

IS4231

Information Security Management

Lecture 2

Compliance: Law and Ethics

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Email: yanglu@comp.nus.edu.sg :: **Tel:** 6516 6791 :: **Office:** COM2-02-46

Learning Objectives

- ▶ **Compliance**
 - ▶ Professional Ethics
 - ▶ Laws
 - ▶ Sectoral Regulations

I. Professional Ethics



Professional Code of Ethics

▶ ACM Code of Conduct

▶ I. General Ethical Principles

- ▶ I.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
- ▶ I.2 Avoid harm
- ▶ I.3 Be honest and trustworthy
- ▶ I.4 Be fair and take action not to discriminate
- ▶ I.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts
- ▶ I.6 Respect privacy
- ▶ I.7 Honor confidentiality

Professional Code of Ethics

- ▶ ACM Code of Conduct (cont.)

- ▶ 2. Professional Responsibilities

- ▶ 2.1 Strive to achieve high quality in both the processes and products of professional work.
 - ▶ 2.2 Maintain high standards of professional competence, conduct, and ethical practice.
 - ▶ 2.3 Know and respect existing rules pertaining to professional work.
 - ▶ 2.4 Accept and provide appropriate professional review.
 - ▶ 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
 - ▶ 2.6 Perform work only in areas of competence.
 - ▶ 2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.
 - ▶ 2.8 Access computing and communication resources only when authorized or when compelled by the public good.
 - ▶ 2.9 Design and implement systems that are robustly and usably secure.

- ▶ 3. Professional Leadership Principles

- ▶ 4. Compliance with the Code

Professional Code of Ethics

- ▶ International Information Systems Security Certification Consortium, Inc. (ISC)²
 - ▶ www.isc2.org
- ▶ SANS
 - ▶ www.sans.org
- ▶ Information Systems Audit and Control Association (ISACA)
 - ▶ www.isaca.org
- ▶ Information Systems Security Association (ISSA)
 - ▶ www.issa.org

Violation Cases

- ▶ ACM Code of Conduct
 - ▶ 1.3 Be honest and trustworthy

TECHNOLOGY

Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data

[Leer en español](#)

By MIKE ISAAC, KATIE BENNER and SHEERA FRENKEL NOV. 21, 2017



Uber's headquarters in San Francisco. The ride-hailing company said information on driver and rider names, emails and telephone numbers had been compromised in a data breach. Ryan Young for The New York Times

SAN FRANCISCO — Uber disclosed Tuesday that hackers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year after paying a \$100,000 ransom.

The deal was arranged by the company's chief security officer and under the watch of the former chief executive, Travis Kalanick, according to several current and former employees who spoke on the condition of anonymity because the details were private.

The security officer, Joe Sullivan, has been fired. Mr. Kalanick was forced out in June, although he remains on Uber's board.

Uber acquiesced to the demands, and then went further. The company tracked down the hackers and pushed them to sign nondisclosure agreements, according to the people familiar with the matter. To further conceal the damage, Uber executives also made it appear as if the payout had been part of a “bug bounty” — a common practice among technology companies in which they pay hackers to attack their software to test for soft spots.

The details of the attack remained hidden until Tuesday. The ride-hailing company said it had discovered the breach as part of a board investigation into Uber's business practices.

Source: <https://www.nytimes.com/2017/11/21/technology/uber-hack.html?searchResultPosition=1>

RELATED COV



Violation Case

► ACM Code of Conduct

► 1.3 Be honest and trustworthy

Uber to Pay \$148 Million Penalty to Settle 2016 Data Breach

The disclosure came on the heels of a punishing year for Uber, which was wracked by scandal, legal setbacks and an exodus of high-level executives. In September 2017, Uber brought in Dara Khosrowshahi as chief executive from [Expedia Group](#) Inc. to help revamp its image and improve transparency. He [learned of the breach within weeks of taking the helm](#) and disclosed it to investors before the broader disclosure last November.

Uber Chief Legal Officer Tony West wrote Wednesday, in a post on the Uber website, that the company decided to disclose the incident in accordance with principles including transparency and accountability. “An important component of living up to those principles means taking responsibility for past mistakes, learning from them, and moving forward,” Mr. West wrote.

