A New Perspective on Cyber Security Threats: A Focus on the Epidemiological Triangle Model

Jungjoo Oh, Minkyung Song, Yeram Lim, Minhui Seo and Wonhyung Park*

Dept of Convergence Security Engineering, Sungshin Women's University, Republic of Korea.
[winteroot, 20200690, 20200952, 20211066, whpark]@sungshin.ac.kr

Abstract

Traditional cybersecurity models face limitations in understanding and responding to complex cyber threats. Therefore, this study proposes a model to analyze and respond to cybersecurity threats from a new perspective by introducing the epidemiological triangle model. Through this model, we understand the similarity between infectious disease and cybersecurity threats and study the role of the host (asset) and the environment (security environment). By offering a holistic view, this model will provide a basis for effectively understanding and responding to the occurrence and spread of cybersecurity threats.

Keywords : Cybersecurity Model, Epidemiological Triangle Model, Security Threat

1 Introduction

With the recent development of new technologies such as AI and IoT, cyberattacks are on the rise and the scale of damage is increasing. However, the traditional cybersecurity model focuses on the technical aspect, which has limitations in fully understanding and responding to the overall cybersecurity ecosystem. To overcome this, this study presents a new perspective on cybersecurity threats by introducing the epidemiological triangle model. This study aims to provide a comprehensive understanding and response to cybersecurity strategies.

The 7th International Conference on Mobile Internet Security (MobiSec' 23), Dec. 19-21, 2023, Okinawa, JAPAN, Article No. P-24

* Corresponding author: Dept of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Republic of Korea, Email: whpark@ sungshin.ac.kr

2 Epidemiological Triangle Model

The epidemiological triangle model is one of the most universally recognized epidemiological models of infectious disease outbreaks. According to this model, infectious diseases are caused by a combination of agent, host, and environmental factors (Sniezko, 1974). Agent is a factor that can cause diseases such as viruses, bacteria, and fungi. Host is an individual in which a disease can occur. The outcome of exposure to an agent depends on the host's susceptibility and immunity. Environmental factors include physical, social, and cultural factors. Environmental factors can increase the risk of exposure to infectious agents or increase susceptibility to infection (Seventer & Hochberg, 2017).

3 Applying the Model to Cyber Security Threats

The epidemiological triangle model can be applied to the cybersecurity model as follows. First, security threats, including malware, can be treated as pathogens because they gain access to the host and cause damage. To prevent the spread of malware, real-time detection and remediation of malware through antivirus, detection systems, etc. is required. Hosts can be assets (systems, networks, data, etc.). Backdoors, rootkits, software vulnerabilities, etc. can be factors that increase the susceptibility of assets. We can increase the resistance of the security asset by patching the vulnerability, simulating hacking, etc. Environmental factors can be responded to with a cybersecurity environment. Environments that are prone to cyber infectious diseases may include vulnerable system and network configurations, weak security policies, and lack of security awareness among users. Environmental factors can be improved by conducting security education, building security infrastructure, and separating networks.

4 Implications

There are many similarities between epidemiology and malware propagation models, and several papers have attempted to compare them (Modini et al, 2020). However, these studies are mainly limited to technical aspects and lack a comprehensive perspective. This study attempts to provide a comprehensive understanding of the various factors that affect the occurrence and spread of cybersecurity threats through the Epidemiological Triangle Model. However, there are limitations in that epidemiology and cybersecurity do not correspond perfectly. In future research, it is necessary to analyze the two models comparatively and refine the scope of this model.

5 Conclusion

The epidemiological triangle model offers a new perspective on cybersecurity threats, providing a foundation for effectively understanding and responding to the occurrence and spread of cyberattacks.

Acknowledgement :This work was partly supported by grants of the Korea Institute for Advancement of Technology (KIAT) funded by the Korean Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist) and the MSIT under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310) supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

References

[1]Modini, J., Lynar, T., Sitnikova, E., & Joiner, K. (2020, June). Applications of epidemiology to cybersecurity. In *European Conference on Cyber Warfare and Security* (pp. 483-490). Academic Conferences International Limited.
[2]Snieszko, S. F. (1974). The effects of environmental stress on outbreaks of infectious diseases of fishes. *Journal of Fish Biology*, *6*(2), 197-208.
[3]Van Seventer, J. M., & Hochberg, N. S. (2017). Principles of infectious diseases: transmission, diagnosis, prevention, and control. *International encyclopedia of public health*, 22-39.