Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (955-964)

Challenges and Threats of Cybercrime in Indonesia: A Review of Legal and Information Technology Aspects Related to Ransomware Attacks on Indonesia's National Data Center

Muhamad Adystia Sunggara[1], & Syafri Hariansah[2]

Abstract

This article discusses the challenges and threats to cybercrime in Indonesia, focusing on two main aspects—law and information technology. Through an in-depth analysis of the applicable laws and regulations and the development of information technology, this study aims to identify the weaknesses and challenges faced in combating cybercrime in Indonesia. Additionally, this article presents several recommendations for improving the effectiveness of cybercrime threats. This research methodology is based on studies and analyses related to the potential threats and challenges of cybercrime from the aspects of legal and information technology, as described in several modern publications. This study used a qualitative approach and secondary data analysis. Recommendations that can be drawn from this study include the need to improve infrastructure and human resources in the security field and increase investment in training and human resources for law enforcement agencies. This can consist of more intensive training programs in information technology crime, data risk recovery management, coordination and cooperation between the public and private sectors, and adaptation and development of real-time threat-monitoring technology using artificial intelligence.

Keywords: Criminal Law; National Security; Cyber Crime; Computer Forensics; Cybersecurity; Ransomware

Introduction

As information and communication technology certainly has a positive impact on various aspects of life, but it also has the potential to result in cybercrime (Widiasari & Thalib, 2022). Cybercrime has become a growing concern in Indonesia, with a significant increase in various digital crimes (Irfan et al., 2018). Notably, the rapid development of technology has brought new challenges to maintaining cybersecurity and protecting individuals and organizations from malicious cyber activities (Ishak, 2023).

In recent years, the number of Internet users in Indonesia has reached more than 221 million, with a significant penetration rate among the younger generation and the business sector. However, broader access to the Internet and digital technology also raises new data security and privacy challenges. Cybercriminals can exploit security gaps in digital infrastructure to steal personal information, redirect users to fake websites to steal money, or even manipulate systems to extort money from companies or individuals and conduct ransomware attacks (Javaid et al., 2023).

Handling cybercrime is not easy because, in addition to its characteristics, existing legal regulations in Indonesia have not been able to cover the development of crimes committed in cyberspace (Nugroho & Chandrawulan, 2023). The

[1] Faculty of Law, Pertiba University. Email: dr.m.adystiasunggara@gmail.com
[2] Faculty of Law, Pertiba University. Email: hariansah@studentui@gmail.com

existing personal data protection regulations in Indonesia are based only on Law Number 19 of 2016, concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

The Electronic Information and Transactions Law (UU ITE) protects personal rights, e-commerce principles, jurisdictional issues, unfair business competition, consumer protection, intellectual property rights, cybercrime, and international law. Law enforcement activities essentially include the use of a criminal justice system to combat crime. Law enforcement policies include criminal law policy (Senjaya, 2021), as well as the use of legal remedies, including criminal law, as strategies to address social issues (Hamzani et al., 2020).

Effective law enforcement is essential for combating cybercrime; however, Indonesia faces significant challenges in this sector (Bawono, 2019). The shortage of specialized training and expertise among law enforcement officers, as well as the lack of resources and technological capabilities, has hampered practical law enforcement efforts and the ability to investigate and prosecute cyber-related cases.

Cybercrime can be committed anywhere and anytime with an Internet connection and adequate equipment. Ransomware attacks are a pressing problem in Indonesia. Data from the National Cyber and Crypto Agency (BSSN) show a 30% increase in ransomware attacks in 2022 compared to the previous year. Most recently, on June 20, 2024, the public and government were shocked by a ransomware attack on Indonesia's National Data Center (PDN). The attack held the victim's data hostage by encrypting it. The victim or target party could not access the data until they paid a ransom to the perpetrator, who provided the key to opening the victim's files or documents. The ransom demanded in the attack on the PDN was USD 8 million, or approximately IDR 131 billion (Connatse, 2024). The ransomware attack on PDN was a technical issue and a serious threat to social, economic, and national security. This incident reveals that protecting the national data infrastructure is crucial for maintaining information security and preventing significant losses.

