Interdisciplinary Journal of Advanced Research and Innovation
Volume 2 No. 2 2024 E-ISSN xxxx-xxxx
https://ijari.publicascientificsolution.com/index.php/rv

CASE STUDY OF CYBERCRIME IMPLEMENTATION IN TECHNOLOGY DEVELOPMENT

Deitje Pongoh[1], Fanny Jouke Doringin[2], Roby Stevi Lumbu[3], Yehuda Yura[4], Hizkia Rampi[5], Dennis Timpua[6], Albed Maulana[7], Junior Assa[8], Chievo Simoboh[9]
Politeknik Negeri Manado
pongohdeitjie@gmail.com[1], fannydoringin@gmail.com[2], robylumbu@gmail.com[3], yehudayura03@gmail.com[4], hizkiarampi16@gmail.com[5], denistimpua@gmail.com[6], albaytmaulana007@gmail.com[7], heavenjunior2005@gmail.com[8], chieosimboh@gmail.com[9]

Abstract:
The relentless march of modern technology has undeniably ushered convenience, comfort, and efficiency into various facets of our lives. However, accompanying these technological strides are the looming threats of cybercrime. This article extensively reviews a case study illustrating the implementation of cybercrime within the context of technological progress, meticulously examining its far-reaching impact. Rigorous research is conducted to unravel the intricacies of this case, offering detailed insights into the ongoing efforts to counteract its effects. In today's digital age, cybercrime stands as a formidable and rapidly expanding menace, casting a shadow over critical infrastructure, sensitive data, and organizational stability. Our investigation delves into the profound influence of technological developments on the emergence of diverse cyberattacks and hacking incidents. Be the pivotal roles of proactive monitoring and comprehensive security awareness training. This study advocates for a heightened state of vigilance and underscores the necessity of adopting preemptive measures to navigate the evolving landscape of cyber threats successfully. The quest for effective cybersecurity is portrayed as an ongoing and dynamic endeavor, demanding adaptability and a holistic approach to fortify against the relentless evolution of digital risks.

Keywords: cybercrime, technology, technology development

Corresponding: Albed Maulana
E-mail: albaytmaulana007@gmail.com

INTRODUCTION

The development of information technology has significantly changed the way we interact with the world of business and government (Chege & Wang, 2020). While technological innovations provide great benefits, such as increased efficiency and accessibility of information, these developments also open the door to new threats, the most notable of which is the cybersecurity threat, often referred to as "cybercrime." Cybercrime is a rapidly growing threat in today's digital age important (Lagazio et al., 2014; Rao et al., 2020). Cyber attacks can damage critical infrastructure, steal sensitive data, and disrupt the daily activities of organizations and individuals. In the context of technological development, where information systems are increasingly connected and data becomes more valuable, cyber protection is very important (Kimani et al., 2019; Djenna et al., 2021).

This study aims to investigate and analyze the implementation of cyber security strategies that evolve with technology. In this context, this research aims to investigate Crime in Technology Security, for example, "the most dominating cybercrime trends" or "factors affecting the success of ransomware attacks." Through in-depth analysis and a multidisciplinary approach, we hope to provide better insight

into the cybercrime problems faced today and provide a basis for the development of more effective mitigation strategies.

In the next section of this journal, we will present a literature review detailing previous research relevant to this topic, as well as the methodology used in our research. Finally, we will outline the results of our research and provide relevant conclusions and recommendations. In doing so, we hope this research can contribute to a better understanding of this increasingly troubling phenomenon of cybercrime and provide practical guidance for stakeholders seeking to protect themselves from this threat.

The stakes are higher than ever in this intricate dance between technological advancement and security challenges. The relentless pace at which innovation unfolds is mirrored by the agility of cyber adversaries who exploit vulnerabilities with increasing sophistication (Chindrus & Caruntu, 2023). As organizations and governments race to harness the benefits of a hyper-connected world, the shadow of cyber threats looms larger, demanding a nuanced understanding and proactive defense mechanisms.

The digital era's narrative is not just one of progress; it is equally a narrative of adaptation and resilience (Leurs, 2022). As our systems become more complex, so too must our strategies for safeguarding them. The nefarious actors orchestrating cybercrimes are not confined by borders or traditional notions of conflict. They navigate a digital realm that knows no geographic bounds, presenting a unique challenge that necessitates a global, collaborative response.

Our exploration goes beyond the surface, delving into the intricacies of cyber threats that transcend conventional boundaries (Khan, 2023). Ransomware, in particular, stands as a sentinel of this evolving landscape, with its capacity to cripple entire systems and hold critical data hostage (Ferrag et al., 2023). Understanding the anatomy of such attacks requires more than just technical acumen; it demands a holistic comprehension of the socio-technical ecosystem in which they unfold.

