CYBER SECURITY CHALLENGES IN THE AGE OF DIGITALISATION: HOW CAN COMPUTERS BE PROTECTED?

Loso Judijanto *
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Al-Amin
Universitas Airlangga, Surabaya, Indonesia
al.amin-2024@feb.unair.ac.id

Abstract

In the era of growing digitalisation, cybersecurity challenges have become critical issues that require serious attention from individuals and organisations. Various types of cyber threats such as ransomware, phishing, and DDoS attacks are increasingly sophisticated and diverse, demanding a comprehensive and proactive approach to digital asset protection. Ensuring computers are protected requires a combination of up-to-date security technologies such as antivirus, firewalls, data encryption, and multifactor authentication, as well as strict security policy implementation and ongoing education. Success in meeting these challenges also depends on adaptability and rapid response to dynamic threats, with the development of effective emergency response plans. The right combination of technology, policy and operational preparedness will provide robust and responsive protection amidst the complexity of today's digital landscape.

Keywords: Cyber Security, Digitalisation Era, Computers.

Introduction

In the rapidly growing era of digitalisation, cyber security has become one of the crucial issues faced by individuals, organisations, and governments around the world. The advancement of information and communication technology has brought many benefits, such as easy access to information, operational efficiency, and various innovations that support progress in various fields.

Cyber security is becoming increasingly important in the digitalisation era as almost all aspects of modern life rely on information and communication technology. From financial transactions and personal data processing to business operations and government services, everything is integrated with computer systems and internet networks (Dariyabayevichc, 2023). This dependency creates many loopholes that can be exploited by cyber criminals. A successful attack not only has the potential to cause significant financial loss, but can also damage an organisation's reputation, steal sensitive information, and disrupt critical infrastructure with far-reaching impacts on society. Therefore, maintaining cyber security is a fundamental step to ensure continuity and trust in the digital ecosystem (Al-Rbeawi, 2023).

In addition, with the proliferation of Internet of Things (IoT) technology and smart devices, the number of potential entry points for attacks is also increasing. Any device connected to the internet network can become a target for cyberattacks, which in turn can affect other devices connected to the same network. Strong cyber security not only protects data and systems from external threats, but also ensures each country's digital sovereignty and safeguards individuals' privacy rights (Perwej et al., 2021). Without adequate security, the benefits and potential offered by the digitalisation era will not be fully utilised, and may even backfire, bringing new risks. Therefore, cyber security is a key pillar that must be considered and enhanced as the adoption of digital technology becomes more widespread. However, along with these benefits also come new challenges, one of which is cyber security threats (Husain et al., 2023).

Cybersecurity threats take many forms, ranging from malware, phishing, hacking, to ransomware attacks, all of which can cause huge losses both financially and reputationally. Based on reports from various cybersecurity organisations, the number of cyber attacks increases significantly every year. These attacks not only target large companies, but also individuals and small organisations that are often less prepared to deal with these threats (Bellatreche et al., 2021).

Computers, as one of the key devices in the digital ecosystem, are the main target of many cyber-attacks. The insecurity of computer systems can be caused by various factors, such as software flaws, user carelessness, and lack of understanding of good security practices. This vulnerability is exacerbated by the openness of the internet network that allows cyber criminals to perform their actions from anywhere in the world (Bala et al., 2023).

Therefore, efforts to protect computers from cyber-attacks have become very important. This protection involves a variety of initiatives, ranging from the development of more secure software, the implementation of firewalls and antivirus, to educating users on the importance of good security practices, such as the use of strong passwords and being aware of phishing emails (Maulana & Fajar, 2023).

This research examines the main challenges faced in cyber security, especially on computer devices, and presents strategies and solutions that can be applied to improve security. Thus, it is expected to contribute to making a more secure and trusted digital environment.

Research Methods

The study in this research uses literature. Literature research is a method used to collect, review and analyse data or information that has been published on a particular topic. (Firman, 2018); (Suyitno, 2021).

Results and Discussion

Identification of Cyber Security Challenges

Cybersecurity refers to the practice of protecting systems, networks, and programmes from malicious digital attacks. Cyberattacks usually have the goal of stealing, altering, or destroying sensitive information, disrupting business operations, or extorting money from users (Maulana & Fajar, 2023). In this context, cybersecurity includes various techniques and procedures used to ensure the integrity, confidentiality, and availability of information processed and stored in computer systems and networks. Some of the key components of cybersecurity include network security, application security, information security, operational security, and disaster recovery plans as well as end-user awareness and training (Tan et al., 2022).