Ransomware is a type of malware that encrypts data on a computer system and requires a ransom to return the data (Aurangzeb et al., 2017). According to a Cybersecurity Ventures report, global losses owing to ransomware attacks are estimated to reach 20 billion USD by 2021, and this figure is predicted to continue to increase with technological developments (Morgan, 2021). Ransomware has evolved from a low-tech tool first observed in the field to a highly sophisticated tool currently used by cybercriminals. Owing to its evolution, ransomware now poses a serious threat to every sector of society, including governments, businesses, and citizens (Nagar, 2024).

A comparison of legal responses to cybercrime in various countries reveals a variety of approaches that can be used as references for Indonesia. In the United States, for example, there are laws such as the Computer Fraud and Abuse Act and the Cybersecurity Information Sharing Act, which support collaboration between the public and private sectors in sharing information about cyber threats. The

European Union regulates this issue through the General Data Protection Regulation and Cybersecurity Act and encourages cooperation between member states through the European Cybercrime Centre (EC3). Singapore has developed a Cybersecurity Act and established a Cyber Security Agency that focuses on preventing and responding to cyber incidents while providing training to raise public awareness. From this comparison, it is evident that clear legislation, coordinated law enforcement, cross-sector cooperation, and ongoing education programs are key elements in dealing with cybercrime effectively and can be adopted to improve the legal response in Indonesia.

This study aims to identify the challenges and threats of cybercrime in Indonesia from two main aspects: law and information technology (IT). By reviewing the applicable laws and regulations and the development of IT, this study aims to identify the challenges and threats of cybercrime in Indonesia, analyze the legal aspects and role of IT in combating cybercrime, and provide recommendations to improve the effectiveness of tackling cybercrime. In addition, a comprehensive and sustainable approach is required, such as security policies, education and training, monitoring and early detection, regular data backup, incident mitigation plans, and evaluations.

Materials and Methods

This research methodology is based on studying and analyzing the potential threats and challenges of cybercrime from the legal and IT aspects described in several modern publications. This study used a qualitative approach along with secondary data analysis. Primary data were obtained from case studies of IT crimes in Indonesia in recent years, one of which concerned ransomware attacks and personal data protection. Data were collected through literature review, interviews with cybersecurity experts, and analysis of ransomware attack cases in Indonesia. Indonesia was chosen for this case study because it is one of the countries with rapid growth in Internet users and IT. This creates opportunities but also increases the risk of cybercrime.

During the interview process, we asked the following questions: *What is your view on the latest trends in cybercrime in Indonesia? What steps are usually taken by organizations to protect themselves from ransomware attacks? What are the main challenges faced in protecting personal data in this digital era? How do you assess the effectiveness of current regulations in protecting personal data in Indonesia?*

The data sources used included reports from the BSSN, academic research, news articles, and legal documents related to cybercrime. In addition, the author analyzed existing policies and regulations to assess their effectiveness in dealing with ransomware attacks. Additionally, this study involved a statistical analysis to describe the trend of ransomware attacks in Indonesia. Data obtained from the BSSN and other related institutions are used to describe attack patterns, the most vulnerable sectors, and the economic impacts of the attacks. Using this method, it

is hoped that a deeper understanding of the challenges and threats of cybercrime can be obtained, as well as solutions that can be applied to improve cybersecurity in Indonesia.

Furthermore, interviews with cybersecurity practitioners and law enforcers were conducted to gain a broader perspective on the challenges faced in law enforcement related to cybercrime. This approach is expected to provide a comprehensive picture of the current situation and the steps that need to be taken to address cybersecurity issues in Indonesia, as well as to identify challenges and potential solutions from legal and practical perspectives.

Results and Discussion

Secondary data analysis reveals that IT crimes in Indonesia have increased significantly over the past few years. Based on data from the Indonesian National Police, there was a 25% increase in IT crime cases in 2023 compared to the previous year. The most common type of crime was identity theft, which recorded a 30% spike, followed by online fraud, with a 20% increase.

In the context of cybercrime, especially ransomware attacks on Indonesia's PDN, several key challenges must be identified and addressed.