As we embark on this journey, our commitment extends beyond analysis for its own sake. We strive not only to diagnose the symptoms but to prescribe effective remedies. By unveiling the threads that weave the fabric of contemporary cyber threats, we aim to empower decision-makers with insights that transcend the reactive, fostering a proactive posture against the ever-evolving specter of cybercrime. The forthcoming sections will illuminate the path forward, offering a comprehensive exploration that serves as both a testament to our understanding of the challenge at hand and a blueprint for a more resilient digital future.

METHOD

In this research, the author employed a multifaceted approach to understand and analyze the impact of cybercrime in the realm of technology. The primary method involved direct observation of real cases, allowing for an in-depth examination of the manifestations and consequences of cybercrime. The author scrutinized instances reported in various online platforms, news articles, and legal records, extracting valuable insights into the evolving nature of cyber threats. Additionally, the research incorporated an extensive literature review, wherein the author conducted a comprehensive analysis derived from diverse sources. This included a thorough examination of academic publications, research papers, and reports sourced from reputable social media platforms. The utilization of these informational channels provided a holistic view of cybercrime's growth, encompassing both practical, real-world cases and theoretical perspectives presented in scholarly literature. The combination of direct observation and a comprehensive literature review aimed to provide a nuanced understanding of the multifaceted landscape of cybercrime within the context of technological advancements. This approach allowed the research to draw connections between real-world occurrences and the broader academic

discourse, contributing to a more holistic and informed assessment of the impact and growth of cybercrime.

RESULT AND DISCUSSION

The Importance of Cybersecurity Education: Our data shows that most cyberattacks can be avoided through simple measures such as updating software and using strong passwords. Cybersecurity education is, therefore, key in protecting against these attacks. We recommended a broader education campaign to raise awareness of the threat of cybercrime.

Role Of Government and Private Sector: In the face of cyberattacks, collaboration between the government and the private sector is crucial. The government needs to push for regulations that require stricter security practices, while companies and institutions should increase their efforts in protecting data and infrastructure (Atkins & Lawson, 2022).

Security Technology Development: We recognize that cyberattacks are constantly evolving, and cyber actors are always looking for new loopholes. Therefore, the development of more advanced and adaptive security technologies also needs to be a focus in the fight against cybercrime. The importance of Traceability and Enforcement: We emphasize the importance of tracking and enforcing the laws against cyber criminals. There is a need for stronger international cooperation in identifying and prosecuting cyber offenders.

Promoting Responsible Online Behavior: Alongside formal education, fostering a culture of responsible online behavior is essential. This includes promoting habits such as being cautious about clicking on suspicious links, verifying the authenticity of emails, and avoiding sharing sensitive information indiscriminately.

Incident Response Planning: Developing and regularly updating incident response plans is crucial for organizations. This involves outlining clear procedures to follow in the event of a cyber incident, ensuring a swift and coordinated response to minimize potential damage.

Public-Private Information Sharing: Encouraging the sharing of threat intelligence and information between the public and private sectors can enhance the overall cybersecurity posture. This collaboration allows for a more comprehensive understanding of emerging threats and effective strategies to counteract them.

Investment in Cybersecurity Workforce: Recognizing the shortage of skilled cybersecurity professionals, there should be a concerted effort to invest in training programs and initiatives to build a robust cybersecurity workforce. This includes promoting STEM education and providing resources for continuous professional development.

User-Friendly Security Measures: Designing and implementing user-friendly security measures can encourage individuals to adopt and maintain good cybersecurity practices. Intuitive interfaces, clear instructions, and user education contribute to making security measures more accessible and effective.

International Cybersecurity Standards: Working towards establishing and adhering to international cybersecurity standards can provide a unified framework for addressing cyber threats globally. This helps create a consistent and interoperable approach to cybersecurity practices across borders.

The hacker we took was Bjorka: Bjorka made waves in 2022. The name comes from an account on the dark web, and a lot of data is leaked from there. It was noted that Bjorka once claimed to have 26 million Indihome customers' browsing histories, 1.3 billion SIM Card registration data, and 105 million KPU data. Through his Telegram group, Bjorka spread the personal data of a number of public officials, such as the Minister of Communication and Information, Johnny Plate. The information

contains NIK, Family Card number, address, telephone number, names of family members, and Vaccine ID (Bestari, 2022).

Cyber Crime Trends: We identified that phishing attacks are the most common type of attacks against individuals, while ransomware attacks tend to target businesses and government agencies (Alabdan, 2020). We also found that most cyberattacks occur on weekends and during non-working hours.

Perpetrators' Motivations: Our analysis shows that the primary motive behind cybercrime is financial, with perpetrators seeking material gain from the target (De Kimpe, 2020; Smith, 2021). However, there are also ideologically or politically motivated perpetrators who aim to damage reputations by influencing politics.

