

IS4231

Information Security Management

Introduction to InfoSec Management

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

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

Expectations and Perspective

- ▶ In the whole module, we discuss how to better manage information security in an organization at a top manager role.
- ▶ You take the role of the Chief Information Security Officer (CISO) in the organization



|

Learning Objectives

- ▶ Cybersecurity situation background
- ▶ What is information security?
- ▶ What is management?

I. Background

2021 Colonial Pipeline Ransomware Attack

Search

Bloomberg

Sig



Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

5 June 2021, 03:58 GMT+8

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.

The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked, he said. However, Carmakal said he isn't certain that's how hackers obtained the password, and he said investigators may never know for certain how the credential was obtained.



Storage tanks at a Colonial Pipeline Inc. facility in Avenel, New Jersey. Photographer: Mark Kauzlarich/Bloomberg

Source: <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

2020 SolarWinds Hack

Software update

Hackers had gained access through a SolarWinds software called Orion, using malware disguised as a software update.

SolarWinds provides network-monitoring and other technical services to thousands of organisations around the world, including most Fortune 500 companies and government agencies in North America, Europe, Asia and the Middle East. The firm has an office in Suntec City.

According to reports, more than 18,000 private and government users had downloaded this tainted software update, which reportedly allowed hackers to monitor internal e-mails at some of the top agencies in the US.

Agencies that may have been impacted include the Centres for Disease Control and Prevention in the US, as well as the country's State Department and the Justice Department.

It has been reported that last year, SolarWinds was alerted to the fact that anyone could access its update server by using the password "solarwinds123", exposing a jarring vulnerability in the firm's system.



Software-based supply chain attack



Source: <https://www.straitstimes.com/singapore/no-reason-to-believe-singapore-was-a-target-in-fireeye-hack-csa>

2020 Lazada Data Breach

Singapore

Lazada suffers data breach; personal information from 1.1 million RedMart accounts for sale online

By Jeraldine Yap

30 Oct 2020 08:55PM

(Updated: 30 Oct 2020 11:36PM)

The screenshot shows a forum post with the following text:

abases
M

October 28, 2020 at 11:25 PM This post was last modified: October 28, 2020 at 11:31 PM by ExpertData. Edited 1 time in total.

Selling exclusive private databases. These databases are fresh and have never been sold before. Limited sales.

[eCommerce] Singapore - Redmart.lazada.sg - 1.1 million - Year 2020 - (email, password oscommerce, address, name, phone, partial credit cards) - \$100k
[eCommerce] United Kingdom - Everything5pounds.com - 2.9 million - Year 2020 - (email, password oscommerce/wordpress, name, gender, phone)
[Education] Brazil - Geekie.com.br - 8.1 million - Year 2020 - (email, password bcrypt-sha256/sha512, username, name, birthdate, gender, cpf, inep, phone, address)
[Finance] Indonesia - Cermati.com - 2.9 million - Year 2020 - (email, password bcrypt, name, address, phone, revenue, bank, tax number, id number, gender, address)
[Finance] Mexico - Clip.mx - 4.7 million - Year 2020 - (email, phone) - Sample: [view sample](#)
[Finance] United States - Katapult.com - 2.2 million - Year 2020 - (email, password pbkdf2-sha256/unknown, name) - Sample: [view sample](#)
[Food and Drink] Singapore/Hong Kong/Thailand - Eatigo.com - 2.8 million - Year 2020 - (email, password md5, name, phone, gender, facebook id & token, address)
[Food and Drink] Thailand - Wongnai.com - 4.3 million - Year 2020 - (email, password md5, ip, facebook & twitter id, names, birthdate, phone, zip) - Sample: [view sample](#)
[Food and Drink] United States - Toddycafe.com - 129k - Year 2020 - (email, password unknown, name, phone, address) - Sample: [view sample](#)
[Games] Vietnam - Game24h.vn - 779k - Year 2020 - (email, password md5, username, birthdate, name) - Sample: [view sample](#)
[Lifestyle] India - Wedmegood.com - 1.3 million - Year 2020 - (email, password sha512, phone, facebook id) - Sample: [view sample](#)
[Software] India - W3layouts.com - 789k - Year 2020 - (email, password bcrypt, ip, country, city, state, phone, name) - Sample: [view sample](#)
[Software] Italy/Egypt - Apps-builder.com - 386k - Year 2020 - (email, password md5crypt, ip, name, country) - Sample: [view sample](#)
[Software] United States - Invideo.io - 571k - Year 2020 - (email, password bcrypt, name, phone) - Sample: [view sample](#)
[Software] Worldwide - Coupoontools.com - 1 million - Year 2020 - (email, password bcrypt, name, phone, gender, birthdate) - Sample: [view sample](#)
[Sports] Brazil - Athletico.com.br - 162k - Year 2018 - (email, password md5, name, cpf, birthdate) - Sample: [view sample](#)
[Sports] United States - Fantasycruncher.com - 227k - Year 2020 - (email, password bcrypt/sha1, username, ip) - Sample: [view sample](#)

"This RedMart-only information is more

an 18 months out of date and not linked

to any Lazada database. The user information that was illegally accessed include names, phone numbers, email and mailing addresses, encrypted passwords and partial credit card numbers. We have taken immediate action to block unauthorised access to the database."

[SEE MORE](#)

Source: <https://www.channelnewsasia.com/news/singapore/lazada-redmart-data-breach-personal-information-millions-account-13415688>

2018 SingHealth Data Breach

Singapore

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.



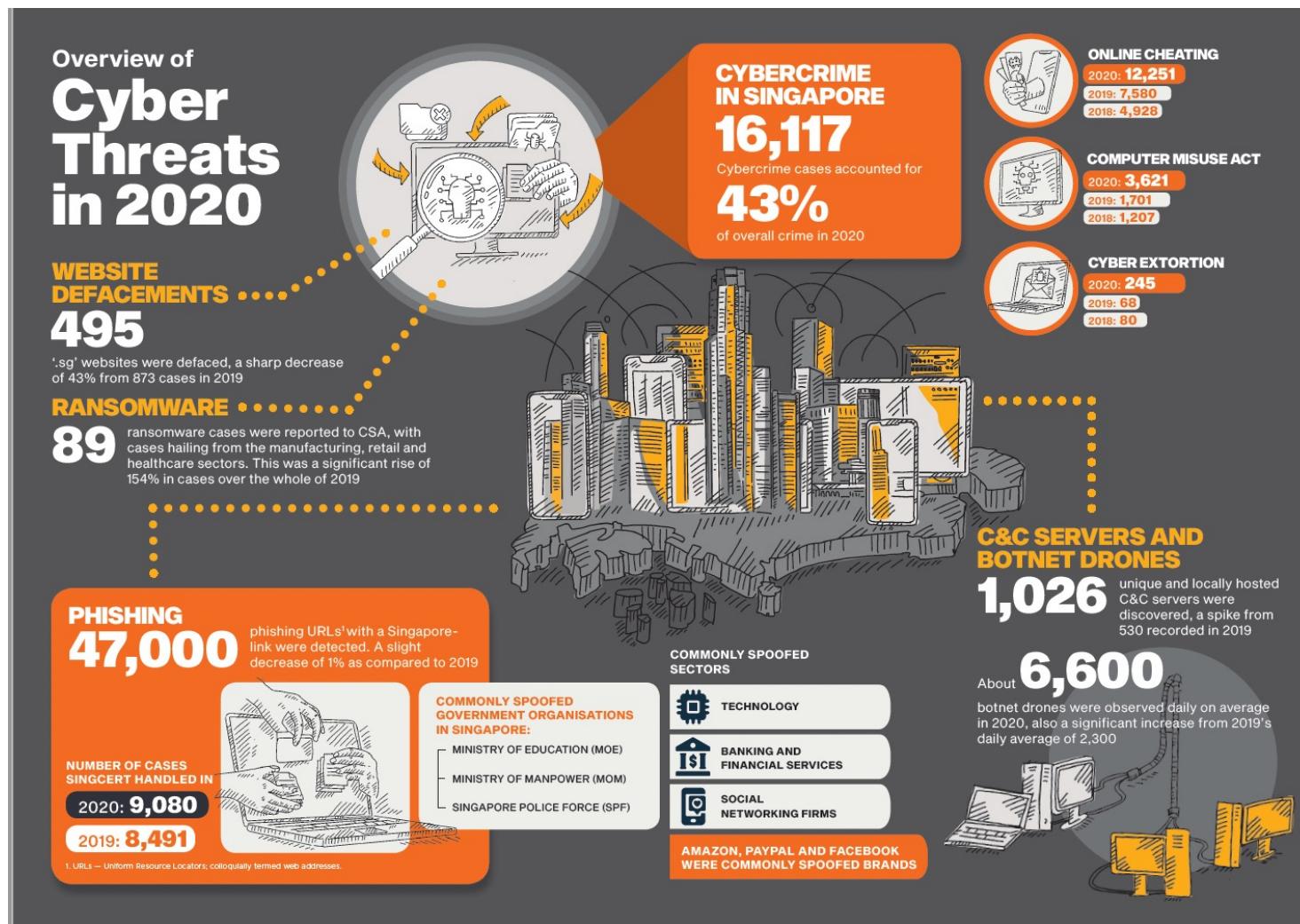
The "most serious breach of personal data" in Singapore's history took place last month, with 1.5 million SingHealth patients' records accessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken, according to the Ministry of Health and Ministry of Communications and Information. Lee Li Ying has more with the story.

SINGAPORE: The "most serious breach of personal data" in Singapore's history took place last month, with 1.5 million SingHealth patients' records accessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken, according to the Ministry of Health and Ministry of Communications and Information.

Among those affected was Prime Minister Lee Hsien Loong, with the attackers "specifically and repeatedly targeting" his personal particulars and information of his outpatient dispensed medicines, the ministries said in a joint release on Friday (Jul 20).

<https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318>

Singapore Cybersecurity



Source: <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>

Pandemic has affected - Lifestyle: More online transactions and purchases (food/grocery/things)
 - Workstyle: Working from home and requiring more online services

Singapore Cybersecurity

SPOTLIGHT ON CYBER THREATS

Stalking the Pandemic Trajectory

Global Observations



Customisation of lures.

Healthcare sector a key target.



Dec 2019 - Mar 2020

Coronavirus spread across the globe. Singapore reported first case. World Health Organisation declared COVID-19 a pandemic.

Local Observations



2. The observations covered in the timeline were derived from reports from cybersecurity firms, online sources and media reports.

Advanced Persistent Threat.

Peak in phishing lures targeting homebound individuals, relief and stimulus measures.



Ransomware escalated.

Rise in data leaks and credentials put up for sale.

Cyber espionage of COVID-19 research heated up.



Mar - May 2020

More than one-third of humanity under some form of lockdown. Singapore's Circuit Breaker measures kicked in.

Spike in COVID-19-related phishing, scams and ransomware cases.

Key targets: Healthcare, Education.

Zoom for home-based teaching suspended after lesson hijacking incident.



Throughout 2020, threat actors capitalised on a series of COVID-19-related milestones to carry out their malicious cyber activities. In Singapore, observations of COVID-19-related cyber threats, such as phishing and ransomware, were generally in line with global trends and coincided with the rise of work-from-home arrangements, as individuals and businesses adopted new technologies to maintain business continuity. With the increasing reliance on digital infrastructure and keen public interest in vaccine developments and distribution, threat actors are likely to continue adjusting their tactics to match the pandemic's trajectory².

Intensification of vaccine-related cyber incidents

Three APT* groups reportedly targeted seven COVID-19 vaccine makers.

Cyber espionage and ransomware attacks targeted vaccine research centres, regulatory bodies (European Medicines Agency hack), and vaccine distribution channels.

Authorities warned of surge in vaccine-related cybercrime.



Jun - Jul 2020

Global cases surpassed 10M. Singapore moved into Phase 2 of reopening. Countries started to ease lockdown measures.

Takes COVID-19 contact tracing apps, including TraceTogether app, with the ability to deliver malware detected.

Singapore a target of global phishing campaign on government support.

Resurgence of cases globally as countries try to restart economies. Rollout of approved vaccines globally.

Increasing trend of Business Email Compromise (BEC) and data breaches/leaks.



Alert by Singapore Police Force warning of vaccination scams.

SINGAPORE CYBER LANDSCAPE 2020 11

10 SINGAPORE CYBER LANDSCAPE 2020

Source: <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>

Singapore Cybersecurity Agency



 Singapore Government
Integrity • Service • Excellence

[CONTACT INFO](#) . [FEEDBACK](#) . [FAQ](#) . [SITEMAP](#)



A⁻

A⁺

Search



[Home](#) | [About Us](#) | [News](#) | [Industry Programmes](#) | [SingCERT](#) | [GOsafeonline](#) | [Careers](#)



The Cyber Security Agency of Singapore (CSA) is the national agency overseeing cybersecurity strategy, operations, education, outreach, and ecosystem development.

Singapore Cybersecurity Strategy

- ▶ **Pillar One:** These national level strategies are also similar to organisation level strategies
 - ▶ Building a Resilient Infrastructure
- ▶ **Pillar Two:**
 - ▶ Creating a Safer Cyberspace
- ▶ **Pillar Three:**
 - ▶ Vibrant Cybersecurity Ecosystem
- ▶ **Pillar Four:**
 - ▶ Strengthening International Partnerships

- There is a need to know how to identify what kind of device / product require what kind of standards / requirements
- There is a need to know how to improve education
 - cannot just rely on the technical people to just strengthen security
- How to improve organisation security talent
- How to collaborate with customers / service providers and ensure that they have the require standards / specifications for their security infrastructure

Singapore Cybersecurity Strategy Cont.

- ▶ **Pillar One:**
 - ▶ Building a Resilient Infrastructure
 - ▶ This Pillar ensures that essential services are resilient to minimize impact to our day-to-day lives in the event of a cyber-attack.
 - ▶ E.g.,
 - ▶ **Cybersecurity Act, Feb 2018**
 - A new cybersecurity bill in 2018
 - Strengthened security controls for Critical information infrastructure (CII) sectors Recent moves to protect essential services / CII
 - ▶ **Singapore's Operational Technology (OT) Cybersecurity Masterplan 2019**

Singapore Cybersecurity Strategy Cont.

▶ Pillar Two:

- ▶ Creating a Safer Cyberspace
 - ▶ This Pillar comprises initiatives to engage businesses and the public to collectively build a safer and more secure cyberspace.
- ▶ E.g.,
 - ▶ Singapore's Safer Cyberspace Masterplan 2020
 - ▶ DPC amended the Personal Data Protection Act to enhance consumer protection and encourage data innovation.
 - ▶ Cybersecurity Labelling Scheme (CLS)
 - For network-connected smart devices in early 2020
 - A first in the Asia Pacific region
 - Comprise different levels of cybersecurity ratings to help consumers make informed choices about the security features of the smart devices they purchase.
 - ▶ SG cyber safe trustmark by 2021
 - ▶ National Cybersecurity Awareness Campaign

Singapore Cybersecurity Strategy Cont.

- ▶ Pillar Three:
 - ▶ Developing a Vibrant Cybersecurity Ecosystem
 - ▶ This Pillar is aimed at enhancing the vibrancy and sustainability of Singapore's cybersecurity industry, and its research and talent pipelines.
 - ▶ E.g.,
 - ▶ Enhancing the cybersecurity workforce and encouraging industry innovation in Singapore
 - Diverse cybersecurity competitions and awards
 - SG Cyber Woman
 - Cybersecurity research investment
 - S\$8.4m national cybersecurity lab launched at NUS in 2017

Singapore Cybersecurity Strategy Cont.

▶ Pillar Four:

▶ Strengthening International Partnerships

To help standardise and improve cyber security frameworks

▶ E.g.,

- ▶ The 4th ASEAN ministerial conference on Cybersecurity (AMCC) in Oct 2019
 - Drafted the ASEAN Cybersecurity Coordination Mechanism Proposal paper
- ▶ CSA signed MOUs with New Zealand and the Republic of Korea in 2019, to increase professional exchanges and sharing of best practices for cybersecurity defense

Temasek holding portion of investments will be in promising cyber security start up - such as companies in israel

Government is trying to invest and acquire these cyber security companies - maybe to gain advantage in the future with such research

2.What is Information Security about?

What is Information Security About? (cont.)

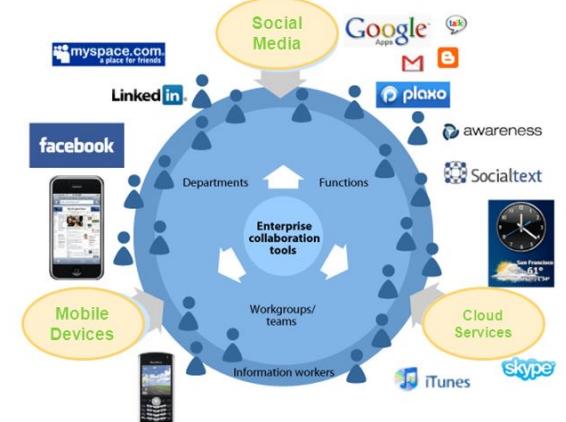
“We have technology people to handle technology problems”



Mainframe Age -> IT Consumerization



IT CONSUMERIZATION



What is Information Security About? (cont.)

- ▶ Information security planning and funding decisions should involve THREE distinct groups of managers and professionals, or communities of interest:
 - ▶ *Those in the field of information security*
 - ▶ Protects the organization's information assets from the many threats from the many threats they face
 - ▶ *Those in the field of IT*
 - ▶ Supports the business objectives of the organization by supplying and supporting IT that is appropriate to the organization's needs
 - ▶ *Those from the rest of the organization*
 - ▶ Articulates and communicates organizational policy and objectives and allocates resources to the other groups
 - especially in ensuring that their access to the assets cannot be compromised

What is Information Security About?

- ▶ Minimize the risk of loss or damage to the organization's information assets
- ▶ Information assets: information that has value to the organization, and the systems that store, process, and transmit the information

Specialized Areas of Security

- ▶ **Physical security**
 - ▶ Protecting people, physical assets (e.g., hardware), and the workplace from various threats
 - ▶ Unauthorized access, fire, natural disasters, etc.
- ▶ **Operations security**
 - ▶ The protection of the details of an organization's operations and activities
- ▶ **Communications security**
 - ▶ Protection of all communication media, technology, and content
- ▶ **Cyber (or computer) security**
 - ▶ The protection of computerized information processing systems and the data they contain and process.
- ▶ **Network security**
 - ▶ A subset of communication security cybersecurity
 - ▶ Protecting data networking devices, connections, and content

What Is Security? (cont.)

▶ **Information security (InfoSec):**

- ▶ Protection of the *confidentiality, integrity, and availability* of information assets, whether in *storage, processing, or transmission*, via the application of *policy, education, training and awareness, and technology*.

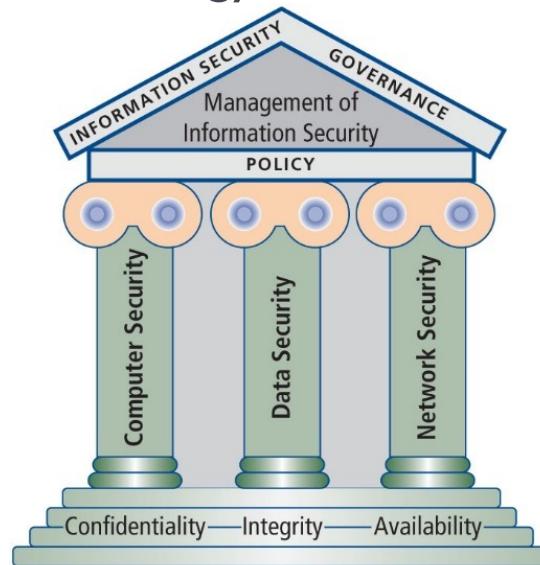


Figure 1-1 Components of information security

CNSS Security Model

- ▶ Also known as McCumber Cube
 - ▶ Helps understand key aspects of InfoSec
 - ▶ Main goal is to identify gaps in the coverage of an InfoSec program
 - ▶ Covers three dimensions central to InfoSec:
 - ▶ Information characteristics
 - ▶ Information location
 - ▶ Security control categories

CNSS Security Model (cont.)

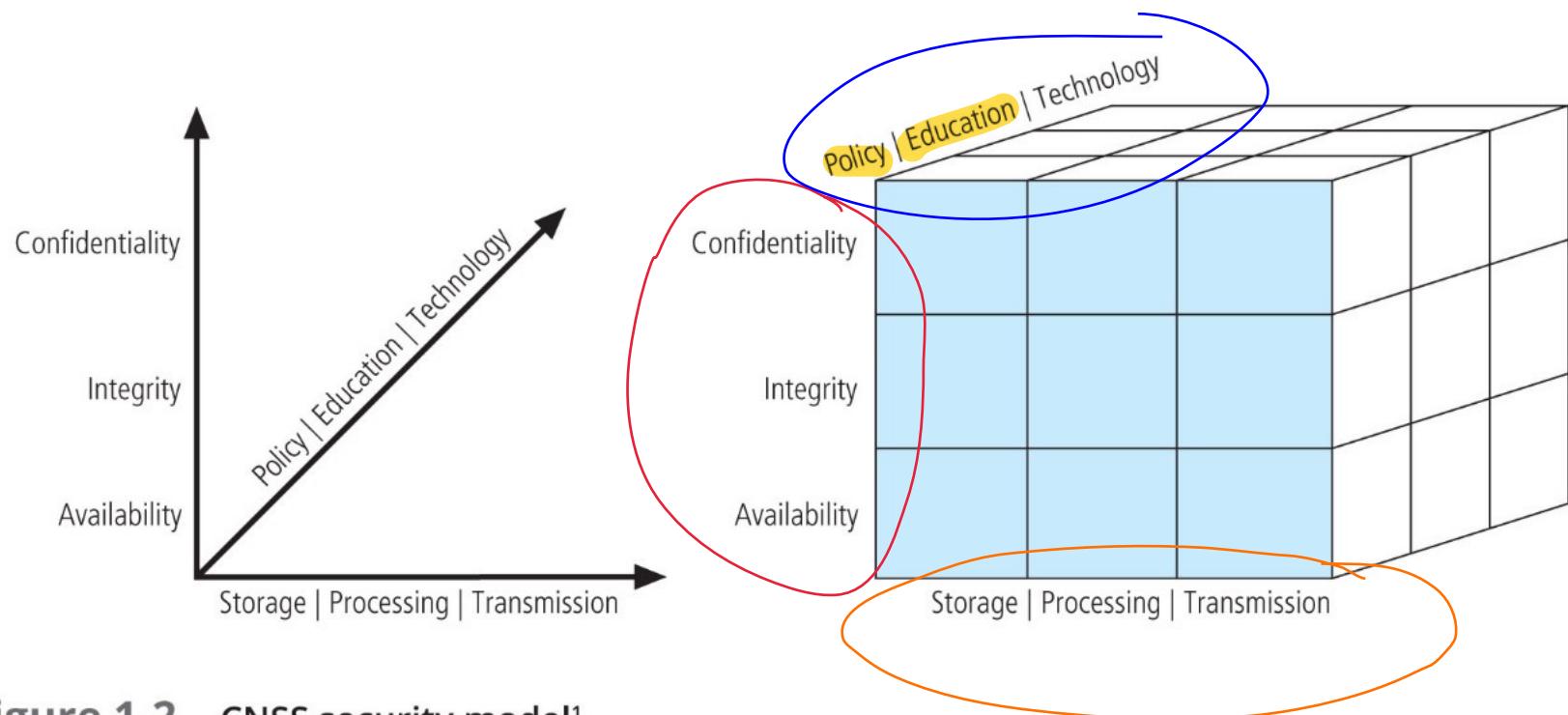


Figure 1-2 CNSS security model¹

there are 27 cells to focus on individually

14TH NATIONAL COMPUTER SECURITY CONFERENCE

October 1-4, 1991
Omni Shoreham Hotel
Washington, D.C.



INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL

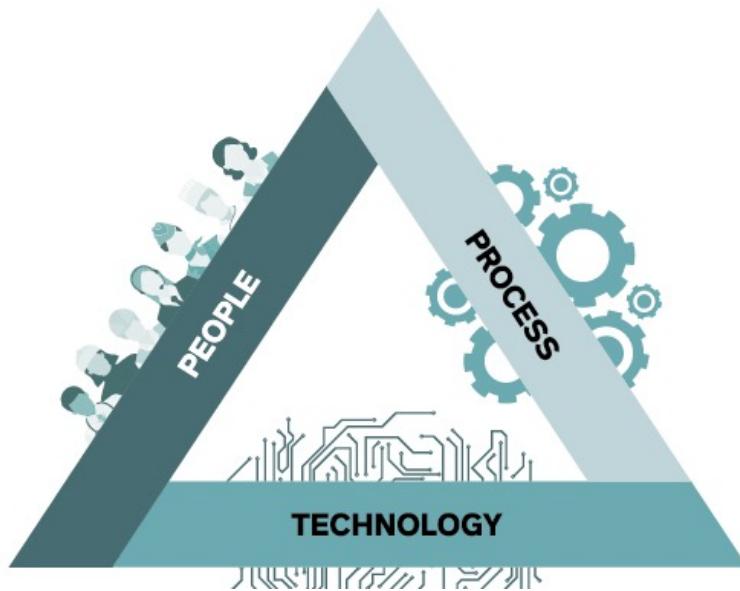
Capt John R. McCumber
Joint Staff/J6K
The Pentagon
Washington, DC 20318-6000

INTRODUCTION

At speech to the 13th National Computer Security Conference on 3 October 1990, Michelle VanCleave, Assistant Director for National Security Affairs, Executive Office of the President stated, "We need a comprehensive model for understanding the threat to our automated information systems." I believe I have developed that model. This model not only addresses the threat, it functions as an assessment, systems development, and evaluation tool. The model is unique in that it stands independent of technology. Its application is universal and is not constrained by organizational differences. As with all well-defined fundamental concepts, it is unnecessary to alter the premise even as technology and human understanding evolve.

Trifecta of People, Process, and Technology

- ▶ Proposed by Bruce Schneier in 1990s, origins from Harold Leavitt's Diamond model theory in 1965



The C.I.A. Triad

- ▶ Key characteristics of information that make it valuable to an organization.