1. Weakness in IT Infrastructure

Outdated System: Some data centers still use obsolete hardware and software systems, which can be loopholes for ransomware attacks. Notably, regular system updates and maintenance are often neglected.

Weaknesses in Security Settings: The absence or weakness of security settings such as effective firewalls, intrusion detection systems, or data encryption can leave data centers vulnerable to attacks. According to Borky & Bradley (2019), firewalls perform packet inspection, IDS/IPS, DLP, and perhaps additional perimeter security tasks, in addition to guarding Supervisory Control systems. Depending on the functionality provided through the Web Ports, Web Application Firewalls may be necessary.

2. Lack of Resources and Expertise

Cybersecurity Expertise Deficit: The limited number of qualified cybersecurity experts makes it difficult to manage and maintain secure IT systems. The lack of adequate resources and training for law enforcement agencies is a serious obstacle in dealing with IT crimes (Harkin & Whelan 2021). Increasing investments in human resource training and providing the latest technology to support investigation and law enforcement are crucial.

Budget Constraints: Many organizations, including government agencies, have limited budgets to invest in the latest security technologies and personnel training, which hampers security-strengthening efforts.

3. Difficulties in Law Enforcement

Complex Law Enforcement: Cybercrime often involves perpetrators from multiple countries, making law enforcement complex and requiring effective international coordination. Collecting digital evidence and tracking perpetrators frequently require significant time and resources.

Inadequate Regulation: Existing laws and regulations may not fully cover all aspects of emerging cybercrimes. The need for regulatory updates to keep pace with technological developments and new attack methods remains a challenge. The ambiguities of several articles need to be addressed. Recommendations for further updates to the UU ITE must be considered by seeking input from legal experts and relevant stakeholders to ensure the clarity and accuracy of the regulations. According to Lewallen (2021), the range and types of assets that are more susceptible to cyberattacks have expanded owing to new technology. Consequently, more government agencies now have the authority to handle cybersecurity-related matters. Although the goal of cybersecurity legislation is to reduce cyber risks and improve protection, the uncertainty that arises from frequent changes or the introduction of new regulations can substantially influence an organization's response plan (Kianpour & Raza, 2024).

4. Dependence on Technology and Data

Sensitive Data Storage: The PDN stores highly sensitive and critical information, which makes it a prime target for ransomware actors. Vulnerabilities in the management and protection of data pose a high risk in the event of an attack (Cybersecurity & Infrastructure Security Agency, 2021).

Lack of Effective Recovery Plans: Many organizations do not have comprehensive or adequate disaster recovery plans. Without a clear recovery plan, recovery from a ransomware attack becomes more difficult and time-consuming (Chen et al., 2021).

5. Awareness and Education

Lack of Cybersecurity Awareness: Many individuals and organizations are unaware of risks and threats. A lack of knowledge about good security practices and early signs of an attack can lead to delays in detection and response. The current higher education model for cybersecurity remains inadequate in certain areas and fails to provide a holistic solution to the root causes of the skill gap (AlDaajeh et al., 2022).

Lack of Training: Inadequate or irregular cybersecurity training leaves staff unprepared for ransomware attacks. Ongoing education and intensive training are necessary to improve patient preparedness.

6. Coordination and Collaboration

Inter-Agency Coordination: Lack of coordination between government agencies and the private sector can slow the response to ransomware attacks. Better collaboration and information-sharing between entities are essential for addressing cyber threats.

International Cooperation: Sinece ransomware attacks are often global, international cooperation in law enforcement and intelligence sharing is essential but is frequently difficult to achieve According to Sarkar & Shukla, (2023) symbiotic collaboration between the public and private sectors is required, as is a joint effort between private entities and law enforcement agencies to combat cybercrime.

.

7. Evolving Threats

Increasingly Sophisticated Attack Techniques: Ransomware attackers continue to evolve their techniques, making the detection and prevention of such attacks increasingly difficult. This innovation in attack technology requires a more advanced approach to cyber-defense.

