http://www.businesstimes.com.sg/opinion/firms-must-put-in-place-sufficient-cybersecurity-measures

COMMENTARY

Firms must put in place sufficient cybersecurity measures

Tuesday, May 9, 2017 - 05:50

by
STEVE TAN

WITH increasing access to mobile devices and the Internet, the amount of data created annually worldwide is predicted to soar to 180 zettabytes (180 trillion gigabytes) in 2025, with some 80 billion devices connected to the Internet.

As organisations look towards data to track consumer patterns and guide business direction, they should also be mindful of the legal regulations that govern the protection of data and the possibility of a data breach. In the past year, we have seen some of the largest data breaches in history with millions of accounts compromised and the release of personal data such as addresses and telephone numbers for sale on the black market.

Such high-profile data breaches have been increasing in size and prevalence in recent years, with cyber criminals (and even state actors) taking keen interest in obtaining sensitive corporate and personal information. Besides such hacking attacks, a data breach can also arise from employee mischief or neglect, an inadvertent leak, lack of or failure in security measures, just to name a few.

ADVERTISING

inRead invented by Teads

Regardless of the cause, the threat of data breaches is imminent and can have severe repercussions for organisations, especially if they are found guilty of failing to take sufficient measures to secure their data.

Singapore's data protection law has one of the highest fines in Asia with each breach subject to a potential fine of S$1 million. Similarly, breaching Europe's new General Data Protection Regulation can result in a fine of the larger of either 20 million euros (S$30.7 million) or 4 per cent of the organisation's global annual turnover.

SEE ALSO: Threat of cyberattack is biggest fear for businesses: survey
Beyond financial penalties, a data breach can cause irreversible damage to a company's reputation as well as potentially significant damages payable in civil liability to third parties, not to mention possible personal criminal liability for senior management.

Ensuring compliance in an evolving landscape

Organisations should be well aware of the prevailing legal regulations that govern ever growing popular technology solutions such as cloud storage, collection, analysis, and offshore storage of customer data.

Here are a few tips for organisations to ensure that they comply with the legal regulations where they operate in.

- *Have a clear understanding of how personal data is used and managed in the organisation*

Some questions that business leaders need to ask include what personal data has been collected, who has access to this data, whether the purposes of processing of such personal data are lawful, where and how it is kept and secured, and how long such personal data is kept on file. In some instances, data storage and protection is managed on behalf of an organisation by an outsourced service provider.

Organisations need to ensure that they understand the level of protection to the data provided by the outsourced service provider and ascertain whether regulations, including sector-specific ones, permit offshoring or cross-border data sharing. In some countries, there appears to be a growing trend of data localisation which means organisations are not permitted to transfer any such data overseas. Data protection regulations in Asean countries are also set to develop in future in light of commitments arising from the formation of the Asean Economic Community (AEC) in end-2015 and the continued digitalisation of everything. Singapore, Malaysia and the Philippines are currently the only countries with dedicated robust data protection laws, and it is only a matter of time before the rest of the Asean countries follow suit, with significant implications for foreign organisations operating in those countries.

- *Conduct regular audits and penetration testing*

The authorities do recognise the fact that cyber criminals often use sophisticated measures in their attacks. However, as seen with the many data breaches around the world, it is most often the case that the organisation itself has failed to have sufficient security measures in place. It is also a known fact that many organisations are not doing enough to protect customer data or their important data. At the bare minimum, organisations need to meet the regulatory standards for data protection and compliance. Beyond this, they should also conduct regular audits and security assessments such as penetration testing, to ensure the integrity of their security framework and that employees are abiding by set guidelines, especially when handling sensitive information.

- *Be willing to seek external advice*

By working closely with professionals such as specialised lawyers with the relevant expertise, organisations will be able to have a better understanding of other factors that could affect their business decisions, such as a digital transformation initiative to move data to the cloud. Legal advice is also important for organisations that operate in a highly regulated industry, such as financial institutions, which could have sector-specific laws that add on a further layer of compliance by the organisation. In the event of a data breach or cyberattack resulting in leaked data, that organisation would suffer the brunt of not only data protection laws but also sector-specific laws.

Ultimately, the burden of cybersecurity falls on the organisation itself, and regulations call for them to ensure that sufficient security measures and practices are put in place. The proper use, storage, and security of data should not be seen solely as the responsibility of "a few good men" within the organisation such as the IT head or the data protection officer, but rather as a culture that permeates throughout the entire organisation.

New technological innovations have the potential to disrupt current practices and pose challenges for security management, but with the right data protection measures in place, organisations will be able to take full advantage of these to drive their business forward.

- **The writer is partner and deputy head, Technology, Media & Telecommunications, at Rajah & Tann LLP. He will be speaking at CommunicAsia2017 Summit on May 24 on the topic "Grappling with the Internet of Things, Disruptive Technology, Cloud of Things and Data Privacy"**

DATA PROTECTION DATA BREACHES

MORE FROM THE BUSINESS TIMES

Adidas strikes gold by turning 40-year-old vintage into hipster shoes
May 04, 2017

Alphabet loves Google CEO so much he gets hundreds of millions
Apr 29, 2017

Dealers slash prices ahead of 600% rise in COE quota for commercial vehicles
Apr 24, 2017

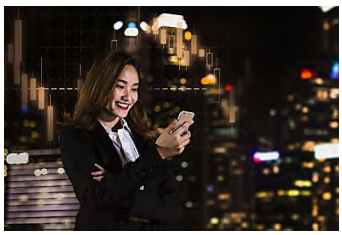
The digital reinvention of an Asian bank
May 02, 2017

FROM AROUND THE WEB

How Older Men Tighten Their Skin
The Modern Man Today

Insider Tips to Set Up A Successful Internet Business
Ace Profits Academy

Why 2017 is the Best Time to Invest in Stocks
valueinvestingcollege.clickfunnels.com



7 Reasons Singaporeans Should Choose To Trade With IG
Create Account on IG now

Recommended by

PRINT ARCHIVE

MON | TUE | WED | THU | FRI | SAT

SUBSCRIBE TO THE BUSINESS TIMES NOW : CALL +65 388 3838 | BTSUBSCRIBE.SG

© 2017 SINGAPORE PRESS HOLDINGS LTD. REGN NO. 198402668E