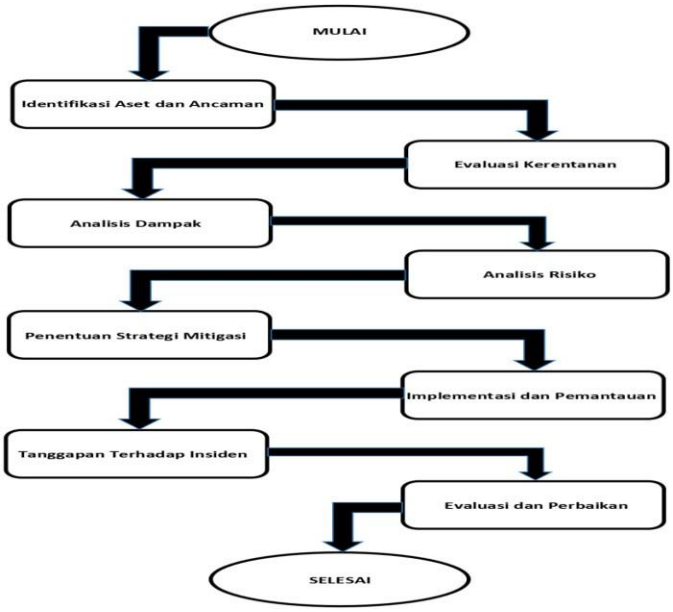

Figure 1. Diagram depicting the stages of Risk Analysis research in dealing with cyber attacks

Description of Image Reference Stages

1. Asset and Threat Identification: Identify all information assets and IT infrastructure that are critical to the company, as well as identify cyber threats that could threaten those assets.
2. Vulnerability Assessment: Evaluate the vulnerability of each asset to the identified threats. This includes consideration of software weaknesses, poor system configurations, and weak security policies.
3. Impact analysis: Analyzing the potential impact of any threat on a company's assets and operations. These impacts can include financial losses, reputation, loss of data, and operational disruptions.
4. Risk assessment: Measuring the risk for each combination of threats and vulnerabilities by considering the likelihood of an attack and its impact.
5. Definition of mitigation strategy: Choosing the right security controls to reduce or eliminate risk, and planning their implementation.
6. Implementation and Monitoring: Implement selected security controls and monitor systems and environments to detect attacks or failures in security controls.
7. Incident response: Create a clear and structured response plan to an incident to deal with a cyber attack if it occurs.
8. Evaluation and Improvement: Periodically evaluate the performance of cybersecurity programs and risk analysis to identify areas that need improvement, as well as to make continuous improvements to the risk analysis process and cybersecurity strategy.

RESULT AND DISCUSSION

Cybersecurity is a set of policies, principles, protections, security, recommendations, opportunity control strategies, actions, training, premium applications, assurances, and data used to protect our world, online companies, and

user assets (Indah et al., 2022). Cyberattacks are a phenomenon with a level of development that follows technological developments and advancements. Cyberattacks are typically categorized into two categories: (1) attacks on system software or hardware, (2) data manipulation, and (3) deprivation of system accessibility from other users so that they cannot access the system (Wahib et al., 2022).

Risiko	Dampak	Probabilitas	Tingkat Risiko
Phishing			
Malware			
Serangan DDoS			
Insider Threats			
Ransomware			

Tinggi
Sedang
Rendah

Figure 2. Risk is evaluated by combining impact and probability using a risk matrix

Cybersecurity protects cyber structures from cyber threats. Dual security protects structures and records from illegal access through confidentiality, integrity, authentication, anti-repudiation, and record availability, which protects you from cyberattacks. Protection combines security, detection, and response capabilities for the healing facts of the system (Indah et al., 2022). International cybersecurity cooperation aims to ensure a high level of national protection against cyber threats through the exchange of international information and experience, the promotion of mutual trust, the protection of human rights and fundamental freedoms in cyberspace, and the strengthening of relations between countries (Saleh et al., 2022). However, to provide a rough estimate, here are some estimates that may apply in general:

Year	Type of Attack	Attack Frequency	Impact	Trend	Amount
2020	Phishing	High	Displayed User Data	Increase	4
	Ransomware	Medium	Operational Disorder	Stable	3
	Malware	High	Financial Loss	Increase	1
2021	Phishing	High	Account Security Error	Decreasing	4
	DDoS	Medium	Downtime Website	Stable	1
	Insider Threats	Low	Employee Data Leakage	Increase	1
2022	Phishing	Medium	Customer data theft	Increase	4
	Ransomware	High	High Ransom Request	Increase	3
	Supply Chain Attack	Rendah	Supply Chain Disruption	Increase	1
2023	Phishing	High	Unauthorized Account Access	Stable	4
	Ransomware	High	System Downtime	Increase	3
	Zero-Day Exploits	Medium	Software Vulnerability	Increase	1

Figure 3. Explanation of the types of attacks.

Small and medium-sized enterprises (SMEs): SMEs are often targeted by cyberattacks because they may have limited resources to implement sophisticated security measures. The percentage of SMEs that are frequently exposed to cyberattacks may be higher, can reach more than 50% depending on their level of security.

Large companies: Large companies may have more resources to deal with cyberattacks, including larger security budgets and trained security teams. Nonetheless, because they have complex infrastructure and valuable data, they remain an attractive target for attackers. The percentage of large companies that are frequently exposed to cyberattacks can range from 20% to 50%□ Specific Industry Sectors: Some industry sectors, such as banking, finance, technology, and healthcare, are often prime targets for cyberattacks because they store sensitive and important data. The percentage of companies in these sectors that are frequently exposed to cyberattacks may be higher than other sectors.

Security Awareness and Education Level: Companies that have a strong security culture and employees trained in detecting and mitigating cyberattacks may have a higher success rate in combating such attacks. Therefore, the percentage of companies affected by cyberattacks can be reduced among these companies. It should be noted that these are only rough estimates and the actual number may vary depending on the specific conditions in each situation. It is important to conduct a comprehensive security evaluation and choose the right course of action to prevent cyber threats to the company. Information technology drives global economic growth in two ways. First, increasing demand for information technology products. Second, advances in information technology have made business transactions easier, especially in the financial and business sectors in general (Budarsa et al., 2022).

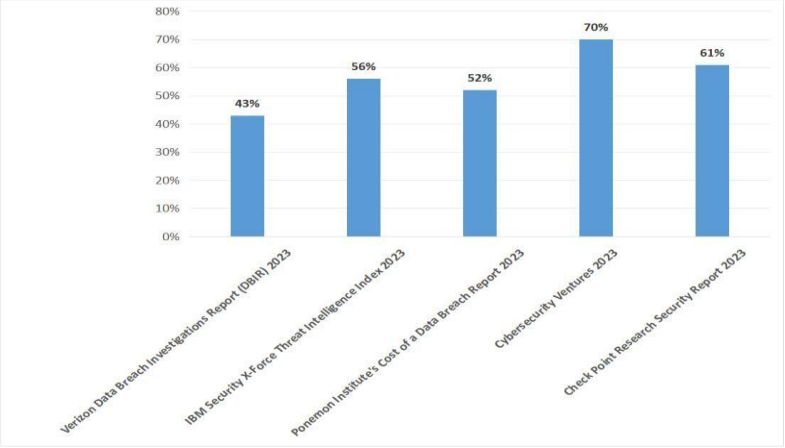

Figure 4. Percentage of Company Data Frequently Affected by Cyberattacks (2023)

Data Analysis of the Percentage of Companies Frequently Affected by Cyber Attacks (2023):

1. Verizon Data Breach Investigation Report (DBIR) 2023 This report reveals that 43% of the companies surveyed have experienced a cybersecurity incident.
2. IBM Security X-Force Threat Intelligence Index 2023 More than 56% of companies surveyed by IBM have experienced a cyberattack. Ransomware

threats are particularly prominent in this report, which suggests that companies need to improve their security measures.