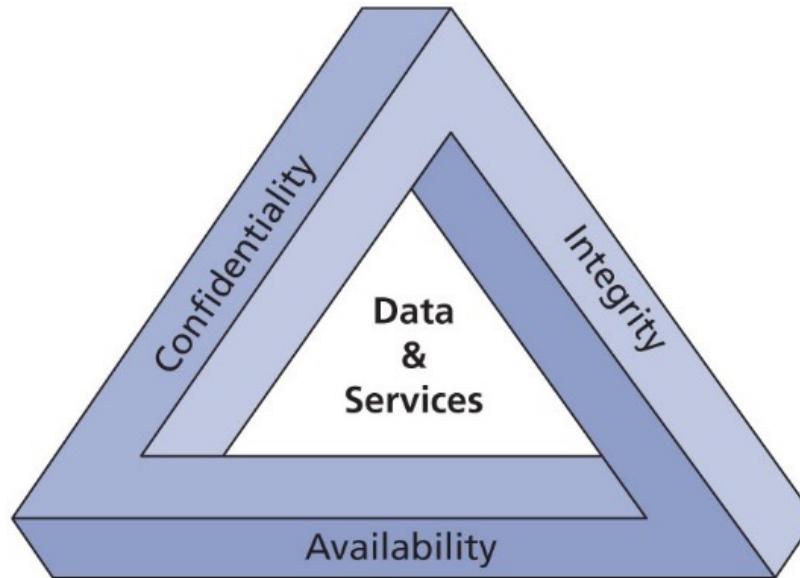


Figure 1-3 The C.I.A. triad

The C.I.A. Triad- Confidentiality

- ▶ **Confidentiality:**
 - ▶ An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems
 - ▶ Limiting access to information only to those who need it, and preventing access by those who don't
- ▶ To protect the confidentiality of information, a number of measures are used:
 - ▶ Information classification
 - ▶ Secure document (and data) storage
 - ▶ Application of general security policies
 - ▶ Education of information custodians and end users
 - ▶ Cryptography (encryption)

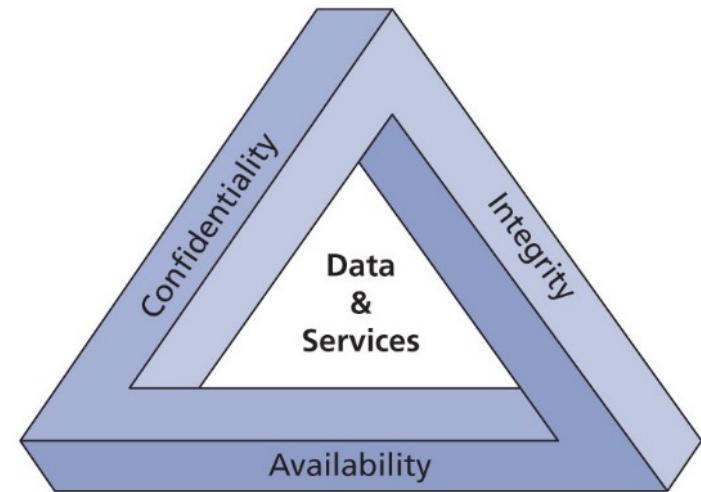


Figure 1-3 The C.I.A. triad

The C.I.A. Triad-Integrity

▶ Integrity:

- ▶ An attribute of information that describes how data is whole, complete, and uncorrupted
- ▶ The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
- ▶ Corruption can occur while information is being entered, stored, or transmitted

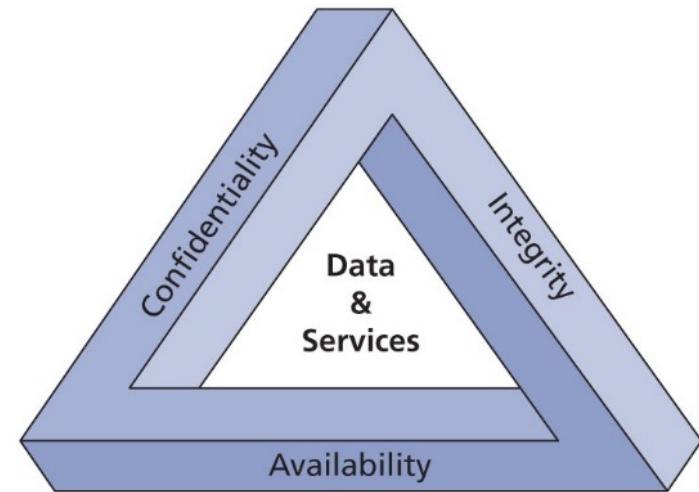


Figure 1-3 The C.I.A. triad

The C.I.A. Triad-Availability

- ▶ **Availability:**
 - ▶ An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction
 - ▶ Availability of information means that authorized users, either people or other systems, have access to it in a usable format

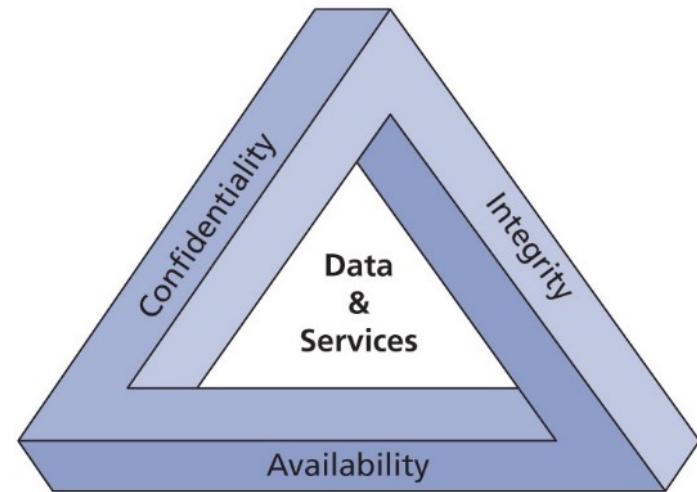


Figure 1-3 The C.I.A. triad

The C.I.A. Triad Extension

- ▶ Over time C.I.A. triangle has been expanded to include:

- ▶ Privacy → user
 - ▶ Identification
 - ▶ Authentication
 - ▶ Authorization
 - ▶ Accountability
- } system

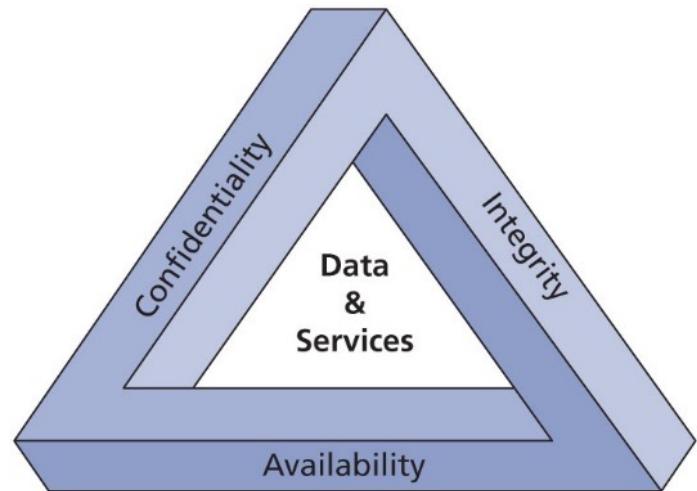


Figure 1-3 The C.I.A. triad

The C.I.A. Triad Extension (cont.)

► Privacy

- ▶ The information that is collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected
- ▶ Information will be used only in ways approved by the person who provided it

 What situations where confidentiality is secured but privacy compromised

 What situations where confidentiality is compromised but privacy is not

► Identification

- ▶ An information system possesses the characteristic of identification when it is able to recognize individual users
- ▶ First step in gaining access to secured materials, and it serves as the foundation for subsequent authentication and authorization.
- ▶ It is typically performed by means of a user name or other ID

The C.I.A. Triad Extension (cont.)

▶ **Authentication**

- ▶ It is the process by which a control establishes whether a user (or system) has the identity it claims to have

▶ **Authorization**

- ▶ Defines what the user (whether a person or a computer) has been specifically and explicitly permitted by the proper authority to do
- ▶ Example: access, modify, or delete information

The C.I.A. Triad Extension (cont.)

- ▶ **Accountability:**
 - ▶ Occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process
 - ▶ Example: Audit logs that track user activity on an information system provide accountability

3.What is Management?

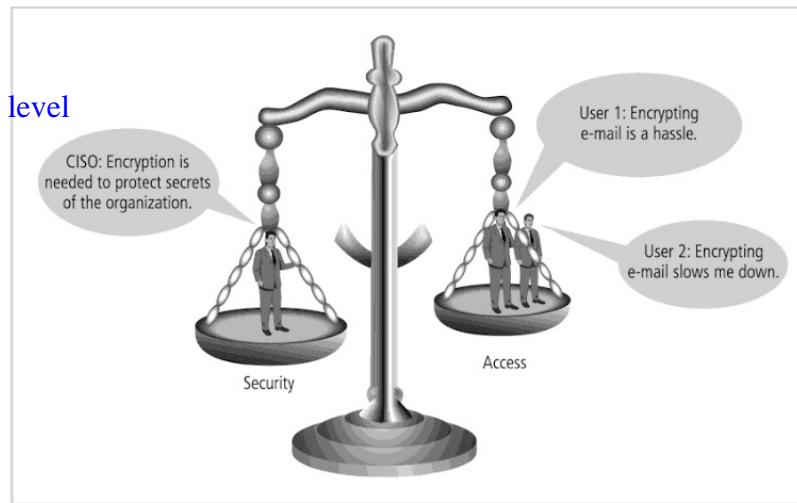
What is Management

- ▶ The process of achieving objectives using a given set of resources
- ▶ A manager is a member of the organization assigned to marshal and administer resources, coordinate the completion of tasks, and handle the many roles necessary to complete the desired objectives
- ▶ Managerial roles
 - ▶ Informational role
 - ▶ Interpersonal role
 - ▶ Decisional role

Balancing Information Security and Access

- ▶ Impossible to obtain perfect information security – A process and not a goal.
- ▶ Security should be considered a balance between protection and availability.
- ▶ To achieve **balance**, the level of security must allow reasonable access, yet protect against threats.

maintain security risk at an acceptable level
- looking at cost and benefit way



Principles of Information Security management

- ▶ The unique functions of information security management are known as the six Ps:
 - ▶ Planning
 - ▶ Policy
 - ▶ Programs
 - ▶ Protection
 - ▶ People
 - ▶ Project Management

InfoSec Planning

- ▶ Includes activities necessary to support the design, creation, and implementation of InfoSec strategies
- ▶ Types of InfoSec plans:
 - ▶ Incident response planning
 - ▶ Business continuity planning
 - ▶ Disaster recovery planning
 - ▶ Policy planning
 - ▶ Personnel planning
 - ▶ Technology rollout planning
 - ▶ Risk management planning
 - ▶ Security program planning including education, training and awareness

Policy

- ▶ A set of organizational guidelines that dictate certain behavior within the organization
- ▶ Three general categories of policy:
 - ▶ Enterprise information security policy (EISP)
 - ▶ Set the tone for the InfoSec department
 - ▶ E.g., Harvard Enterprise Information Security Policy, NUS
 - ▶ Issue-specific security policy (ISSP)
 - ▶ Sets of rules that define acceptable behavior within a specific organizational resource
 - ▶ System-specific policies (SysSPs)
 - ▶ Control the configuration and/or use of a piece of equipment or technology

Programs

- ▶ InfoSec operations that are specifically managed as separate entities
- ▶ Example:
 - ▶ A security education training and awareness (SETA) program
 - ▶ A risk management program
 - ▶ Contingency program
 - ▶ Physical security program
 - Complete with fire, physical access, gates, guards, and so on
 - ▶ Programs dedicated to client/customer privacy and awareness

Protection

- ▶ Executed via a set of risk management activities including
 - ▶ Risk assessment and control
 - ▶ Protection mechanisms
 - ▶ Technologies
 - ▶ Tools

People

- ▶ People are the most critical link in the information security program
- ▶ This area of InfoSec includes security personnel and the security of personnel, as well as aspects of the SETA program mentioned earlier

Projects

- ▶ Information security is a process, not a project, however, each element of an information security program must be managed as a project, even if the overall program is perpetually ongoing
 - ▶ E.g., implementing a security policy, implementing a new firewall



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
 - ▶ I.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
 - ▶ I.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

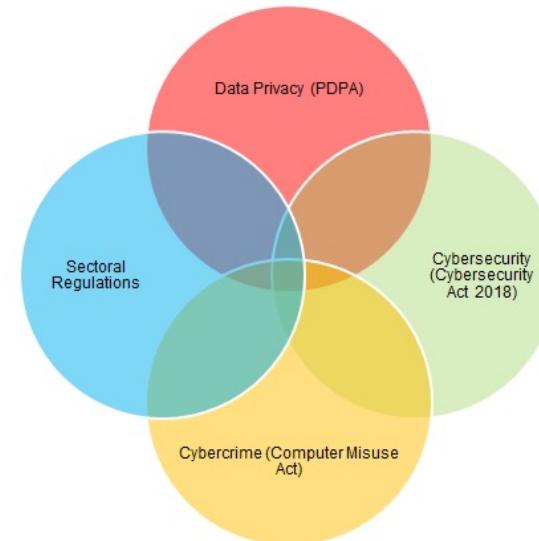
- ▶ A way of deterrence
 - ▶ Preventing an illegal or unethical activity
 - ▶ Effectiveness deterrence
 - ▶ Fear of penalty
 - ▶ Probability of being caught
 - ▶ Probability of penalty being administered

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 CIs against cyber-attacks.

The Act provides a framework for the designation of CIs. It provides CII owners with clarity on their obligations to protect CIs 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 formation 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 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 require the restriction



Cybersecurity Code of Practice for CII

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

Cybersecurity Code of Practice for CII cont.

- ▶ It is intended to specify the **minimum protection policies** that a CIO 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

PDPA does not apply to IRAS

INLAND REVENUE AUTHORITY OF SINGAPORE

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

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

Search Within IRAS Website

Home Individuals Businesses GST Property Other Taxes Schemes e-Services LOGIN

 Monitoring your business revenue to determine whether you need to register for GST? From 2019, do so at the end of every calendar year. Learn more

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.

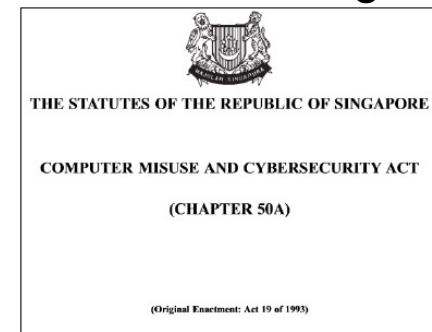
- Hacking/Hacking attempt

- 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

f t ...

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

▶ MASTRM 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

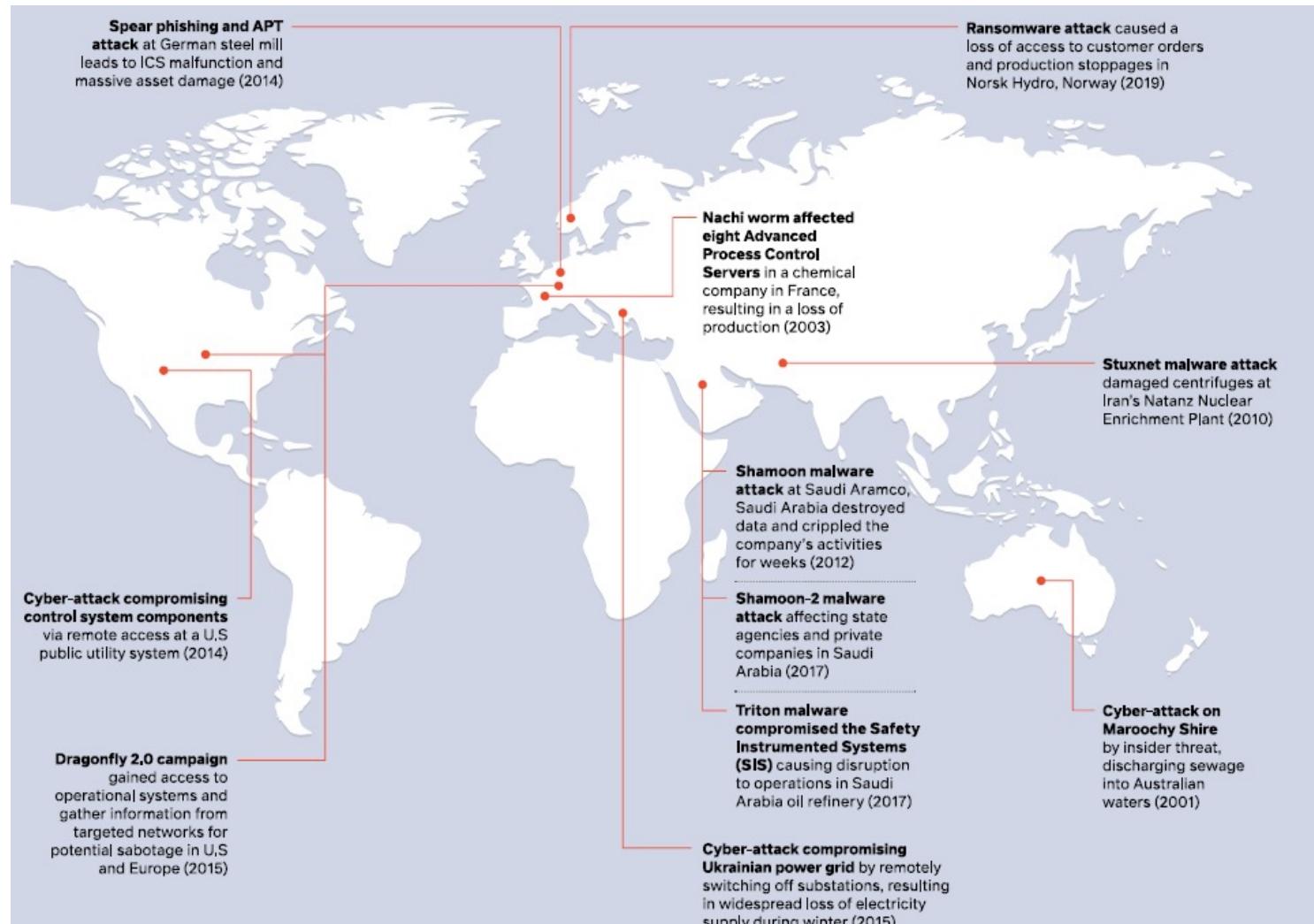
- ▶ MAS releases new amendments to TRM Guidelines
 - ▶ 18 Jan 2021
 - ▶ The responsibilities of the board of directors (or a committee delegated by it) and senior management in relation to the governance and oversight of technology risk.
 - E.g., a sound and robust risk management framework
 - ▶ Secure 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

IS4231

Information Security Management

Lecture 3

Governance and Planning for Security

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

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

Learning Objectives

- ▶ Strategic organizational planning for information security (InfoSec)
- ▶ Information security implementation approach
- ▶ Discuss the importance of information security governance



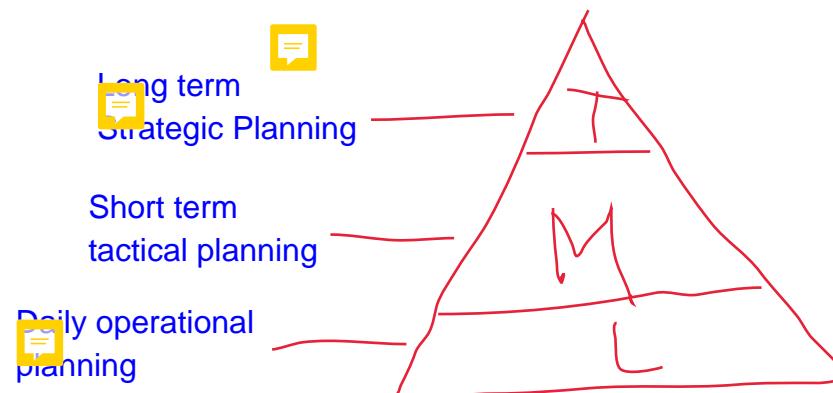
|

Strategic Planning

Strategic Planning

▶ Strategic planning

- ▶ Lays out the long-term direction to be taken by the organization
- ▶ Guides organizational efforts by focusing resources on specific, clearly defined goals
- ▶ May have to be revised or updated due to an ever-changing environment



Creating a Strategic Plan

- ▶ A clearly directed strategy flows from top to bottom, and a systematic approach is required to translate it into a program that can inform and lead all members of the organization
- ▶ Organization develops a general strategy
 - ▶ Then creates specific strategic plans for major divisions
 - ▶ Each level or division translates those objectives into more specific objectives for the level below

Top-down Strategic Planning

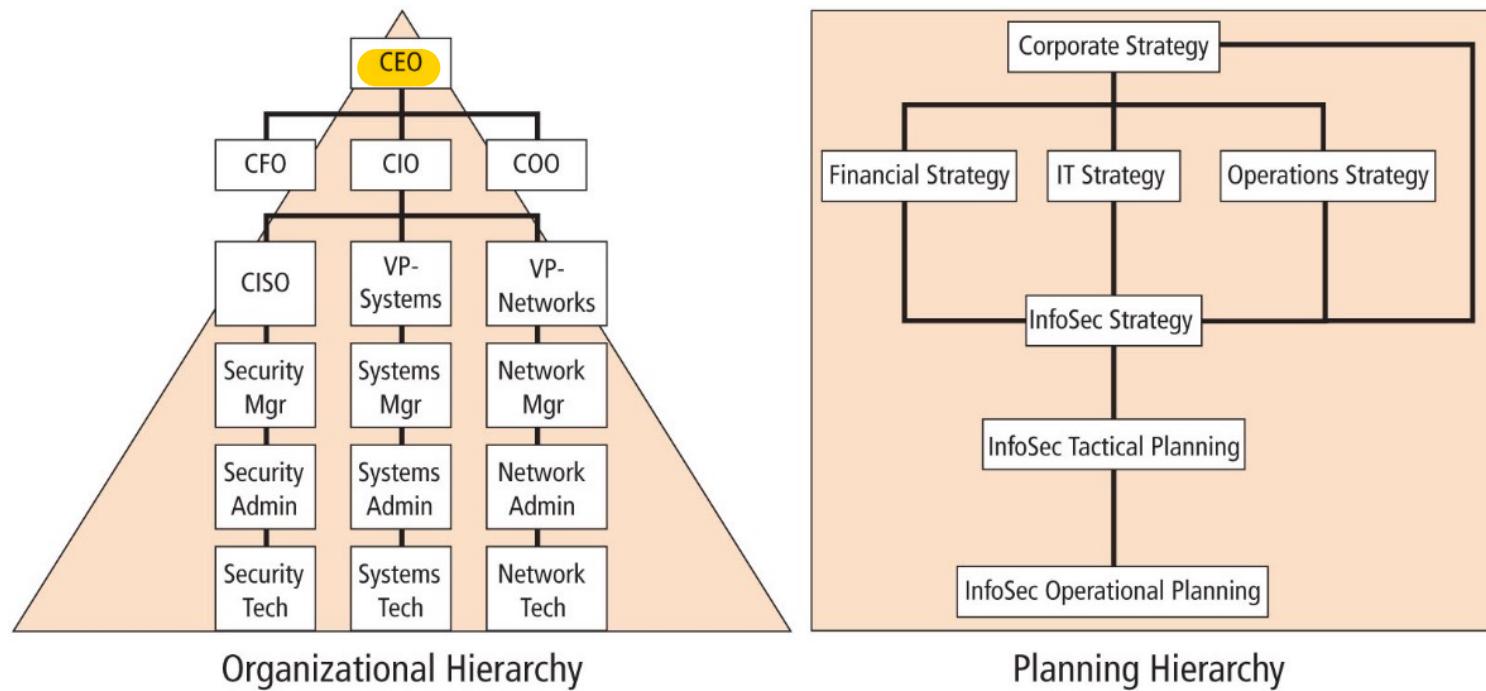
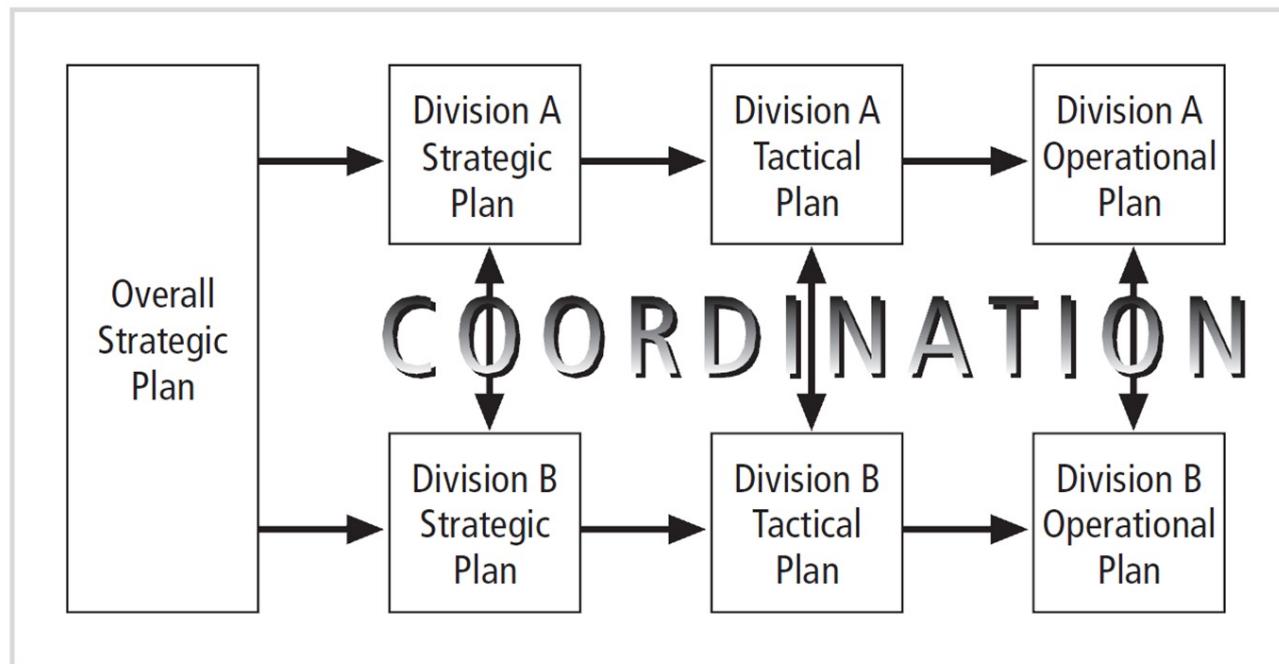


Figure 3-2 Top-down strategic planning

Planning Levels

- ▶ Strategic planning transforms general statement, sweeping statements towards specific and applied objectives
- ▶ Strategic plans used to create tactical plans, which are in turn used to develop operational plans



Planning Levels (cont.)

▶ **Tactical plans**

- ▶ Have a more short-term focus than strategic planning
 - ▶ Usually 1-3 years
- ▶ Each applicable strategic goal is broken down into a series of incremental objectives
- ▶ Critical components
 - ▶ Budgeting
 - ▶ Resource allocation
 - ▶ Personnel
- ▶ Often include:
 - ▶ Project plans, resource acquisition planning documents (e.g., **product specifications**), project budgets, project reviews, and monthly and annual reports

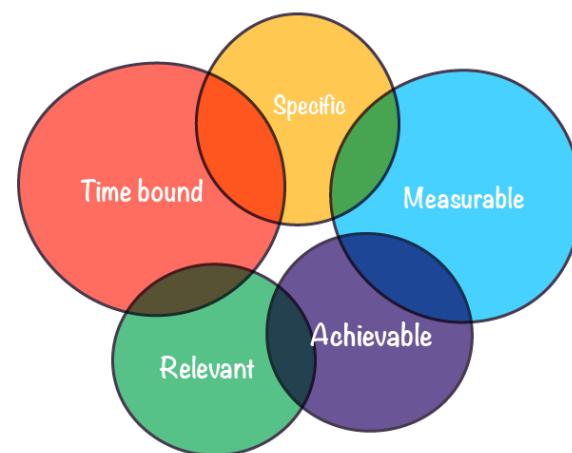
The CISO and the security managers use the tactical plan to organize, prioritize and acquire resources necessary for the major projects and to provide support for the overall strategic plan.

Planning Levels (cont.)

- ▶ **Operational plans**
 - ▶ Derived from the tactical plans
 - ▶ Used by managers and employees to organize ongoing, day-to-day tasks
 - ▶ Often include:
 - ▶ Clearly defined coordination activities that span department boundaries
 - ▶ Communication requirements
 - ▶ Weekly meetings
 - ▶ Summaries
 - ▶ Progress reports
 - ▶ Etc.

Planning Levels (cont.)

- ▶ Tasks at the tactical and operational levels must have objectives that are – SMART
 - ▶ A well-established tool that you can use to plan and achieve your goals
 - ▶ **S**pecific
 - ▶ **M**easurable
 - ▶ **A**chievable
 - ▶ **R**elevant
 - ▶ **T**ime-bound
- Evaluate
Revised



 Avoid using only 1 single metric to measure

Discussion: Patch Management

- ▶ **S**pecific
- ▶ **M**easurable
- ▶ **A**chievable
- ▶ **R**elevant
- ▶ **T**ime-bound

the optimal way is for the higher levels to first plan based on the environment on high level - then adapt based on feedback given on the lower levels

Recent situations:

Who led the digital transformation of your company?

- A) CEO
- B) CTO
-  C) COVID-19

Digital Transformation Quiz SUSANNE WOLK (TWITTER)

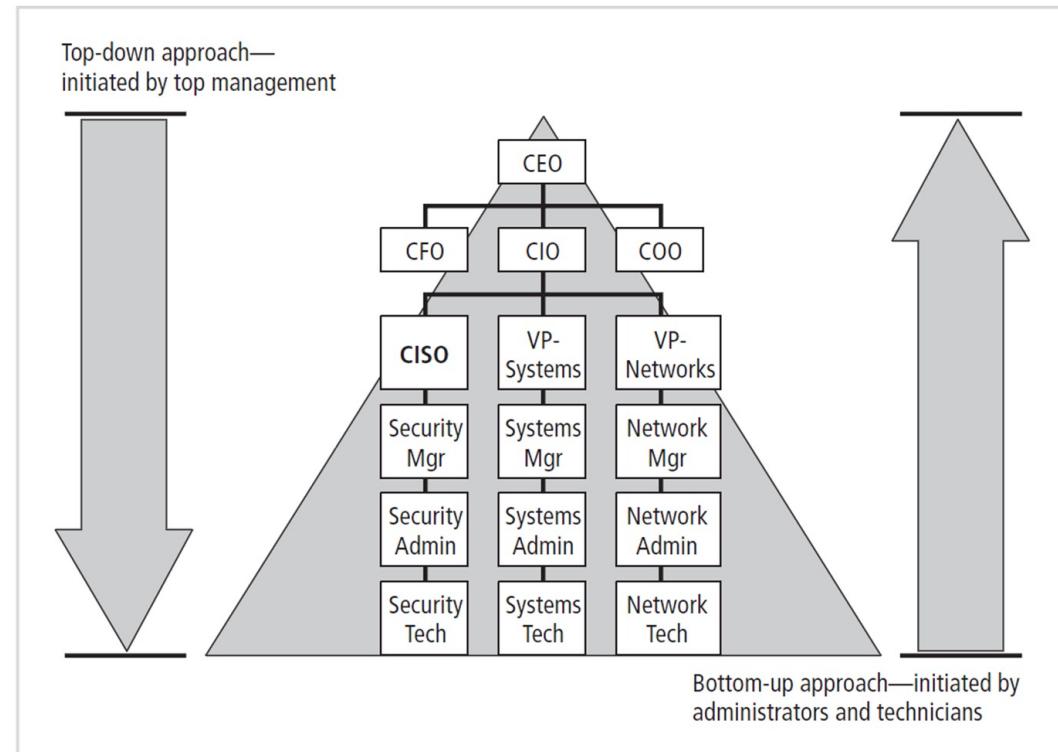
Recent situations discussions

- ▶ **Strategic planning:**
 - ▶ Digital transformation in every aspect
- ▶ **IT planning:**
 - ▶ High quality information service enabling and supporting digital transformation
- ▶ **InfoSec planning:**
 - ▶ Make sure the high quality information service are provided in securely and in conformance with all national information processing, information security, and privacy statutes and guidelines in facilitating digital transformation.

Planning for InfoSec Implementation

Top-down vs. Bottom-up

- ▶ InfoSec implementation can be accomplished in two ways:
 - ▶ Top-down
 - ▶ Initiated by top management
 - ▶ Bottom-up
 - ▶ Initiated by administrators and technicians



Top-down Approach

- ▶ **Description**
 - ▶ Information security begins as a formal program, proposed and coordinated by high-level managers with executive management support to provide resources; give direction; issue policies, procedures, and processes; dictate the goals of expected outcomes of the project; and determine who is accountable for each of the required action
- ▶ **Advantage:**
 - ▶ Strong upper-management support
 - ▶ Dedicated champion
 - ▶ Dedicated funding
 - ▶ A clear planning and implementation process
 - ▶ Holistic approach to support the entire organization

Top-down Approach

▶ Challenges

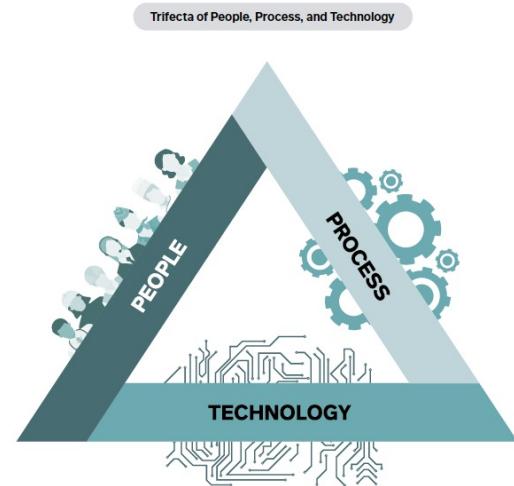
- ▶ High-level management must **buy into** the effort and provide full support to all departments
- ▶ Must have a **champion**
 - ▶ An executive with enough influence to move the project forward
- ▶ Involvement and support of end users is critical

Bottom-up Approach

- ▶ **Description**
 - ▶ Information security begins as system and network administrators attempt to improve the security of their system
- ▶ **Advantage**
 - ▶ Utilize the technical expertise of the individual administrators who work with the information systems on a daily basis
- ▶ **Disadvantage**
 - ▶ Lack of coordinated planning from upper management
 - ▶ Lack of coordination between departments
 - ▶ Lack of the provision of sufficient resources
- ▶ **Seldom works in the long term**

InfoSec Planning

- ▶ Includes activities necessary to support the design, creation, and implementation of InfoSec strategies
- ▶ Types of InfoSec plans:
 - ▶ Policy planning
 - ▶ Personnel planning
 - ▶ Technology rollout planning
 - ▶ Security program planning including education, training and awareness
 - ▶ Risk management planning
 - ▶ Incident response planning
 - ▶ Disaster recovery planning
 - ▶ Business continuity planning



Recent situations:

Singapore

COVID-19: Jail, fines for employers who do not allow employees to work from home where possible



Office workers at Raffles Place in Singapore. (File photo: Marcus Mark Ramos)



ad hoc approach since it is unexpected

02 Apr 2020 04:28PM

(Updated: 02 Apr 2020 11:17PM)

SINGAPORE: Employers who do not make facilities available for members of staff to work from home where reasonable could be jailed or fined, under changes to the Infectious Diseases Act.

An addition to the Act published in the Government Gazette on Wednesday (Apr 1) night lays out the penalties employers face for not directing staff to work from home where possible or not implementing safe distancing measures at work, among others.

The flexible work arrangements are aimed at curbing the spread of COVID-19 in Singapore.

On Tuesday, Manpower Minister Josephine Teo said companies that do not allow telecommuting wherever possible might face stop-work orders or other penalties.

She added that the Ministry of Manpower (MOM) plans to have more than 100 enforcement officers conduct checks on companies.

Source: <https://www.channelnewsasia.com/news/singapore/covid-19-work-from-home-singapore-jail-fines-coronavirus-12602224>

Recent challenges: Remote working

- ▶ **Strategic planning:**
 - ▶ Remote working would be the “New Normal”
- ▶ **IT planning:**
 - ▶ High quality information service supporting remote working
 - ▶ Operational plans:
 - ▶ Technology
 - ▶ Process
 - ▶ People
- ▶ **InfoSec planning:**
 - ▶ Make sure remote working are conducted in a secured way.
 - ▶ Operational plans
 - ▶ Technology
 - E.g., VPN, remote access controls, MFA, email security solutions, anti-spam solutions, endpoint protection solutions
 - ▶ Process
 - E.g., Telecommuting Policy, Acceptable Use Policy, device management, contingency plan
 - ▶ People
 - E.g., Education and training, A/B team arrangement

Information Security Governance

Information Security Governance

- ▶ **Governance is**
 - ▶ The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly"
 - ▶ InfoSec governance objectives must be addressed at the highest levels of an organization's management team
 - ▶ In order to be effective and offer a sustainable approach
 - ▶ **GRG**
 - ▶ Governance, Risk Management, and Compliance
- ▶ 22

Example: NUS InfoSec Governance

Chapter 3 NUS IT Security Policy: IT Security Management

1 Purpose and scope

This chapter defines the various roles within NUS that are assigned responsibilities pertaining to the protection of information resources.

2 Introduction

Everyone associated with NUS has a role in information security. Due care must be exercised in the protection of IT information resources by clearly defining roles and responsibilities of management and users relating to information security.

3 Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

3.2 Information security responsibilities

3.2.1 Management of Computer Centre sets strategic direction for NUS information security initiatives and provides support, commitment and resources for NUS information security initiatives.

3.2.2 Please refer to the NUS Data Management Policy for the details of the roles and responsibilities of the following:

Data Owner
Data Stewards
Data Managers
System Owners
Data Users
Data Administrators
Database Administrators
Application Developers
Infocomm Security Group

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.

Governance

Information Security Governance (cont.)

► Why need InfoSec governance

1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organization
2. Verifying that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacy

InfoSec Governance Responsibilities

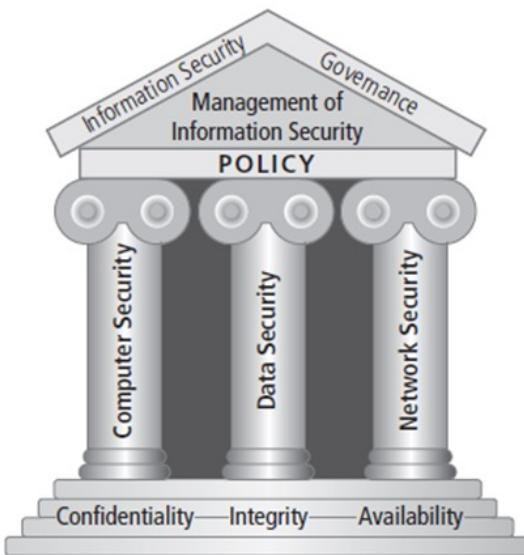


Figure 1-1 Components of information security



Figure 3-5 Information security governance responsibilities¹⁰

Source: IT Governance Institute.

Information Security Governance (cont.)

▶ Benefits of InfoSec governance:

- ▶ An *increase in share value for organizations*
- ▶ Increased *predictability and reduced uncertainty* of business operations by lowering information-security-related risks to definable and acceptable levels
- ▶ Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care
- ▶ Optimization of the allocation of limited security resources
- ▶ Assurance of effective InfoSec policy and policy compliance
- ▶ A firm foundation for efficient and effective risk management, process improvement, and rapid incident response
- ▶ A level of assurance that critical decisions are not based on faulty information
- ▶ Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response



this planning will encompass a full/whole cycle

Information Security Governance Program

- ▶ When developing an InfoSec governance program, the designers should ensure that the program includes:
 - ▶ An effective security organizational structure
 - ▶ A comprehensive security strategy explicitly linked with business and IT objectives
 - ▶ An InfoSec risk management methodology
 - ▶ A security strategy that talks about the value of information being protected and delivered
 - ▶ Security policies that address each aspect of strategy, control, and regulation
 - ▶ A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
 - ▶ Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
 - ▶ A process to ensure continued evaluation and updating of security policies, standards, procedures, and risks

ISO/IEC 27014: Governance of Information Security

- ▶ ISO 27014:2013 is the ISO 27000 series standard for Governance of Information Security
- ▶ The standard specifies six high-level “action-oriented” information security governance principles:
 1. Establish organization-wide information security
 2. Adopt a risk-based approach
 3. Set the direction of investment decisions
 4. Ensure conformance with internal and external requirements
 5. Foster a security-positive environment
 6. Review performance in relation to business outcomes

ISO/IEC 27014: Governance of Information Security

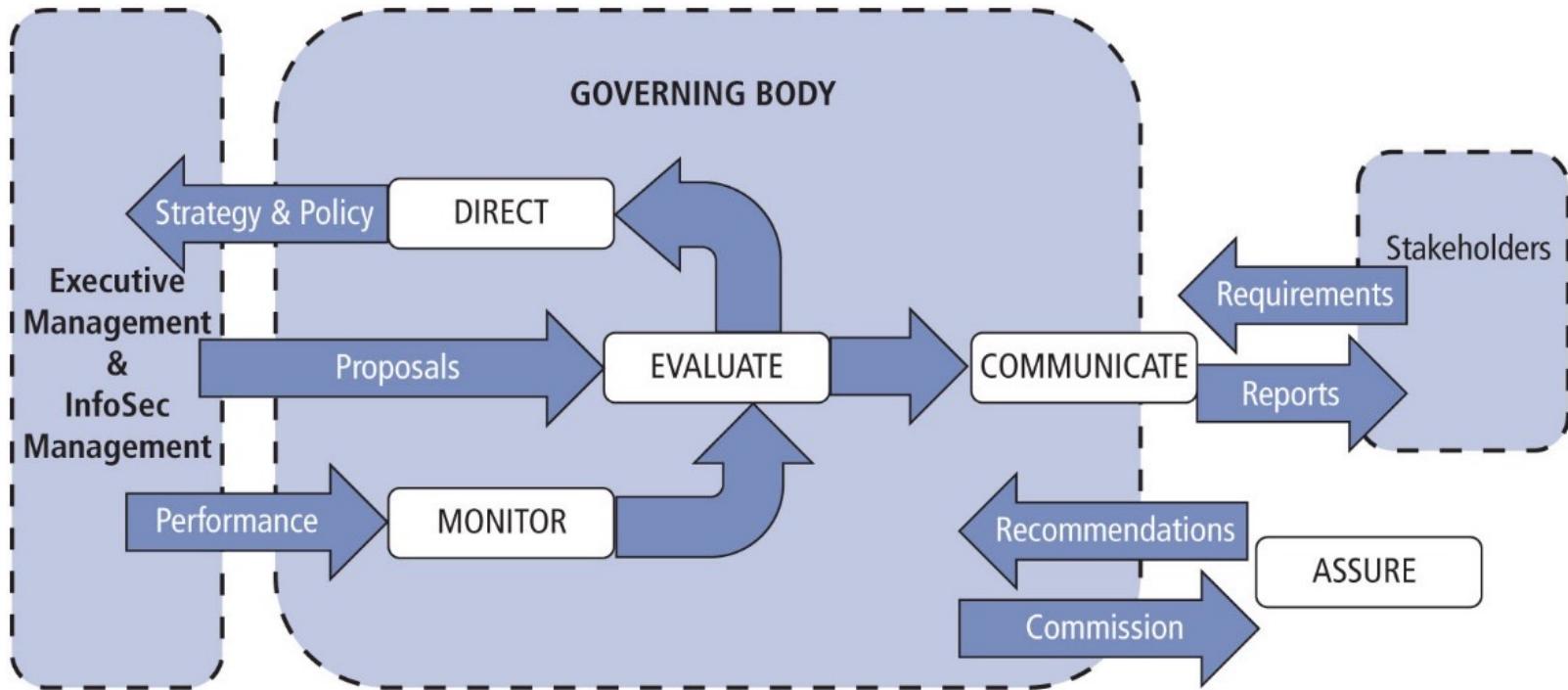


Figure 3-7 ISO/IEC 27014:2013 governance processes¹⁹

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

Case: SingHealth Data Breach

- ▶ Enhancements to Governance and Organisational Structures
 - ▶ At the Ministry, the MOH Chief Information Security Officer (CISO) is currently also the Director of Cyber Security Governance at IHiS. We will separate these roles. The MOH CISO will be supported by a dedicated office in MOH and report to the Permanent Secretary. The MOH CISO office will be the cybersecurity sector lead for the healthcare sector. It will coordinate efforts to protect Critical Information Infrastructure in the healthcare sector, and ensure that the sector fulfils its regulatory obligations under the Cybersecurity Act. For its part, IHiS will have its own separate Director of Cyber Security Governance.”

Source: <https://www.moh.gov.sg/news-highlights/details/ministerial-statement-on-the-committee-of-inquiry-into-the-cyber-attack-on-singhealth-s-it-system>

difference policy/structure level vs implementation level

Next Week

- ▶ Information Security Policy
 - ▶ Chapter 4

IS4231

Information Security Management

Lecture 4

InfoSec Policies

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 4

Learning Objectives

- ▶ Describe the three major types of information security policy and discuss the major components of each
 - ▶ Enterprise information security program policy
 - ▶ Issue-specific security policy
 - ▶ System-specific security policy



|

What are Information Security Policies?

- ▶ Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets

Audience are for the other employees in the company

- ▶ Stipulate what is proper behavior when using information and information assets
 - ▶ Provide structure in the workplace
 - ▶ Create a productive & effective work environment, free from unnecessary distractions and inappropriate actions
 - ▶ Essential foundation of an effective InfoSec program
-
- ▶ Policies are the least expensive means of control and often the most difficult to implement

What are Information Security Policies? (cont.)

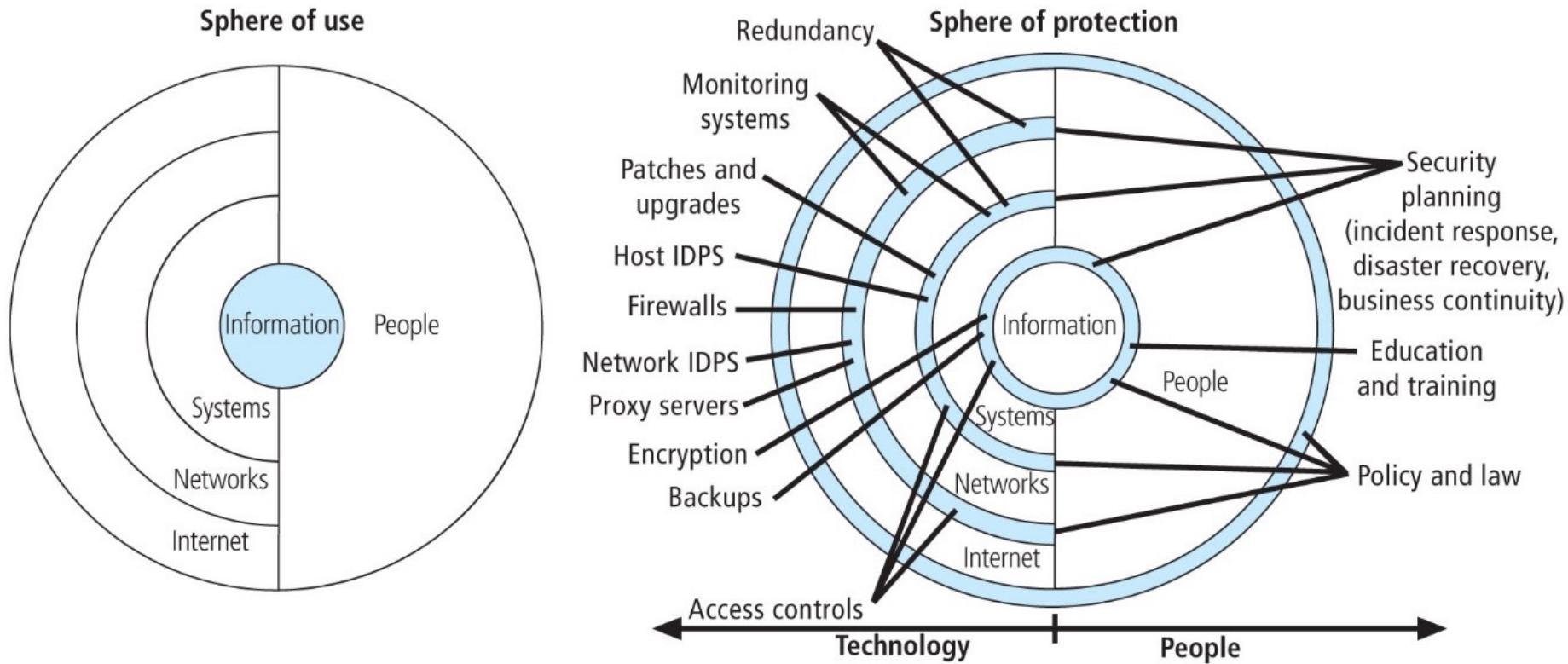
“Policies are important reference documents for internal audits and for the resolution of legal disputes about management’s due diligence, and policy documents can act as a clear statement of management’s intent”

-Information Security Policies Made Easy



For the SingHealth data breach - there are already flaws at a policy level

Spheres of Security



Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

Figure 4-1 Spheres of security

Basic Rules and Guidelines

- ▶ Some basic rules when shaping a policy:
 - ▶ Policy should never conflict with law
 - ▶ Policy must be able to stand up in court if challenged
 - ▶ Policy must be properly supported and administered

- ▶ Guidelines help the formulation of IT and InfoSec policy:
 - ▶ All policies must contribute to the success of the organization
 - ▶ Management must ensure the adequate sharing of responsibility for proper use of information systems
 - ▶ End users of information systems should be involved in the steps of policy formulation

Policy, Standards, and Practices (cont.)

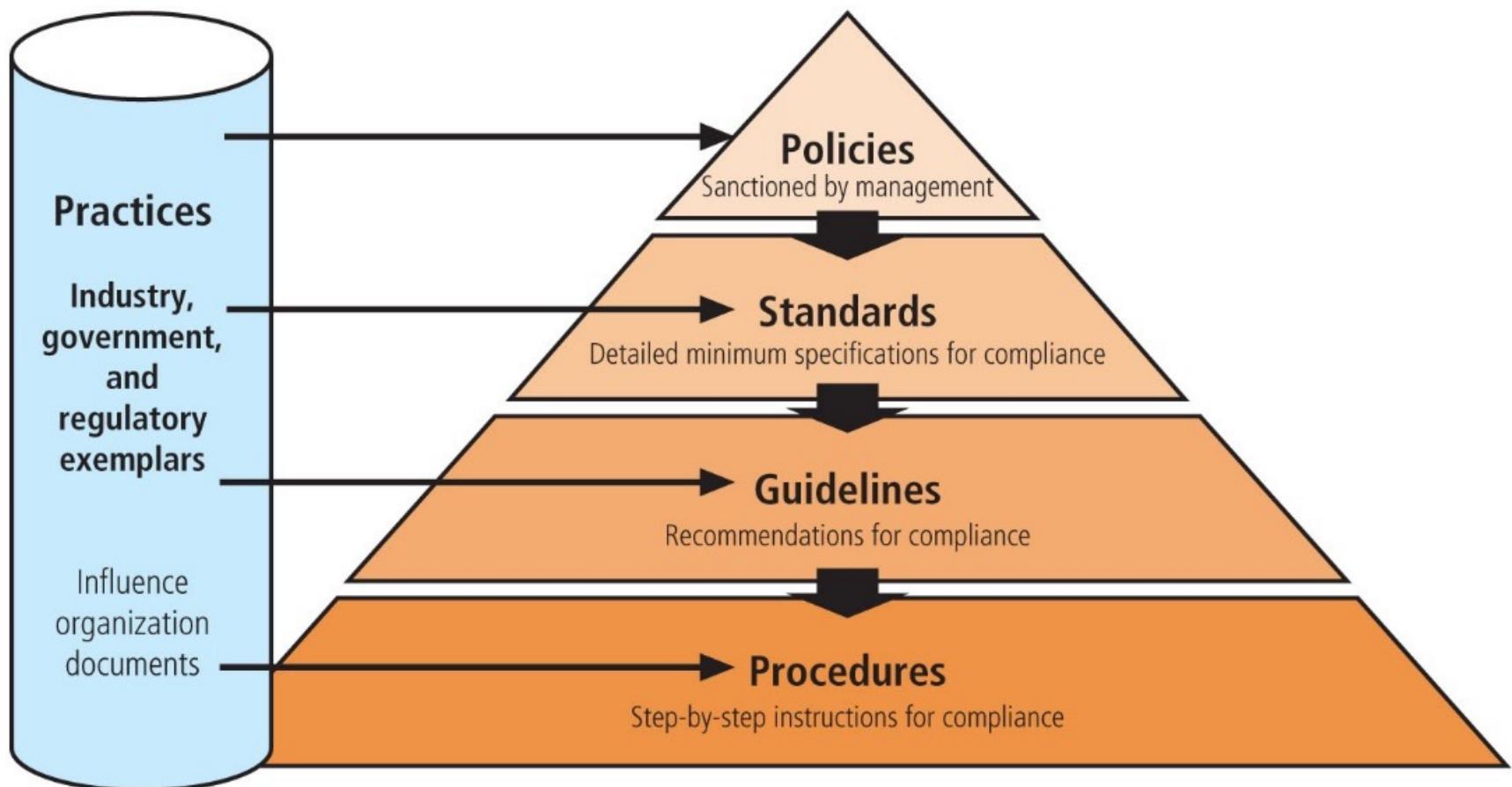


Figure 4-3 Policies, standards, practices, procedures, and guidelines

Policy, Standards, and Practices

- ▶ **Policies:** define what you can do and can not do, whereas the other documents focus on the how
- ▶ **Standards:** A detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance.
- ▶ **Practices, procedures, and guidelines:** explain how employees are to comply with policy.

Example

Need all to have a complete set - to ensure that everyone, including those who are not as competent using tech are able to understand and follow

- ▶ **Policy:**
 - ▶ Use strong passwords, frequently changed
- ▶ **Standard:**
 - ▶ Must be at least 8 characters, with at least one number, one letter, and one special character
- ▶ **Guideline:**
 - ▶ “We recommend you don’t use family or pet name, or parts of your birthday information, phone number in your password”
- ▶ **Practices**
 - ▶ Change semi-annually
- ▶ **Procedures**
 - ▶ Step-by-step instructions “first click Windows Start button, then...”

if there is a need to trust the end users to be honest, then it might not be too successful

Successful Policy Characteristics

- ▶ **Endorsed**
 - ▶ Management supports the policy
- ▶ **Relevant**
 - ▶ The policy is applicable and supports the goals of the organization
- ▶ **Realistic**
 - ▶ The policy makes sense
- ▶ **Attainable**
 - ▶ The policy can be successfully implemented
- ▶ **Adaptable**
 - ▶ The policy can be changed
- ▶ **Enforceable**
 - ▶ Controls that can be used to support and enforce the policy exist
- ▶ **Inclusive**
 - ▶ The policy scope includes all relevant parties

Three types of InfoSec Policies

- ▶ A complete Infosec policy must define three types of information security policy:
 - ▶ Enterprise information security program policy
 - ▶ Issue-specific information security policies
 - ▶ Systems-specific policies
- ▶ Based on NIST's "Special Publication 800-14"
 - ▶ NIST: National Institute of Standards and Technology
 - ▶ Outlined what is required of senior managers when writing InfoSec policy



Enterprise information security program policy (EISP)

What is an EISP?

- ▶ **EISP**
 - ▶ The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts.
- ▶ **Also knowns as**
 - ▶ Security program policy
 - ▶ General security policy
 - ▶ IT security policy
 - ▶ High-level InfoSec policy
 - ▶ InfoSec policy
- ▶ **Must directly support the organization's vision and mission statements.**

EISP Elements

- ▶ EISP documents should include:
 - ▶ An overview of the corporate **philosophy** on security
 - ▶ Information on the **structure** of the InfoSec organization and individuals who fulfill the **InfoSec roles**
 - ▶ Fully articulated **responsibilities** for security that are **shared by all members of the organization** (employees, contractors, consultants, partners, and visitors)
 - ▶ Fully articulated **responsibilities** for security that are **unique to each role within the organization**

EISP Elements

Table 4-1 Components of the EISP

Component	Description
Purpose	<p>Answers the question, "What is this policy for?" Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis:</p> <p><i>This document will:</i></p> <ul style="list-style-type: none">• <i>Identify the elements of a good security policy</i>• <i>Explain the need for information security</i>• <i>Specify the various categories of information security</i>• <i>Identify the information security responsibilities and roles</i>• <i>Identify appropriate levels of security through standards and guidelines</i> <p><i>This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.⁵</i></p>
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
References	Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.

Chapter 1 NUS IT Security Policy: Introduction to Information Technology (IT) Security Policy

Purpose and Scope

1 Purpose and scope

The purpose of this Policy is to define the minimum security measures required for the protection of information systems as well as the information contained and processed by the systems. These controls are described throughout the remaining sections of the Policy.

2 Introduction

Information in IT Systems is an asset which, like other important business assets, has value and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure operations continuity and minimize business damage and maximize return on IT investments.

The National University of Singapore (NUS) information systems landscape comprises of a broad range of information systems from personal Internet/Intranet web servers to highly sensitive and critical corporate systems. The systems have different characteristics in the following key areas:

- Sensitivity of information
- Criticality to operations of the University, Departments and Faculties
- Risk exposure
- Potential impact to NUS in the event of a security breach

The implementation and management of the security of this diverse range of systems, with varying security requirements, throughout the entire system life cycle, will be addressed by the NUS IT Security Policy.

The Policy defines security measures so that NUS information assets are protected and consistency in the implementation and practice of security throughout NUS can be achieved.

Definition of information security

Need for information security

Philosophies

Compliance

3.2 Intended audience

3.2.1 This IT Security Policy is intended to be read by all staff and students of NUS and all other external parties that have dealings with NUS information system resources, including the use, design, audit, implementation and maintenance of these resources.

3.3 Key security objectives

3.3.1 Information security is characterized here as the preservation of three key security objectives:

- Confidentiality: ensuring that information is accessible only to authorized users;
- Integrity: safeguarding the accuracy and completeness of information and information processing systems;
- Availability: ensuring that authorised users have access to information and associated assets when required.

Increasingly, organizations and their information systems and networks are faced with security threats that attempt to compromise one or more of the above security objectives. These threats, from a wide range of sources, include computer-assisted fraud, espionage, sabotage, vandalism, fire or flood, computer viruses, computer hacking and denial of service attacks. Incidents and attacks arising from such threats have become more common and attacks have become more ambitious and increasingly sophisticated.

Information security is a process, which is achieved by implementing a suitable set of security measures, covering physical, environmental, personnel, technical and organisation structures security standards and procedures. These controls, as defined in the NUS IT Security Policy together with more detailed security procedures and guidelines, need to be established to ensure that NUS information systems and assets are adequately protected from a wide range of security threats.

3.4 Non-compliance

3.4.1 Every staff, student and external party that has dealings with NUS information system resources is responsible for protecting and preserving the information in accordance with NUS IT Security Policy

Non-compliance with NUS IT Security Policy is viewed seriously and will result in disciplinary action up to and including legal action and termination.

Chapter 3 NUS IT Security Policy: IT Security Management

Governance
Responsibilities
Unique roles

1 Purpose and scope

This chapter defines the various roles within NUS that are assigned responsibilities pertaining to the protection of information resources.

2 Introduction

Everyone associated with NUS has a role in information security. Due care must be exercised in the protection of IT information resources by clearly defining roles and responsibilities of management and users relating to information security.

3 Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

3.2 Information security responsibilities

3.2.1 Management of Computer Centre sets strategic direction for NUS information security initiatives and provides support, commitment and resources for NUS information security initiatives.

3.2.2 Please refer to the NUS Data Management Policy for the details of the roles and responsibilities of the following:

Data Owner
Data Stewards
Data Managers
System Owners
Data Users
Data Administrators
Database Administrators
Application Developers
Infocomm Security Group

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.



Even for data users, there must be policies in place to ensure data users are accountable for any misconduct

Students are not considered owners - even the students emails/work/research paper

Domains

Table of Contents

Chapter 1	Introduction to Information Technology (IT) Security Policy	3
Chapter 2	Risk Analysis for Information Systems	5
Chapter 3	IT Security Management	7
Chapter 4	Access Control Security	10
Chapter 5	Personnel Security	18
Chapter 6	Physical and Environmental Security	20
Chapter 7	Network Management	26
Chapter 8	Operations Management.....	30
Chapter 9	Incident Management.....	36
Chapter 10	System Development and Maintenance.....	38
Chapter 11	Compliance	45

Issue-Specific Security Policy (ISSP)

What is an ISSP?

- ▶ **ISSP**
 - ▶ An organization policy that provides detailed, targeted guidance to instruct all members of the organization in the use of **a resource**, such as one of its process or technologies.
 - ▶ Referred to as *fair and responsible use policies*
- ▶ **An effective ISSP** SOP
 - ▶ It articulates the organization's expectations about how its technology-based system should be used
 - ▶ It documents how the technology-based system is controlled and identifies the processes and authorities that provide this control
 - ▶ It indemnifies the organization against liability for an employee's inappropriate or illegal use of the system

What is an ISSP? (cont.)

- ▶ Every organization's ISSP has three characteristics:
 - ▶ Address specific technology-based systems
 - ▶ **Require frequent updates**
 - ▶ Contain an issue statement on the organization's position on an issue

ISSP Topics

- ▶ Use of electronic mail, IM, and other communications apps
- ▶ Use of the Internet, the Web, and company networks by company equipment
- ▶ Malware protection requirements
- ▶ Use of nonorganizationally issued software or hardware on organization assets
- ▶ Use of organizational information on nonorganizationally owned computers
- ▶ Prohibitions against hacking or testing security controls or attempting to modify or escalate privileges
- ▶ Personal and/or home use of company equipment
- ▶ Removal of organizational equipment from organizational property
- ▶ Use of personal equipment on company networks (BYOD)
- ▶ Use of personal technology during work hours
- ▶ Use of photocopying and scanning equipment
- ▶ Requirements for storage and access to company information while outside company facilities
- ▶ Specifications for the methods, scheduling, conduct, and testing of data backups
- ▶ Requirements for the collection, use, and destruction of information assets
- ▶ Storage of access control credentials by users

ISSP Elements

- ▶ **Statement of Purpose:** outline the scope and applicability of the policy
 - ▶ Scope and Applicability
 - ▶ Definition of Technology Addressed
 - ▶ Responsibilities
- ▶ **Authorized Access and Usage of Equipment:** explain who can use the technology governed by the policy and by what purposes
 - ▶ User Access
 - ▶ Fair and Responsible Use
 - ▶ Protection of Privacy
- ▶ **Prohibited Usage of Equipment:** outlines what it cannot be used for
 - ▶ Disruptive Use or Misuse
 - ▶ Criminal Use
 - ▶ Offensive or Harassing Materials
 - ▶ Copyrighted, Licensed or other Intellectual Property
 - ▶ Other Restrictions
- ▶ **Systems Management:** specify users' and systems administrators' responsibilities
 - ▶ Management of Stored Materials
 - ▶ Employer Monitoring
 - ▶ Virus Protection
 - ▶ Physical Security
 - ▶ Encryption
- ▶ **Violations of Policy**
 - ▶ Procedures for Reporting Violations
 - ▶ Penalties for Violations
- ▶ **Policy Review and Modification**
 - ▶ Scheduled Review of Policy and Procedures for Modification
- ▶ **Limitations of Liability**
 - ▶ Statements of Liability or Disclaimers

Example: NUS Data Management Policy

NUS DATA MANAGEMENT POLICY

Policy Information	
Category	Governance/Administrative/Operational
Department Responsible	NUS Information Technology (NUS IT)
Contact	Email: dmp@nus.edu.sg
Governance (approved by)	Data Governance and Management Steering Committee (DGMSC)
Audience (applies to)	All users of University Data including: <ul style="list-style-type: none">• NUS Faculty and Staff• Part-time Teaching Staff• Contingent (casual/temporary) Staff• NUS and Non-NUS Student assistants, interns, helpers or volunteers (e.g. in departments, NUSSU, clubs and societies, halls and residences)• Volunteers• Contractors, vendors, temporary workers
Brief Purpose	Defines general principles to govern the appropriate collection, use, maintenance, disclosure, disposal and protection of University Data
Initial Version	Version 1.6 – 15 May 2007
Current Version	Version 3.0 – 1 May 2020

Example: NUS Data Management Policy

1. PURPOSE

- 1.1 The NUS Data Management Policy ("DMP") governs the collection, use, maintenance, disclosure, disposal and protection of University Data and defines the general principles to safeguard University Data.

The six general principles are:

- (i) Shared Responsibility through Data Stewardship and Usage
- (ii) Confidentiality through Data Classification
- (iii) Single Source of Truth through Data Collection and Storage
- (iv) Need To Know through Data Sharing and Disclosure
- (v) Need To Keep through Data Retention and Disposal
- (vi) Security through Data Protection

Single source of truth is important for access control

- 1.2 Users must adhere to the DMP and use University Data only for the University's purposes to advance its interests. A secure, reliable and accessible University Data source is a valuable asset that will enable the University to make effective decisions to meet the University's education and research objectives as well as comply with the law.
- 1.3 The DMP serves as an overarching policy for all data management-related documents and activities in the University. As such, all data management-related policies, standards, procedures and guidelines must be aligned with the DMP.

2. DEFINITIONS AND SCOPE

- 2.1 Please refer to **Appendix A** for all Definitions referenced in this DMP.
- 2.2 University Data refers to any data or information created, collected, processed, derived or used in any form or medium by the University and its representatives, regardless of where or how it is stored, its mode of transmission, who is using it, or, from where or how its access is gained.

University Data includes both electronic and non-electronic forms of data.

It includes Administrative Data and Research Data (both of which include Personal Data and Analytics Data).

It excludes Teaching and Instructional Materials.

Case: NUS Email Usage Policy #1

5.4 Email

Email is used frequently for correspondence internally and externally for teaching, research, learning, administration or otherwise carry out the functions and purposes of the University.

- (i) Users shall not email or transmit defamatory, threatening or abusive messages or any messages that may be reasonably construed as such.
- (ii) Users shall not send annoying, abusive or unwanted messages to others.
- (iii) Users shall not send unsolicited mass emails within or external to the University, except for purposes specific to the functions and purposes of the University, or which have been approved by a Dean or Director or University representative with equal or higher authority, and in accordance with the requirements of law.
- (iv) Users shall not forward messages containing general appeals or warnings like 'virus warnings', 'request for help', by mass mail or otherwise. Users should instead send these messages to the University's NUS IT's helpdesk for verification.
- (v) Users shall not forge the identity of or impersonate another person in an email.
- (vi) Users shall not knowingly transmit by email any harmful or malicious content (e.g. viruses) or any other content or material that may otherwise violate the civil and criminal laws of Singapore.
- (vii) Users shall not misuse mailing lists to flood an individual, group or the email system with numerous or large emails.

Case: NUS Email Usage Policy #2

5.5 Staff and Contingent Worker Email

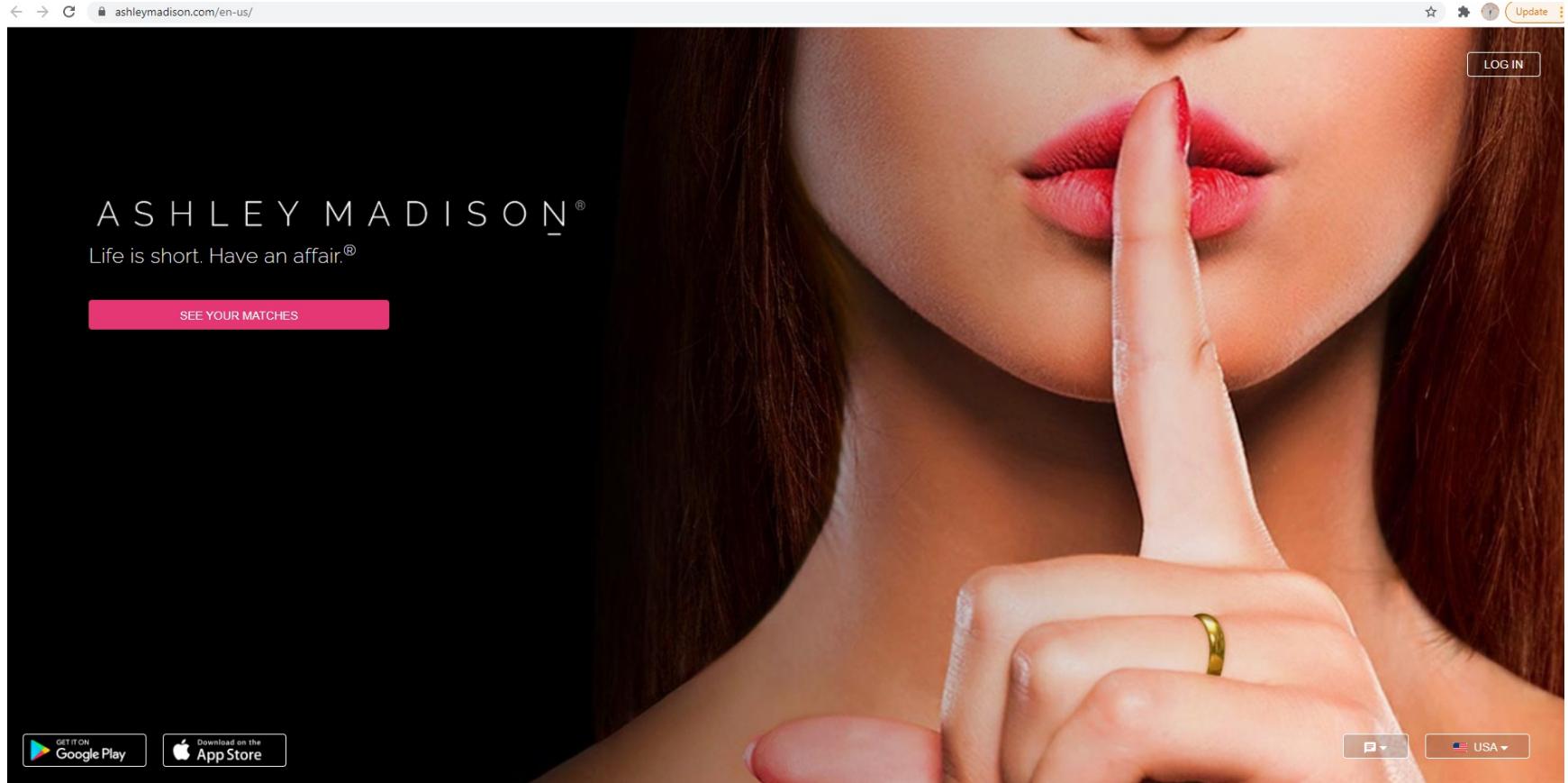
- (i) Staff and Contingent Workers may use their University Assigned Email Accounts (as defined in the Guidelines for Acceptable Use Policy for NUS IT Resources) for incidental personal purposes provided that such use does not:
 - (a) interfere with the University's operations;
 - (b) interfere with the staff's employment or other obligations to the University; or
 - (c) burden the University with noticeable costs.
- (ii) All Executive and Professional staff, Non-academic staff and Academic Appointment Holder (as defined in Appendix A), shall always use their University Assigned Email Accounts for official correspondence. Staff will compromise the

NUS INTERNAL



privacy and confidentiality of University data by not using their University Assigned Email Account or redirecting the email message from their University Assigned Email Account.

Case: Ashley-Madison Data Breach 2015



Case: Ashley-Madison Data Breach 2015

ASHLEY MADISON HACK TIMELINE: KEY EVENTS IN THE ASHLEY MADISON DATA BREACH STORY

AVID LIFE MEDIA EMPLOYEES GET 'THUNDERSTRUCK'

July 12, 2015: Avid Life Media (Ashley Madison's parent firm) employees log in to find a message from Impact Team threatening to release company and customer data unless the Ashley Madison and Established Men websites are shut down. Impact Team's ransom message is accompanied by the AC/DC song "Thunderstruck."

IMPACT TEAM ANNOUNCES HACK OF ASHLEY MADISON

July 19, 2015: Impact Team publishes their warning message on Pastebin, this time setting a 30 day window for Avid Life Media to shut down the sites before the information is released. The warning is followed by an article from security journalist Brian Krebs announcing the Ashley Madison data breach.

AVID LIFE MEDIA RESPONDS

July 20, 2015: Avid Life Media issues two statements acknowledging "an attempt by an unauthorized party to gain access to our systems" and announcing a joint investigation conducted by Ashley Madison, law enforcement, and the cybersecurity service provider Cucurum.

IMPACT TEAM RELEASES TWO ASHLEY MADISON USER NAMES

July 22, 2015: Impact Team releases the names and information of two Ashley Madison users - a man from Brockton, MA and a man from Ontario, Canada - in the first data leak to come from the hack.

Source: <https://digitalguardian.com/blog/timeline-ashley-madison-hack>

'TIME'S UP' FOR ASHLEY MADISON: THE FIRST DATA DUMP

August 18, 2015: Impact Team's 30 day window expires, but Ashley Madison and Established Men are still online. In a Pastebin post titled "TIME'S UP," Impact Team publishes the first major Ashley Madison user data dump, a torrent file containing nearly 10gb of user email addresses. Media outlets and researchers alike scramble to analyze and validate the data.

ANOTHER STATEMENT FROM AVID LIFE MEDIA

August 18, 2015: Following the first data dump, Avid Life Media issues another statement on the hack detailing their investigation and asking for information on the incident.

Ashley Madison User Emails Published By Category

August 18, 2015: A categorical breakdown of the email addresses disclosed in the first data dump is posted to Pastebin, revealing many government, military, and corporate addresses that were used to sign up for Ashley Madison accounts.

FIRST DATA DUMP CONFIRMED REAL

August 18-19, 2015: After a nearly day-long media frenzy met with much speculation over the validity of the leaked data, Brian Krebs discloses that numerous Ashley Madison account holders have confirmed that their information was published.

ASHLEY MADISON SEARCH WEBSITES APPEAR

August 19-20, 2015: As researchers continue to sift through the first data dump, search websites pop up that let users search to see if their email addresses were leaked.

System-Specific Security Policy (SysSPs)

What are SysSPs?

- ▶ **SysSPs:**
 - ▶ Organizational policies that often function as standards or procedures to be used when configuring or maintaining systems.
 - ▶ E.g., to configure and operate a network firewall
- ▶ **Two general kinds of SysSPs:**
 - ▶ Managerial Guidance SysSPs
 - ▶ To guide the implementation and configuration of technology
 - ▶ Technical Specification SysSPs
 - ▶ System administrators directions on implementing managerial policy
 - ▶ Each type of equipment has its own type of policies
 - ▶ Two general methods of implementing such technical controls:
 - Access control lists
 - Configuration rules

What are SysSPs?

- ▶ **Access control lists**
 - ▶ Include the user access lists, matrices, and capability tables that govern the rights and privileges
 - ▶ In general ACLs regulate:
 - ▶ Who can use the system
 - ▶ What authorized users can access
 - ▶ When authorized users can access the system
 - ▶ Where authorized users can access the system from
 - ▶ How authorized users can access the system
- ▶ **Configuration rules**
 - ▶ Configuration rules are instructional codes that guide the execution of the system when information is passing through it



What are SysSPs?

Source: packet "from." **Destination:** packet "to."
Zone: port of origin or destination of the packet.
Address: IP address. **User:** predefined user groups.

Action specifies whether the packet from Source: is allowed or dropped.

Rules 16 and 17 specify any packet involving use of the BitTorrent application is automatically dropped.

Rule 22 ensures any user in the Internal (Trusted) network: L3-Trust is able to access any external Web site.

The screenshot shows the Palo Alto Networks Firewall configuration interface. The main window displays a table of firewall rules. A callout box points to rule 16, which denies BitTorrent traffic from any source to any destination. Another callout box points to rule 22, which allows traffic from the L3-Trust zone to any destination. A third callout box points to the Tag Browser window, which lists various security tags and their associated rules. The interface includes tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, and Device, along with a search bar and various configuration options at the top.

Name	Zone	Address	User	Zone	Address	Application	Service	Action
13 DemoApp-KnownUser...	p2	L3-Untrust	any	know...	p2	L3-Untrust	Local-Untrust	Allow
14 SSH-Shared-DenyAll	p2	L3-Untrust	any	any	p2	L3-Untrust	Local Untrust	Deny
15 WebDynamicDemo	p2	L3-Untrust	web-access...	any	p2	L3-Trust	any	Allow
16 BitTorrent-Deny-Unt...	p2	L3-TAP	any	unkn...	p2	L3-TAP	any	Drop
17 BitTorrent-Deny-Sr...	p2	L3-TAP	10.154.168.19...	any	p2	L3-TAP	any	Drop
18 MineMeld-SSH	p2	L3-Untrust	199.167.52.0/22	any	p2	L3-Trust	MineMeld	Allow
			CorpDSL				ssh	
			CorpLab				ssl	
			CorpNet					
19 MineMeld-web-feed	p2	L3-Untrust	any	any	p2	L3-Trust	MineMeld	Allow
20 MineMeld-console	p2	L3-Untrust	any	know...	p2	L3-Trust	MineMeld	Allow
21 MineMeld-console...	p2	L3-Untrust	any	any	p2	L3-Trust	MineMeld	Deny
22 Web-Browsing	p2	L3-Trust	any	any	p2	L3-Untrust	any	Allow
			ssl				application-default	
			web-browsing				TCP-8443	
23 Inbound SaaS	p2	L3-Untrust	US	any	p2	L3-Trust	99.99.99.99	Allow
			clicktools				ssl	
			sd				application-default	

Figure 4-7 Sample Palo Alto firewall configuration rules

Source: Palo Alto Software, Inc.

Guidelines for Effective Policy Development and Implementation

Roles involved in Policy Development and Implementation

- ▶ Chief information security officer (CISO)
- ▶ Cybersecurity steering committee
- ▶ Compliance officer
- ▶ Privacy officer risk officer
- ▶ Internal audit
- ▶ Incident response team
- ▶ Data owners
- ▶ Data custodians
- ▶ Data users
- ▶ Etc.

Guidelines for Effective Policy

- ▶ For policies to be effective, they must be properly:
 1. Developed using industry-accepted practices, and formally approved by management
 2. Distributed using all appropriate methods
 3. Read by all employees
 4. Understood by all employees
 5. Formally agreed to by act or affirmation
 6. Uniformly applied and enforced

Policy Development and Implementation Using the SecSDLC

- ▶ A policy development or redevelopment project should be
 - ▶ Well planned
 - ▶ Properly funded
 - ▶ Aggressively managed to ensure that it is completed on time and budget
- ▶ Use adaptation of SecSDLC for complete policy life-cycle

1. Investigation Phase

- ▶ The policy development team should attain:
 - ▶ Support from senior management
 - ▶ Support and active involvement of IT management, specifically the CIO
 - ▶ Clear articulation of goals
 - ▶ Participation of the correct individuals from the communities of interest affected by the policies
 - ▶ Assign a project champion with sufficient stature and prestige
 - ▶ Acquire a capable project manager
 - ▶ A detailed outline of the scope of the policy development project and sound estimates for the cost and scheduling of the project

2. Analysis Phase

- ▶ The Analysis phase should include the following activities:
 - ▶ A new or recent risk assessment or IT audit documenting the current InfoSec needs of the organization
 - ▶ The gathering of key reference materials—including any existing policies
- ▶ Determine the fundamental policy philosophy
 - ▶ “Whitelist” approach
 - ▶ “That which is not permitted is prohibited”
 - ▶ “Blacklist” approach
 - ▶ “That which is not prohibited is permitted”

NUS uses an blacklist approach

3. Design Phase

- ▶ The first task in the design phase is the *drafting* of the actual policy document
- ▶ There are a number of references and resources available
 - ▶ The Web
 - ▶ Government Sites
 - ▶ Professional Literature
 - ▶ Peer networks
 - ▶ Professional Consultants
- ▶ Next, the development team or committee reviews the work makes recommendations about its revision
- ▶ Once the committee approves the document, it goes to the approving manager or executive for sign-off

4. Implementation Phase

- ▶ The team must create a plan to *distribute* and verify the distribution of the policies
- ▶ Members of the organization must explicitly acknowledge that they have received and read the policy (compliance)
- ▶ The simplest way
 - ▶ Attach a cover sheet that states “I have received, read, understood, and agreed to this policy”
 - ▶ The employee’s signature and date provide a paper trail of his or her receipt of the policy
- ▶ A stronger mechanism
 - ▶ A compliance assessment

5. Maintenance Phase

- ▶ The policy development team monitors, maintains, and modifies the policy
- ▶ The policy should have a built-in mechanism via which users can report problems with the policy
 - ▶ Preferably anonymously

this is to help CIO owners to check and review their policies

- For CII 1 year
- For normal 5 years

Next Week

- ▶ Developing InfoSec Program
 - ▶ Chapter 5

IS4231

Information Security Management

Lecture 5

Developing the Security Programme

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 5

Learning Objectives

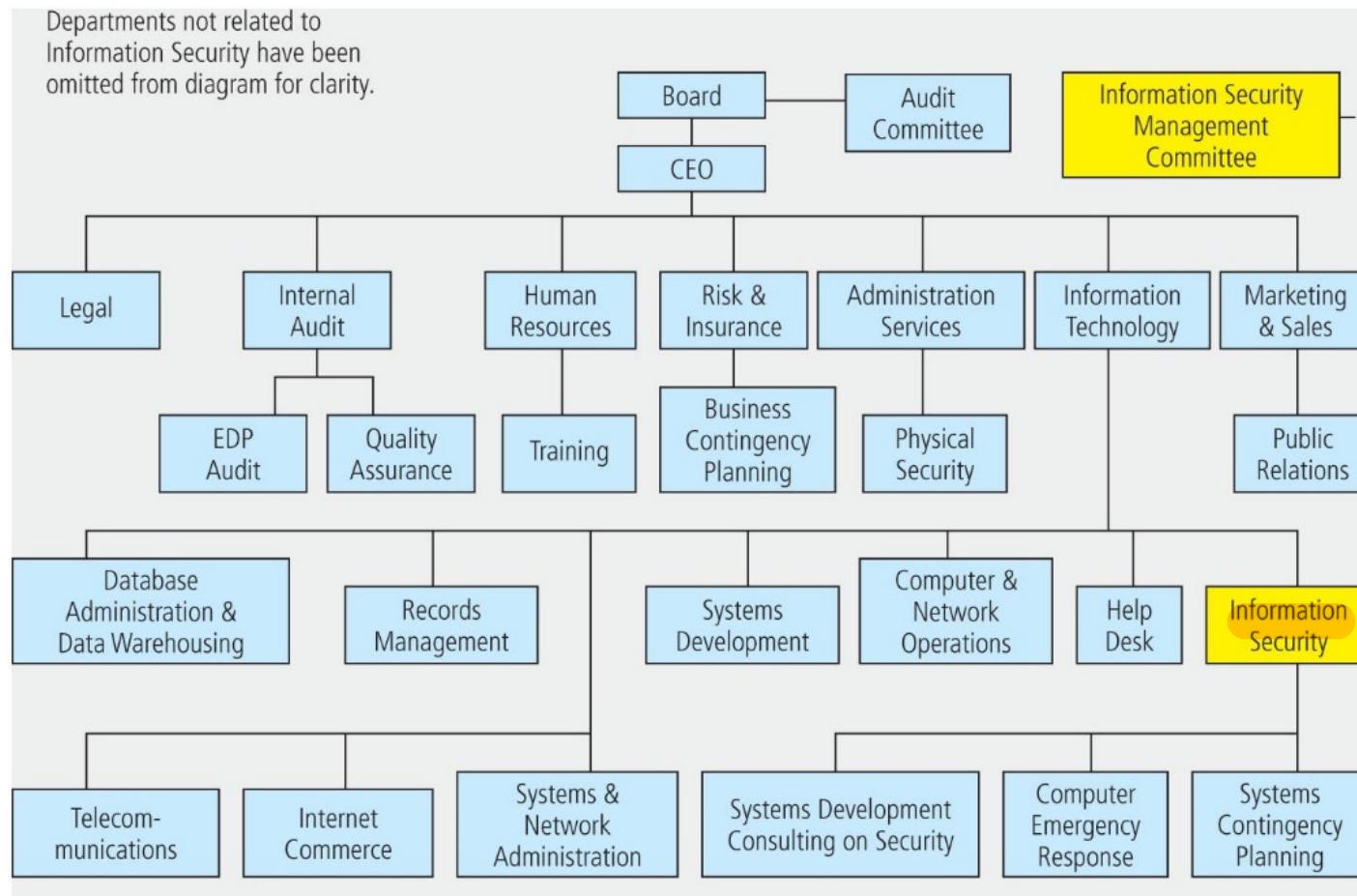
- ▶ List and describe the functional components of an information security program
 - ▶ Placing InfoSec Within an Organization
 - ▶ Components of the Security Program
 - ▶ Staffing the Security Function
- ▶ Components of a security program



|

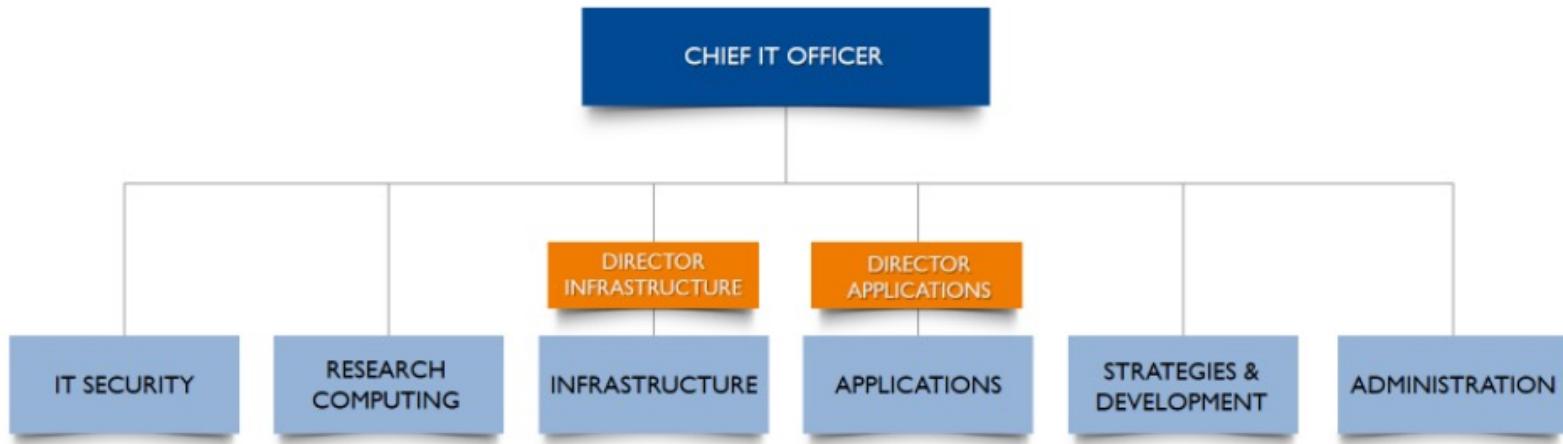
Placing InfoSec Within an Organization

Option 1: InfoSec Reports to IT Dept



Example: NUS

NUS IT ORGANISATION CHART



Source: <https://nusit.nus.edu.sg/about/organisation-structure/>

Option 1: InfoSec Reports to IT Dept

▶ Pros:

- ▶ CIO understands IS technical issues, **shared common language**
- ▶  Only CIO between InfoSec manager and CEO, **efficient communication**

▶ Cons:

- ▶ Inherent conflict of interest when confronted with resource allocation decisions or when required to make trade-offs
 - ▶ e.g., cost minimization, enhanced user friendliness, rapid time-to-market with a new product or service



Discussion: SingHealth Data Breach

► Organizational Structure in iHiS

“Reflecting on the structure of incident reporting at IHiS, he pointed out that its IT security team is a sub-unit of its infrastructure services, which sits within IHiS' delivery group. Reported security issues could thus be overlooked in favour of service delivery objectives.”

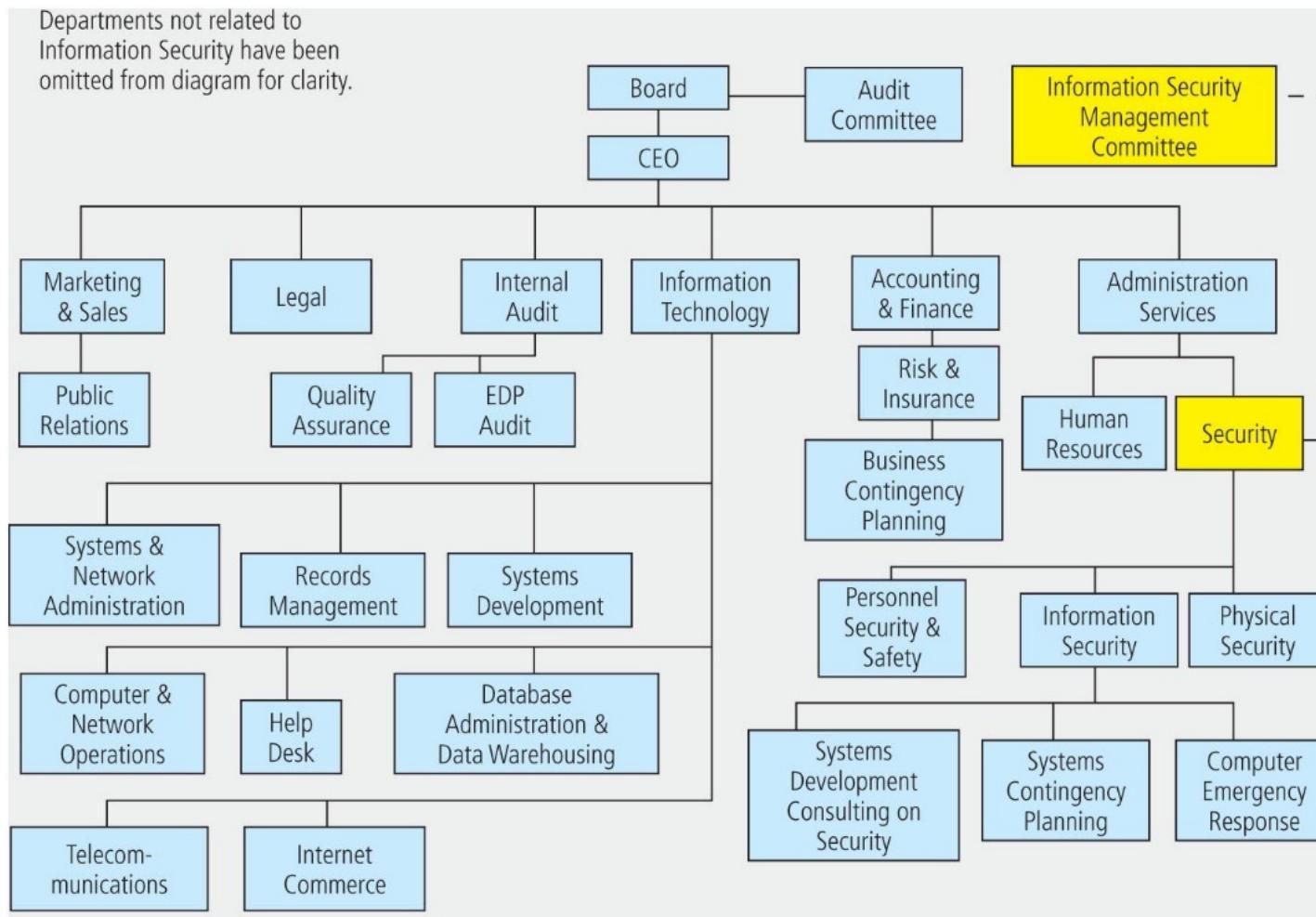
“The structure could mean the security team does not get proper access to appropriate-level managers, which makes it difficult to escalate problems. Key decision-makers might also not be fully aware of security and operational concerns.”



— Mr David Koh, CSA chief

Source: <https://www.straitstimes.com/singapore/senior-leaders-have-key-role-in-cyber-security-commissioner>

Option 2: InfoSec Reports to Broadly Defined Security Dept



Option 2: InfoSec Reports to Security Dept

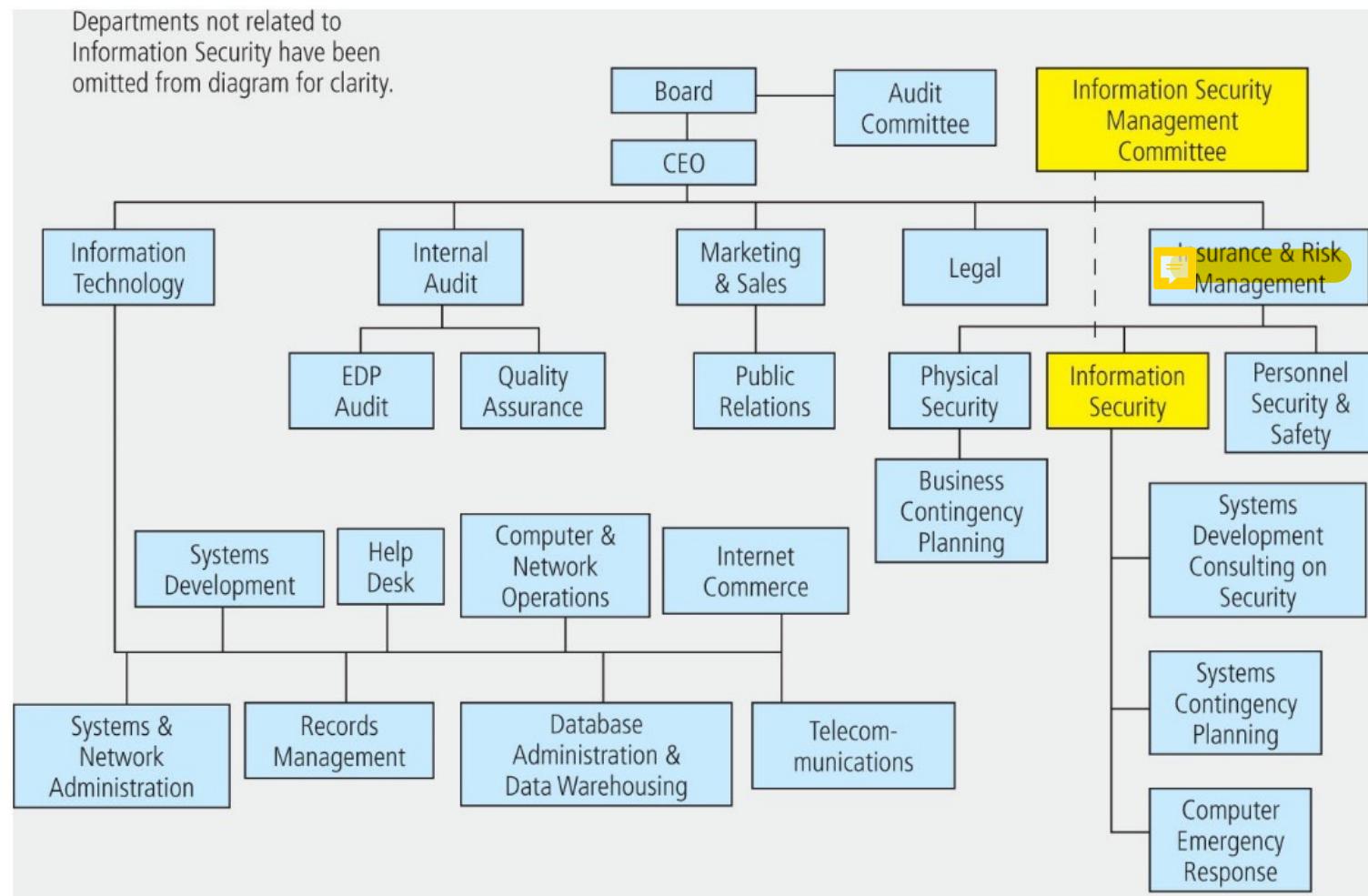
▶ Pros:

- ▶ It facilitates communication with others who have both a security perspective and related security responsibilities.

▶ Cons:

- ▶ InfoSec staff might be uncomfortable, see themselves as high-tech workers.
- ▶ The budget for physical security has not increased much over  the years, the top management may underestimate the resources InfoSec function will need.
- ▶ Security manager often lack an appreciation of information system technology, poor communicator with top management

Option 3: InfoSec Reports to Insurance & Risk Management Dept



Option 3: Infosec Reports to Insurance & Risk Management Dept

▶ Pros:

- ▶ It fosters an integrated risk management perspective
 - ▶ A centralized perspective prioritizes and compares all risks across the organization

▶ Cons:

- ▶ Chief risk managers not familiar with IT technology, lack shared language
- ▶ Its focus is quite strategic, the operational and administrative aspects of information security may not get enough attention and support
- ▶ Adopted for information intensive organizations
 - ▶ E.g., banks, stock brokerages

Example: OCBC Org Chart

Mr Vincent Choo



Group Risk Management

Mr Vincent Choo was appointed Head of Group Risk Management on 1 August 2014.

As Chief Risk Officer, he covers the full spectrum of risk, including Credit, Technology and Information Security, Liquidity, Market and Operational Risk Management. He reports jointly to both Group CEO and the Board Risk Management Committee of OCBC Bank. Mr Choo joined OCBC Bank from Deutsche Bank AG where his last appointment was Managing Director and Chief Risk Officer for Asia Pacific. In his 20 years at Deutsche Bank AG, he served in a number of senior roles including Head of Market Risk Management for Asia Pacific, with additional responsibilities for Traded Credit Products, and Head of New Product Approval for Asia. He holds a Master of Arts in Economics from University of Akron.

Mr Praveen Raina



Group Operations and Technology

Mr Praveen Raina was appointed Head of Group Operations and Technology in June 2021.

Mr Raina joined OCBC Bank in August 2008 and has held various senior positions in Group Operations and Technology. He was responsible for the bank's innovation efforts in technology development to deliver positive customer experience and capabilities across its touchpoints.

 is to develop IT solutions

Source: <https://www.ocbc.com/group/who-we-are/leaders-management-team.html>

Other approaches:

- ▶ Current movement: separate information security from the IT division
 - ▶ CISO report to CEO directly
 - ▶ E.g.,
 - ▶ Standard Chartered Korea
 - <https://www.standardchartered.co.kr/np/en/cms/cm/bi/EnOrganizationchart.jsp?menuId=HE05010500000000&rnb=4>

▶ Combined roles

- ▶ E.g.,
 - ▶ Rakuten Global Structure
 - <https://global.rakuten.com/corp/about/organization.html>

Staffing the Security Function

Staffing the Security Function

- ▶ A typical organization has a number of individuals with information security responsibilities
- ▶ While the titles used may be different, most of the job functions fit into one of the following:
 - ▶ Chief information security officer (CISO)
 - ▶ Security managers
 - ▶ Security administrators and analysts
 - ▶ Security technicians
 - ▶ Security staffers and watchstanders
 - ▶ Security consultants
 - ▶ Security officers and investigators
 - ▶ Help desk personnel

Information Security Positions

▶ InfoSec Roles

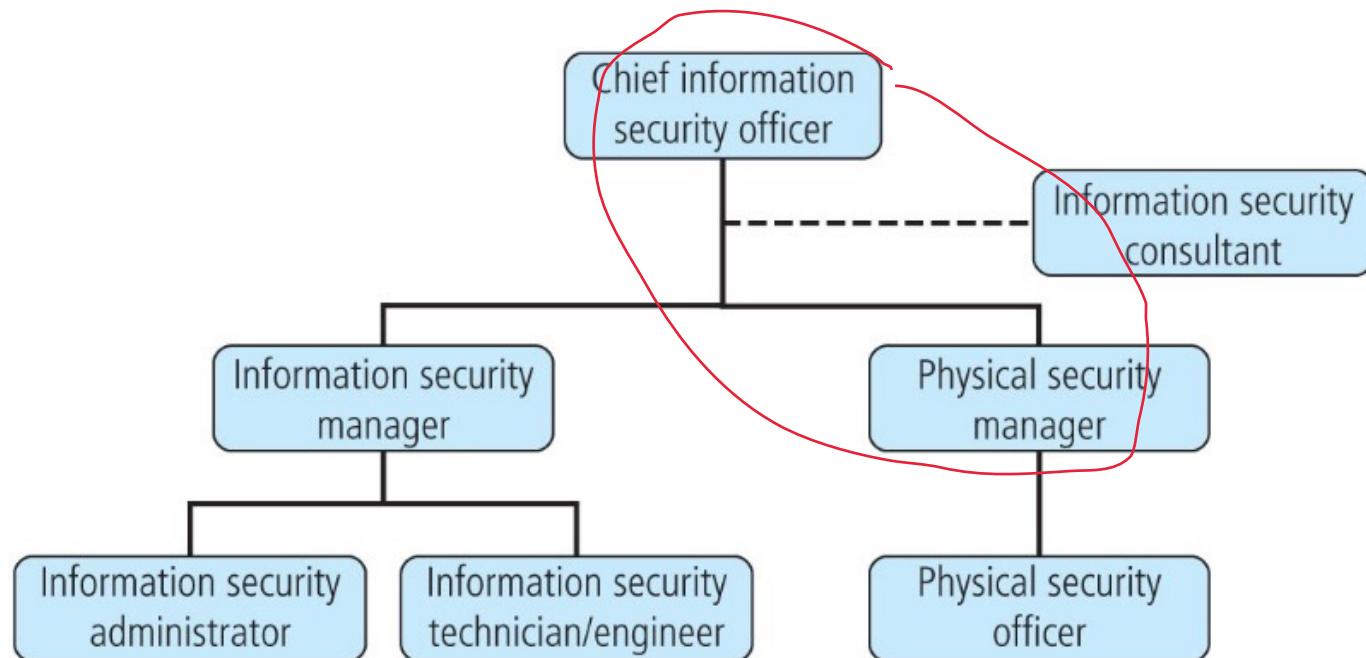


Figure 5-10 InfoSec roles

Information Security Positions

- ▶ **The CISO, or in some cases, the CSO**
 - ▶ is usually the top InfoSec officer in the organization and is the spokesperson for the security team and responsible for the overall InfoSec program
- ▶ **Security Managers**
 - ▶ accountable for the day-to-day operations of the InfoSec program
- ▶ **Security Administrators and Analysts**
 - ▶ The security administrator is a hybrid of a security technician and a security manager, with both technical knowledge and managerial skill

Information Security Positions

- ▶ **Security Technician**
 - ▶ A technically qualified individual who may configure firewalls and IDPSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technical controls are properly implemented
- ▶ **Security Staffers and Watchstanders**
 - ▶ Who perform routine watchstanding or administrative activities
- ▶ **Security Consultants**
 - ▶ An independent expert in some aspect of InfoSec
 - ▶ Usually brought in when the organization makes the decision to outsource one or more aspects of its security program
 - ▶ While it is usually preferable to involve a formal managed security services (MSS) company, qualified individual consultants are available for hire to organizations that do not choose to hire an MSS company

Information Security Positions

- ▶ **Security Officers and Investigators**
 - ▶ Occasionally, the physical security and InfoSec programs are blended into a single, converged functional unit
 - ▶ When that occurs, several roles are added to the pure IT security program, including physical security officers and investigators
- ▶ **Help desk**
 - ▶ Which enhances the security team's ability to identify potential problems

Some Staffing Model and Ratio...

- ▶ For every 500 to 750 IT users, you need one security operations full-time equivalent (FTE).
- ▶ For every 1,500 to 2,000 IT users, you need one security architecture FTE.
- ▶ For organizations with more than 4,000 IT users, you need to have a named security manager.
- ▶ For every 5,000 IT users, you need an IT risk FTE (this number varies significantly if you use a tool or are heavily regulated).
- ▶ Organizations with more than 7,500 IT users should have a dedicated security team with formal direct-line and dotted-line relationships.



Currently NUS has 50000 IT users (but ITSec has around 12)

Components of A Security Program

Information Security Program

- ▶ The structure and organization of the efforts to manage risks to an organization's information assets.
- ▶ Variables determining how a given organization chooses to structure its InfoSec program:
 - ▶ Organizational culture
 - ▶ Size
 - ▶ Security budget
 - ▶ etc

Elements of InfoSec Program

► NIST model

Table 5-2 Elements of a Security Program

Primary Element	Components
Policy	Program policy, issue-specific policy, system-specific policy
Program management	Central security program, system-level program
Risk management	Risk assessment, risk mitigation, uncertainty analysis
Life-cycle planning	Security plan, initiation phase, development/acquisition phase, implementation phase, operation/maintenance phase
Personnel/user issues	Staffing, user administration
Preparing for contingencies and disasters	Business plan, identify resources, develop scenarios, develop strategies, test and revise plan
Computer security incident handling	Incident detection, reaction, recovery, follow-up
Awareness and training	SETA plans, awareness projects, policy and procedure training
Security considerations in computer support and operations	Help desk integration, defending against social engineering, improving system administration
Physical and environmental security	Guards, gates, locks and keys, alarms
Identification and authentication	Identification, authentication, passwords, advanced authentication
Logical access control	Access criteria, access control mechanisms
Audit trails	System logs, log review processes, log consolidation and management
Cryptography	TKI, VPN, key management, key recovery

Source: NIST.

Elements of InfoSec Program

▶ ISO/IEC 27002: 2013 ISMS guideline

- ▶ 0. Introduction
- ▶ 1. Scope
- ▶ 2. Normative references
- ▶ 3. Terms and definitions
- ▶ 4. Structure of this standard
- ▶ 5. Information security policies
- ▶ 6. Organization of information security
- ▶ 7. Human resource security
- ▶ 8. Asset management
- ▶ 9. Access Control
- ▶ 10. Cryptography
- ▶ 11. Physical and environmental security
- ▶ 12. Operations security
- ▶ 13. Communication security
- ▶ 14. System acquisition, development, and maintenance
- ▶ 15. Supplier relationships
- ▶ 16. Information security incident management
- ▶ 17. Information security aspects of business continuity management
- ▶ 18. Compliance

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

I. Information security policies

- ▶ Management direction for information security
 - Review the organization's policies for information risk, security and related areas (e.g., governance, risk management, privacy, business continuity, compliance, HR, physical site security, change management, logging, classification, assets management, system development and acquisition...)
 - E.g., is there clear evidence of a sensibly designed and managed overall framework/structure/hierarchy?
 - E.g., Are the policies reasonably comprehensive, covering all relevant information risks and control areas?
 - E.g., How are the policies authorized, communicated, understood, and accepted?
 - Etc.

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

2. Organizations of information security

▶ Internal organization

- Information security roles and responsibilities
 - E.g., Is information risk and security given sufficient emphasis and management support?
 - E.g., Is there a senior management involved governance on InfoSec related issues?
 - E.g., Are roles and responsibilities clearly defined and assigned to suitable skilled individuals?
 - E.g., Are the information flow operating effectively in practice?
 - E.g., Is there adequate awareness of and support for the information risk and security structure and governance arrangement?

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

3. Human resources security

- ▶ Prior to employment
 - Screening
 - Terms and Conditions of employment**
- ▶ During employment
 - Information security awareness, education and training
- ▶ **Termination and change of employment**

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

4. Asset management

▶ Assets inventory

- Inventory List
 - E.g., digital data, hardcopy information, software, infrastructure, information service and service provider, physical security and safety, business relationship, people

- Ownership list

▶ Information classification

- Classification of information
- Labelling of information

Risk based approach - label via criticality of data

▶ Media handling

- Management of removable data
- Disposal of media
- Physical media transfer

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

5. Access control

- ▶ Business requirements of access control
 - ▶ Access control policy
- ▶ User access management
 - ▶ User registration and de-registration
 - ▶ User access provisioning
 - ▶ Management of privileged access rights
 - ▶ Management of secret authentication information of users
 - ▶ Review of user access rights
 - ▶ Removal or adjustment of access rights
- ▶ User responsibilities

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

6. Cryptography

▶ Cryptographic controls

- Principles
- Standards
- A risk-based process

▶ Key management

- Equipment protection
- Rules
- Back up
- Logging and auditing

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

7. Physical and environment security

- ▶ Secure areas
 - Physical security perimeter
 - Physical entry controls
 - Securing offices, rooms, and facilities
 - Protecting against external and external threats
 - Working in secure areas
 - Delivery and loading areas
- ▶ Equipment
 - Equipment siting and protection
 - Supporting utilities
 - Cabling security
 - Equipment maintenance
 - Removal of assets
 - Security of equipment and assets off-premises
 - Secure disposal or re-use of equipment
 - Unattended user equipment
 - Clear desk and clear screen policy

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

8. Operational security

- Operational procedures and responsibilities
 - Documented operating procedures
 - Change management
 - Capacity management
 - Separation of development, testing and operational environment
- Protection from malware
- Backup
- Logging and monitoring
- Control of operational software
- Technical vulnerability management
 - E.g., Are patches assessed for applicability and risks before being implemented?
 - E.g., Are the process for implementing urgent patches sufficiently slick and comprehensive?
 - E.g., To what extent does the organization depend on automated patch management, in effect accepting the associated risks of implementing rogue patches?
- Audit considerations

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

9. Communication security

- Network security management
 - Network controls
 - Security of network services
 - Segregation in network services
- Information transfer
 - Information transfer policies and procedures
 - Agreements on information transfer
 - Electronic messaging
 - Confidentiality or non-disclosure agreements

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

10. System acquisition, development and maintenance

- Security requirements of information systems
- Security in development and support processes
 - Secure development policy
 - System change control procedures
 - Technical review of applications after operating platform changes
 - Restrictions on changes to software packages
 - Secure system engineering principles
 - ▶ E.g.  DevSecOps
 - Secure development environments
 - Outsourced development
 - System security testing
 - System acceptance testing
- Test data

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

III. Supplier relationships

- ▶ Information security in supplier relationships
 - Information security policy for supplier relationships
 - Addressing security within supplier agreement
- ▶ Supplier service delivery management
 - Monitoring and review supplier services
 - Managing changes to supplier services

Elements of InfoSec Program

▶ ISO 27K ISMS Guideline

I2. Information security incident management

- Responsibilities and procedures

I3. Business continuity management

- Business continuity
- Redundancies

I4. Compliance

- Compliance with legal and contractual requirements
- Information security review
 - Independent review of information security
 - Compliance with security policies and standards
 - Technical compliance review

Next Week

- ▶ Security Management Practices
 - ▶ Chapter 9

IS4231

Information Security Management

Lecture 6

Security Management Practices

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 9

Learning Objectives

- ▶ List the elements of key information security management practices
 - ▶ Security employment practices
- ▶ Describe the key components of a security performance measurement program
 - ▶ Type 1: Implementation Measures
 - ▶ Type 2: Effectiveness/Efficiency Measures
 - ▶ Type 3: Impact Measures



Security Employment Practices

Hiring

- ▶ From an information security perspective, the hiring of employees is laden with potential security pitfalls
- ▶ The CISO, in cooperation with the CIO and relevant information security managers, should establish a dialogue with HR personnel so that InfoSec considerations become part of the hiring process



Background checks



Certifications



EMPLOYMENT POLICY

1. PURPOSE

The purpose of this policy is to define expectations, roles and responsibilities of all HAL employees with regular to regulatory hiring and employment compliance.

2. SCOPE

This policy applies to all HAL employees, management, contractors, interns and volunteers. This policy address all aspects of recruitment, hiring, evaluation and termination of HAL employees and contractors.

This policy describes HAL's objectives and policies regarding the maintenance of privacy and personnel information specifically including personally identifiable information (PII) and protected health information (PHI).

Policies

Non-Disclosure Agreement

(Confidentiality Agreement)

1. The confidential information to be disclosed by Discloser under this Agreement ("Confidential Information") can be described as and includes:

Technical and business information relating to Discloser's proprietary ideas, patentable ideas, copyrights and/or trade secrets, existing and/or contemplated products and services, software, schematics, research and development, production, costs, profit and margin information, finances and financial projections, customers, clients, marketing, and current or future business plans and models, regardless of whether such information is designated as "Confidential Information" at the time of its disclosure.

In addition to the above, Confidential Information shall also include, and the Recipient shall have a duty to protect, other confidential and/or sensitive information which is (a) disclosed by Discloser in

Covenants and agreements



EMPLOYMENT CONTRACT

THIS AGREEMENT, made as of the 21 day of March, 2016.

Between:

Hierarchical Access Limited Corporation Ltd.,
a company incorporated pursuant to the laws of the State of Georgia
(hereinafter referred to as "the Employer")

"And"

John Doe, (hereinafter referred to as "the Employee")

WHEREAS the Employee and the Employer wish to enter into an employment agreement governing the terms and conditions of employment;

THIS AGREEMENT WITNESSETH that in consideration of the premises and mutual covenants and agreements hereinafter contained, and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged by the parties hereto), it is agreed by and between the parties hereto as follows:

i. Term of Employment

The employment of the Employee shall commence the date hereof and continue for an indefinite term until terminated in accordance with the provisions of this agreement.

Contracts

Figure 9-1 Hiring issues

Source: Top left: iStock.com/Hailshadow. Bottom center: iStock.com/MichaelDeLeon.

Background Checks

- ▶ A **background check** should be conducted before the organization extends an offer to any candidate, regardless of job level
- ▶ Common types include:
 - Identity
 - Education and credential
 - Previous employment verification
 - References
 - Worker's compensation history
 - Motor vehicle records
 - Drug history
 - Medical history
 - Credit history
 - Civil court history
 - Criminal court history

Background Checks Issues

▶ Singapore HIV Data Leak Case, 2019

US court finds Farrera-Brochez guilty in Singapore HIV data leak case



ST VIDEOS ▶

Degrees from Vanderbilt University, a doctorate from the Sorbonne, and a teaching certificate from Kentucky state in the United States. American Mikhy Farrera Brochez, 34, had none of these, but he had forged the certificates and used them to obtain teaching positions here over a period of eight years.

Background Checks Issues

Law graduate fined S\$10,000 for doctoring NUS degree certificate, transcript to improve job prospects

Published 18 JANUARY, 2018 UPDATED 18 JANUARY, 2018

2434 Shares



SINGAPORE — Months after being called to the Bar, Jaya Anil Kumar doctored her grades for 21 modules in her degree transcript to burnish her academic performance when she applied to join the public legal service, but was not offered a job.

Three years later, the 29-year-old tried the same trick again, forging her results further for 18 modules such that she appeared to hold a Second Upper honours degree from the National University of Singapore (NUS).

Source: <https://www.todayonline.com/singapore/law-graduate-fined-s10000-doctoring-nus-degree-certificate-transcript-improve-job>

Background Checks

Dear [REDACTED]

As part of the government's [Smart Nation initiative](#), NUS is issuing electronic (e-) degree scrolls/graduate diplomas and transcripts to our graduates with effect from 2019.

These e-documents will facilitate mobility as graduates may share them with potential employers, universities or other parties, who may access and validate them at their own time and convenience through the secured [OpenCerts platform](#) based on blockchain technology.

We are pleased to enclose an e-copy of your certificate and transcript (if applicable) with this email.

Please read the following on how to use the e-documents:

How do I view the document?



Can I save a copy?



How do I share the document?



Drag and drop the attached *OpenCerts file* into the Viewer on the [OpenCerts website](#).

Yes, you may download the attached *OpenCerts file* to your computer.

If you had a Singapore Identity Card or a Foreign Identification Number (FIN) when you were studying at NUS, then a copy of the file has also been deposited into the Skills Passport of your individual [MySkillsFuture](#) account. [Click here](#) (FAQ Q3) for more information. Once logged in, you may [link your account to a social media account](#) for easy retrieval in future.

For more information, you may like to visit our website [here](#).

Should you have any questions, please send an email to transcript@nus.edu.sg. Thank you.

With best wishes

SHAW Lay Pheng (Ms)
Registrar
National University of Singapore

Personnel Security Practices

- ▶ There are various ways of monitoring and controlling employees to minimize their opportunities to misuse information – ***Insider Threat***
- ▶ Separation of duties
 - ▶ Also known as segregation of duties
 - ▶ Work is divided up. Each team member performs only his or her portion of the task sequence
 - ▶  **Control the odds of collusion**
 - separation of duties main objective is to prevent conflict of interest
- ▶ Two-man control
 - ▶ Also known as **dual control**
 - dual control main objective is to minimise errors
 - ▶ It requires that two individuals to work together to complete. In some cases, review and approve each other's work before the task is considered complete



Finance domain will usually champion such ideas since they handle massive amount of sensitive data

- opening vault need both key (person and employee)

- user updating particulars need 2 person to approve the update

Examples:

▶ Separation of duties

- ▶ Software development

 - ▶ developing vs. testing

- ▶ Data backup

 - ▶ data backup vs. mounts and dismounts the physical media

▶ Two man in control

- ▶ Data center security

 - ▶ Monitor and limit access to server racks

 - ▶ “It requires that two cards with authorized access to the rack be scanned within ten seconds of one another in order for a server rack door to be opened.”

 - E.g., Identicard Access Control

Examples:

NSA Implements 'Two-Man Rule' to Prevent Future Leaks

In the wake of the Edward Snowden leak, the National Security Agency (NSA) has put in place a "two-man rule" that requires two people to be present for the transfer of sensitive information.

"NSA has instituted a two-person rule for systems administrators who have the highest privileges," an NSA spokesperson said via email.

The news was first reported by the Associated Press, which spoke to NSA chief Keith Alexander on the sidelines of the Aspen Security Forum in Colorado.

Alexander told the news service that the NSA is currently testing out this two-person rule within the agency, and would roll it out at the Pentagon and other intelligence agencies at a later date. One item on the agenda is coming up with rules for sites that currently only have one system admin, he told the AP.

Source: <https://www.pcmag.com/news/nsa-implements-two-man-rule-to-prevent-future-leaks>

Personnel Security Practices (cont.)

- ▶ Need to know and least privilege
 - ▶ Need to know
 - ▶ The principle of limiting users' access privileges to only the specific information required to perform their assigned tasks.
 - ▶ Least privilege
 - ▶ The principle that ensures no unnecessary access to data exists by regulating members so that they can perform only the minimum data manipulation necessary
 - ▶ It implies need-to-know.

need to know focuses on the data access
least privileged focuses on the rights

Personnel Security Practices (cont.)

▶ Job rotation

- ▶ It requires that every employee be able to perform the work of at least one other employee
- ▶ Cross train employees
- ▶ If that approach is not feasible, an alternative is *task rotation*, in which all critical tasks can be performed by multiple individuals
- ▶ For similar reasons, each employee should be required to take a *mandatory vacation*, of at least one week per year
- ▶ This policy gives the organization a chance to perform a detailed review of everyone's work



Minnesota Office of the State Auditor

Rebecca Otto



[About Our Office](#) | [Latest News](#) | [Reports & Data](#) | [For Local Officials](#) | [Auditing](#) | [Investigations](#) | [Forms](#) | [Contact Us](#) | [Google Custom Search](#)

Mandatory Vacations

Public entities should consider a mandatory vacation policy for employees – especially those with financial responsibilities. When an employee never takes a day off from work, it may be a red flag for fraud. Employees who engage in fraud may resist taking a vacation, fearing that someone else doing their job in their absence may discover the irregularities.

For a mandatory vacation to be effective as a fraud deterrent and detection tool, someone else must be cross-trained in the bookkeeping and cash functions and must perform the work during the mandated vacation.

Date this Avoiding Pitfall was most recently published: 05/25/2018

[Privacy Policy](#) | [Accessibility Information](#) | © 2018 Office of the Minnesota State Auditor



Termination Issues

- ▶ When an employee leaves an organization, the following tasks must be performed:
 - ▶ The former employee's access to the organization's systems must be disabled
 - ▶ The former employee must return all removable media, technology, and data
 - ▶ The former employee's hard drives must be secured
 - ▶ File cabinet locks must be changed
 - ▶ Office door locks must be changed
 - ▶ The former employee's keycard access must be revoked
 - ▶ The former employee's personal effects must be removed from the premises
 - ▶ The former employee should be escorted from the premises, once keys, keycards, and other business property have been turned over

 However - in practice it will be difficult to ensure that such regulations will be followed by the employee

Since they would not be able to have information of where the employee went afterwards

- Usually these cases are hard to detect and only detectable on an ad hoc basis

Termination Issues (cont.)

- ▶ In addition to performing these tasks, many organizations conduct an **exit interview** to remind the employee of any contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee's tenure in the organization
- ▶  **Not-to-compete or non-compete clause**
 - ▶ Prevent them from working for a direct competitor within a specified time frame
 - ▶ A few months to several years
- ▶  **Garden Leave**
 - ▶ A way to restrict the flow of proprietary information when an employee leaves to join a competitor
 - ▶ Buffer time
- ▶ **Non-Disclosure Agreement**

Garden Leave - company will still be paid by company
vs

Non-Compete - a promise after leaving the company

Garden Leave

BHP Billiton hires new global IT chief, ditches CIO title

Mining giant BHP Billiton has hired a former General Motors executive into its new top IT role, replacing global chief information officer Chris Crozier, whose title has been retired following his departure.

Crozier is understood to have left the role he filled for six years last month after being promoted to a vice president position, but very shortly after departed the organisation and is currently on gardening leave.

Source: <https://www.itnews.com.au/news/bhp-billiton-hires-new-global-it-chief-ditches-cio-title-410404#:~:text=Diane%20Jurgens%20takes%20over%20after,been%20retired%20following%20his%20departure>.

Performance Measurement in InfoSec Management

InfoSec Performance Management

- ▶ Information security performance management is the process of *designing, implementing and managing* the use of the collected data elements (called measures or metrics) to determine the effectiveness of the overall security program
- ▶ Performance measurements (or measures) are *data points* or *computed trends* that may indicate the effectiveness of security countermeasures or controls—*technical and managerial*—as implemented in the organization

Four Benefits of Using Measures

1. Increase accountability
2. Improve information security effectiveness
3. Demonstrate compliance
4. Provide quantifiable inputs for resource allocation decisions

What Should Be Communicated?

- ▶ Information for security stakeholders and other people involved in performance measurement (5WIH)
 - ▶ Why should these statistics be collected?
 - ▶ Objective
 - ▶ What specific data will be collected?
 - ▶ Concept
 - ▶ When will these statistics be collected?
 - ▶ Situation
 - ▶ Where (at what point in the function's process) will these statistics be collected?
 - ▶ Business practice
 - ▶ Who will collect these statistics?
 - ▶ People
 - ▶ How will these statistics be collected?
 - ▶ Method

InfoSec Performance Management (cont.)

- ▶ Organizations use three types of measurements:
 - ▶ Type I: Those that determine the effectiveness of the execution of InfoSec policy (like ISSPs)
 - ▶ Implementation measures, used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures
 - E.g., the percentage of information systems with password policies configured as required
 - E.g., the percentage of servers within a system with a standard configuration
 - At first, the results of these measures might be less than 100 percent. However, as the information security programs and its associated policies and procedures mature, results should reach and remain at 100 percent

InfoSec Performance Management (cont.)

- ▶ Organizations use three types of measurements:
 - ▶ Type 2: Those that determine the effectiveness and/or efficiency of the delivery of information security services
 - ▶ Effectiveness/Efficiency Measures
 - ▶ Effectiveness: the robustness of the result itself
 - ▶ Efficiency: the timeliness of the result

InfoSec Performance Management (cont.)

- ▶ Organizations use three types of measurements:
 - ▶ Type 3: Those that assess the impact of an incident or other security event on the organization or its mission
 - ▶ Impact measures
 - Cost savings produced by information security program
 - Costs incurred by responding to attacks and breaches
 - Level of public trust in your organization gained or maintained by the information security program

Factors to Consider When Devising Measures

- ▶ According to *NIST SP 800-55 RI - Performance Measurement Guide for Information Security*, the following factors must be considered during development and implementation of an information security performance management program
 - ▶ They must be quantifiable (percentages, averages, and numbers)
 - ▶ Data that supports the measures needs to be readily obtainable
 - ▶ Only repeatable information security processes should be considered for measurement
 - ▶ Measures must be useful for tracking performance and directing resources

Measures Development & Selection

- ▶ Specifying information security measures
 - ▶ One of the critical tasks in the measurement process is to assess and quantify what will be measured
 - ▶ Must identify, assess and quantify the measures that characterize the target
 - ▶ It is critical (but difficult) to get the right measures from the outset
 - ▶ Cyclical reviews will expose shortcomings in wrongly specified or inadequate measures
 - ▶ A lot of variation

Measures Development & Selection (cont.)

- ▶ Establish performance targets
 - ▶ So that you can define what success means in the security program
 - ▶ Implementation measures typically target 100% completion of specific tasks
 - ▶ Performance targets for effectiveness/efficiency much more complex
 - ▶ Measures may not be quantifiable, so must be stated in terms of qualitative, reasoned descriptions of what constitutes success

Performance Measurement Template and Instructions

Table 9-1 Performance Measurements Template and Instructions

Field	Data
Measurement ID	The unique identifier used to measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source. It should be meaningful to the source and/or use of the measurement.
Goal	Statement of strategic goal and/or InfoSec goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and InfoSec goals can be included. For example, InfoSec goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific InfoSec goal extracted from agency documentation, or identify an InfoSec program goal that would contribute to the selected strategic goal.
Measurement	Statement of measurement. Identify precisely the numeric element to be measured. Start with one of percentage, number, frequency, average, or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Any related security controls providing supporting data should be identified. If the measures are applicable to a specific FIPS 199 impact level (high, moderate, or low), provide that means of evaluation.
Measurement type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.

Performance Measurement Template and Instructions (cont.)

Table 9-1 Performance Measurements Template and Instructions (*continued*)

Field	Data
Implementation evidence	<p>Use of implementation evidence to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure.</p> <ol style="list-style-type: none">For manual data collection, identify questions and data elements that would provide data inputs necessary to calculate measure's formula, qualify measure for acceptance, and validate provided information.For each question or query, list status security control number from NIST SP 800-53 that provides information, if applicable.If measure is applicable to a specific FIPS 199 impact level, questions should state impact level.For automated data collection, identify data elements that would be required for formula, qualify measure for acceptance, and validate information provided.
Frequency	<p>Indication of how often the data is collected and analyzed, and how often the data is reported.</p> <p>State the frequency of data collection based on a rate of change in a particular security control that is being evaluated. State the frequency of data reporting based on external reporting requirements and internal customer preferences.</p>
Responsible parties	<p>Indication of the following key stakeholders:</p> <ul style="list-style-type: none">Information owner: Identify organizational component, an individual who owns required pieces of information.Information collector: Identify the organizational component and individual responsible for collecting the data. If possible, the information collector should be a different person from the information owner or even a representative of a different organizational unit, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.Information customer: Identify the organizational component and individual who will receive the data.
Data source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting format	Indication of how the measure will be reported, such as pie charts, line charts, bar graphs, or other format. State the type of format or provide a sample.

Table 9-2 Performance Measurement Example

Field	Example Data
Measurement ID	Security training coverage
Goal	Strategic goal: Ensure a high-quality workforce supported by modern and secure infrastructure and operational capabilities. InfoSec goal: Ensure that organization personnel are adequately trained to carry out their assigned InfoSec-related duties and responsibilities.
Measurement	The percentage of InfoSec personnel who have received security training.
Measure type	Implementation
Formula	Number of InfoSec personnel who have completed security training within the past year divided by the total number of InfoSec personnel, then multiplied by 100
Target	100 percent
Implementation evidence	<ol style="list-style-type: none">Are significant security responsibilities defined with qualifications criteria and documented in policy? Yes/NoAre records kept regarding which employees have significant security responsibilities? Yes/NoHow many employees in your department have significant security responsibilities?Are training records maintained? Yes/NoHow many of those with significant security responsibilities have received the required training?If all personnel have not received training, document all reasons that apply:<ol style="list-style-type: none">Insufficient fundingInsufficient timeCourses unavailableEmployee not registeredOther (specify)
Frequency	Collected as training is delivered Reported annually
Responsible parties	Information owner: training division Information collector: training division Information customer: CIO
Data source	Training and awareness tracking records
Reporting format	Pie chart illustrating the percentage of security personnel who have received training versus those who have not received training. If performance is below target, pie chart illustrating causes of performance falling short of targets.

Performance Measurement Example

Examples of Possible Security Performance Measures

- ▶ Percentage of the organization's information systems budget devoted to information security
- ▶ Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
- ▶ Percentage of remote access points used to gain unauthorized access
- ▶ Percentage of information systems personnel that have received security training
- ▶ Average frequency of audit records review and analysis for inappropriate activity
- ▶ Percentage of new systems that have completed certification and accreditation prior to their implementation
- ▶ Percentage approved and implemented configuration changes identified in the latest automated baseline configuration
- ▶ Percentage of information systems that have conducted annual contingency plan testing
- ▶ Percentage of users with access to shared accounts
- ▶ Percentage of incidents reported within required time frame per applicable incident category
- ▶ Percentage of system components that undergo maintenance in accordance with formal maintenance schedules

Examples of Possible Security Performance Measures (cont.)

- ▶ Percentage of media that passes sanitization procedures testing
- ▶ Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets
- ▶ Percentage of employees who are authorized access to information systems only after they sign an acknowledgment that they have read and understood the appropriate policies
- ▶ Percentage of individual screened before being granted access to organizational information and information systems
- ▶ Percentage of vulnerabilities remediated within organization- specified time frames
- ▶ Percentage of system and service acquisition contracts that include security requirements and/or specifications
- ▶ Percentage of mobile computers and devices that perform all cryptographic operations using organizationally specified cryptographic modules operating in approved modes of operations
- ▶ Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated

Reporting InfoSec Performance Measurements

- ▶ In most cases, simply listing the measurements collected does not adequately convey their meaning
- ▶ In addition, you must make decisions about how to present correlated metrics
- ▶ The CISO must also consider to whom the results of the performance measures program should be disseminated, and how they should be delivered

Reporting InfoSec Performance Measurements

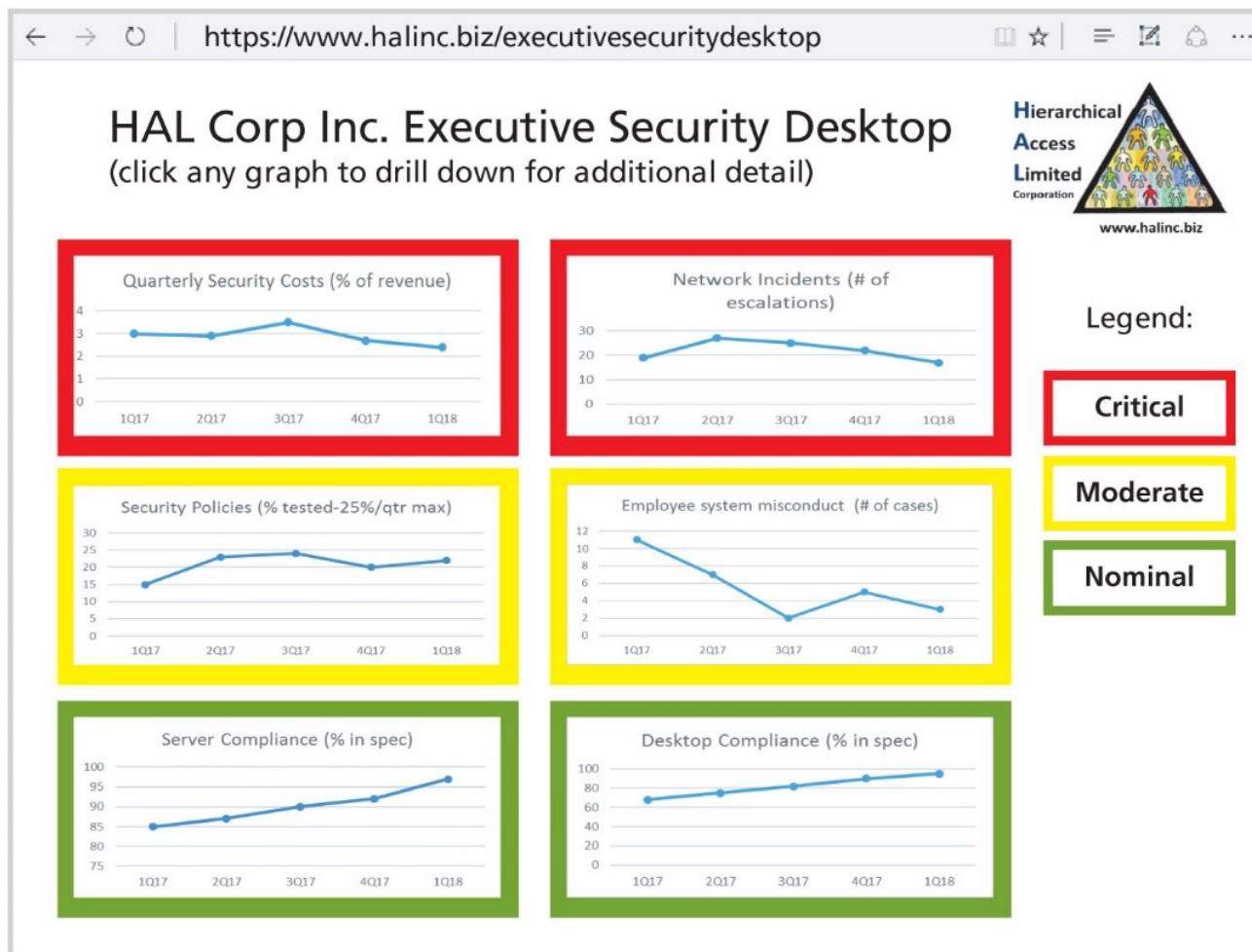


Figure 9-5 Security dashboard

Next week

- ▶ L7 Security Management Models

IS4231

Information Security Management

Lecture 7

Security Management Models

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 8

Learning Objectives

- ▶ **Describe the prevalent information security management models that can be used as security frameworks**
 - ▶ These are the security frameworks you start with
- ▶ **Lower Level Security Models**
 - ▶ These are used to help flesh out aspects of the framework
 - ▶ Types of models
 - ▶ Security evaluation models



|

Security Management Models

Security Management Models

- ▶ Sources
 - ▶ Public domain sources
 - ▶ Proprietary models

- ▶ Models
 - ▶ ISO/IEC 27000 series
 - ▶ NIST security models
 - ▶ COBIT
 - ▶ PCI DSS
 - ▶ ISF the Standards
 - ▶ CIS Standards
 - ▶ Others

ISO/IEC 27000 series

ISO/IEC 27000 Series

- ▶ Deal specifically with InfoSec matters
 - ▶ Deliberately broad in scope so that it can be used by organizations of all sizes and kinds
 - ▶ Use it to guide assessment of InfoSec risks, then implement security controls appropriate to their needs
 - ▶ Full standards list:
 - ▶ <https://www.iso27001security.com/html/iso27000.html>

ISO 27000 Series Samples

- ▶ 27000: Overview and vocabulary
- ▶ 27001: InfoSec Mgmt System Specification
- ▶ 27002:Code of Practice for InfoSec Mgmt
- ▶ 27003: InfoSec Mgmt Systems Implementation Guidance
- ▶ 27004: InfoSec Measurements
- ▶ 27005: ISMS Risk Management
- ▶ 27006: Requirements for Bodies Providing Audit and Certification of an ISMS
- ▶ 27007: Guidelines for ISMS Auditing
- ▶ 27008: Guidelines for InfoSec Auditing
- ▶ 27010: Guidelines for Inter-sector and Inter-organizational Communications
- ▶ 27011: Guidelines for Telecomm orgs
- ▶ 27013: Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ▶ 27014: InfoSec Governance Framework
- ▶ 27015: InfoSec Mgmt Guidelines for Financial Services
- ▶ 27016: InfoSec and Organizational Economics
- ▶ 27017:  Code of practice for InfoSec controls for cloud computing services based on ISO/IEC 27002
- ▶ 27018: Code of practice for PII protection in public clouds acting as PII processors
- ▶ 27023: Mapping the revised editions of ISO/IEC 27001 and 27002
- ▶ 27031: Guidelines for information and communication technology readiness for business continuity
- ▶ 27032: Guidelines for cybersecurity
- ▶ 27033: Network security
- ▶ 27034: Application security
- ▶ 27701: *The international standard for privacy information management*

ISO/IEC 27001

- ▶ ISO/IEC 27001:2013 - “Information Technology - Security techniques - Information security management systems - Requirements”
 - ▶ Latest revision in 2013
 - ▶ Provides information for how to implement ISO/IEC 27002 and set up an Information Security Management System (ISMS)
 - ▶ Serves better as an assessment tool
 - ▶ Whether the organization system has meet with the security standards

ISO/IEC 27001 (cont.)

Standards | All about ISO | Taking part | **Store** | Search | 

Standards catalogue | Publications and products

[Home](#) > Store > Standards catalogue > Browse by ICS > 03 > 03.100 > 03.100.70 > ISO/IEC 27001:2013

ISO/IEC 27001:2013

 Preview

Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

General information 

Current status : Published	Publication date : 2013-10
Edition : 2	Number of pages : 23
Technical Committee : ISO/IEC JTC 1/SC 27 IT Security techniques	

Buy this standard

Format	Language
<input checked="" type="checkbox"/> PDF + Color PDF + ePub	English ▾
PDF + ePub	English ▾
PDF + ePub + Redline	English ▾
Paper	English ▾
PDF	Arabic ▾

SGD 173 CHF 118 

Example: NUS



Home About Highlights Services Support Contact [Join US!](#)

[myEmail](#) [Staff Portal](#) [Student Portal](#) [nTouch](#)



Achieved Information Security Management System (ISMS) Framework And ISO 27001 Certification

2009



Proudly achieved Information Security Management System (ISMS) framework and ISO 27001 certification on InfoComm security, network services, system services, database administration and data centre operations, and setting best practice in security management in Higher Education.

Estimated Certification Costs

Estimated ISO 27001 certification costs

The table below displays the recommended ISMS audit time according to the size of the organisation, as stipulated in ISO/IEC 27006:2015.

No. of people working for the organisation	No. of days** (Minimum audit time)	Estimated certification cost ***
1 - 45	3 - 6	£2850 - £5,700
46 - 125	7 - 8	£6,650 - £7,600
126-425	9 – 10	£8,550 - £9,500
426-625	11	£10,450
626-875	12	£11,400
876-1175	13	£12,350
1176-1550	14	£13,300
1551-2025	15	£14,250

Source: <https://www.itgovernance.co.uk/iso27001-certification-costs>

Example: Trend Micro

- ▶ The Trend Micro ISMS scope includes the following services:

Endpoint Application Control	Active Update
Deep Discovery Analyzer as a Service	Mobile App Reputation Service
Deep Discovery Analyzer as a Service Add-on	Cloud App Security
Deep Security as a Service	DirectPass
Email Reputation Service	Mobile Security
Web Reputation Service	Encryption Service
File Reputation Service	Remote Manager
Smart Protection Network	Worry-Free Business Security Service
Hosted Email Security	IoT Security
Hosted Mobile Security	Home Network Security
InterScan Web Security as a Service	Yamato Backend (VPN, NBA, ISC)
Apex One as a Service	Email Security
Product Licensing Service	Cloud Edge Cloud Management
Threat Investigation Center	Email Security Platform for Service Provider

ISO/IEC 27002

- ▶ ISO/IEC 27002:2013 - “Information Technology - Security techniques - Code of practice for information security management”
 - ▶ One of the most widely referenced InfoSec management models
 - ▶ Originally published as British Standard BS 7799
 - ▶ Adopted as an international standard framework for InfoSec by the ISO and the IEC as ISO/IEC 17799
 - ▶ Last revised in 2013
 - ▶ Gives best practice recommendations on InfoSec management to those initiating, implementing or maintaining InfoSec management systems

ISO/IEC 27002 (cont.)

- ▶ ISO/IEC 27002:2013 (the most last version)
 - ▶ Provides information on more than 100 controls over 14 security control clauses
 - ▶ For organizations that want information about implementing security controls.
 - ▶  Works as a *guidance document*

ISO/IEC 27002 (cont.)

▶ ISO/IEC 27002: 2013 structure

- ▶ 0. Introduction
- ▶ 1. Scope
- ▶ 2. Normative references
- ▶ 3. Terms and definitions
- ▶ 4. Structure of this standard
- ▶ 5. Information security policies
- ▶ 6. Organization of information security
- ▶ 7. Human resource security
- ▶ 8. Asset management
- ▶ 9. Access Control
- ▶ 10. Cryptography
- ▶ 11. Physical and environmental security
- ▶ 12. Operations security
- ▶ 13. Communication security
- ▶ 14. System acquisition, development, and maintenance
- ▶ 15. Supplier relationships
- ▶ 16. Information security incident management
- ▶ 17. Information security aspects of business continuity management
- ▶ 18. Compliance

ISO/IEC 27701

- ▶ ISO/IEC 27701:2019 – “Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for **privacy** information management - Requirements and guidelines”
 - ▶ A new standard in the ISO27000 series
 - ▶ It specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for *privacy management* within the context of the organization.
 - ▶ It specifies PIMS-related requirements and provides guidance for *PII controllers* and *PII processors* holding responsibility and accountability for PII processing.

help companies to comply with GDPR / PDPA

Discussions:

- ▶ **Question:**
 - ▶ What kind of ISO 27000 standards should AWS, as a cloud service provider, be certified with?

AWS has certification for compliance with
ISO/IEC
27001:2013,
27017:2015,
27018:2019,
27701:2019,
9001:2015,
and CSA STAR CCM v3.0.1

CSA STAR Program

- ▶ **CSA – Cloud Security Alliance**
 - ▶ A non-profit org whose mission is to “promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”
- ▶ **STAR – Security, Trust, Assurance, and Risk**
 - ▶ A program to hep customers assess and select a Cloud Service Provider through a three-step program of self-assessment, third-party audit, and continuous monitoring.
 - ▶ The certification leverages the requirements of the ISO/IEC 27001: 2013 Information security management systems standards together with the CSA Cloud Control Matrix

CSA STAR Program (cont.)

- ▶ Reference documents
 - ▶ CCM (Cloud Control Matrix)
 - ▶ CAIQ (The Consensus Assessments Initiative Questionnaire)
 - ▶ Offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency

unlike ISO 27017 and 27018 which are proprietary - CSA STAR is free for referencing

NIST Security Models



About NIST

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.

NIST Security Models

- ▶ Two advantages over the ISO/IEC 27000 standards:
 - ▶ Freely available at no charge
 - ▶ They have been available for some time and thus have been broadly reviewed (and updated) by government and industry professionals
 - ▶ SP 800-12 Rev.1, *An Introduction to Information Security*
 - ▶ SP 800-30 Rev.1, *Guide for Conducting Risk Assessments*
 - ▶ SP 800-53 Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*
 - ▶ SP 800-55 Rev.1, *Performance Measurement Guide for Information Security*
 - ▶ SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
 - ▶ SP 800-53 Rev.5, *Security and Privacy Controls for Information Systems and Organizations*
 - ▶ SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*
 - <https://csrc.nist.gov/publications/sp800>

Examples:

▶ FIREYE:



LEARN MORE >

NIST 800-171

National Institute of Standards and Technology Special Publication 800-171 was released in June 2015. It focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in non-federal information systems and organizations and defines security requirements to achieve that objective.  FireEye has undergone a self-assessment that confirmed compliance with NIST 800-171 controls. FireEye continually evaluates compliance with NIST 800-171.

▶ AWS:

Is AWS compliant with the NIST 800-53 framework?