Case example about Bjorka :

1) Bjorka claims to have pocketed 26 million IndiHome customers' browsing history. The data includes keywords, email, name, gender, and National Identification Number (NIK).
2) Bjorka is again the actor behind the leak of 1.3 billion SIM card registration data said to belong to the Ministry of Communication and Information Technology (Kominfo). The data was sold for US$ 500 thousand or around Rp 745.6 million. The 87 GB of data is claimed to contain NIK, cellphone number, telecommunications provider, and registration date.
3) Bjorka is acting up again. This time, the data he leaked was 105 million Indonesian people's data related to the general election from the General Election Commission (KPU). This information on the breach was uploaded to the forum by Bjorka on September 6, 2022. The upload was entitled Indonesia Citizenship Database From KPU 105M. The data that was successfully obtained were NIK, Family Card, full name, place and date of birth, gender, and age. In the spoiler data, it appears that the data comes from the South Sulawesi and Southeast Sulawesi regions.
4) After spreading sensitive data several times on the Breached Forum, Bjorka then spread personal data allegedly belonging to a number of Indonesian public officials through his Telegram group. Bjorka carried out this action over the weekend, from September 10 to 11, 2022, starting with data belonging to the Minister of Communication and Information Technology (Menkominfo) Johnny G Plate (Dewi, 2022).
5) A total of 44 million MyPertamina application users were leaked by Bjorka, and sold for Rp392 million in BitCoin. This was revealed in his latest upload entitled “MYPERTAMINA INDONESIA 44 MILLION” on the BreachForums website, dated Thursday (10/11) at 02.31 AM (Bestari, 2022).

CONCLUSION

In conclusion, this journal has provided a comprehensive overview of the impact of cybercrime in the present technological era. The findings underscore the intricate and ever-evolving nature of cybersecurity challenges. The current landscape necessitates active and multi-layered protective measures to mitigate the risks associated with cybercrime. The dangers posed by cyber threats are multifaceted, encompassing a range of malicious activities that exploit vulnerabilities in technological systems. To safeguard against these threats, the implementation of robust security measures is imperative. This includes the deployment of advanced security software capable of detecting and thwarting various cyber threats. Regular updates to both software and security protocols are crucial to stay ahead of emerging risks and vulnerabilities. Moreover, the enforcement of strict security policies is essential in establishing a resilient defense against cybercrime. These policies should encompass comprehensive guidelines for data protection, access controls, and incident response protocols. By

promoting a culture of cybersecurity awareness and adherence to these policies, organizations and individuals alike can contribute to a more secure technological environment. In navigating the complex landscape of cyber threats, the call for collaborative efforts between individuals, organizations, and governments becomes increasingly urgent. Continuous research, education, and the implementation of innovative security technologies are essential components of this collective defense against cybercrime. As we move forward in the technological era, a proactive and vigilant approach to cybersecurity will be paramount in ensuring a safe and secure digital future.

REFERENCES

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 168.

Atkins, S., & Lawson, Chappell. (2022). Integration of Effort: Securing Critical Infrastructure from Cyberattack. Public Administration Review, 82(4), 771–775.

Bestari, N. P. (2022). No Title. Retrieved from CNBC Indonesia website: https://www.cnbcindonesia.com/tech/20221226135118-37-400166/hacker-bjorka-tantang-pemerintah-ri-saya-menunggu-digerebek/1

Chege, Samwel Macharia, & Wang, Daoping. (2020). Information technology innovation and its impact on job creation by SMEs in developing countries: an analysis of the literature review. Technology Analysis & Strategic Management, 32(3), 256–271.

Chindrus, Cristian, & Caruntu, Constantin Florin. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587.

De Kimpe, Lies. (2020). The human face of cybercrime: Identifying targets, victims, and their coping mechanisms. University of Antwerp.

Dewi, I. R. (2022). Hacker Bjorka is Back, Data Apa Saja yang Pernah Dibocorkan? Retrieved from CNBC Indonesia website: https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan

Djenna, Amir, Harous, Saad, & Saidouni, Djamel Eddine. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

Ferrag, M. A., Kantzavelou, I., Maglaras, L., & Janicke, Helge. (2023). Hybrid Threats, Cyberterrorism and Cyberwarfare. CRC Press.

Khan, Muhammad J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105–116.

Kimani, Kenneth, Oduol, Vitalice, & Langat, Kibet. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36–49.

Lagazio, M., Sherif, N., & Cushman, Mike. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, 58–74.

Leurs, Koen. (2022). Resilience and Digital Inclusion: The Digital Re-making of Vulnerability? In Vulnerable People and Digital Inclusion: Theoretical and Applied Perspectives (pp. 27–46). Springer.

Rao, Yerra Shankar, Pradhan, Debasish, Panda, Tarini Charana, & Rath, Ranjita. (2020). Digital crime and its impact in present society. International Journal of Engineering Research & Technology, 8(1), 1–6.

Smith, T. (2021). A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime.