Press Release

FOR IMMEDIATE RELEASE

KPMG's Consumer Loss Barometer highlights disconnect in the event of a data breach

Latest KPMG report reveals mismatch between consumer expectations and security executive priorities

PETALING JAYA, 11 April 2019 – The continuous evolution of digital transformation is outstripping the pace of cybersecurity in organizations. As a result, we're witnessing a fundamental disconnect between consumer expectations and concerns, and the ability of organizations to meet those expectations, according to KPMG's Consumer Loss Barometer report.

The global survey of more than 2,000 consumers and 1,800 Chief Information Security Officers (CISOs) was conducted to assess whether there has been a shift in consumer expectations regarding digital trust, and whether organizations are placing the consumer's security front and centre of their digital product offerings.

KPMG's study found that consumers continue to have reservations about the possible misuse of their private details, with 69% of consumers globally reported concerns about their technology being compromised. In particular, respondents from Malaysia are most concerned about apps (95%), Wi-Fi (82%) and cloud (77%) being compromised. It was further discovered that 49% of consumers from Malaysia said they have had their financial information compromised, higher than the global average of 37%.

On the matter of trust in social media and cloud platforms, 48% of consumers in Malaysia indicated they limit the amount of personal data stored online due to security and privacy concerns. Moreover, 45% indicated that they would like companies and organizations they interact with to disclose measures taken to protect their privacy and security.

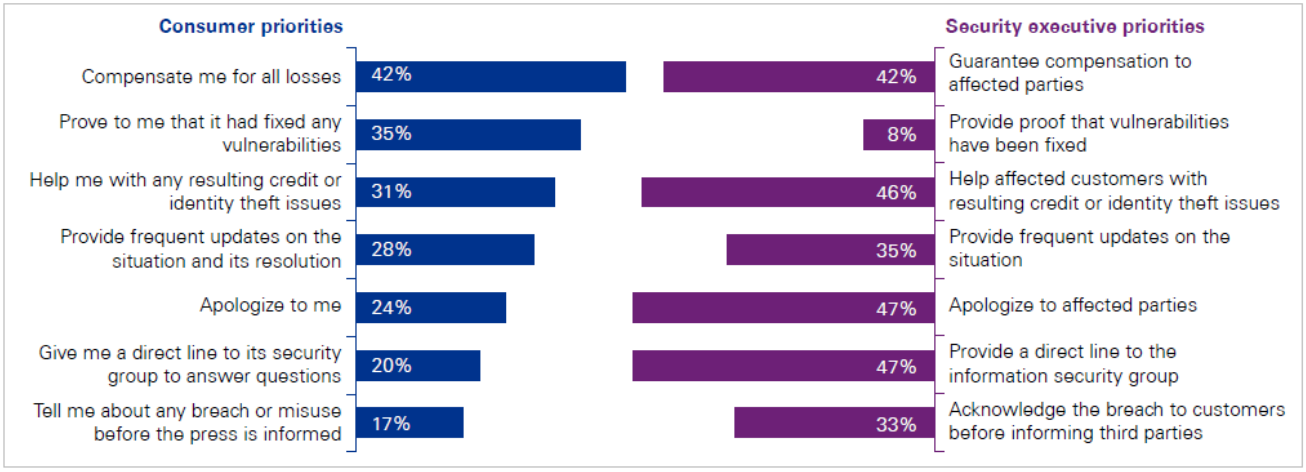
On the other hand, two-thirds of CISOs say they prioritize financial loss and reputational risk over the impact on customer trust. According to the **Executive Director of KPMG's Emerging Tech Risk and Cyber unit in Malaysia, Ubaid Mustafa Qadiri**, the mismatch between consumer expectations and security executive priorities is a grave concern.

"It's clear that organizations are still prioritizing their bottom line ahead of consumer expectations and concerns, despite the opportunity to use effective cybersecurity strategy to build consumer confidence and engagement. Companies should not wait until an incident occurs to act; in times of crises, consumer trust will be lost," Ubaid cautioned.

Apologies are not sufficient

In the event of a breach, consumers prefer compensation (42%) and proof of a fix (35%) over an apology (24%). Conversely, CISOs say they would prioritize an apology over provision of those details (47% and 8% respectively).

Ubaid commented, “As technology innovation progresses, consumers are revising upward their expectations on how organizations deliver digital products and services, and expect security as integral to their digital experience. The gap in expectations between consumers and enterprises offers a tremendous opportunity for forward-thinking organizations to redesign their relationship with their customers, putting trust at the centre of how they do business. For organizations that have prioritized on building their cyber resilience capabilities, now is the time to extend this message to their customers.”



Source: Consumer Loss Barometer. Economics of trust. 2019.

Other notable global findings:

— **Value within the organization**: The vast majority (83%) of CISO respondents brief their board on at least a quarterly or semi-annual basis, demonstrating that executives now rate cybersecurity threats as a significant risk to organizational growth. But when cyber is omitted from the digital business value chain, a trust ecosystem is not delivered and a significant commercial opportunity is missed.

— **Mobile technologies**: 75% of consumers said they were concerned about theft or misuse of personal information collected by their mobile device. Mobile device makers and network

providers can differentiate themselves by building consumer trust in digital channels for such sectors as healthcare and banking, not just in the mobile products and services they provide.

— **Shared responsibility**: Almost half (47%) of consumers believe that their financial institution should have full or joint authority for ensuring that mobile devices used for banking are secured. Whether or not financial institutions regard it as their responsibility, they need to show they take the security of their customer's information seriously, both in their clients' interactions with them and their clients' broader security needs.

To read KPMG's report and view statistics out of Malaysia, visit
www.kpmg.com.my/ConsumerLossBarometer

About the survey

The data published in this report are based on a survey of 1,802 CISOs (or equivalent) in 24 markets, across 12 industries. The respondents were from companies with annual revenues between US$100 million to US$10 billion or more. Consumer data was based on a survey of 2,151 consumers in 24 markets including Malaysia. The sample included all age categories, with a higher percentage of Millennials and Gen Xers, as well as being diversified by gender.

###

For media queries, please contact:

Kimberly Sammy
Manager, Marketing & Communications
KPMG in Malaysia
Direct: +603 7721 3924
Email: kimberlysammy@kpmg.com.my

Syazlina Nasir
Executive, Marketing & Communications
KPMG in Malaysia
Direct: +603 7721 3728
Email: syazlinanasir@kpmg.com.my