INFORMATION AND NETWORK SECURITY GUIDELINES

MCMC'S GUIDELINES TIMELY, SAY EXPERTS

Framework encourages firms to boost cybersecurity and builds trust among stakeholders

LUQMAN HAKIM
KUALA LUMPUR
news@nst.com.my

THE Malaysian Communications and Multimedia Commission's recently introduced Information and Network Security Guidelines (INSG) is a timely step to bolster the country's cybersecurity infrastructure, experts said.

Universiti Tun Hussein Onn Malaysia's Information Security Research Centre researcher Dr Zubaile Abdullah described the move as positive and forward-thinking.

"Positioning INSG as a best practices framework rather than an immediate regulation is a collaborative approach, allowing organisations to adopt the guidelines progressively," he told the *New Straits Times*.

He said the initiative could increase awareness, improve readiness and gain trust.

"This will encourage organisations to prioritise cybersecurity as a business-critical function.

"Adoption of INSG will enhance the capability of Malaysian organisations to respond to cyberthreats, reducing the risks of breaches, malware attacks or other cybercrime-related threats.

"The inclusive development process builds trust among stakeholders and sets a strong precedent for future initiatives."

However, Zubaile cautioned that organisations could face challenges in complying with the guidelines.

He said smaller companies might lack the financial or technical resources to implement the best practices.

He added that organisations might struggle to find skilled personnel to execute the guidelines.

"Some organisations may view the guidelines as non-essential, especially if they do not perceive themselves as high-risk targets.

"They may be more motivated to implement the guidelines if there are clear benefits, such as tax breaks, certification programmes or public recognition," he said.

Associate Professor Dr Muhamad Khairulnizam Zaini from Universiti Teknologi Mara's College of Computing, Informatics and Mathematics said the guidelines could lead to stronger public-private collaboration and increased investment in cybersecurity research and technologies.

Dr Zubaile Abdullah

INSG, he said, could improve public awareness to ensure that all stakeholders were equipped to deal with cybersecurity threats.

"I believe that the guidelines will drive a shift towards more robust cybersecurity culture and practices, especially in this nation.

"And I also anticipate that those organisations will become more vigilant, especially in identifying cybersecurity threats and able to adopt the preventive measures."

He added that while challenges might arise, such as implementation and cost, they were manageable.

Associate Professor Dr Muhamad Khairulnizam Zaini

"Critical sectors that need to adopt the guidelines include telecommunications, banking and healthcare.

"These organisations are the ones that need to significantly adapt to the guidelines because we know the nature of data in these organisations or sectors is huge."

Earlier, Bernama reported that MCMC had introduced INSG to enhance information and network security and resilience of the country's communications and multimedia industry.

In a statement yesterday, MCMC said INSG served as a best-practices framework and was not mandatory.

"It is applicable to all service providers under the Communications and Multimedia Act 1998.

"However, other industries can also adopt INSG as part of their cybersecurity measures if deemed necessary," it said.

MCMC encouraged companies to operationalise these best practices to strengthen cybersecurity across the communications and multimedia industry.

"This approach allows service providers sufficient time to adapt to INSG and provide feedback for improvement.

"INSG is not about adding extra regulations.

"Instead, it aims to enhance the capability and readiness of service providers to manage cyber risks, mitigate data breaches, minimise disruptions through the strengthened network infrastructure, and protect consumers from online harms," it said.

During the development phase of INSG, MCMC had engaged with various stakeholders, including cybersecurity firms, security consultants, licensees' data centres and cloud service providers, ministries, government agencies, regulators, non-governmental organisations and the academia, besides its affiliated forums.

"The feedback, suggestions and insights provided were carefully evaluated and, where appropriate, were incorporated into INSG.

"This inclusive and transparent approach underscores MCMC's commitment to address the diverse needs and concerns of stakeholders while ensuring adherence to best practices in cybersecurity management," the statement said.

MCMC viewed INSG as a pivotal step in safeguarding Malaysia's digital ecosystem, ensuring secure and resilient network infrastructures for all.

It highlighted the commission's efforts to address the challenges of an increasingly complex cyber landscape, while fostering trust and safety in the nation's digital environment.

For more information, visit www.mcmc.gov.my.