The agreement also requires Uber to adopt better data breach notification and security practices and a corporate integrity program for employees to report unethical behavior, and to hire an independent third party to assess data security practices.

“This record settlement should send a clear message: we have zero tolerance for those who skirt the law and leave consumer and employee information vulnerable to exploitation,” Ms. Underwood, whose office took the lead in the multistate investigatory process, said in prepared remarks. New York will receive about \$5.1 million.

Uber, under Mr. Khosrowshahi, has beefed up its legal team including hiring its first chief privacy officer, chief compliance officer and a chief trust and security officer.



Source: <https://www.wsj.com/articles/uber-to-pay-148-million-penalty-to-settle-2016-data-breach-1537983127>

2. Laws

Information Security and Law

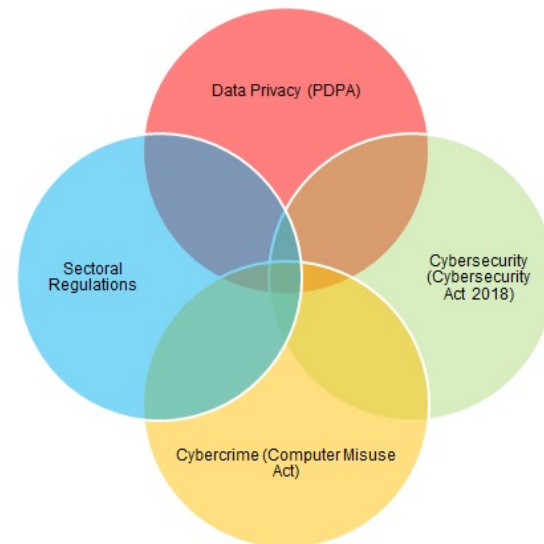
- ▶ A way of **deterrence**
 - ▶ Preventing an illegal or unethical activity
 - ▶ Effectiveness deterrence
 - ▶ Fear of **penalty**
 - ▶ Probability of being caught
 - ▶ **Probability of penalty being administered**

Currently IP infringement laws are ineffective



Cyber Security Legal Framework

- ▶ Businesses will now have to contend with the following in managing cyber risk:
 - ▶ Cybersecurity – the Cybersecurity Act 2018 (if applicable)
 - ▶ Data Privacy – the Personal Data Protection Act 2012 (Act 26 of 2012)
 - ▶ Cybercrime – the Computer Misuse Act (Cap. 50A)
 - ▶ Sectoral Regulations



2.1 Cybersecurity Act

Information Security and Law

▶ Local laws

▶ Cybersecurity Act

first movers in the SEA region

- ▶ March, 2018
- ▶ An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to regulate cybersecurity service providers, and for matters related thereto, and to make consequential or related amendments to certain other written laws.
- ▶ <https://sso.agc.gov.sg/Acts-Supp/9-2018/>



REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

ACTS SUPPLEMENT

Published by Authority

NO. 9]

FRIDAY, MARCH 16

[2018

First published in the Government Gazette, Electronic Edition, on 12 March 2018 at 5 pm.

Cybersecurity Act 2018

▶ Critical information infrastructure (CII)

- ▶ It refers to a computer or a computer system located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore.
- ▶ 11 critical sectors:
 - ▶ Energy
 - ▶ Water
 - ▶ Banking and finance
 - ▶ Healthcare
 - ▶ Land transport
 - ▶ Aviation
 - ▶ Maritime
 - ▶ Info-communications
 - ▶ Media
 - ▶ Security and emergency services
 - ▶ Government

Cybersecurity Act 2018



Strengthen the protection of CII against cyber-attacks.

The Act provides a framework for the designation of CII. It provides CII owners with clarity on their obligations to protect CII from cyber-attacks, and requires the owners to report cybersecurity incidents to CSA.



Authorise CSA to prevent and respond to cybersecurity threats and incidents.

The Act empowers the Commissioner of Cybersecurity to investigate cyber threats and incidents to determine their impact and prevent further harm. These powers are calibrated based on the severity of the threat or incident and the measures required.



Establish a framework for sharing cybersecurity information.

The Act facilitates information sharing, which is critical as timely information helps the Government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request for information, and for the protection and sharing of such information.



Establish a light-touch licensing framework for cybersecurity service providers.

Some cybersecurity services can be sensitive because the service providers performing them would know where the vulnerabilities in clients' computer systems are. Licensing cybersecurity service providers will give businesses and clients more assurance in engaging such services.

Cybersecurity Act 2018

▶ Cybersecurity Commissioner

- ▶ the “Commissioner”, as a regulator for the sector
 - ▶ Has the power to designate any computer or computer systems as CII
 - ▶ The designation is effective for 5 years

▶ Licensing for certain service providers

- ▶ Penetration testing
- ▶ Managed security operation centre (SOC) monitoring service

 This is the light touch - only these 2 services that requires the restriction

Cybersecurity Code of Practice for CII

- ▶ It is intended to specify the minimum protection policies that a CIIO shall implement to ensure the cybersecurity of its CII.
 - ▶ Governance requirements
 - ▶ Authorities, roles, and responsibilities
 - ▶ Risk management
 - ▶ Policies, standards and guidelines
 - ▶ Security by design
 - ▶ Identification requirements
 - ▶ Asset management
 - ▶ Access control
 - ▶ System hardening
 - ▶ Remote connection
 - ▶ Removable storage media
 - ▶ Vulnerability assessment and penetration testing

management structure level

identification requirements

Cybersecurity Code of Practice for CII cont.

- ▶ It is intended to specify the **minimum protection policies** that a CIIO shall implement to ensure the cybersecurity of its CII.
 - ▶ Monitoring and detection requirements
 - ▶ Cybersecurity incident response requirements
 - ▶ Incident
 - ▶ Crisis
 - ▶ Cybersecurity awareness and information sharing requirements
 - ▶ Cybersecurity exercise requirements
 - ▶ Resiliency requirements
 - ▶ Business Continuity (BC) plan
 - ▶ Disaster Recovery (DR) plan
 - ▶ Vendor management

2.2 Personal Data Protection Act 2012

Information Security and Law

▶ Local laws (cont.)

▶ Personal Data Protection Act 2012

- ▶ To govern the **collection, use and disclosure** of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.
- ▶ <https://sso.agc.gov.sg/Act/PDPA2012>
- ▶ <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

PERSONAL DATA PROTECTION ACT 2012

(No. 26 of 2012)

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY



PDPA

▶ Part VI - Care of Personal Data

▶ Accuracy of personal data

- ▶ “An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete”

▶ Protection of personal data

- ▶  An organisation shall protect personal data in its possession or under its control by  making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.”

Use CIA to plan

PDPA

▶ Part VI - Care of Personal Data

▶ Retention of personal data

- ▶ “An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —
 - (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and
 - (b) retention is no longer necessary for legal or business purposes.

▶ Transfer of personal data outside Singapore

- ▶ “An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.”

PDPA2012

- ▶ Data Protection Officer (DPO)
 - ▶ to oversee the data protection responsibilities within the organization and ensure compliance with the PDPA.
- ▶ The possible responsibilities of a DPO may include, but are not limited to, the following:
 - ▶ Ensure compliance of PDPA when developing and implementing policies and processes for handling personal data;
 - ▶ Foster a data protection culture among employees and communicate personal data protection policies to stakeholders;
 - ▶ Manage personal data protection related queries and complaints;
 - ▶ Alert management to any risks that might arise with regard to personal data; and
 - ▶ Liaise with the PDPC on data protection matters, if necessary.

Recent Updates # 1

- ▶ Data Protection for NRIC and Other National Identification Numbers
 - ▶ Apply from Sep 1, 2019
 - ▶ <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf>
 - ▶ “From 1 September 2019, organisations are expected to stop collecting, using or disclosing customers' NRIC and other national identification numbers where it is not required under the law or necessary to establish or verify an individual's identity to a high degree of fidelity.”

Discussion

- ▶ Data Protection for NRIC and Other National Identification Numbers
 - ▶ Scenarios that organizations can collect NRIC number?
 - ▶ 1. Joining an organization as a new employee
 - ▶ 2. Redemption of free parking
 - ▶ 3. Enrolling into a private education institution
 - ▶ 4. Checking into a hotel
 - ▶ 5. Participating in a lucky draw
 - ▶ 6. Online Purchase of movie tickets
 - ▶ 7. Subscribing to a mobile phone line
 - ▶ 8. Seeking treatment at a medical clinic
 - ▶ 9. Submitting feedback or registering interest in a product or service
 - ▶ 10. Signing up for retail membership

Recent Updates #2

▶ PDPA(Amendment) Bill

▶ Effective: 1 Feb 2021

▶ Key amendment that is relevant in security aspect

▶ An increase in the cap on financial penalties

- Previous cap: S\$ 1 million
- Current: 10% of the offending organisation's annual turnover in Singapore if its gross annual turnover in Singapore exceeds S\$10 million, or S\$1 million, whichever is higher.

▶ Data breach notification

- The PDPC – as soon as practicable, no later than 72 hours (3 calendar days) after establishing that the data breach is
 - likely to result in significant harm or impact to the individuals to whom the individual relates, or
 - of a significant scale
 - the breach affects the personal data of 500 or more individuals
- Affected Individuals/Others (e.g., parents of young children) – as soon as practicable

2018 SingHealth Data Breach Case

Singapore

PDPC fines IHiS, SingHealth combined S\$1 million for data breach following cyberattack



SINGAPORE: The Personal Data Protection Commission (PDPC) has slapped a fine of S\$750,000 on IHiS and S\$250,000 on SingHealth for breaching their data protection obligations under the Personal Data Protection Act (PDPA), it said in a statement on Tuesday (Jan 15).

"PDPC's investigations into the data breach arising from a cyberattack on SingHealth's patient database system, found that IHiS had failed to take adequate security measures to protect the personal data in its possession," said the statement.

"PDPC found that the SingHealth personnel handling security incidents was unfamiliar with the incident response process, overly dependent on IHiS, and failed to understand and take further steps to understand the significance of the information provided by IHiS after it was surfaced.

"Even if organisations delegate work to vendors, organisations as data controllers must ultimately take responsibility for the personal data that they have collected from their customers."

These financial penalties are the highest ever imposed by PDPC to date, the commission said. Both organisations are to pay their fines within 30 days.

Source:

<https://www.channelnewsasia.com/news/singapore/ihi-s-singhealth-fined-1-million-data-breach-cyberattack-11124156>

Recent Updates #3

- ▶ Personal Data Protection (Notification of Data Breaches) Regulations 2021
 - ▶ Effective: 1 Feb 2021
 - ▶ Provide that a data breach will be deemed to result in **significant harm** to an individual if it relates to:
 - ▶ Certain prescribed information relating to such individual, including, for example, such individual's full name, alias, identification number, salary or remuneration, income from goods or property sale(s), credit, debit or charge card or bank account number and information that identifies the individual as being subject to certain investigations, arrests, programme, court orders, etc.; or
 - ▶ Both (i) the individual's account identifier (e.g., name or number) and (ii) the password, security code, access code, response to a security question, biometric data or other data used or required to access or use the individual's account with an organisation.

PDPA2012 Application Scope



INLAND REVENUE
AUTHORITY
OF SINGAPORE

PDPA does not apply to IRAS



Text size A A A Singapore Government
Integrity · Service · Excellence

Search



Within IRAS Website

About IRAS · Careers · News & Events · Publications · Useful Links · Contact Us · Feedback · Sitemap



Individuals

Businesses

GST

Property

Other Taxes

Schemes

e-Services

LOGIN

The banner features a laptop screen showing a bar chart with four bars of increasing height, labeled 'JANUARY' and 'DECEMBER'. A magnifying glass is positioned over the chart, highlighting a point labeled '> \$1 million'. To the right of the chart, a blue box contains the text: 'Monitoring your business revenue to determine whether you need to register for GST?'. Below this, it says 'From 2019, do so at the end of every calendar year.' and a 'Learn more' button.

