The Secret to Securing Your Digital Transformation

Digital transformation offers significant opportunities for organisations to innovate and grow, but there are inherent risks that need to be addressed. *Mr Martin Khoo, Principal Lecturer & Consultant, Digital Strategy & Leadership Practice, NUS-ISS; speaking at the NUS-ISS Virtual Learning Festival 2023 on the topic 'The Importance of Cybersecurity for Digital Transformation'.* A report by Check Point Research revealed that the Asia Pacific (APAC) region witnessed the highest year-on-year increase in weekly cyberattacks during the first quarter of 2023. On average, each organisation in APAC is hit by 1,835 attacks per week. Why is our region a hotbed for cybercrime? Several factors are at play, says Mr Martin Khoo, Principal Lecturer & Consultant, Digital Strategy & Leadership Practice, NUS-ISS. “These include rapid digital transformation, a young, digital-savvy population, the rise of hybrid work and collaboration technologies.” It’s therefore imperative that cybersecurity is incorporated into the digital transformation process from the get go, Martin emphasises. Additionally, it is the responsibility of all stakeholders. “Government agencies in various countries will need to develop national-level programmes. Businesses will have to invest in cybersecurity at the organisation level, while individuals like you and me need to know how to protect ourselves and our data from threat actors.” **Key cybersecurity considerations** How can organisations mitigate the risks associated with digital transformation and improve their security posture? Martin highlights three areas: risk assessment, incident response and recovery, and continuous monitoring and testing. Digital transformation introduces new risks, especially regarding data security and privacy, he says. Organisations must assess these risks and develop a cybersecurity strategy to address them. “As businesses collect more customer data, they have a duty of care to make sure these data are managed securely. Compliance with regulations (such as PDPA in Singapore and GDPR in Europe) is crucial.” But despite best efforts, no system is entirely immune to cyber threats. Organisations need an incident response plan to quickly and effectively manage incidents when they occur. Regular testing and exercising of the plan are essential, particularly for regulated sectors like banking and finance. On top of that, proactive monitoring of IT infrastructure is crucial for detecting and responding to threats promptly. “Regular vulnerability assessments and penetration testing help identify and mitigate potential weaknesses before attackers exploit them,” Martin adds. “Two ways to do so are through vulnerability assessment, where you scan your environment to identify and patch weak spots, or penetration testing, where you put on the hat of an attacker and try to penetrate your own system.” **Aligning cybersecurity strategy with business outcomes** A cybersecurity strategy is not developed in isolation. “It needs to be crafted to align with the organisation’s broader business goals and objectives,” says Martin. The strategy translates into an actionable plan that enhances the organisation’s cybersecurity posture and resilience. At this stage, the cybersecurity strategy should focus on overarching goals and outcomes, and be technology agnostic, he adds. Typically, a cybersecurity strategy spans three to five years. But a regular review is crucial – ideally on an annual basis. This is because the cybersecurity landscape is dynamic, with new threats constantly emerging. “Regular review ensures that the strategy remains relevant and effective in addressing evolving threats.” On the organisation level, a cybersecurity strategy

should be a key decision item for the board. Martin stresses that it will require the endorsement and approval of the board, as well as the commitment to provide the necessary funding. “Without adequate funding, it is challenging to implement the initiatives outlined in the strategy effectively,” he explains. **Cybersecurity needs to be powered by skilled talent** Last but not least, a robust cybersecurity strategy has to be supported by skilled cybersecurity personnel who can implement and manage the necessary initiatives. “Take for example the national cybersecurity strategies in Singapore and the United States – they both highlight the importance of building a strong pool of trained cybersecurity professionals to address the evolving cyber threats.” In Singapore, initiatives, such as the Talent Development Fund, were launched as part of Singapore Cybersecurity Strategy to build a pipeline of skilled cybersecurity talent. Institutes of Higher Learning, such as NUS-ISS, also offer a range of cybersecurity certification programmes to increase the pool of cybersecurity trained personnels to meet industry needs. As businesses continue to embark on their digital transformation journeys, cybersecurity will remain a critical enabler. It can even become a competitive advantage, says Martin. “In today's data-driven world, customers are increasingly concerned about the security of their personal information. By demonstrating a commitment to protecting customer data, businesses can build trust and loyalty among their customer base, thereby creating a strong foundation for long-term success.” Watch the recorded NUS-ISS Virtual Learning Festival 2023 talk on NUS-ISS' YouTube Channel here.

For more information on NUS-ISS Executive Education Programmes in Cybersecurity, visit here.

Back to Newsroom