Research by Dupont (2019) suggested that policy monitoring and surveillance methodologies could be developed in various fields to control cybercrime. The following recommendations can be submitted based on identifying cybersecurity challenges.

1. **Strengthening IT Infrastructure**

Periodic System Updates: A comprehensive IT infrastructure audit is conducted to identify outdated hardware and software systems. Periodic update programs must be implemented in all data centers, particularly those that handle sensitive information. The government could allocate special budgets to ensure these updates

Implementation of Layered Security: Ensure that all data centers have layered security arrangements, including strong firewalls, intrusion detection systems (IDS/IPS), data encryption, and appropriate web application firewalls. Prioritize the use of the latest technology for perimeter protection.

2. **Development of Resources and Expertise**

Increase Human Resource Capacity: Invest heavily in training and certifying cybersecurity experts. Partnerships with universities and technology training institutions can increase the number of competent experts involved.

Additional Budget for Security: Increases budget allocations for cybersecurity, procures advanced technology, and provides personnel with ongoing training programs.

3. **Effective Law Enforcement**

International Coordination: Develop a stronger international cooperation network to address cross-border cybercrime.

Regulatory Revision: Revise and update the UU ITE and related regulations to close existing legal loopholes. Collaborate with legal experts and stakeholders to ensure that these regulations align with technological developments.

4. **Technology and Data Risk Management**

Strengthen Data Protection: Implement stricter data management standards, including end-to-end encryption and strict access controls for sensitive data. Secure, encrypted backup systems must be implemented.

Disaster Recovery Plan: Every organization should have a comprehensive disaster recovery plan. This plan should be tested regularly to ensure its effectiveness against ransomware attacks

5. **Coordination and Collaboration Between Agencies**

Establish a Cyber Emergency Response Team: To expedite the response to ransomware attacks, a cyber emergency response team (Computer Security Incident Response Team or CSIRT) consisting of various government agencies and the private sector should be formed.

Enhance Public-Private Cooperation: Strengthen cooperation between the public and private sectors in sharing intelligence and technology related to cybersecurity. This includes collaboration in the research and development (R&D) of cyber defense solutions

6. **Adapt to Evolving Threats**

Threat Monitoring and Analysis: Implementation of real-time monitoring technology to detect suspicious activities. Artificial intelligence and machine learning can help analyze attack patterns and provide early warnings. **Research and Development (R&D)**: Encourage R&D in cybersecurity to anticipate new attack techniques. This includes the development of tools and methodologies for monitoring cyber threats.

By implementing this solution, the government hopes to strengthen its national security by facing the challenges of growing IT crimes. Collaborative efforts from the government, private sector, and society are needed to create a safer digital environment.

Conclusion

IT crimes in Indonesia have reached a level requiring serious attention and proactive action from the government, law enforcement agencies, and the private sector. The increasing number of cases, especially of identity theft and online fraud, creates an urgency to update and strengthen legal regulations. The evaluation of UU ITE highlights the need for revisions to address the remaining ambiguity and ensure sustainability in dealing with the continuity and evolution of IT crimes. Suggestions made in this study include the need to improve infrastructure and human resources in the security field. Increased investment in training and human resources for law enforcement agencies. This can include more intensive training programs in IT crimes, data risk recovery management, coordination and cooperation between the public and private sectors, and adaptation and

development of real-time threat-monitoring technology using artificial intelligence.

Overall, to protect the public and companies from the risks of IT crimes, careful regulatory changes and an increased capacity of law enforcement agencies must be implemented, as well as preventive efforts and cross-sector cooperation. By adopting this holistic approach, it is hoped that Indonesia can respond to and overcome IT crimes more effectively and ensure future cybersecurity sustainability.

Recommendations

Based on the research we have conducted, we can provide several recommendations that can be made to face cyber security challenges and threats in Indonesia, including:

1. Revising Legal Regulations

Evaluate and revise the UU ITE to address existing ambiguities and strengthen legal provisions related to IT crimes.

2. Improving Security Infrastructure

The government needs to invest in developing a better cybersecurity infrastructure, including real-time threat monitoring and response systems.