3. Ponemon Institutes Data Breach Cost Report 2023 Ponemon Institutes states that 52% of companies experience data breaches. The report also highlights the average cost of data breaches, which continues to increase every year.
4. Cybersecurity Ventures 2023 Cybersecurity Ventures estimates that 70% of companies experience some form of cyberattack. They also highlighted an increase in attacks targeting small and medium-sized companies, which are often less prepared than large companies.

Nama Perusahaan	Jenis Serangan	Dampak Serangan	Langkah Respons
Microsoft	Phishing	Data pelanggan bocor, akses ke akun Office 365	Peningkatan otentikasi multi-faktor, pelatihan keamanan karyawan
twitter	Social Engineering	Akun beberapa selebritas dan perusahaan besar diretas	Peningkatan keamanan akun, audit internal
UBER	Credential Stuffing	Data pelanggan bocor, informasi pembayaran terekspos	Implementasi kebijakan password yang lebih kuat, MFA
T-Mobile	Data Breach	Data pribadi jutaan pelanggan bocor	Peningkatan sistem deteksi intrusi, peningkatan enkripsi data
Meta	Malware	Kerusakan sistem internal, pencurian data pengguna	Peningkatan perangkat lunak keamanan, pelatihan karyawan
American Airlines	Ransomware	Data pelanggan dan informasi penerbangan disandera	Penguatan prosedur backup, implementasi solusi anti-ransomware
CISCO	Phishing & Malware	Data karyawan dicuri, gangguan operasional	Pelatihan kesadaran keamanan, peningkatan perlindungan endpoint
SAMSUNG	Data Breach	Data karyawan dan pelanggan bocor	Audit keamanan, peningkatan kebijakan akses data
NVIDIA	Ransomware	Pencurian data rahasia perusahaan, gangguan produksi	Implementasi solusi keamanan tambahan, penguatan backup
LastPass	Data Breach	Data vault password pengguna bocor	Peningkatan enkripsi data, audit keamanan komprehensif

Figure 5. Major Companies Affected by Cyberattacks in 2023

5. Check Point Security Research Report 2023 Check Point Research reports that 61% of companies have experienced cybersecurity incidents, with malware and phishing as the main threats. They emphasized the importance of awareness and staff training to reduce the risk of attacks.

Types of Attacks Explained

a. Phishing: An attempt to trick customers through email to steal sensitive information such as logins and passwords.
b. Social Engineering: Psychological manipulation to gain unauthorized access or confidential information.
c. Credential Stuffing: Automated attacks that use leaked credentials from other data breaches.
d. Data Breach: Theft of personal or confidential data that occurs as a result of unauthorized access to company systems.
e. Malware: Malicious software used to damage systems, steal data, or disrupt operations.

f. Ransomware: An attack that encrypts the victim's data and demands a ransom to return it.

Impact of the Attack

a. Data Leaks: Leaks of personal data of customers or employees that can be used for malicious activities.
b. Operational Disruption: Disruption of service or business operations that results in downtime and financial losses.
c. Loss of Trust: A decrease in trust from customers and business partners that can have a long-term impact on a company's reputation.

Response Steps

a. Multi-Factor Authentication (MFA): The use of more than one verification method to access the system.
b. Employee Security Training: Regular training to increase employee awareness and knowledge against cyber threats.
c. Intrusion Detection Systems: Technology solutions that detect and respond to suspicious activity on the network.
d. Data Encryption: The process of securing data so that only authorized parties can access it.
e. Data Backup: Periodically keep copies of important data for recovery in the event of an attack.

CONCLUSION

The conclusion of this study confirms that in the increasingly advanced digital era, information technology companies face serious challenges from increasingly complex cyber threats. Attacks such as hacking, malware, and ransomware not only threaten financial losses, but can also damage reputations and disrupt business operations. Therefore, it is important for companies to implement effective risk management, including through risk analysis methodologies such as OCTAVE, which allow for systematic identification and mitigation of risks. By understanding the potential impact of any threat on information assets, companies can design appropriate mitigation strategies, such as the implementation of security technologies and employee training. Awareness of cybersecurity among employees is also a key factor in reducing risk, given that cyberattacks often take advantage of human weaknesses.

Finally, this study emphasizes the need for collaboration between the government, the private sector, and education to strengthen cybersecurity in Indonesia. While some institutions have embarked on efforts to provide education on cybersecurity, much remains to be done to ensure that all levels of society are prepared for cyber threats. With increased education and awareness, it is hoped that companies can better protect their data and infrastructure, as well as contribute to overall national cybersecurity.

REFERENCES

Aji, M. P. (2023). *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)*.

Atkinson, R. D., & Castro, D. (2008). Digital quality of life: Understanding the personal and social benefits of the information technology revolution. *Available at SSRN 1278185*.

Brown, J. S., & Duguid, P. (2017). *The social life of information: Updated, with a new preface*. Harvard Business Review Press.

Budarsa, N., Indrawan, G., & Gunadi, A. (2022). Analisis Risiko Keamanan Informasi Menggunakan Metode OCTAVE ALLEGRO dan Analytical Hierarchy Process pada Data Center Pemerintah Kabupaten Buleleng. *Jurnal Ilmu Komputer Indonesia (JIK)*, *7*(1).

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi dan Informasi (JATI)*, *12*(2), 106. https://doi.org/10.34010/jati.v12i2

Emmanuel, P. N., & Maulany, R. (2023). Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House. *KREA-TIF: Jurnal Teknik Informatika*, *11*(1), 37–52. https://doi.org/10.32832/krea-tif.v11i1.14179

Fitroh, Q. A., & Sugiantoro, B. (2023). Peran Ethical Hacking dalam Memerangi Cyberthreats. *Jurnal Ilmiah Informatika (JIF)*. http://ejournal.upbatam.ac.id/index.php/jif

Indah, F., Sidabutar, A., & Annisa, N. (2022). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 1–8. https://ejournal.kreatifcemerlang.id/index.php/jbpi

Laksana, T. G., & Mulyani, S. (2024). Faktor-Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan. *Jurnal dengan p-ISSN 1907-8765 dan e-ISSN 2548-6128*. https://doi.org/10.25105/prio.v11i2.18960

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) di Indonesia. *Jurnal Review Pendidikan dan Pengajaran*, *6*(4). http://journal.universitaspahlawan.ac.id/index.php/jrpp

Partipilo, F. R., & Stroppa, M. (2023). Humanitarian organisations under cyber-attack: emerging threats and humanitarian actors' responsibilities under international human rights law. In *Responsible Behaviour in Cyberspace: Global Narratives and Practice* (hal. 238–257). Publications Office of the European Union.

Raja, S., Imaizumi, S., Kelly, T., Narimatsu, J., & Paradi-Guilford, C. (2013). *Connecting to work: How information and communication technologies could help expand employment opportunities*.

Saleh, A. K., Yuliana, A. D. S., & Pramudian, G. W. (2022). *Digital Security in Estonia*.

Samudra, Y., Hidayat, A., & Wahyu, M. F. (2023). Pengenalan Cyber Security

Sebagai Fundamental Keamanan Data Pada Era Digital. *AMMA: Jurnal Pengabdian Masyarakat*, *1*(12), 1594–1601.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen*, *1*(2), 172–191. https://doi.org/10.47861/sammajiva.v1i2.226

Supradono, B. (2009). Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika*, *2*(1), 4–8. http://jurnal.unimus.ac.id

Wahib, P., Narotama, A. T., Rijki, N. M., Sahrudin, Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, *1*(2).

Widiyasti, D., Rusi, I., & Febriyanto, F. (2023). Manajemen Risiko Keamanan Teknologi Informasi Menggunakan Metode OCTAVE Allegro dan Kontrol ISO/IEC 27001:2013 (Studi Kasus: PLN UP2D Kalimantan Barat). *Coding: Jurnal Komputer dan Aplikasi*, *11*(2), 227–237.

Yamin, M. (2019). Information technologies of 21st century and their impact on the society. *International Journal of Information Technology*, *11*(4), 759–766.