Yes, AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls, as well as additional FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both AWS GovCloud (US) and the AWS US East/West Region. For more information, see the [AWS FedRAMP compliance](#) webpage, or the following FedRAMP Marketplace webpages:

- [AWS East/West Region complete list of authorizing agencies](#)
- [AWS GovCloud \(US\) complete list of authorizing agencies](#)
- [AWS GovCloud JAB P-ATO at the high baseline](#)

COBIT

COBIT

their focus is on the Enterprise Risk - not just focused on security itself

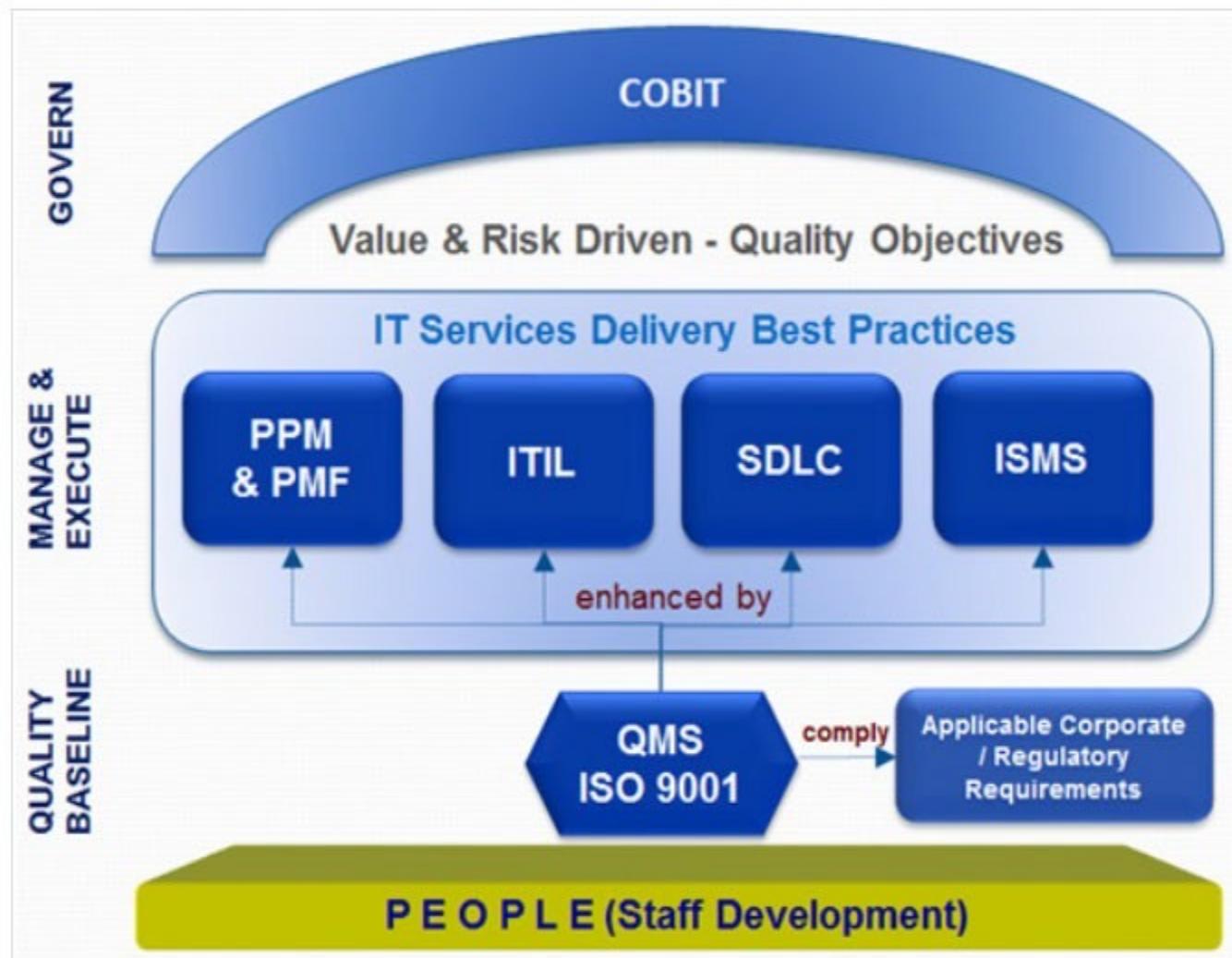
- ▶ “Control Objectives for Information and Related Technology”(COBIT)
 - ▶ Provides advice about the implementation of sound controls and control objectives for InfoSec
 - ▶ Created in 1992 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- ▶ COBIT 2019
 - ▶ A Business framework for the governance and management of Enterprise IT

COBIT 2019

- ▶ Six principles focus on the governance and management of IT:
 - ▶ Principle 1: Provide stakeholders value
 - ▶ Principle 2: A holistic approach
 - ▶ Principle 3: Dynamic governance system
 - ▶ Principle 4: Governance distinct from management
 - ▶ Principle 5: Tailored to enterprise need
 - ▶ Principle 6: End-to-end governance system

Example: NUS

for an organisation - different models will help different aspects of the organisation and can pick and choose for specific areas to focus on



PCI DSS

PCI Industry Security Standards

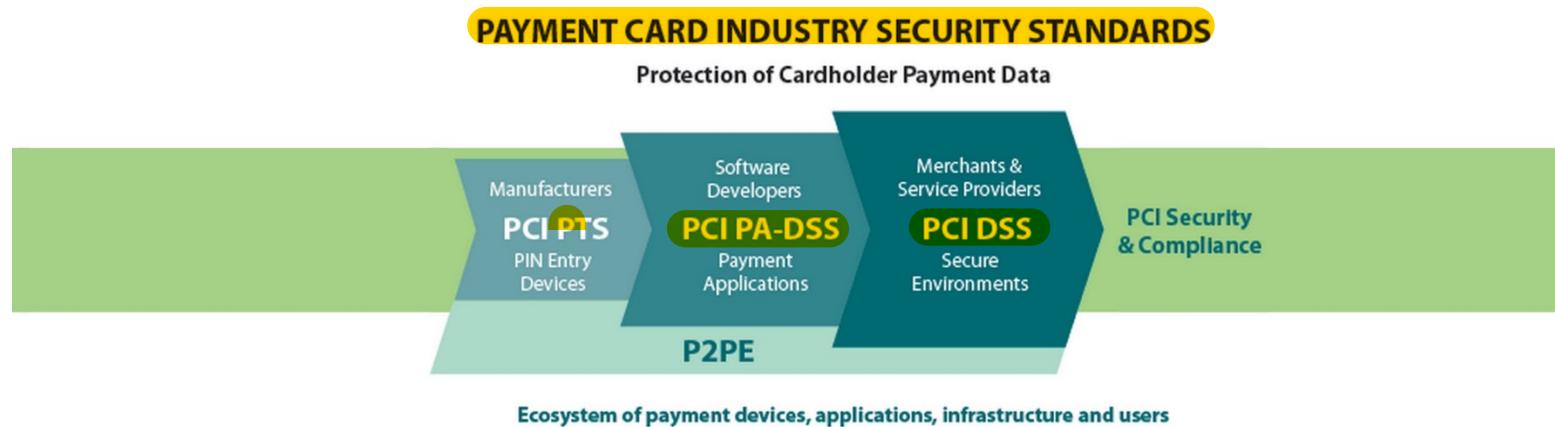
- ▶ Payment Card Industry Data Security Standards
 - ▶ A set of industry standards that are mandated for any organization that handle credit, debit and specialty payment cards.
 - ▶ Created by the Payment Card Industry Security Standards Council in an effort to reduce credit card fraud.
 - ▶ <https://www.pcisecuritystandards.org/>

The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in ownership, governance, and execution of the Council's work.



PCI Industry Security Standards (cont.)

- ▶ The PCI Data security standards help protect the safety of that data.
- ▶ They set the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.



even a random store needs to ensure they are compliant with PCI PA-DSS

Source: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

PCI DSS

- ▶ Includes three sets of documents
 - ▶ PCI DSS requirements and security assessment procedures (the Standards)
 - ▶ PCI DSS self-assessment (self-determined surveys to determine status of compliance), and documents for attestation of compliance
 - ▶ PCI DSS support documents (e.g., glossary, abbreviations and acronyms, reference guide)

PCI DSS (cont.)



more clear cut / specific standards as compared to ISO

► The standard focusing on 12 requirements in 6 areas

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

PCI DSS (cont.)

- ▶ How do companies comply with PCI DSS?
 - ▶ Have an **External Qualified Security Assessor (QSA)** assess your applicable environment and then create a Report on Compliance (ROC) and Attestation of Compliance (AOC)
 - ▶ most common for entities that handle large volumes of transactions
 - ▶ Or, perform a Self-Assessment Questionnaire (SAQ)
 - ▶ most common for entities that handle smaller volumes of transaction
- ▶ Certificate validity
 - ▶ Valid for 1 year from the date the certificate is issued.
 - ▶ E.g., PayPal, Lazada, GrabPay
 - <https://www.paypal.com/sg/webapps/mpp/pci-compliance>
 - <https://www.grab.com/sg/pay/security/>

PCI DSS (cont.)

- ▶ Merchant compliance levels:
 - ▶ E.g., level 1, level 2, level 3, level 4
 - ▶ Depends on the merchant level (i.e., transaction volume) and slightly varies across different credit card companies (e.g., Visa, MasterCard, AMEX)
 - ▶ Taking VISA as example:

Merchant Level	Description
1	Any merchant – regardless of acceptance channel – processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant – regardless of acceptance channel – processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants – regardless of acceptance channel – processing up to 1M Visa transactions per year.

PCI DSS – VISA Standards

- ✓ Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region
 - Level 1

Every year:

- File a Report on Compliance ("ROC") by a Qualified Security Assessor ("QSA") or Internal Auditor if signed by an officer of the company. We recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification.
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

[similar to FTC order for zoom](#)

- ✓ 1 to 6 million Visa transactions annually across all channels – Level 2

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

- ✓ 20,000 to 1 million Visa e-commerce transactions annually – Level 3

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

- ✓ Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually – Level 4

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV") (if applicable)

PCI DSS (cont.) – Mastercard Standards

Site data protection merchant levels

Category	Criteria	Requirements
Level 1	<ul style="list-style-type: none">Any merchant that has suffered a hack or an attack that resulted in an Account Data Compromise (ADC) EventAny merchant having more than six million total combined Mastercard and Maestro transactions annuallyAny merchant meeting the Level 1 criteria of VisaAny merchant that Mastercard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	<ul style="list-style-type: none">Annual PCI DSS assessment resulting in the completion of a Report on Compliance (ROC)¹
Level 2	<ul style="list-style-type: none">Any merchant with more than one million but less than or equal to six million total combined Mastercard and Maestro transactions annuallyAny merchant meeting the Level 2 criteria of Visa	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)²
Level 3	<ul style="list-style-type: none">Any merchant with more than 20,000 combined Mastercard and Maestro e-commerce transactions annually but less than or equal to one million total combined Mastercard and Maestro e-commerce transactions annuallyAny merchant meeting the Level 3 criteria of Visa	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)³
Level 4	<ul style="list-style-type: none">All other merchants⁴	<ul style="list-style-type: none">Annual Self-Assessment Questionnaire (SAQ)³

PCI DSS (cont.)

▶ Self-validation tool

- ▶ Self-Assessment Questionnaire (SAQ)
- ▶ Ideal for small merchants and service providers that are not required to submit a report on compliance, to assess their level of cardholder data security

▶ Levels

- A - simplest

- A-EP

- B

depending on the business on how they handle transactions or how they design their payment systems

- B-IP

- C-VT

- C

- P2PE-HW

- D - most complicated

Other Security Management Models

- ▶ **ISF Standard of Good Practice for Information Security**
 - ▶ ISF: Information Security Forum
 - ▶ <https://www.securityforum.org/>
 - ▶ Founded in 1989, an independent, not-for-profit association
 - ▶ Comprehensive coverage of information security controls and information risk-related guidance.
 - ▶ ISF Benchmarks
- ▶ **CIS Cybersecurity Best Practices**
 - ▶ CIS: Center for Internet Security
 - ▶ <https://www.cisecurity.org/>
 - ▶ Founded in 2000, a non-for-profit entity
 - ▶ CIS Controls and CIS Benchmarks

Other Security Management Models (cont.)

- ▶ **The Information Technology Infrastructure Library (ITIL)**
 - ▶ A collection of methods and practices useful for managing the development and operation of information technology infrastructures
 - ▶ E.g.,
 - Incident management
 - Change management
 - Problem management
 - Service-level management
 - Continuity management
 - Configuration management
 - Release management
 - Capacity management
 - Financial management
 - Availability management
 - Security management
 - Help desk management
 - Knowledge management
 - ▶ The ITIL has been produced as *a series of books*, each of which covers an IT management topic

Lower Level Security Models

Security Architecture Evaluation Models

- Common Criteria

Common Criteria

- ▶ Common Criteria for Information Technology Security Evaluation - an international standard for computer security certification
 - ▶ Often called “Common Criteria” or “CC”
 - ▶ International standard for computer security certification (ISO/IEC 15408)
 - ▶ <https://www.commoncriteriaportal.org/>
- ▶ Downsides of CC certification
 - ▶ Certification process can be lengthy, costly, not timely
 - ▶ Certification of a system doesn’t necessarily mean that it is completely secure

heavily requires documentation for them to check

Common Criteria (cont.)

The screenshot shows the official website for Common Criteria. At the top left is the logo 'Common Criteria' with a globe icon. To its right is a search bar and a 'Search' button. Below the logo is a 'LOGIN' button with an arrow. A horizontal menu bar contains links for 'HOME', 'ABOUT THE CC', 'PUBLICATIONS', 'TECHNICAL COMMUNITIES', 'CERTIFIED PRODUCTS', 'COLLABORATIVE PPS', 'PROTECTION PROFILES', 'ICCC', and 'NEWS'. The main content area features a large image of a printed circuit board (PCB) with various electronic components. Overlaid on this image is the text 'THE COMMON CRITERIA'. On the left side of the main content area, there is a section titled 'Common Criteria' which contains text about the CC and CEM, and a bulleted list of evaluation processes. On the right side, there is a sidebar titled 'NEWS' containing a list of recent news items with dates and brief descriptions.

Common Criteria

The [Common Criteria for Information Technology Security Evaluation](#) (CC), and the companion [Common Methodology for Information Technology Security Evaluation](#) (CEM) are the technical basis for an international agreement, the [Common Criteria Recognition Arrangement](#) (CCRA), which ensures that:

- [Products](#) can be evaluated by competent and independent [licensed laboratories](#) so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- [Supporting documents](#), are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of [Certificate Authorizing Schemes](#), with this certification being based on the result of their evaluation;
- [These certificates](#) are recognized by all the signatories of the [CCRA](#).

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

Certificate Authorizing Members

A row of flags representing the countries that are members of the Certificate Authorizing Schemes. The flags include Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Austria, Czech Republic, Denmark, Ethiopia, Finland, and Greece.

Certificate Consuming Members

A row of flags representing the countries that use the Common Criteria standard. The flags include the Netherlands, New Zealand, Norway, South Korea, Sri Lanka, Sweden, Turkey, Hungary, Poland, Israel, Pakistan, Spain, and Qatar.

meanwhile China has their own standard - do not use CC

Common Criteria (cont.)

- ▶ CC terminology
 - ▶ Target of evaluation (ToE)-the system being evaluated
 - ▶ Protection profile (PP)  user-generated specification for security requirements
 - ▶ Security target (ST)  document describing the ToE's security properties  relationship btwn PP and ST
 - ▶ Security functional requirement (SERs)-catalog of a product's security function
 - ▶ Evaluation assurance level (EAL)-the rating or grading of a ToE after evaluation
- ▶ The Target of Evaluation (i.e., system being evaluated) is awarded an Evaluation Assurance Level (EAL)

Common Criteria (cont.)

- ▶ CC EAL scale (lowest to highest assurance):
 - *EAL1: Functionally Tested*
 - *EAL2: Structurally Tested*
 - *EAL3: Methodically Tested and Checked*
 - *EAL4: Methodically Designed, Tested, and Reviewed*
 - *EAL5: Semi-formally Designed and Tested*
 - *EAL6: Semi-formally Verified Design and Tested*
 - *EAL7: Formally Verified Design and Tested*

The level allocated is by company choosing which level they want to be tested against

CSA Common Criteria

About the Common Criteria (CC)

The genesis of CC was developed through a collaboration among national security and standards organisations in Canada, France, Germany, the Netherlands, the United Kingdom and the United States as a common standard to replace their existing security evaluation criteria.

The CC is now recognised as the ISO/IEC 15408. The CC is adopted by members of the Common Criteria Recognition Arrangement (CCRA) in order to facilitate mutual recognition of evaluation and certification results. As a result, consumers can benefit from having a wider choice of CC certified IT products, and developers will benefit from having greater access to markets and understanding of the security requirements (described in the form of collaborative Protection Profiles). The CC harmonises the evaluation of IT products by defining a common set of security functions which product developers use to establish the security requirements of their IT products in a standardised language. The Common Methodology for IT Security Evaluation (CEM) (ISO/IEC 18045) is used for evaluating the product against the established security requirements, confirming that the product is capable of meeting these requirements with an appropriate level of assurance.

The Singapore Common Criteria Scheme (SCCS) is established to provide a cost effective regime for the info-communications industry to evaluate and certify their IT products against the CC standard in Singapore. The SCCS is owned and managed by the Cyber Security Agency of Singapore (CSA).

Discussion

- ▶ Any Trend Micro product is certified under CC scheme?

CC EAL2+ for Deep Security and Tipping Point (2 products)



CSA Cybersecurity Labelling Scheme

- ▶ An initiative under the *Safer Cyberspace Masterplan SG*
 - ▶ Scope
 - ▶ Network-connected smart devices
 - ▶ Labelling scheme
 - ▶ It will provide an indication of the level of security that is embedded in the products, based on a series of assessment and tests on:
 - a. Meeting basic security requirements such as ensuring unique default passwords,
 - b. adherence to the principles of Security-by-Design, [Related to DevSec Ops](#)
 - c. absence of common software vulnerabilities, and
 - d. resistance to basic penetration testing
 - ▶ Benchmark
 - ▶ Will be aligned with European Standard EN 303 645 ‘Cyber Security for Consumer Internet of Things’.

CSA Cybersecurity Labelling Scheme (cont.)

▶ Product list

- ▶ <https://www.csa.gov.sg/Programmes/cybersecurity-labelling/Product-List>
- ▶ E.g.,
 - ▶ TraceTogether Token
 - ▶ Nest Wifi Router H2D

CREST

- ▶ A not-for-profit accreditation body that represents and supports the technical information security market.
- ▶ What it provides?
 - ▶ Internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.
 - ▶ The de factor standard in UK and Australia

different regions will have different standards



Next Week

- ▶ Risk Management – Assessing Risk
 - ▶ Chapter 6

IS4231

Information Security Management

Lecture 8

Risk Management – Assessing Risk

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 6

Learning Objectives

- ▶ Define risk management and its role in the organization
- ▶ Describe risk management techniques to identify and prioritize risk factors for information assets
- ▶ Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur



Risk management can be very general - just discussing enterprise risk

Topics

- ▶ Risk management role and process
- ▶ Risk identification
- ▶ Risk assessment
- ▶ Risk evaluation

Introduction to Risk Management

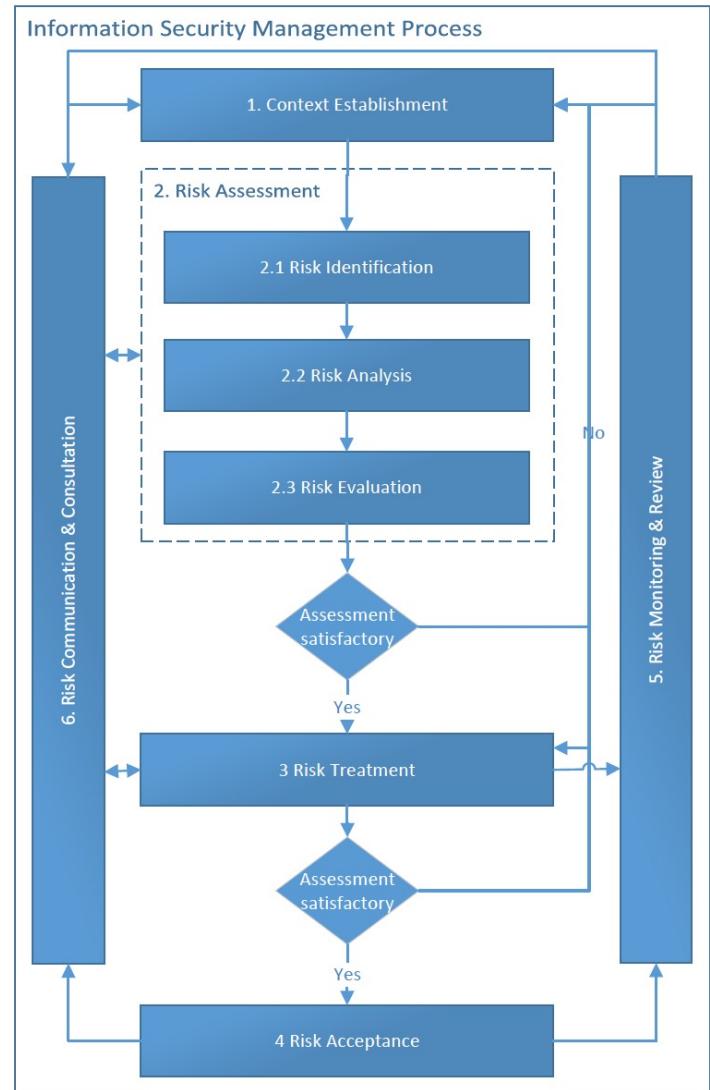
Why Risk Management

▶ Risk Management

- ▶ The process of discovering and assessing the risks to an organization's operations and determining how those risks can be controlled and mitigated
- ▶ The process involved discovering and understanding answers to some key questions regarding the risk associated with an organization's information assets:
 - ▶ Where and what is the risk (risk identification)?
 - ▶ How severe is the current level of risk (risk analysis)?
 - ▶ Is the current level of risk acceptable (risk evaluation)?
 - ▶ What do I need to do to bring the risk to an acceptable level (risk treatment)?

Introduction to Risk Management

- ▶ ISO27005: Risk Management
 - ▶ ISMS risk management process
 - ▶ 1. Context Establishment
 - ▶ 2. Risk Assessment
 - 2.1 risk identification
 - 2.2 risk analysis
 - 2.3 risk evaluation
 - ▶ 3. Risk Treatment
 - ▶ 4. Risk Acceptance
 - ▶ 5. Risk Monitoring & Review
 - ▶ 6. Risk Communication & Consultation



Introduction to Risk Management (cont.)

- ▶ IRAM₂
 - ▶ ISF Information Risk Assessment Methodology 2
 - ▶ Six-phase process for information risk management
 - 1. Scoping
 - 2. BIA
 - Assess worst-case scenarios—the potential business impact if information assets become compromised
 - 3. Threat profiling
 - Mapping different types of threats, both malicious and accidental, that could potentially affect the business



Introduction to Risk Management (cont.)

- ▶ IRAM₂
 - ▶ ISF Information Risk Assessment Methodology 2
 - ▶ Six-phase process for information risk management
 - 4. Vulnerability assessment:
 - Assess your vulnerabilities to different threat events and the strength of any controls already in place
 - 5. Risk evaluation
 - Evaluates the organization's risk appetite and likelihood of a successful threat in light of the previous findings.
 - 6. Risk treatment
 - Develop practical approaches to address the information risks which have been identified.



Risk Identification: Assets Analysis

Risk Assessment

- ▶ **What information assets do I own?**
 - ▶ Which ones are the most important ones?
- ▶ **What are the threats against them?**
 - ▶ Which threats pose the most danger?
- ▶ **How vulnerable am I?**
 - ▶ Which vulnerabilities should be addressed with high priority?

Thus, threat agents use vulnerabilities to attack information assets

Risk Identification

- ▶ Risk Identification
 - ▶ The recognition, enumeration, and documentation of risks to an organization's information assets
- ▶ It begins with the process of self-examination
- ▶ Managers:
 - 1) Identify the organization's information assets
 - 2) Classify and categorize them into useful groups
 - 3) Prioritize them by overall importance

Identification of Information Assets

▶ Information Assets

- ▶ Any asset that collects, stores, processes, or transmits information, or any collection, set, or databases of information that is of value to the organizations.

6 main categories

- ▶ People
- ▶ Procedure
- ▶ Data
- ▶ Software
- ▶ Hardware
- ▶ Networking

Table 6-1 Organizational Assets Used in Systems

Information System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business-standard procedures IT and business-sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications Operating systems Utilities Security components
Hardware	Hardware	Systems and peripherals Security devices Network-attached process control devices and other embedded systems (Internet of Things)
Networking	Networking	Local area network components Intranet components Internet or extranet components Cloud-based components

Identifying Hardware, Software, and Network Assets

- ▶ Many organizations use asset inventory systems to keep track of their hardware, network, and software components

different organisations might have different ways to store and manage each asset

- ▶ When deciding which attributes to track for each information asset, consider the following list of potential attributes:

- ▶ Name
- ▶ Asset tag
- ▶ IP address
- ▶ MAC address
- ▶ Asset type
- ▶ Serial number
- ▶ Manufacturer name
- Manufacturer's model or part number
- Software version, update revision, or FCO number
- Physical location
- Logical location
- Controlling entity

Identifying People, Procedures and Data Assets

- ▶ **People**
 - ▶ Position name/number/ID
 - ▶ Supervisor name/number/ID
 - ▶ Security clearance level
 - ▶ Special skills
- ▶ **Procedures**
 - ▶ Description
 - ▶ Intended purpose
 - ▶ Software/hardware/networking elements to which it is tied
 - ▶ Location where it is stored for reference
 - ▶ Location where it is stored for update purposes
- ▶ **Data**
 - ▶ Classification
 - ▶ Owner/creator/manager
 - ▶ Size of data structure
 - ▶ Data structure used
 - ▶ Online or offline
 - ▶ Location
 - ▶ Backup procedures

ISO27k: Asset Management

- ▶ **Inventory of assets:**
 - ▶ Digital data
 - ▶ Hardcopy information
 - ▶ Software
 - ▶ Infrastructure
 - ▶ Information services and service providers
 - ▶ Physical security and safety related
 - ▶ Business relationships
 - ▶ People

ISO27k: Asset Management (cont.)

- ▶ **Inventory of assets:**
 - ▶ Digital data
 - ▶ E.g., business data of all kinds and all locations; IT/support data; etc.,
 - ▶ Hardcopy information
 - ▶ E.g., system and process documentation (covering specifications, architecture and design, installation, operation, use , management...); licenses, agreements and contracts; disaster recovery plans; etc.,
 - ▶ Software
 - ▶ E.g., system software plus patches and vulnerability disclosures; applications, IT management utilities, databases and middleware; etc.;
 - ▶ Infrastructure
 - ▶ E.g., servers, network devices (e.g., routers, switches, load balancers,VPN devices, web proxy servers), security devices (e.g., gateways and firewalls, IDPS, SIEM), communications devices (e.g., modems, Internet connections), cables, end user devices, etc.;

ISO27k: Asset Management (cont.)

- ▶ **Inventory of assets:**
 - ▶ **Information services and service providers**
 - ▶ E.g., Internet and cloud services, Pentest services; etc.,;
 - ▶ **Physical security and safety related**
 - ▶ E.g., smoke detectors, alarms and fire suppression systems; power provision including UPS and generators; air conditioning plus temperature monitoring and alarms; server racks, card access controls, keys; etc.;
 - ▶ **Business relationships** ie: contracts are considered business secrets
 - ▶ With external parties e.g., suppliers, partners, etc.;
 - ▶ **People**
 - ▶ In particular, any critical or valuable individuals with unique knowledge, experience skills.

Classifying and Categorizing Information Assets

- ▶ Determine whether initial asset categories are meaningful to the organization
- ▶ Inventory should reflect each asset's sensitivity and security priority
 - ▶ A data classification scheme should be developed that categorize the assets based on their sensitivity and security needs
 - ▶ The category that an information asset is put into is indication of the level of protection needed
- ▶ Classification categories must be
 - ▶ *Comprehensive*
 - ▶ All inventories fit into a category
 - ▶ ***Mutually exclusive***
 - ▶ Each asset is found in only one category

Question:

- ▶ **Public Key Infrastructure Certificate Authority**
 - ▶ Software/security component/cryptography
 - ▶ Software/security component/PKI

No this will not satisfy mutually exclusive criteria

Assessing Values for Information Assets

- ▶ Assign a **relative value** to each information asset
- ▶ Use comparative judgments to ensure the most valuable information assets are given the highest priority in the implementation of safeguards and controls:
 - ▶ Which information asset is *the most critical* to the success of the organization?
 - ▶ Which information asset generates *the most revenue*?
 - ▶ Which information asset generates *the highest profitability*?
 - ▶ Which information asset is *the most expensive to replace*?
 - ▶ Which information asset is *the most expensive to protect*?
 - ▶ Which information asset's loss or compromise would be *the most embarrassing* or *cause the greatest liability*?

Sample Asset Classification Worksheet

System Name: <u>SLS E-Commerce</u> Date Evaluated: <u>February 2018</u> Evaluated By: <u>D. Jones</u>		
Information assets	Data classification	 Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1 — home page and core site	Public	Critical
Web server #2 — Application server	Private	Critical
Notes: BOL: Bill of Lading DMZ: Demilitarized Zone EDI: Electronic Data Interchange SSL: Secure Sockets Layer		

Figure 6-3 Sample asset classification scheme

Prioritizing (Rank Ordering) Information Assets

- ▶ The final step in the risk identification process is to prioritize, or rank order the assets
- ▶ This goal can be achieved by using a weighted table analysis

Table 6-2 Example of a Weighted Factor Analysis Worksheet

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
<i>Criterion weight (1-100); must total 100</i>	30	40	30	100
EDI Document Set 1— Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2— Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2— Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Note: In the table, EDI = Electronic Data Interchange and SSL = Secure Sockets Layer.

Example: NUS Risk Analysis

3 Performing Risk Analysis

3.1 Conduct of risk analysis

3.1.1 For high impact projects, risk analysis should be performed at the initiation stage of the systems development project so that the required controls can be incorporated to the design of the system and the business processes. Risk analysis should also be performed after the system is in operation and whenever significant new developments are initiated.

3.2 Risk Analysis Process

3.2.1 A business impact analysis should be performed to assess the impact if a security breach were to occur.

Security breaches involving data or IT services, can be in the form of:

- A loss of confidentiality;
- A loss of integrity; or
- A loss of availability.

Business impact can include, but is not limited to:

- Disruptions to NUS operations;
- Legal liabilities
- Direct or indirect financial losses;
- Damage to the University's reputation and good standing; and
- Infringement of privacy issues.