Upcoming
Due Dates
[View all dates](#)

01
MAR

01
MAR

31
MAR

31
MAR

POPULAR

2019 Property Tax Bills
Property Owners

Corporate Tax Filing Season
2018
Companies

Tax Season 2018 – About Your
Tax Bill
Locals

Tax Season 2018 - All You
Need To Know
Locals

Checking if a Business is GST-
Registered
GST-Registered Businesses

Public agency list:

- ▶ <https://sso.agc.gov.sg/SL/PDPA2012-SI49-2013?DocDate=20180329#pr2->

Private companies overseas - even those without a physical office - will be subjected to PDPA as long as they are collecting SG customer data



2.3. Computer Misuse Act



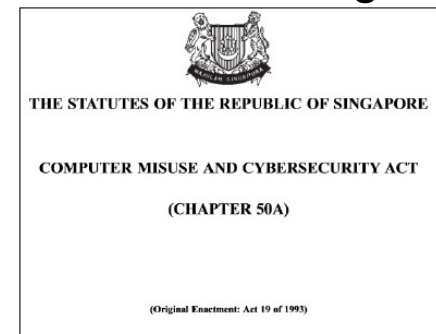
Information Security and Law

▶ Local laws (cont.)

Focus on the individuals instead of the company

▶ Computer Misuse Act

- ▶ An Act to make provision for securing computer material against **unauthorised access or modification**, to require or authorise the taking of measures to ensure cybersecurity, and for matters related thereto.
 - ☐ Hacking/Hacking attempt
 - ☐ Unauthorized
 - ☐ Access/modification/use/interception/obstruction/disclosure
 - ☐ Attacks to protected computers
- ▶ <https://sso.agc.gov.sg/Act/CMA1993?ValidDate=20180831&ProvIds=legis>



Computer Misuse Act

3. Unauthorised access to computer material
4. Access with intent to commit or facilitate commission of offence
5. Unauthorised modification of computer material
6. Unauthorised use or interception of computer service
7. Unauthorised obstruction of use of computer
8. Unauthorised disclosure of access code
- 8A. Supplying, etc., personal information obtained in contravention of certain provisions
- 8B. Obtaining, etc., items for use in certain offences
9. Enhanced punishment for offences involving protected computers
10. Abetments and attempts punishable as offences

Recent Violation

3 men charged with crimes related to obtaining personal details of Singtel, StarHub customers

PUBLISHED DEC 16, 2020, 11:13 AM SGT



SINGAPORE - Three Singaporean men accused of committing crimes related to obtaining personal details of Singtel and StarHub customers appeared before a district court on Wednesday (Dec 16).

[insiders](#)

Two of them, Foo Cheek Ann Kelvin, 32, and Zhang Jiazheng, 38, are said to have used computers at their workplaces to illicitly access the subscriber databases of Singtel and StarHub respectively.

The **third man, Lim Zong Xian Philbert, 33, faces three charges of bribing another man, Lee Cheng Yan, 37, with a total of \$1,000 to get customers' details from the telcos in 2017.**

“We also tightened our systems and processes as well as conducted additional staff awareness training on data protection, to further safeguard StarHub information. As the matter is now before the courts, it is not appropriate for us to comment on the ongoing judicial proceedings,” StarHub added.

Those convicted of using a computer to secure access to data without authority can be jailed for up to two years, fined up to \$5,000 or both. Repeat offenders can be jailed for up to three years, fined up to \$10,000 or both.

For each offence of corruption, offenders can be jailed up to five years, or fined up to \$100,000, or both.

Source:

<https://www.straitstimes.com/singapore/courts-crime/3-men-charged-with-crimes-related-to-obtaining-personal-details-of-telco>

3. Sectoral Regulations



Sectoral Regulations

- ▶  **MAS** Technology Risk Management (TRM) Guidelines
 - ▶ June 2013
 - ▶ A set of best practices that provide financial institutions with guidance on the oversight of technology risk management, security practices and controls to address technology risks
 - ❑ Establishing a sound and robust technology risk management framework.
 - ❑ Strengthening system security, reliability, resiliency, and recoverability.
 - ❑ Deploying strong authentication to protect customer data, transactions and systems.
 - ❑ <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines--21-June-2013.pdf>

Sectoral Regulations

▶ MAS TRM Guidelines

▶ MAS Notice PSN05

- ▶ Notice to operators and settlement situations of designated payment systems, 5 Dec 2019
- ▶ Notice on technology risk management

Technology Risk Management

4 A bank shall put in place a framework and process to identify critical systems.

5 A bank shall make all reasonable effort to maintain high availability for critical systems. The bank shall ensure that the **maximum unscheduled downtime** for each critical system that affects the bank's operations or service to its customers does not exceed a total of 4 hours within any period of 12 months.