The basic concept in cybersecurity involves several key principles such as Confidentiality, Integrity, and Availability known as the CIA model. Confidentiality aims to protect data from unauthorised access, integrity ensures that data is accurate and not unlawfully altered, while availability ensures that data and systems remain accessible to authorised users when needed (Georgiou et al., 2021). In addition to the CIA model, concepts such as risk management, threat mitigation, and incident detection and response are also important parts of the cybersecurity framework. All of these aim to identify, protect, detect, respond to, and recover from potentially damaging cyber incidents (Gombár et al., 2024).

Important aspects of cybersecurity include several key elements that include technology, processes, and people. In terms of technology, important aspects include the use of anti-virus software, firewalls, encryption, and intrusion detection systems to protect data and networks. Processes include the implementation of security policies, access management, and regular controls and risk assessments to maintain the overall resilience of the system. The human factor is equally important, involving security training and awareness for end users to recognise potential threats such as phishing and social engineering, as well as building a proactive security culture within the organisation. Cooperation and communication between all of these factors is crucial to creating a secure cyber environment that is resilient to cyber attacks and threats (Nair et al., 2024).

Cybersecurity must always be aware of various types of threats that can disrupt or damage systems and data. Malware (malicious software) is one of the most common forms of threats, including viruses, worms, trojan horses, spyware and adware. Viruses can spread from one computer to another, infecting devices and corrupting files. Worms work in a similar way, but can spread on their own without the need for a host (Azambuja et al., 2023). Trojans are hidden in programs that appear legitimate but have malicious purposes. Meanwhile, spyware and adware collect users' personal information without their knowledge and often display unwanted adverts (Kumar et al., 2023).

Phishing is an attack that attempts to trick individuals into providing personal or sensitive information such as passwords and credit card numbers. This is usually done through fake emails or websites that appear legitimate. Ransomware is a type of malware that encrypts the victim's data and then demands a ransom to restore access. In addition, there is DDoS (Distributed Denial of Service) which attacks by flooding the target system or network with excessive traffic, thus making the service unavailable (Al-Rbeawi, 2023). Zero-day exploits take advantage of software vulnerabilities that are not yet known by their authors, providing an opportunity for attackers before fixes are applied. Through understanding and being aware of these different forms of threats, effective protection and response measures can be implemented to maintain cybersecurity (Achar et al., 2022).

Cybersecurity is heavily influenced by the **latest technological** advancements that are constantly evolving to counteract increasingly complex threats. Technologies such as artificial intelligence (AI) and machine learning (ML) are now being applied to detect patterns and anomalies that may signal a cyberattack. More advanced encryption technologies are also being implemented to protect data both in transit and in storage. Additionally, developments in blockchain offer new methods to secure digital transactions and data storage. The adoption of more up-to-date antivirus and firewall software also plays an important role in improving the security posture (Vadiyala, 2021).

Internal company policies are another aspect that largely determines the effectiveness of cybersecurity. These policies include various procedures and standards that all parties in the organisation must follow to keep information safe. For example, strict access management ensures that only authorised individuals can access sensitive data. Regular training and education on best security practices, including how to recognise phishing and similar threats, is also crucial. In addition, solid data backup policies ensure that critical information can be recovered quickly after an attack (Zhang et al., 2021).

Regulations and industry standards also play a big role in shaping cybersecurity practices. Regulations such as GDPR (General Data Protection Regulation) in Europe and HIPAA (Health Insurance Portability and Accountability Act) in the United States dictate how sensitive data should be protected and managed. Compliance with international standards such as ISO/IEC 27001 helps organisations ensure that they follow best practices in information security management. In addition to strengthening internal security, these regulations and standards can also increase the trust of customers and business partners, which is invaluable in maintaining a company's reputation and integrity (Holovkin et al., 2021).

Furthermore, the factor of collaboration and information exchange cannot be ignored in the world of cybersecurity. Organisations that work together to share threat intelligence and best practices are often better prepared for attacks. This collaboration can be between companies and cybersecurity authorities, as well as with fellow organisations in the same industry. Exchanging information on the latest threats, attack techniques and mitigation methods allows organisations to stay one step ahead of attackers. This also involves participating in cyber forums and communities, and adopting a well-coordinated incident response approach (Safitra et al., 2023).

