Crowe

Safekeeping Company Data in the IoT Era

An Article By Amos Law, Executive Director, Risk Advisory

Audit / Tax / Advisory

Smart decisions. Lasting value.

Is your data at risk of being stolen?

The frequency and scale of data breaches have reached unprecedented levels in recent years – to the extent that there is no need to look far for horror stories. In October 2017, it was discovered that the personal data of 46 million mobile users registered in Malaysia had been leaked and put up for sale online.[1]

More than a year on, and the perpetrators have still not been found, no reparations have been made, and the trail appears to have gone cold. What has been unearthed is that the leak may not have been from any of the 12 telecommunication companies affected, but instead from a subcontractor of the regulator -- Malaysian Communications and Multimedia Commission.

Not only did this contractor have access to personal data of practically every single Malaysian to run a blocking service for deactivated numbers, that service was not even operational at the time the leak was discovered.[2]

The data leak also included 81,309 records from the Malaysian Medical Council, Malaysian Medical Association, and Malaysian Dental Association -- taking privacy violations to a new level.[3]

With the increase of smart devices and Internet of Things (IoT) applications that blur the lines between personal and work i.e. work phone vs personal phone, corporations are potentially exposed to malicious hackers on even more fronts than before.

3,353,172,708

Compromised Data

Records Lost or Stolen

18,525,816 **every day**

771,909 **every hour**

12,865 **every minute**

214 **every second**

In its Breach Level Index covering cases in the first six months of 2018, digital security firm Gemalto[4] found that of the 944 incidents recorded worldwide, the majority of breaches were identity thefts (65%) and perpetrated by malicious outsiders (56%). The index also showed that Asia Pacific (APAC) accounted for 338 of those incidents, second only to North America at 559.

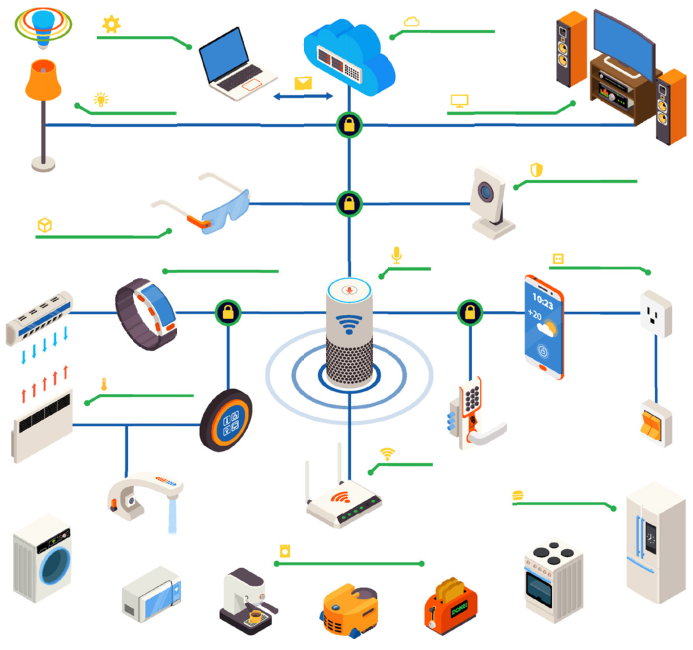
Majority of Breaches were ...

65% Identity Thefts

56% Malicious Outsiders

Hackers are not only gunning for bigger and more valuable troves of data, but are also taking advantage of countries and companies in APAC that are investing in new technologies like IoT, machine learning, and big data without upgrading cyber security technologies to cater to new exposure outlets.

The Internet of Things (IoT)



This is a two-fold problem for many Malaysian corporates – not only does identity theft open businesses to legal liability for contravening data protection and privacy laws that are sweeping the region, but breaches substantially erode customer and other stakeholders' trust.

Cybersecurity Ventures sees digital crime losses passing US$6 trillion by 2021, double the losses in 2015. Cisco expects these losses to include attacks against IoT devices, of which there will be 26 billion in 2020 (three times the global population). Many IoT devices have small operating systems, where security is an afterthought. With cybersecurity, prevention is infinitely better than cure.[5]

The Four Measures that go a long way in preventing breaches

Spend your security dollars wisely. Corporations may be spending more year-on-year on cybersecurity, but these new investments are not going to make a jolt of difference if they are still predicated on the old-fashioned notion of perimeter i.e. protecting your hardware via anti-virus and firewalls. Since the traditional perimeter of the enterprise has been blown up by the cloud, the new perimeter is the data itself and the users accessing that data. Secure the cloud.