6 A bank shall establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The bank shall validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing.

Sectoral Regulations

▶ MAS releases new amendments to TRM Guidelines

▶ 18 Jan 2021

- ▶ The responsibilities of the board of directors (or a committee delegated by it) and senior management in relation to the governance and oversight of technology risk.
 - E.g., a sound and robust risk management framework
- ▶ Secure software development and management
 - Secure by design in Agile software development and DevOps management
- ▶ Managing risks arising from emerging technologies
 - Virtualisation security
 - IoT
- ▶ Access from:
 - <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf>

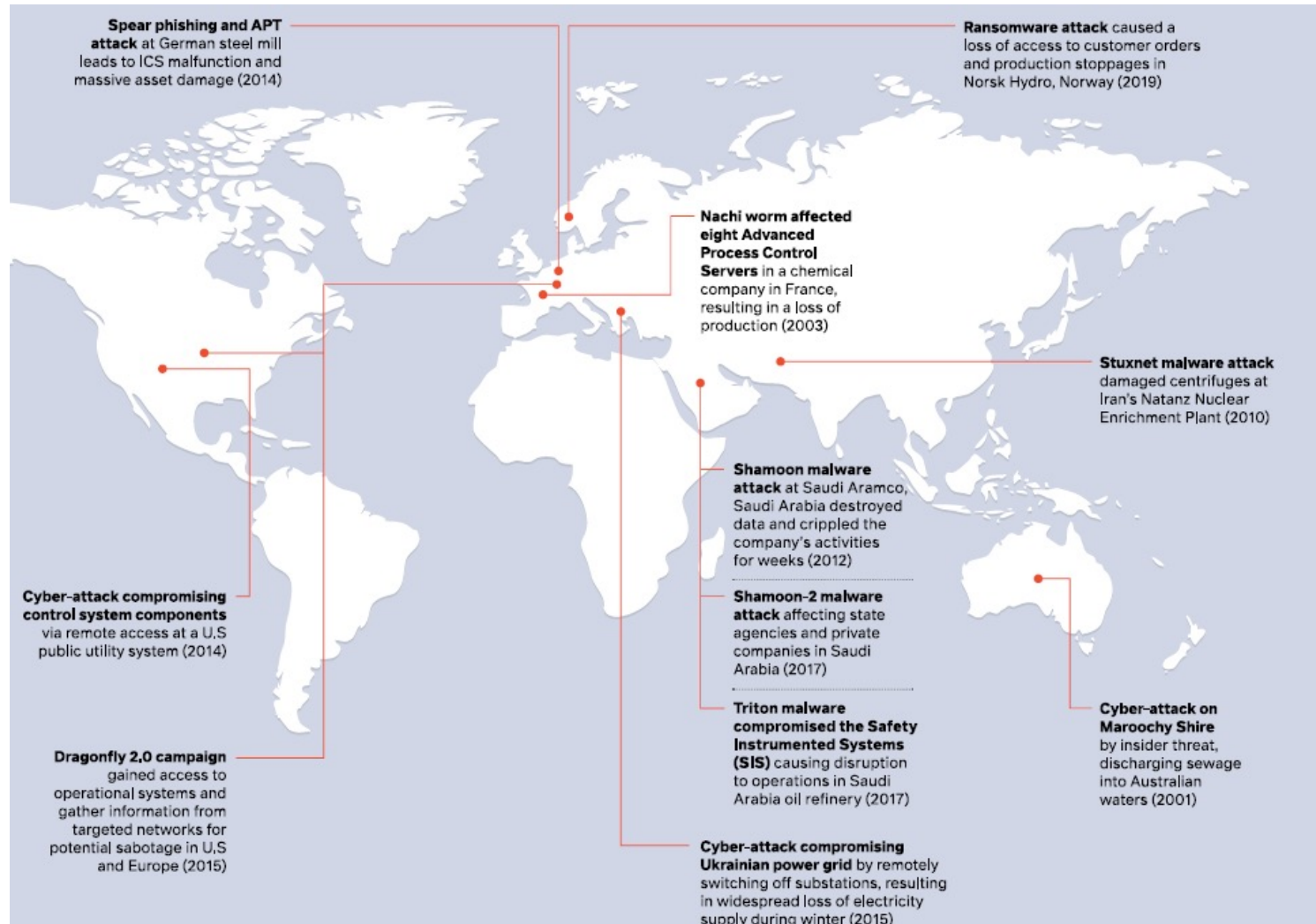
SG's OT Cybersecurity Masterplan 2019

▶ Operational technology (OT)