Equally important is the role of user awareness and education in strengthening security. Many cyberattacks capitalise on weaknesses at the individual level, such as a lack of knowledge about phishing or the use of weak passwords. Therefore, an ongoing cybersecurity education programme is essential. Through structured security training, employees gain the necessary knowledge and skills to recognise and respond to various forms of cyber threats. In addition, a strong cybersecurity culture is achieved through active involvement and commitment from all levels of the organisation (Safitra et al., 2023).

Cybersecurity is thus the result of a combination of various complementary factors. The latest technologies provide advanced tools and methods to protect data and detect threats, while internal company policies ensure that every aspect of operations adheres to strict security standards. Industry regulations and standards provide a framework to follow to ensure compliance and mitigate risks. In addition, collaboration and information sharing strengthen threat response capabilities, and user education and awareness ensure that individuals within the organisation do not become exploitable weak points. By integrating all these factors, organisations can build a robust cybersecurity strategy that is resilient to threats.

Computer Protection Methods

Computer security requires a holistic approach that covers various aspects. One basic yet highly effective method is the implementation of antivirus and anti-malware. These programs serve as the first line of defence by detecting, blocking, and removing malware before they can damage the system. Regularly updating antivirus software is crucial, as new threats emerge every day. Additionally, the use of firewalls can be an additional layer to monitor and control the flow of network traffic, ensuring that only safe and legitimate traffic is allowed to reach the device (Kouroupis & Sotiropoulos, 2024).

In addition, data encryption is an important method for protecting sensitive information. Encryption serves to convert data into a format that cannot be read by unauthorised parties, unless they have the appropriate encryption key. This is especially important not only for data that is stored (data at rest), but also for data that is transmitted (data in transit) over public or private networks. End-to-end encryption on communication services such as email and instant messaging applications ensures that only the intended recipient can read the message (Saniuk & Grabowska, 2021).

Another method is multi-factor authentication (MFA), which adds an extra layer of security beyond a single password. MFA requires two or more forms of identification (e.g., a combination of something the user knows, like a password; something they have, like a smartphone; and something they are, like a fingerprint). By making unauthorised login attempts more difficult, MFA significantly reduces the risk of unauthorised access to accounts and systems. In business environments, implementing role-based access control (RBAC) is also important so that employees only have access to data and systems that are appropriate to their job requirements (Aditya et al., 2022).

Finally, regular backups and patch management are steps that cannot be ignored. Performing regular data backups ensures that data can be recovered quickly in the event of data loss due to a ransomware attack or system failure. Backup data should be stored in a separate location to avoid any damage that may occur to the primary storage. Meanwhile, patch management involves applying software updates that are meant to patch security vulnerabilities. This includes not only the operating system but also the applications and hardware used. The combination of these various protection methods can help create a more secure computing environment that is protected from various cyber threats.

Proactive Computer Security Strategy

Proactive security strategies focus on preventing threats before they can exploit system vulnerabilities. One of the main approaches in this strategy is active monitoring. Active monitoring systems constantly analyse network and system activity to detect suspicious patterns or anomalies. With tools such as SIEM (Security Information and Event Management), companies can collect and analyse log data from various devices to identify potential threats in real-time. Proactive monitoring allows preventive measures to be taken before cyberattacks become more serious (Verma et al., 2021).

In addition to monitoring, regular risk and vulnerability assessments are also an essential part of a proactive security strategy. These assessments include penetration testing where security experts try to break into systems using the same techniques used by hackers. Through these periodic assessments, organisations can identify weaknesses in their systems and fix them before they are exploited by unauthorised parties. Updates of assessment results should be made to ensure continuous addressing of changing risks (Thakur, 2024).

The implementation of strong security policies is also important as a proactive measure. These policies include guidelines on the use of strong passwords, network access rules, and measures for identity and access management. Cybersecurity education and training for employees increases awareness and knowledge of best practices, helping them recognise and avoid threats such as phishing. Good policies coupled with user awareness provide a strong foundation for maintaining organisational information security (Oruj, 2023).

Finally, it is crucial to have a solid and tested incident response plan. An incident response plan should include step-by-step procedures to be followed in an emergency situation to mitigate the impact of a cyberattack. This includes incident identification, incident content, threat eradication, and system recovery. Incident simulations and cyber fire drills can help emergency response teams to be better prepared and responsive in the event of a real attack. Combining these strategies effectively ensures that organisations not only react to threats but are also active in preventing them, creating a more resilient security posture.

Conclusion

In the age of digitalisation, cybersecurity challenges are becoming increasingly complex as technology develops and connectivity increases. Cyberattacks are not only becoming more sophisticated, but also more diverse, including in the form of ransomware, phishing and DDoS attacks. One of the key challenges is ensuring that these constantly connected systems are safe from evolving threats. Individuals and organisations must therefore adopt a more comprehensive and proactive approach to protecting their digital assets.

Computers can be better protected through a combination of the right technology and policies. Using up-to-date security software, such as antivirus and firewalls, is an important basic step. However, this should be complemented with data encryption and multifactor authentication for an added layer of protection. In addition, strict implementation of security policies, including ongoing education of users and employees on cybersecurity practices, is critical to building awareness and resilience to social engineering threats such as phishing.

Success in addressing cybersecurity challenges also depends on the ability to adapt and respond quickly to dynamic threats. Developing a well-thought-out emergency response plan and regular testing of the plan can help in minimising the impact of a cyberattack should one occur. The combination of cutting-edge technology, effective policies, and operational preparedness will ensure that computers and other related systems have robust and responsive protection amidst the complexity of today's digital landscape.

References

Achar, S., Vijayendra, K., Hussain, S., & ... (2022). Business Trends in Digital Era: A Review. *Journal of ..., Query date: 2024-10-23 19:23:27*. http://publish7promo.com/id/eprint/1645/

Aditya, A., Wulandari, C., & Loso, L. (2022). Cyber Notary: Between Notary Opportunities And Challenges In Facing The Era Of Digital Disruption 4.0 Towards 5.0.

International Journal of Law …, Query date: 2024-10-23 19:23:27. https://jurnal.unissula.ac.id/index.php/ijls/article/view/20365

Al-Rbeawi, S. (2023). A review of modern approaches of digitalization in oil and gas industry. *Upstream Oil and Gas Technology*, *Query date: 2024-10-23 19:23:27*. https://www.sciencedirect.com/science/article/pii/S2666260423000130

Azambuja, A. D., Plesker, C., Schützer, K., Anderl, R., & ... (2023). Artificial intelligence-based cyber security in the context of industry 4.0—A survey. *Electronics*, *Query date: 2024-10-23 19:23:27*. https://www.mdpi.com/2079-9292/12/8/1920

Bala, I., Mijwil, M., Ali, G., & Sadıkoğlu, E. (2023). *Analysing the connection between ai and industry 4.0 from a cybersecurity perspective: Defending the smart revolution*. dir.muni.ac.ug. http://dir.muni.ac.ug/handle/20.500.12260/568

Bellatreche, L., Chernishev, G., Corral, A., Ouchani, S., & ... (2021). *Advances in Model and Data Engineering in the Digitalization Era*. Springer. https://doi.org/10.1007/978-3-030-87657-9

Dariyabayevichc, U. (2023). A Comprehensive Analysis of Ecological Law in the Cyber Era. *International Journal of Law and Policy*, *Query date: 2024-10-23 19:23:27*. https://irshadjournals.com/index.php/ijlp/article/view/58

Firman, F.-. (2018). *PENELITIAN KUALITATIF DAN KUANTITATIF*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31227/osf.io/4nq5e

Georgiou, K., Mittas, N., Mamalikidis, I., & ... (2021). Analyzing the roles and competence demand for digitalization in the oil and gas 4.0 era. *IEEE …*, *Query date: 2024-10-23 19:23:27*. https://ieeexplore.ieee.org/abstract/document/9598932/

Gombár, M., Vagaská, A., Korauš, A., & Račková, P. (2024). Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0. *Mathematics*, *Query date: 2024-10-23 19:23:27*. https://www.mdpi.com/2227-7390/12/2/343

Holovkin, B., Tavolzhanskyi, O., & ... (2021). Corruption as a cybersecurity threat in the new world order. *… : The Quarterly Journal*, *Query date: 2024-10-23 19:23:27*. https://procon.bg/ru/system/files/20.2.07_corruption.pdf

