# Cyber-resilience in the age of digital

Written by The Economist INTELLIGENCE UNIT

Foreword by Rama Sridhar, executive vice-president, digital and emerging partnerships and new payment flows, Asia-Pacific, Mastercard

**The emerging digital democracy in Asia is bringing viral development and optimism to Asia's middle class and the underserved. Regulators across Asia-Pacific have also enthusiastically and firmly adopted "digital nation" agendas, further driving digitalisation.**

Billions of people, millions of small and medium-sized enterprises (SMEs), and thousands of corporations in this part of the world are all witnessing a growth revolution empowered by cheap smartphones, robust telecom infrastructure and the thriving technology platforms that are bringing them more convenience, control and choice. The Internet of Things (IoT) and artificial intelligence (AI) are further changing the way we live and do business—mostly for the better.

As an eternal optimist, I could stop here. But for an honest debate, the counter point is crucial. Numbers mislead, particularly when we examine the diversity of economies around the region. There are still large segments of consumers and institutions that haven't gone digital. Why would that be?

Fear is the oldest and most primal deterrent to the adoption of change and, for many, the fear of going digital is a real impediment. Is this fear of going digital justified?

It is when you acknowledge that while many technology companies are providing convenience, they also have access to vulnerabilities they can exploit. They are tracking your phone when you're not in an app or collecting more of your private data than needed. Home assistants store private conversations, security cameras have flaws, and data breaches occur at companies that have your personal information. Cybercrime targets the defenceless and the vulnerable, and malware attacks all discreetly and collectively reinforce the "digital-phobia" factor. Even blockchain technology, which offers immutability as its USP, has been discovered to store illegal content and hence can be as much part of the problem as a solution. Unquestionably, all of this justifiably undermines our trust in technology.

The need to discuss cyber-security risk is admittedly not original, and the above is but a summary of the terabytes of information available on the subject. However, much still has to be done to put the topic to rest.

Specifically, a three-pronged strategy is required across the ecosystem to fully address the security debates that underpin all digital fears.

1. **Protect personal and private information:** responsible behaviour from companies that collect personal data is critical to easing consumer fears. They must invest in adequate processes, technology and security standards when collecting information from individuals. Likewise, consumers must be cautious about indiscriminately sharing passwords and using weak passwords that compromise personal and private information.

2. **Secure all digital transactions:** to prevent the compromise of a financial transaction at any point in its path, payment systems need to avoid weak authentication methods, unsecured transmission of data across devices and the ecosystem, lack of digital identity certification, and differing standards in financial and non-financial messages and proprietary message protocols.

3. **Defend against attackers:** security infrastructure deployed across multiple components of a value chain can create a risk to the data embedded in any transaction as it flows across its member components. IoT, seamless connectivity across devices, cloud and enterprise resource planning systems, while creating efficiencies, also multiply the risk of a security breach. The connections between devices must be defended.

My vision for a vibrant, open, global and interoperable digital democracy includes a reality where consumer consent to data usage is a fundamental citizen right. Each country's infrastructure includes digital identity services to all—individuals, SMEs and corporates—and national defence strategies include rigorous cyber-security plans. The judicial laws also provide for an ethical and legislative framework to monitor and penalise cyber-criminals and the negligent. All of this will put to rest all citizens' fears of the digital dimension.

A utopian reality? Not really, the region just needs a revolution in policy, education, infrastructure and intent.

## ABOUT THE RESEARCH

*Cyber-resilience in the age of digital* is part of a three-part research programme written by The Economist Intelligence Unit and commissioned by Mastercard, titled *The future of digitalisation in Asia: The challenges and opportunities ahead*.

We would like to thank the following experts for contributing their time and insights:

- Carolyn Chin-Parry, former chief digital officer, Prism
- Paul Jackson, managing director, APAC cyber risk practice leader, Kroll

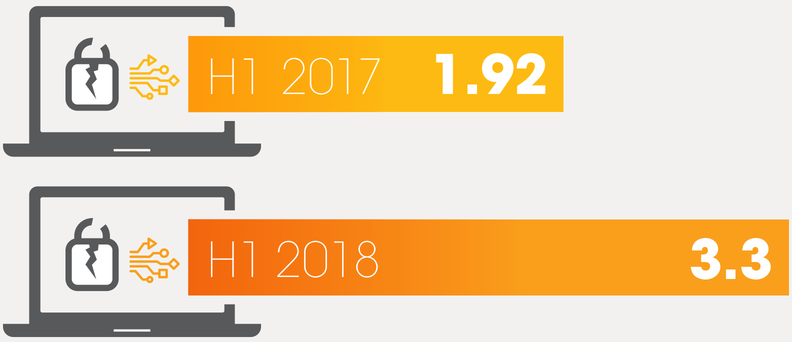
This report was written by Richard Hartung and Michael Gold, and edited by Charles Ross. HuiQi Yow provided editorial support.