- ▶ Technologies involving interconnected devices and computers for the monitoring and control of physical processes.
 - ▶ e.g., manufacturing, transportation, energy and water, etc.
- ▶ Focus area: Industrial control systems (ICS)
 - ▶ Industrial automation systems responsible for data acquisition, visualization, and control of industrial processes.
- ▶ Key Thrusts:
 - ▶ OT cybersecurity training
 - ▶ OT cybersecurity information sharing and analysis center
 - ▶ Strengthening policies and processes
 - ▶ Adopting technologies for cyber resilience

same ideas as the Cybersecurity Act

Global OT Cyberattacks



Source: Singapore Operational Technology Masterplan 2019

Norsk Hydro Cyber Attack

How the Norsk Hydro cyberattack unfolded

[Aug 22, 2019 | 04:00 AM](#) | [New York](#) | [Andrea Hotter](#)

How it happened

It was immediately clear from its impact that the attack was highly sophisticated.

Eivind Kallevik, then chief financial officer and recently appointed head of primary metal, was placed in charge of the emergency response.

“While we don’t have any indication as to who was responsible, it was not a teenager sitting in a basement. Getting entry to our systems isn’t easy. It’s quite scary in terms of the time and resources the hackers used to build credentials and gain access,” he told Fastmarkets.

The hackers had chosen their patient zero months in advance: an email conversation with a Norsk Hydro customer. It was not a classic phishing scheme; incredibly, the malicious software was embedded in an attachment that Norsk Hydro would typically expect to receive as part of a legitimate email conversation with a known counterpart.

“It was a Trojan horse giving the attacker a foothold within our company IT infrastructure. It followed the typical pattern of ransomware attacks in that it had been in our systems for a while,” Kallevik said.

Once the attachment was opened, it allowed the hackers access to the Norsk Hydro system. From that point on, the hackers worked their way into the active directory, which identifies each employee by a username and login to determine they are a legitimate person in the organization.

The hackers worked their way up until they had sufficient administrative rights to move around the Norsk Hydro system freely; at that point, they could even create new accounts. The virus was placed throughout the system and eventually launched by a code.

Very difficult to differentiate IT vs OT in our daily lives



Norsk Hydro Cyber Attack cont.

How the Norsk Hydro cyberattack unfolded

[Aug 22, 2019 | 04:00 AM | New York | Andrea Hotter](#)

Production impact

By affecting the company's ability to access its systems, the attack also impacted industrial production at some of Norsk Hydro's sites.

Fortunately, energy, bauxite and alumina managed to run as normal, while the primary metal plants also continue as usual with a higher degree of manual operations. The inability to connect to the production systems had only a limited operational impact on the rolled products operations, which were mostly back to normal within a couple of days.

Badly affected, however, was Norsk Hydro's extruded solutions business, which relies on highly specialized customer-specific data being fetched from the servers detailing what to produce. As a workaround, any orders that the company had access to on paper had to be manually punched into the systems. Once these were fulfilled, production had to stop.

Relying on manual processes is increasingly viewed as old-fashioned. But one member of the Norsk Hydro sales team at a plant in Belgium became an in-house hero when he revealed that he printed out every order and kept the pages in binders. Fortunately for his colleagues, this meant the plant could continue to produce throughout the crisis.

Other plants were not so lucky - some operations had to temporarily halt production from the outset. In some instances, stockpiles were used to service customer orders.

Back at 85-90% capacity in extruded solutions by April 12, it took more than a month to achieve full operation.

Source: <https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html>



Next Week

- ▶ **Planning for Security**
 - ▶ Ch3