Husain, M., Faisal, M., Sadia, H., Ahmad, T., & Shukla, S. (2023). *Advances in Cyberology and the Advent of the Next-gen Information Revolution*. books.google.com. https://books.google.com/books?hl=en&lr=&id=hinKEAAAQBAJ&oi=fnd&pg=PR1&dq=cyber+digitalization+era+computer&ots=__lNEmN5Wi&sig=RbZ81fG7Gk0xLorLCW6TNiaeyRM

Kouroupis, K., & Sotiropoulos, L. (2024). Cyber Challenges amid the Digital Revolution in Maritime Transport. *Jurid. Trib.-Rev. Compar. &Int'l L.*, *Query date: 2024-10-23 19:23:27*. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/juridtrib14§ion=25

Kumar, S., Gupta, U., Singh, A., & Singh, A. (2023). Artificial intelligence: Revolutionizing cyber security in the digital era. *Journal of Computers …*, *Query date: 2024-10-23 19:23:27*. https://jcmm.co.in/index.php/jcmm/article/view/64

Maulana, Y., & Fajar, I. (2023). Analysis of cyber diplomacy and its challenges for the digital era community. *IAIC Transactions on Sustainable Digital …*, *Query date: 2024-10-23 19:23:27*. https://aptikom-journal.id/itsdi/article/view/587

Nair, M., Deshmukh, A., & Tyagi, A. (2024). Artificial intelligence for cyber security: Current trends and future challenges. … *Secure Computing for Next …*, *Query date: 2024-10-23 19:23:27*. https://doi.org/10.1002/9781394213948.ch5

Oruj, Z. (2023). Cyber Security: Contemporary cyber threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative …*, *Query date: 2024-10-23 19:23:27*. https://jrnl.nau.edu.ua/index.php/DEU/article/view/17309

Perwej, Y., Abbas, S., Dixit, J., Akhtar, N., & ... (2021). A systematic literature review on the cyber security. *International Journal of …*, *Query date: 2024-10-23 19:23:27*. https://hal.science/hal-03509116/

Safitra, M., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *Query date: 2024-10-23 19:23:27*. https://www.mdpi.com/2071-1050/15/18/13369

Saniuk, S., & Grabowska, S. (2021). The concept of cyber-physical networks of small and medium enterprises under personalized manufacturing. *Energies*, *Query date: 2024-10-23 19:23:27*. https://www.mdpi.com/1996-1073/14/17/5273

Suyitno. (2021). *METODE PENELITIAN KUALITATIF KONSEP, PRINSIP DAN OPERASIONALNYA*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31219/osf.io/auqfr

Tan, K., Chi, C., & Lam, K. (2022). Analysis of digital sovereignty and identity: From digitization to digitalization. *arXiv Preprint arXiv:2202.10069*, *Query date: 2024-10-23 19:23:27*. https://arxiv.org/abs/2202.10069

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *Query date: 2024-10-23 19:23:27*. http://jase.a2zjournals.com/index.php/ase/article/view/42

Vadiyala, V. (2021). Byte by Byte: Navigating the Chronology of Digitization and Assessing its Dynamic Influence on Economic Landscapes, Employment Trends, and Social …. *Digitalization & Sustainability Review*, *Query date: 2024-10-23 19:23:27*. https://www.researchgate.net/profile/Vishal-Reddy-Vadiyala/publication/377387435_Byte_by_Byte_Navigating_the_Chronology_of_Digitization_and_Assessing_its_Dynamic_Influence_on_Economic_Landscapes_Employment_Trends_and_Social_Structures/links/65a37ed940ce1c5902dac01e/Byte-by-Byte-Navigating-the-Chronology-of-Digitization-and-Assessing-its-Dynamic-Influence-on-Economic-Landscapes-Employment-Trends-and-Social-Structures.pdf

Verma, A., Surendra, R., Reddy, B., & ... (2021). Cyber security in digital sector. … *Intelligence and Smart …*, *Query date: 2024-10-23 19:23:27*. https://ieeexplore.ieee.org/abstract/document/9395933/

Zhang, B., Yang, B., Wang, C., Wang, Z., Liu, B., & Fang, T. (2021). Computer vision-based construction process sensing for cyber–physical systems: A review. *Sensors*, *Query date: 2024-10-23 19:23:27*. https://www.mdpi.com/1424-8220/21/16/5468