Cyber risks in Malaysia still largely seen as an IT risk rather than a business risk

Marketing Interactive 07/09/2018 Fri 11:47 in Malaysia by Janice Tan

While technology has certainly allowed for several innovations and advancements, it also opens the door to greater cyber risks. This March, the Central Bank of Malaysia fell prey to a cyber attack, which saw hackers attempting to steal money using fraudulent wire transfers.

Last year, personal details of approximately 46.2 million mobile number subscribers in Malaysia were compromised, allegedly the largest data breaches Malaysia has witnessed. Despite the massive data breach that the country has witnessed over the past year, cyber risks are still largely seen as an IT risk rather than a business one.

A recent report by the Asian Institute of Chartered Bankers (AICB) and PwC Malaysia titled “Building a Cyber Resilient Financial Institution: Are you ready for the imminent breach?”, indicated that more than half (58%) of board members from Malaysian banks indicate that the reporting of cybersecurity matters is still predominantly performed by the CIO or CTO. Also, more than 70% of Malaysian banks still rely on their existing IT security or IT operations to perform cybersecurity-related functions and responsibilities.

To avoid potential damage to a financial institution’s bottom line, reputation, brand and intellectual property, the report said that the bank’s executive team should lead the transformation by taking ownership of cyber risk.

Specifically, the executive team should “collaborate up front” to understand how the institution will defend against and respond to cyber risks, and what it will take to make their organisation cyber resilient.

Among the respondents, the majority of banks believe the “full board” has primary responsibility for overseeing cybersecurity risks and challenging management’s assumptions. Meanwhile, 30% said the responsibility falls under the risk management committee. In Malaysia, more than 70% of board respondents rated their management’s cybersecurity strategy as fairly effective.

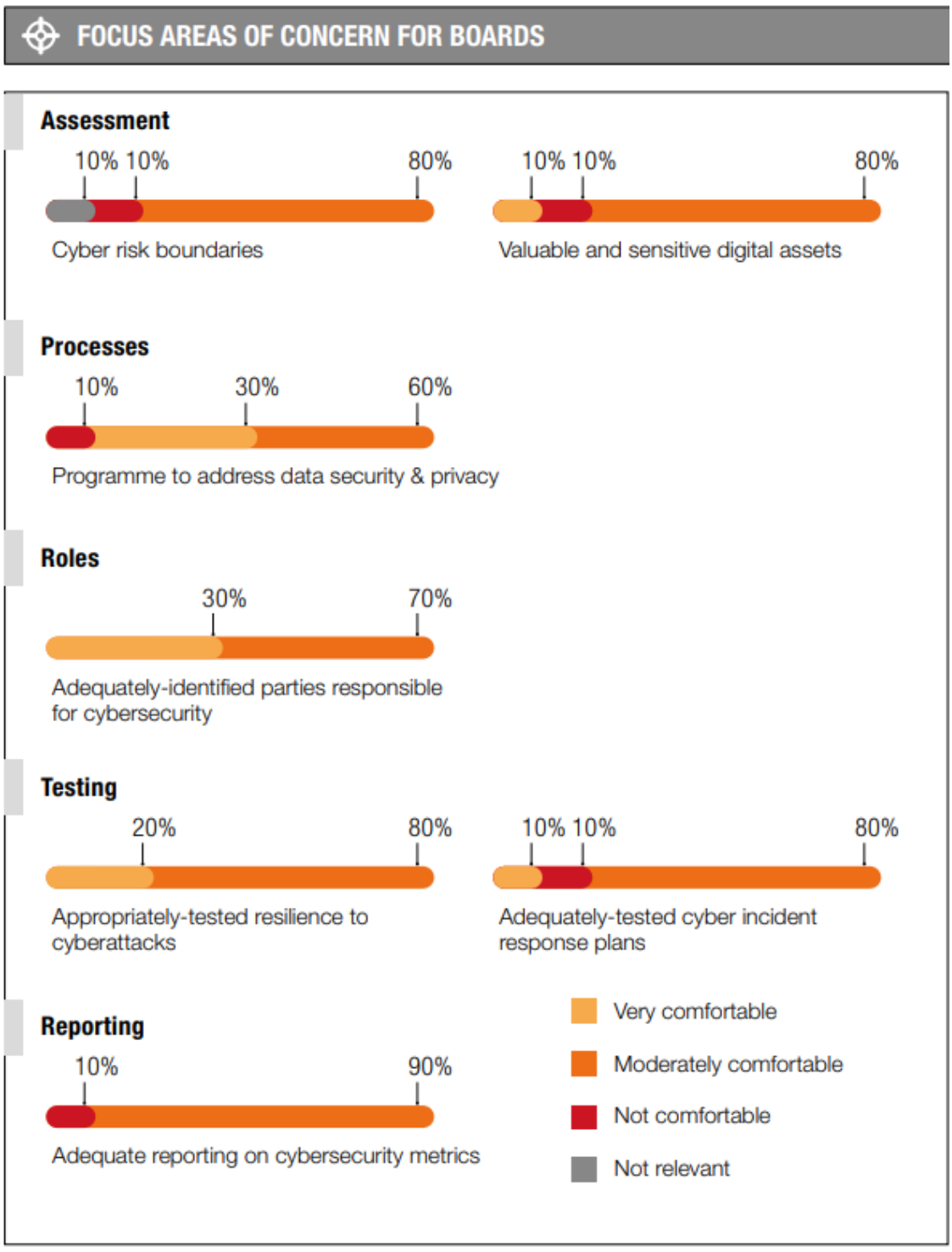
Currently, 75% of the respondents said they are somewhat comfortable with the current reporting metrics on cybersecurity from their management. Of this percentage, 44% are from foreign banks that mainly leverage their global resources.

Meanwhile, 17% of respondents said they are very comfortable that management has adequately tested resistance towards cyber attacks, while 8% stated they are very comfortable that their institutions’ cyber incident response plans have been adequately tested. Respondents from these two groups are from foreign banks.

Among the list of focus areas of concern for boards include adequate reporting on cybersecurity metrics, cyber risk boundaries and programme to address data security and privacy.

Majority (90%) of respondents indicated that they are moderately comfortable with their reporting on cybersecurity metrics. Meanwhile, 80% are moderately comfortable with the assessment of their institution's cyber risk boundaries, while 60% are

moderately comfortable with their institution's programme to address data security and privacy.



The report surveyed 47 people, 79% of which were from senior management while the remaining 21% are board members. The respondents were from foreign and local banks, as well as development financial institutions.