Cybercrime in the Digital Age
Thio Tse Gan, Southeast Asia Cyber Risk Leader
20 July 2017
Global trends & outlook
Cyber-attacks are on the rise

$450 bn\textsuperscript{[1]} was the global cost of cybercrime in 2016.

73%\textsuperscript{[2]} of breaches were financially motivated.

66%\textsuperscript{[2]} of malware was installed via malicious email attachments.

99\textsuperscript{[5]} Global average no. of days attackers maintained presence after infiltration and before detection.

81%\textsuperscript{[2]} of hacking-related breaches leveraged either stolen and/or weak passwords.

43%\textsuperscript{[2]} of breaches used social techniques.

8%\textsuperscript{[2]} of breaches involved any physical actions.

$221\textsuperscript{[3]} Per capita cost of data breach was highest in US in 2016.

2016 Data Breaches By Industry\textsuperscript{[4]}

- Healthcare
- Government
- Financial Services
- Technology
- Retail
- Education
- Hospitality

\textsuperscript{[1]} Hiscox Cyber Readiness Report 2017; \textsuperscript{[2]} Verizon 2017 Data Breach Investigations Report; \textsuperscript{[3]} Ponemon 2016 Cost of Data Breach Study: Global Study; \textsuperscript{[4]} Gemalto Breach Level Index Report 2016; \textsuperscript{[5]} Mandiant M-Trends 2017
Daily Data Breach Statistics – breachlevelindex.com (March Data)

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

5,911,431,189,1

ONLY 4% of breaches were “Secure Breaches” where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

- EVERY DAY: 3,876,349 Records
- EVERY HOUR: 161,515 Records
- EVERY MINUTE: 2,692 Records
- EVERY SECOND: 45 Records
Daily Data Breach Statistics – breachlevelindex.com (15 July)

DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013

9,011,944,056

ONLY 4% of breaches were “Secure Breaches” where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

- EVERY DAY: 5,441,995 Records
- EVERY HOUR: 226,750 Records
- EVERY MINUTE: 3,779 Records
- EVERY SECOND: 63 Records
It is really part of our daily lives

Threat landscape
**COMMENTARY**

Singapore fends off ransomware, but needs to be ready for APTs

**Pirates Of The Caribbean pirated**

The Lazarus Group, acting for impoverished North Korea, has been more brazen in its pursuit of financial gain than others. About two months ago, cyber security company Symantec said it was likely that Lazarus was behind a recent cyber campaign targeting organisations in 31 countries. Researchers have uncovered four pieces of digital evidence suggesting that the Lazarus Group was behind the campaign that sought to infect victims with ‘loader’ software used to stage attacks by installing other malicious programs, Symantec said in a blog.

“We are reasonably certain” that Lazarus was responsible, Symantec researcher Eric Chien said at the time, according to a Reuters report. In February last year, cyber security firms said Lazarus was behind the theft of US$1 million (S$1.1 million) from the central bank of Bangladesh. In that heist, the hackers stole the money from an account that Bangladesh held with the Federal Reserve Bank of New York and transferred it electronically to accounts in the Philippines. The most high profile hacking was in November 2014, when Sony Pictures Entertainment’s network was crippled for weeks. Embarrassing e-mail messages and personal details about movie stars were exposed. It was believed to be in retaliation for Sony’s release of The Interview, a political satire about a fictional plot to kill North Korean leader Kim Jong Un. Sony initially withdrew the film but eventually released it on Christmas Day that year. **REUTERS**
Why?
Attack lifecycle and speed of attack

- Info gathering
- Asset discovery
- Initial invasion
- Asset capture
- Compromise
Implications
“Above the surface” are direct costs commonly associated with data breaches.

“Beneath the surface” are potential impacts that are less understood and rarely revealed to the public eye, many of which are intangible costs that are difficult to quantify, including damage to trade name, loss of intellectual property, or costs associated with operational disruption.
The long trail of cyberattack impacts…

Beyond the initial incident triage, there are impact management and business recovery stages. These stages involve a wide range of business functions in efforts to rebuild operations, improve cybersecurity, and manage customer and third-party relationships, legal matters, investment decisions, and changes in strategic course.
What’s the context
Industry 4.0
Introduction...

[Diagram showing various technological developments and their impact on industry and society]

The human factor
Technological development feeds and enables various trends in society:
Democratisation, social connection, DIY, Decentralisation

[Image of book cover: The Fourth Industrial Revolution by Klaus Schwab]
The 6 D’s of Diamandis and Kotler

- **Digitalization** – Once a technology becomes digitalized, the door is opened to an exponential growth curve (e.g. doubling price/performance every x months).
- **Deceptive** – In the early stages of the technology, it takes a while to get up to speed. In this phase, growth patterns look deceptively linear. In this phase, the technology can be seen as a hype.
- **Disruption** – In the next phase, and often unexpectedly, the technology plays a role in disrupting established industries.
- **Dematerialization** – Many technologies that were expensive in the 1980s or 1990s now come for free in the form of an app on the smartphone. People do not buy a camera, GPS device, music player anymore because it is already available on their smartphone. Physical devices are dematerializing into digital apps.
- **Demonetization** – As a consequence of the D’s before, money is taken out of the equation as technologies become cheaper and cheaper and cheaper. Existing business models evaporate as established revenue streams disappear.
- **Democratization** – As technology becomes cheaper and cheaper, access becomes available to anyone. Powerful technology is not only available for the wealthiest, but is democratized as large parts of the population gets their hands on it.
Innovation Technologies...
What are your concerns?
What are the topics that impacts the CFO

- Robotics
- Cloud
- IoT
- Awareness
Can you see it? Do you own it?