## TAKING THE GOOD WITH THE BAD

**While digital commerce and mobile connectivity are changing lives in positive ways, they also bring significant risks**

While digital commerce and mobile connectivity are changing lives in positive ways, they also bring significant risks. Demonstrating the scope of the issue, digital security firm Gemalto found that 945 data breaches in the first half of 2018 led to 3.3bn data records compromised worldwide, an increase of 72% from the same period in 2017.[1] At the same time, according to research commissioned by Microsoft, 60% of retail organisations in Asia-Pacific are slowing digital transformation projects due to a fear of cyber-attacks, which may cost them millions in direct and indirect economic losses.[2] Along with the bottom-line effects, these cyber-attacks have a significant reputational impact.

**Figure 1: Number of data records compromised worldwide (bn)**



Data protection is now no longer solely the remit of the security community, but draws attention from actors across the spectrum, from consumers—for whom increasingly high-profile data breaches are testing their faith in large firms' trustworthiness—to politicians, who are rolling out regulations like the EU's comprehensive General Data Protection Regulation (GDPR) in order to bring greater order to a data-driven era. Companies that fail to enact robust policies and practices around data-gathering and use—or worse yet, that view data protection as merely an afterthought—are taking a huge risk.

The issue is not that companies are doing nothing but, as consulting giant PwC found, the nature of cybercrime is constantly changing and the approaches companies use to manage them have not

[1] "Data Breaches Compromised 4.5 Billion Records in First Half of 2018", Gemalto, October 9th 2018, https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx

[2] "60 percent of retail organisations in Asia Pacific delay digital transformation progress due to cybersecurity concerns", Microsoft, January 15th 2019, https://news.microsoft.com/en-sg/2019/01/15/60-percent-of-retail-organisations-in-asia-pacific-delay-digital-transformation-progress-due-to-cybersecurity-concerns/

From a regulatory perspective, the Asia-Pacific region is taking a different approach from Europe

kept pace.[3] Key risks for companies today encompass a wide variety of everyday activities—often no more complex than opening an email. Malware and ransomware, not typically part of the everyday lexicon of non-IT staff, can constitute significant threats if allowed to spread within a company's digital arteries. Moreover, these cyber-risks are still primarily seen as IT rather than business concerns, and their management is limited to technical fixes of keeping unauthorised users out of a system rather than dealing with rapidly evolving challenges.

## A PROBLEM IN NEED OF A SOLUTION

From a regulatory perspective, the Asia-Pacific region is taking a different approach from Europe. Governments throughout Asia—such as Australia, the Philippines and South Korea— are implementing new laws aimed at the protection of personal data, observes Paul Jackson of risk consultancy Kroll. He notes that various regulators, such as the Hong Kong Monetary Authority and the Monetary Authority of Singapore, are either enforcing mandatory requirements to self-assess and uplift cyber-security among member firms or issuing guidelines and recommendations. For example, the Hong Kong Securities and Futures Commission has outlined the guidelines for reducing and mitigating hacking risks associated with internet trading, although they are not enforced.[4] These new laws and guidelines are already driving significant change across the region, he says.

However, governments in the region are largely unco-ordinated in their regulations. No one should expect Asia to roll out its own version of the GDPR anytime soon, but regional bodies have been issuing guidelines and strategies for greater international collaboration on cyber-security. The Asia-Pacific Economic Co-operation, for example, has implemented a rulebook for protecting online consumer privacy, subscribed to by a number of regional economies. Under this framework, organisations and companies in the participating jurisdictions are evaluated against set criteria and awarded certifications if they qualify.[5] Meanwhile, the Association of Southeast Asian Nations issued a manifesto on personal data privacy in 2016, meant to upgrade the political body's digital economy into one that is "secure, sustainable and transformative".[6]

[3] *Building a Cyber Resilient Financial Institution*, PwC, 2018, https://www.pwc.com/my/en/assets/publications/2018/aicb-pwc-publication2.pdf

[4] *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*, Hong Kong Securities and Futures Commission, https://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf

[5] Business, Cross Border Privacy Rules System, http://cbprs.org/business/

[6] *ASEAN telecommunications and information technology ministers meeting (TELMIN) framework on personal data protection*, Association of Southeast Asian Nations, November 25th 2016, https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf

Companies need to embed security into everything that they do and instil a "security first" mind-set that extends protection beyond the boundaries of the enterprise

## IN SAFE COMPANY?

Companies should not wait for governments to act, however, but should develop effective cyber-resilience strategies that go beyond technical cyber-security.