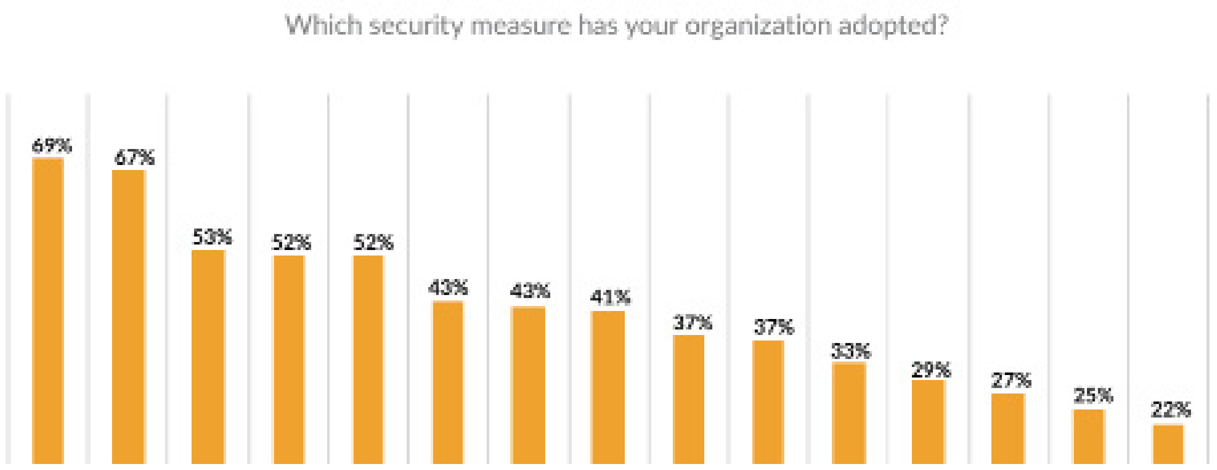
Human errors and poor security practices continue to be a major source of data breaches. Bolster internal security by training employees on cybersecurity measures – and not just at the yearly briefing. Create a reporting culture, and likewise, share and escalate significant breaches to regulators or other authorities. Where possible, share insights and best practices with industry groups.

Encryption can render sensitive data unreadable to attackers when enabled. Gemalto's first half of 2018 Breach Level Index discovered that only 2.2% of data breached globally during the period was encrypted– and thus rendered useless to hackers ("secure breaches").

Access Management including two (or multi)-factor authentication: Just as online banking may require your password as well as a one-time pin, so too can multi-factor authentication be introduced for apps or platforms. In addition, businesses should reduce exposure by limiting access to applications or platforms to only the necessary people.

In addition to these general strategies, consider investing where necessary in more advanced protection technologies such as biometrics and anti-ransomware. Above all, always keep 3 steps in mind:

1. Encrypt all sensitive data at rest and in motion
2. Securely store and manage all of your encryption keys
3. Control access and authentication of users



Title: Cybersecurity measures by APAC organisations
Source: The State of Cybersecurity in Asia-Pacific 2017 whitepaper[6]

With agile new entrants constantly disrupting industries, corporations must equip themselves with knowledge, experience and tools that will keep their infrastructure and information safe, as well as compliant with data and privacy regulations.

Those that do not will be doing so at their own peril.

References

1. BBC. (2017, Oct 31). Malaysian data breach sees 46 million phone numbers leaked. From BBC.com: https://www.bbc.com/news/technology-41816953

2. FMT Reporters. (2017, Nov 28). MCMC contractor under probe over data leak, says report. From Free Malaysia Today: https://www.freemalaysiatoday.com/category/nation/2017/11/28/mcmc-contractor-under-probe-over-data-leak-says-report/

3. Tan, R., & and Nair, S. (2017, Oct 31). M'sia sees biggest mobile data breach. From The Star Online: https://www.thestar.com.my/news/nation/2017/10/31/msia-sees-biggest-mobile-data-breach-over-46-million-subscribed-numbers-at-risk-from-scam-attacks-an/

4. Gemalto NV. (2019). Breach Level Index 2018 First Half Review: Data Privacy and New Regulations Take Center Stage. Amsterdam: Gemalto NV.

5. Cybersecurity Ventures. (2019). Cybercrime Damages $6 Trillion By 2021 . From Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

6. Palo Alto Networks, Inc. (2017). The State of Cybersecurity in Asia-Pacific . Santa Clara, California: Palo Alto Networks, Inc. From https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/the-state-of-cybersecurity-in-asia-pacific.pdf

Crowe

Contact Us

Crowe Governance Sdn. Bhd.
Level 13, Tower C,
Megan Avenue 2,
12 Jalan Yap Kwan Seng,
50450 Kuala Lumpur

Tel. +603 2788 9999

Amos Law
Executive Director,
Risk Advisory
amos.law@crowe.my

About Us

About Crowe Malaysia PLT
Crowe Malaysia PLT is the 5th largest accounting firm in Malaysia and an independent member of Crowe Global. The firm in Malaysia has 13 offices, employs over 1,200 staff, serves mid-to-large companies that are privately-owned, publicly-listed and multinational entities, and is registered with the Audit Oversight Board in Malaysia and the Public Company Accounting Oversight Board in the US.

About Crowe Global
Ranked 8th largest accounting network in the world, Crowe Global has over 250 independent accounting and advisory firms in 130 countries. For almost 100 years, Crowe has made smart decisions for multinational clients working across borders. Our leaders work with governments, regulatory bodies and industry groups to shape the future of the profession worldwide. Their exceptional knowledge of business, local laws and customs provide lasting value to clients undertaking international projects.

www.crowe.my

Crowe Malaysia PLT is a member of Crowe Global, a Swiss verein. Each member firm of Crowe is a separate and independent legal entity. Crowe Malaysia PLT and its affiliates are not responsible or liable for any acts or omissions of Crowe or any other member of Crowe and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe or any other Crowe member.