3. Developing Human Resources

Improve training and education for human resources in the field of cybersecurity, including intensive training for law enforcement agencies so that they can handle IT crimes more effectively.

4. Public–private partnership program

Stronger cooperation between the government, law enforcement agencies, and the private sector to share information and resources for handling cybercrime.

5. Investment in Artificial Intelligence Technology

Develop and adopt artificial intelligence technology to monitor and analyze threats in real time to detect and respond to potential crimes earlier.

6. Public Awareness Campaigns

Implement campaigns to raise public awareness of the risks of IT crimes and how to protect themselves from such threats.

7. Improved Law Enforcement

Encourage stricter law enforcement against cyber-crime offenders by strengthening existing investigative capacity and legal processes.

By implementing these recommendations, it is hoped that Indonesia will be better prepared to face and handle the challenges posed by IT crimes and create a safer environment for the community and business sectors.

References

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers and Security*, *119*(April 2024). https://doi.org/10.1016/j.cose.2022.102754

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A Survey and Trends. *Journal of Information Assurance and Security*, *12*(January 2020), XXX–XXX. www.mirlabs.net/jias/index.html

Bawono, B. T. (2019). Reformation of Law Enforcement of Cyber Crime in Indonesia. *Jurnal Pembaharuan Hukum*, *6*(3), 55. https://doi.org/10.26532/jph.v6i3.9633

Borky, J. M., & Bradley, T. H. (2019). Effective Model-Based Systems Engineering. In *Effective Model-Based Systems Engineering*. https://doi.org/10.1007/978-3-319-95669-5

Chen, P. H., Bodak, R., & Gandhi, N. S. (2021). Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *Journal of Digital Imaging*, *34*(3), 731–740. https://doi.org/10.1007/s10278-021-00466-x

Connatse, M. (2024). *Indonesian government datacenter locked down in $8M ransomware rumble*. The Register. https://www.theregister.com/2024/06/24/indonesia_datacenter_ransomware/

Cybersecurity & Infrastructure Security Agency. (2021). *Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches*.

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, *42*(5), 500–515. https://doi.org/10.1080/0735648X.2019.1691855

Hamzani, A. I., -, S., Asmarudin, I., Rahayu, K., & Aravik, H. (2020). Law Enforcement Problems and Impacts of the Law Development in Indonesia. *International Journal of Psychosocial Rehabilitation*, *24*(04), 3244–3254. https://doi.org/10.37200/ijpr/v24i4/pr201435

Harkin, D., & Whelan, C. (2021). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, *24*(1), 66–76. https://doi.org/10.1177/14613557211036565

Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. (2018). Analyzes of cybercrime expansion in Indonesia and preventive actions. *IOP Conference Series: Materials Science and Engineering*, *434*(1). https://doi.org/10.1088/1757-899X/434/1/012257

Ishak, N. (2023). Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges? *Audito Comparative Law Journal (ACLJ)*, *4*(2), 108–117. https://doi.org/10.22219/aclj.v4i2.26098

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting

cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*(August 2022). https://doi.org/10.1016/j.csa.2023.100016

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, *5*(1), 169–212. https://doi.org/10.1365/s43439-024-00111-7

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation and Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12341

Morgan, S. (2021). 2021 Report: Cyberwarfare In The C-Suite. *Cybercrime Facts and Statistics*, 1–19. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *International Journal of Scientific Research and Management (IJSRM)*, *12*(06), 1282–1298. https://doi.org/10.18535/ijsrm/v12i06.ec09

Nugroho, A., & Chandrawulan, A. A. (2023). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Security Journal*, *36*(4), 651–670. https://doi.org/10.1057/s41284-022-00357-y

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*(October), 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Senjaya, M. (2021). Updating Criminal Law in Civilized Law Enforcement and Social Justice. *International Journal of Science and Society*, *3*(2), 39–46. https://doi.org/10.54783/ijsoc.v3i2.315

Widiasari, N. K. N., & Thalib, E. F. (2022). The Impact of Information Technology Development on Cybercrime Rate in Indonesia. *Journal of Digital Law and Policy*, *1*(2), 73–86. https://doi.org/10.58982/jdlp.v1i2.165