

Summary Post

◀ Initial Post

Summary Post ▶

Display replies in nested form

Settings ▼



Summary Post

by [Oi Lam Siu](#) - Sunday, 12 May 2024, 11:27 AM

In my initial post, I discussed the cybersecurity challenges faced by fully digital enterprises. I also mentioned that small and medium enterprises (SMEs) may not be attractive targets for cybercriminals due to their size, limited data, and lower ability to pay ransoms. However, upon considering the insightful responses from my peers, I realized that SMEs, particularly those acting as vendors and suppliers, can be appealing targets due to their connections with larger businesses.

When SMEs undergo digital transformation as vendors for larger companies, prioritizing cybersecurity becomes crucial to protect themselves and their partners. Despite their size and limited data, SMEs can be attractive targets due to their connections with larger businesses. The first stage of the Cyber Kill Chain, Reconnaissance, involves identifying potential targets, vulnerabilities, and connected third parties (Threat Intelligence, 2022). Cybercriminals often exploit this integration to access more lucrative targets.

To mitigate these risks, I will highlight the following cybersecurity measures that SMEs should implement:

First, implement secure communication channels using encrypted email and secure file transfer protocols to protect sensitive information during transmission.

Second, conduct vendor risk assessments to evaluate cybersecurity practices and provide documentation demonstrating a commitment to security. Compliance with industry-specific cybersecurity standards and regulations is crucial.

Thirdly, provide cybersecurity awareness training to employees on best practices, such as the importance of using strong passwords and being able to recognize and report phishing attempts.

Fourth, develop an incident response plan outlining steps for reporting, containment, investigation, and recovery. Regularly test and update the plan for effectiveness.

Fifth, apply regular system updates and patches to address known vulnerabilities. Establish a reliable data backup strategy using separate and secure locations for backups.

Lastly, continuously monitor with security tools and stay informed about the latest threats and vulnerabilities through threat intelligence services and industry forums.

Implementing these cybersecurity measures helps SMEs enhance their security posture, gain trust from larger business partners, and minimize the risk of cyber attacks or data breaches. Prioritizing cybersecurity during the digital transformation journey is essential for long-term success and maintaining strong business relationships with larger companies.

References

Threat Intelligence. (January 1, 2022) The Cyber Kill Chain: The Seven Steps of a Cyberattack. *EC-Council Cybersecurity Exchange*. Available from: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/#:~:text=The%20Cyber%20Kill%20Chain%20is,can%20take%20in%20each%20stage> [Accessed 12 May 2024].

Maximum rating: -

Permalink Reply



◀ Initial Post

Summary Post ▶