Mr Jackson notes that implementing a cyber-security strategy needs to start from the top, with a vested interest from the leadership that then trickles down throughout the organisation. "It all starts with the employee," he says, listing social engineering, mistakes made by IT in configuring the systems, and lack of maintaining and updating systems among the biggest risks simply implementing two-factor authentication across the board for all access to information and e-mail would solve many problems immediately. While companies are spending on cyber-security, he says it's out of proportion to employee education. Companies need to embed security into everything that they do and instil a "security first" mind-set that extends protection beyond the boundaries of the enterprise, he says.

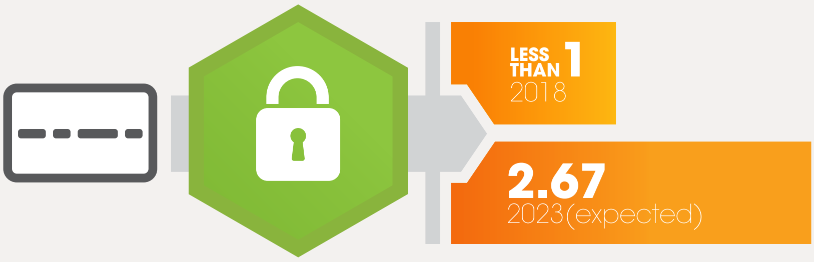
They should also make sure customers truly understand what is happening with their data and teach them how to protect themselves. Indeed, as social media increasingly fuels interaction between companies and consumers online, an emerging challenge for businesses and regulators alike will be to balance corporate and consumer rights and obligations. According to Carolyn Chin-Parry, former chief digital officer of Prism, a large South-east Asian conglomerate, consumers expect companies to protect them and place their trust in the organisations to do the right thing. However, many consumers are not reading the fine print of online agreements and do not proactively review their privacy and security settings. Indeed, most online offerings contain language to the effect that it is the consumer's responsibility to update passwords and privacy settings.

## AN EXPANDING TOOLKIT

While companies come to terms with the rise in cyber-threats, they also need to move quickly to keep up with highly sophisticated cyber-criminals who are likely to launch even more complex attacks. A number of tools are emerging to combat these issues, from machine-learning algorithms that crunch a huge number of data points to detect unusual behaviour in a network, to blockchain-based solutions, which can, in theory, enable a near-unassailable record of a transaction. In the payments space, a process known as tokenisation can secure the movement of money by replacing the payer's account number with a digital "token" restricted to their specific device; the overall market in tokenisation services is expected to rise to US$2.67bn by 2023, from less than US$1bn in 2018.[7]

**Cyber-criminals will soon use AI to design their evasion techniques that enable them to avoid detection and circumvent security**

**Figure 2: Market in tokenisation services (US$bn)**



However, hackers are looking to new technologies as well. For example, software provider McAfee expects that cyber-criminals will soon use AI to design their evasion techniques that enable them to avoid detection and circumvent security.[8] And voice-controlled digital assistants such as Alexa and Siri represent a new opportunity for cyber-criminals to develop malicious code designed to attack both IoT devices and the digital assistants that talk to them.

As a result, technical fixes and solutions will only succeed if underpinned by a wide-ranging, co-ordinated approach from stakeholders at all levels: governments, consumers and companies, including senior management and rank-and-file employees. "The key message is that no organisation or individual can prevent a cyber-attack from happening," says Ms Chin-Parry. "The question is what type of protection, process and policy you have in place."

[7] "Tokenization Market worth $2,670 million by 2023", MarketsandMarkets, https://www.marketsandmarkets.com/PressReleases/tokenization.asp
[8] "McAfee Labs 2019 Threats Predictions Report", McAfee Labs, November 29th 2018, https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions

Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out herein.