It's in the Cloud.
Software as a Service (SaaS)

Increased Processing Power

Access Anywhere

Increased Memory

Distributed Collaboration

Benefits…
• Weak identity, credential and access management
• Insecure interfaces and APIs
• System and application vulnerability
• Account hijacking
• Malicious insiders
• Advanced persistent threats

• Data breaches
• Data loss
• Insufficient due diligence
• Abuse and nefarious use of cloud services
• Denial of service
• Shared technology issues
Cost of IP Breach

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.

- Post-breach customer protection
- Regulatory compliance
- Public relations (PR)
- Attorney fees and litigation
- Cybersecurity improvements
- Loss of intellectual property (IP)
- Devaluation of trade name
- Value of lost contracts
- Lost value of customer relationships
- Impact of operational disruption or destruction
- Increased cost to raise debt
- Insurance premium increases
- Customer breach notification
- Technical investigation

Above the surface: Better-known cyber incident costs
Below the surface: Hidden or less visible costs
Robots?

Robotic Process Automation.
Functions of software robots...

- Opening emails and attachments
- Logging into web/enterprise applications
- Moving files and folders
- Scraping data from the web
- Connecting to system APIs
- Following “if/then” decisions and rules
- Extracting and reformatting data into reports or dashboards
- Extracting structured data from documents
- Collecting social media statistics
- Merging data from multiple places
- Making calculations
- Copying and pasting data
- Filling in forms
- Reading and writing to databases
Benefits...

Cost Savings
Decreased Cycle Times
Flexibility and Scalability
Improved Accuracy
Improved Employee Morale
Detailed Data Capture
Video: How does Robotic Process Automation work?
RPA can make big errors fast or allow small errors to go undetected....
Is it connected?

Internet of Things.
By 2025, approximately 80 billion devices will be connected to the Internet

...approximately 4,800 devices are being connected to the network as we speak. Ten years from now, the figure will mushroom to 152,000 a minute

- Forbes
Applications

- Warehousing
- Remote patient monitoring
- Adaptive Traffic control
- Security Monitoring
- Restocking of shelf
- Building IoT (parking / charging station)
- Building Biometrics (access / smart workspaces)
Video: Data security and the Internet of Things

[Click on the screenshot to view the video on YouTube]
IoT Botnet used to attack and disable Dyn – a critical DNS (directory) authority
Owlet Baby Wi-Fi Monitor...

“Worst IoT Security Of 2016”
a team of researchers was able to take total control of a Jeep SUV using the vehicle’s CAN bus
Video: Hackers Remotely Kill a Jeep on the Highway

[Click on the screenshot to view the video on YouTube]
Final Thoughts.
No such thing as hacker proof

.... if you build it they will come
US health insurer

In May, the company learned that a laptop containing 2.8 million of its personal health information (PHI) records had been stolen from the company’s health care analytics software vendor.
US technology manufacturer

After significant research, development, production, and marketing, the company was six months from a major release of a core product line that supports IoT environments. Earlier versions were deployed in the field for over 12 months across the government, transportation, utilities, smart home, and smart city sectors, and among service providers who support customers in those sectors. The company was informed by a federal agency that the company’s infrastructure was breached by a foreign nation-state. An investigation revealed exfiltration of IP related to multiple product lines and confirmed that 15 of the company’s 30 device product lines were impacted.
• Who is responsible?

• How do we prepare for the impending compromise with adoption of new technology

• What can be done to minimize the risk?
“Cyber literacy can be considered similar to financial literacy,” observed one director.

“Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business.”
11 Questions
Can you answer these questions about your organization?

Do we treat cyber security as a business or IT responsibility?

Do our security goals align with business priorities?

How integral is security in our business culture?

Do we have the basics right? (control over access rights, shared drives, software patching, vulnerability management, virus outbreaks, regulatory security requirements and data leakage prevention?)

How are our third parties securing our most valuable information?

Have we identified and protected our most valuable processes and information?

Are we comprehensively compliant?

How do we evaluate the effectiveness of our security?

How do we monitor our systems and prevent breaches?

What is our plan for responding to a security breach?

Are we adequately resourced and insured?
Contact Information

Our services are offered through a hybrid approach that is a fit-for-purpose combination of advice, implementation and managed security services customized to specific client needs.

To learn more please contact one of our leaders:
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 290 partners and over 7,400 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region. All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2017 Deloitte & Touche Enterprise Risk Services Pte Ltd