Risk Identification: Threats Analysis

What is Threat Assessment?

- ▶ Armed with a properly classified inventory, you can assess potential weakness in each information asset - a process known as threat assessment.
- ▶ Three aspects
 - ▶ Threat identification
 - ▶ Threat assessment
 - ▶ Vulnerability assessment
- ▶ Threats
 - ▶ Circumstance or event that can adversely impact operations, assets, individuals through an information system.
 - ▶ To keep risk management ‘manageable’...
 - ▶ Identify realistic threats and investigate those further

the goal at the end of the day is to find internal weaknesses
- but now it would be to analyse external threats (environment)
to better understand internal vulnerabilities

Threat categories

Table 6-3 Threats to InfoSec

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Source: CACM.

Threat Assessment

- ▶ The following questions can help in understanding the various threats and their potential effects on an information asset
- ▶ Which threats
 - ▶ represent *an actual danger* to our organization's information?
 - ▶ are *internal* and which are *external*?
 - ▶ have the *highest probability of occurrence*?
 - ▶ have the *highest probability of success*?
 - ▶ could result in the *greatest loss* if successful?
 - ▶ are the organization *least prepared to handle*?
 - ▶ *cost the most to protect against*?
 - ▶ *cost the most to recover from*?

Prioritizing Threats

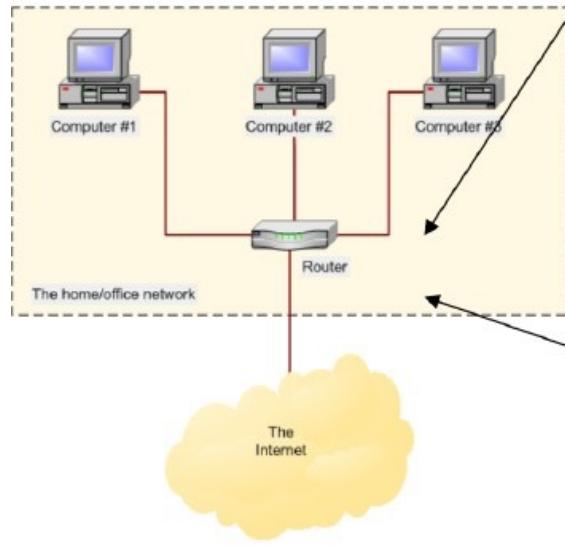
- ▶ Just as it did with information assets, the organization should conduct a weighted table analysis with threats
- ▶ The organization should list the categories of threats it faces, and then select categories that correspond to the questions of interest
- ▶ In extreme cases, the organization may want to perform such an assessment of each threat by asset, if the severity of each threat is different depending on the nature of the information asset under evaluation

Vulnerability Assessment

- ▶ Once the organization has identified and prioritized both its information assets and the threats facing those assets it can begin to compare information asset to threats
- ▶ Review every information asset for all vulnerabilities to every identified threat
 - ▶ Vulnerability =
 - ▶ Specific avenue that threat agents can exploit to attack the information asset
 - ▶ Flaw or weakness in an information asset, security procedure, design or control that can be exploited accidentally or on purpose to breach security of the asset
- ▶ A list should be created for each information asset to document its vulnerability to each possible or likely attack

Table 6-7 Vulnerability Assessment of a DMZ Router

Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	Employees or contractors may cause an outage if configuration errors are made.
Information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
Technical hardware failures or errors	Hardware could fail and cause an outage. Power system failures are always possible.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is stolen.



router

Asset

temperature control in
router/server room is
not adequate ⇒ router
overheats and
shuts down

[control weakness,
design flaw]

net. administrator
allows access to
unauthor. user ⇒
unauthor. user uploads a
virus, router crashes

[control / procedural
weakness]

Vulnerability

**Act of Human
Error or
Failure**

Threat

The TVA Worksheet

- ▶ Two lists produced at the end of risk identification process
 - ▶ Prioritized list of assets and their vulnerabilities
 - ▶ Prioritized list of threats facing the organization based on a weighted table
- ▶ Combine these two lists into a **Threats-Vulnerabilities-Assets (TVA)** worksheet
 - ▶ TIVIAI-Vulnerability I that exists between Threat I and Asset I

Table 6-8 Threat VA Worksheet

	Asset 1	Asset 2	Asset 3	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 ...	T1V1A2 T1V2A2 ...	T1V1A3 ...	T1V1A4 ...							
Threat 2	T2V1A1 T2V2A1 ...	T2V1A2 ...	T2V1A3 ...								
Threat 3	T3V1A1 ...	T3V1A2 ...									
Threat 4	T4V1A1 ...										
Threat 5											
Threat 6											
...											
...											
Threat n											
Priority of effort	1	2	3	4	5	6	7	8	...		
These bands of controls should be continued through all asset-threat pairs.											

Risk Assessment: Risk Analysis

Risk Estimate Factors

- ▶ Risk assessment
 - ▶ Assessing the *relative risk of each vulnerability*
 - ▶ While this number does not mean anything in absolute terms, it enables you to gauge the relative risk associated with each vulnerable information asset, and it facilitates the creation of comparative ratings later in the risk treatment process
 - ▶ Estimating risk is not an exact science; thus some practitioners use **calculated values for risk estimation**, whereas others rely on **broader methods of estimation.**
 - ▶ The goal is to develop a repeatable method to evaluate the relative risk of each of the vulnerabilities that have been identified and added to the list.

Determining the Likelihood of a Threat Event

- ▶ Likelihood is the overall rating - a numerical value on a defined scale - of the probability that a specific vulnerability will be exploited
- ▶ A simple method of assessing risk likelihood is to score the event on a rating scale:

Table 6-10 Risk Likelihood semi-quantitative methods

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months	Will never happen
1	Rare	5% likely in the next 12 months	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months	May happen once every 10 years
3	Moderate	50% likely in the next 12 months	May happen once every 5 years
4	Likely	75% likely in the next 12 months	May happen once every year
5	Almost Certain	100% likely in the next 12 months	May happen multiple times a year

Source: Clearwater Compliance IRM.

Determining the Likelihood of a Threat Event

- ▶ **NIST SP 800-30 r1. Managing Information Security risk Organizations**
 - ▶ Suggested **Likelihood** scale

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the threat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

numeric numbers makes ranking easier

Assessing Potential Impact on Asset Value

- ▶ **Impact – The magnitude of harm resulting from a threat event exploiting a vulnerability (or set of vulnerabilities).**

Table 6-11 Risk Impact

Rank	Description	Example	# of Records	Productivity Hours Lost	Financial Impact
0	Not applicable threat	No impact	N/A	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2	\$20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4	\$175,000
4	Major	One-day interruption, exposure of data	5,000	8	\$2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24	\$20,000,000

Source: Clearwater Compliance IRM.

Risk Determination

- ▶ Most organizations go with a simple formula:
 - ▶ Risk = Likelihood × Impact
- ▶ Practice:
 - ▶ Information asset 2 faced with threat 2 is at risk with general vulnerabilities 2 and 3. The risk rating for A2V2T2 has a Likelihood rating of 4 and an Impact rating of 4. The risk rating for A2V3T2 has a Likelihood rating of 3 and an Impact rating of 2. The resulting risk rating for A2V2T2 / A2V3T2 is ?
 - ▶ A2V2T2 :? 16
 - ▶ A2V3T2 :? 6

Table 6-12 Risk Rating Worksheet

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

Risk Rating Matrix X

		Severe (5)	Low	Medium	High	High	Critical
Impact	Major (4)	Low	Medium	Medium	High	High	High
	Moderate (3)	Low	Low	Medium	Medium	High	High
	Minor (2)	Low	Low	Low	Medium	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low	Low
			Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
	Likelihood						

Risk = Likelihood X Impact

Figure 6-10 Clearwater Compliance IRM risk rating matrix

Source: Clearwater Compliance IRM.

Uncertainty



Uncertainty in estimation can come from

- over estimation
- under estimation

- ▶ It is not possible to know everything about every vulnerability, such as the likelihood of an attack against an asset or how great an impact a successful attack would have on the organization
- ▶ The degree to which a current control can reduce risk is also subject to estimation error
- ▶ Uncertainty is an estimate made by the manager using judgment and experience
- ▶ One formula of estimating risk uses the following:
 - ▶ Risk = Likelihood of the exploitation of a vulnerability x Impact of the information asset **± uncertainty**

Uncertainty

▶ Practice:

- ▶ Information asset 2 faced with threat 2 is at risk with general vulnerabilities 2 and 3. The risk rating for A2V2T2 has a Likelihood rating of 4 and an Impact rating of 4. The risk rating for A2V3T2 has a Likelihood rating of 3 and an Impact rating of 2. You estimate that assumptions and data are 80 percent accurate. The resulting risk rating for A2V2T2 / A2V3T2 is ?
 - ▶ A2V2T2 :?
 - ▶ A2V3T2 :?  ± 1.2

Documenting the Results of Risk Assessment

- ▶ The efforts to compile risks into a comprehensive list allow the organization to make informed choices from the best available information
- ▶ It is also of value for future iterations of the process to document the results in a reusable form

Documenting the Results of Risk Assessment

▶ What to document

- ▶ Risk Scenario
 - ▶ Threat event, vulnerability, asset, consequence
 - E.g., Malware installed on POS terminals with no white-list application installation rule applied, makes credit card data stolen.
- ▶ Identification dateCSA recommendation - also benchmarked with US standard
- ▶ Existing measures
- ▶ Current risk
- ▶ Treatment plan
- ▶ Progress status
- ▶ Residual risk
- ▶ Risk Owner

Risk Evaluation

- ▶ Once the risk ratings are calculated for all TVA triples, the organization needs to decide whether it can live with the analyzed level of risk—in other words, the organization must determine its *risk appetite*
 - ▶ Risk Appetite:
 - ▶ The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility
- ▶ This is the **risk evaluation** stage
- ▶ The organization must translate its risk appetite from the general statement developed by the RM framework team (and based on guidance from the governance group) to a numerical value it can compare to each analyzed risk



NHS and bank will not have the same risk appetite

Risk Evaluation



Figure 6-12 Clearwater Compliance IRM risk threshold

Source: Clearwater Compliance IRM.

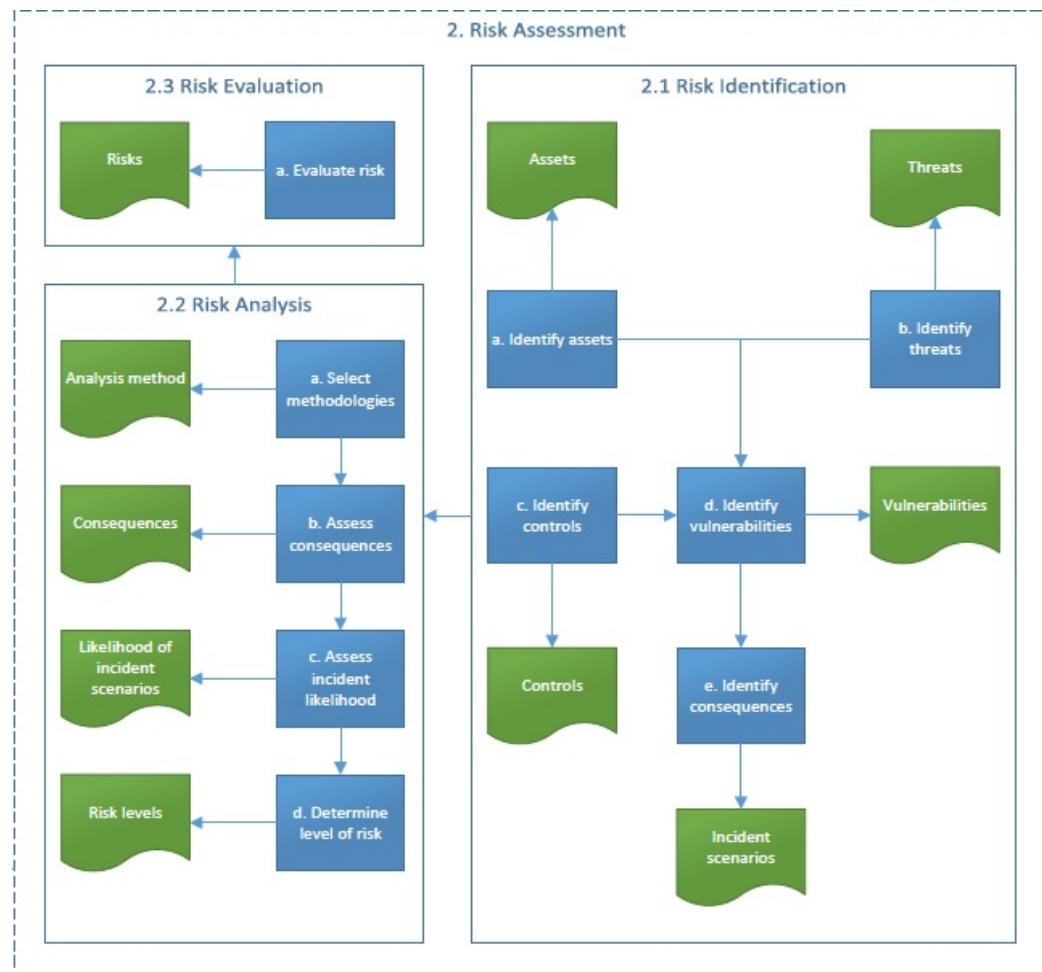
Risk Assessment Deliverables

Table 6-13 Risk Assessment Deliverables

Deliverable	Purpose
Information asset and classification worksheet	Assembles information about information assets, their sensitivity levels, and their value to the organization
Information asset value weighted table analysis	Rank-orders each information asset according to criteria developed by the organization
Threat severity weighted table analysis	Rank-orders each threat to the organization's information assets according to criteria developed by the organization
TVA controls worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization, identifies potential vulnerabilities in the "triples," and incorporates extant and planned controls
Risk ranking worksheet	Assigns a risk-rating ranked value to each TVA triple, incorporating likelihood, impact, and possibly a measure of uncertainty

Risk Assessment

- ▶ ISO27005: Risk Management
 - ▶ 2. Risk Assessment



Next Week

- ▶ Lecture 9 – Risk Treatment
 - ▶ Chapter 7

IS4231

Information Security Management

Lecture 9

Risk Management – Treating Risks

AY 2021/2022 Semester 2

Lecturer: Dr. YANG Lu

Reading: Chapter 7

Learning Objectives

- ▶ Discuss the *strategy options* used to treat risk and be prepared to select from them when given background information
- ▶ Evaluate control alternatives under the defense risk treatment strategy and formulate a cost–benefit analysis (CBA) using existing conceptual frameworks
- ▶ Explain how to maintain and perpetuate controls
- ▶ Describe popular methodologies used in the industry to manage risk



|

Topics

- ▶ Risk treatment strategies
- ▶ Feasibility and cost-benefit analysis
- ▶ Other methods of establishing feasibility
- ▶ Alternative risk management methodologies

► Risk Treatment Strategies

Risk Treatment Strategies

- ▶ An five basic risk control strategies:
 - ▶ *Defense*—Applying safeguards that eliminate or reduce the remaining uncontrolled risk
 - ▶ *Transference*—Shifting risks to other areas or to outside entities
 - ▶ *Mitigation*—Reducing the impact to information assets should an attacker successfully exploit a vulnerability
 - ▶ *Acceptance*—Understanding the consequences of choosing to leave a risk uncontrolled and then properly acknowledging the risk that remains without an attempt at control
 - ▶ *Termination*—Removing or discontinuing the information asset from the organization's operating environment

1. Defense

- ▶ **Attempts to prevent the exploitation of the vulnerability**
- ▶ This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards
- ▶ This approach is sometimes referred to as “avoidance”.
- ▶ Three common methods of risk defense are:
 - ▶ Application of policy
 - ▶ Application of training and education
 - ▶ Implementation of technology

2. Transference

- ▶ Attempts to shift risk to another entity
- ▶ Implement risk sharing by
 - ▶ Revising deployment models
 - ▶ Out-sourcing to other organizations
 - ▶ Implement service contracts with providers with more experience
 - ▶ Buying insurance
- ▶ Transferal may create new risks, or modify existing risks (that have already been identified)
 - ▶ May need additional risk treatment
 - ▶ Can share risk, but (usually) not possible to share liability of an impact

Service Level Agreement

- ▶ The key to an effective transference risk control strategy is the implementation of an *effective service level agreement (SLA)*
- ▶ In some circumstances, an SLA is the only guarantee that an external organization will implement the level of security the client organization wants
- ▶ Recommended four steps to create a successful SLA
 - ▶ Determining objectives
 - ▶ Defining requirements
 - ▶ Setting measurements
 - ▶ Establishing accountability

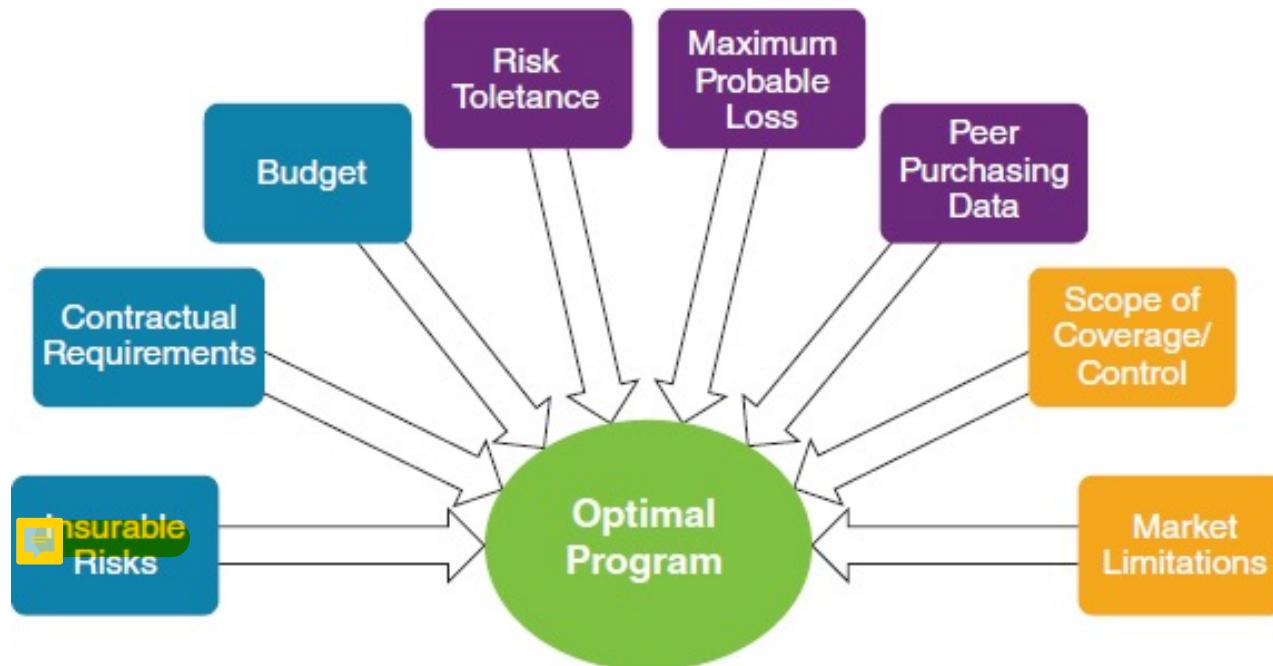
Example: Symantec Hosted Email Security SLA

“Our Service Level Agreement provides money back or other remedies if the following performance levels are not met:

- ▶ Antivirus Effectiveness – 100% protection against known and unknown email viruses
- ▶ Antivirus Accuracy – no more than 0.0001% false positives
- ▶ Antispam Effectiveness – 99% spam capture (95% for email with Asian characters)
- ▶ Antispam Accuracy – no more than 0.0003% false positives
- ▶ Email Delivery – 100% email delivery
- ▶ Latency – average email scanning time within 60 seconds
- ▶ Availability – 100% service uptime”

Buying insurance

- ▶ Typical components that make up an optimal cyber insurance program.



Source: Cybersecurity Handbook, 2017

3. Mitigation

- ▶ Attempt to reduce the impact of loss caused by an incident o disaster
- ▶ Types of mitigation plans
 - ▶ Incident response (IR) plan
 - ▶ Disaster recovery (DR) plan
 - ▶ Business continuity (BC) plan
 - ▶ Crisis management (CM) plan



4. Acceptance

- ▶ Knowingly and objectively accept the risk and do nothing beyond the current level of protection, because
 - ▶ The level of risk **meets the risk acceptance criteria**
 - OR**
 - ▶ The level of risk does *not* meet the risk acceptance criteria but the cost-benefit analysis shows that
 - ▶ The costs of controlling the risk are too high; or
 - ▶ The *benefits* accompanying the controls are extremely unattractive

this will usually based on a economic/monetary perspective

Risk Tolerance

► Risk tolerance table

► E,g.,

Risks companies might tolerate:

1. Power Outage - already have backup / chances are too low
2. Natural Disasters - too many resource limitation/too low chance
3. Tailgating problems - too difficult to control for low security areas

Risk Level	Risk Tolerance Description
Very High	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
Medium High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

5. Termination

- ▶ Like acceptance, the termination risk management strategy is based on the organization's intentional choice not to protect an asset;
 - ▶ Here, however, the organization does not wish the information asset to remain at risk and so removes it from the environment that represents risk
-
- ▶ Examples:
 - ▶ Equipment disposal
 - ▶ Discontinuing a provided service
 - ▶ Firing an employee

Feasibility & Cost-Benefit Analysis

Managing Risk

► Residual risk

- The amount of risk that remains after the organization has implemented policy, education and training, and technical controls and safeguards
- The goal of information security is not to bring residual risk to zero; rather it is to bring it in line with an organization's risk appetite

Go to the assets management -> find the threats & vulnerability -> rank the risks -> control the risks

Managing Risk

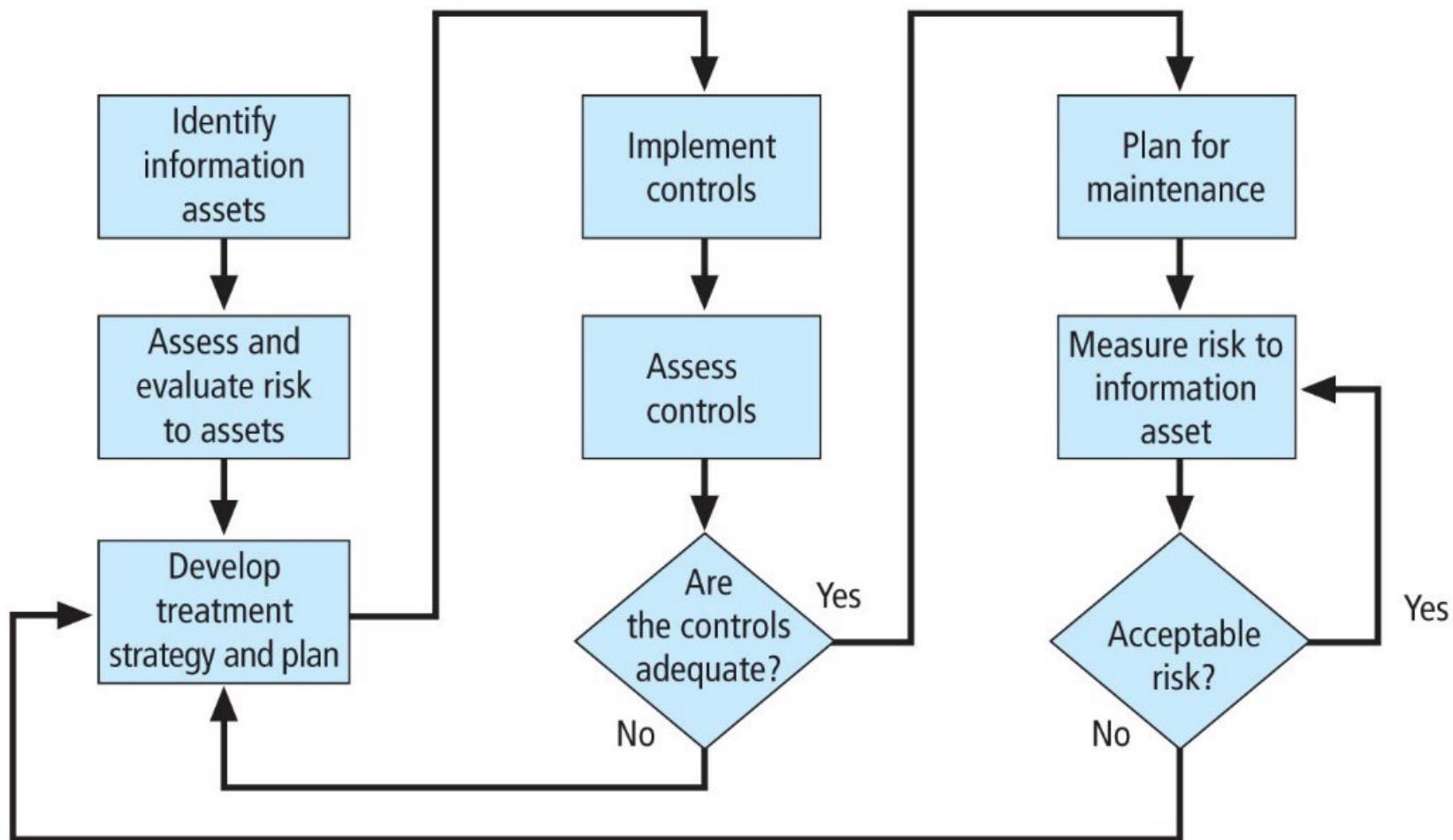


Figure 7-4 Risk treatment cycle

Feasibility Analysis

- ▶ Decision-making method that compares
 - ▶ ***COST*** of protecting an asset by implementing a risk control
vs.
 - ▶ ***ESTIMATED BENEFIT*** that would accrue from implementation of the control
- ▶ Helps in selection and assessment of security controls
- ▶ The commonly used criterion when evaluating a strategy to implement InfoSec controls and safeguards is
 - ▶ **Economic feasibility**

Cost

Total Cost Ownership - to take more perspectives to analyse the cost

- ▶ Life-cycle cost of implementing a control or safeguard includes things like:
 - ▶ Cost of developing or buying hardware, software, and services
 - ▶ Cost of getting personnel trained
 - ▶ Cost of implementation
 - ▶ Installing, configuring, and testing hardware & software
 - ▶ Professional services
 - ▶ Service costs
 - ▶ Vendor fees for maintenance and upgrades
 - ▶ Costs of maintenance
 - ▶ Labor expense to regularly verify, test, maintain, train, and update
 - ▶ Potential cost from the loss of the asset

Benefit

- ▶ The value to the organization of using controls to prevent losses associated with a specific vulnerability
- ▶ To calculate these we need to know
 - ▶ The dollar value of the information assets exposed by the vulnerability (i.e., **asset valuation**)
 - ▶ How much of that value is at risk
 - ▶ How much risk exists for the asset
- ▶ Expressed as the *annualized loss expectancy* (ALE)

Asset Valuation

 commercial entities will be easier to evaluate their branding
- will be highly reflected by their consumer confidence in service/product
- easily quantified/estimated from the financial market performances will be reflected very sensitively and immediately from the share performances

- ▶ The (complex) process of assigning financial value or worth to each **information asset**
- ▶ Different kinds of value, some easy to quantify while others more abstract
 - ▶ Real costs (concrete, easily quantifiable)
 - ▶ E.g., Direct replacement cost / maintenance cost
 - ▶ Perceived or notional value
 - ▶ E.g., Value of the organization's reputation
 - ▶ Acquired value ('real' value higher than intrinsic value)

 how will NUS value their reputation

Asset Valuation Approaches

- ▶ Some approaches of asset valuation include:
 - ▶ Value retained from the cost of creating the information asset
 - ▶ Value retained from past maintenance of the information asset
 - ▶ Value implied by the cost of replacing the information
 - ▶ Value from providing the information
 - ▶ Value acquired from the cost of protecting the information
 - ▶ Value to owners
 - ▶ Value of intellectual property
 - ▶ Value to adversaries
 - ▶ Loss of productivity while the information assets are unavailable
 - ▶ Loss of revenue while information assets are unavailable
 - ▶ Total cost of ownership

Estimation of Potential Loss

- ▶ A traditional model of calculating quantitative cost–benefit analyses involves estimating the likelihood of an attack based on an annualized rate of occurrence and the impact of an attack based on loss expectancy
- ▶ The questions that must be asked: If a vulnerability is exploited
 - ▶ What loss or damage could happen, and what financial impact would it have?
 - ▶ What would it cost to recover from the attack, in addition to the financial impact of damage?
 - ▶ What is the single loss expectancy for each risk?

Step 1: Calculate Single Loss Expectancy for the Vulnerability

- ▶ The most likely loss (in value) from a single exploitation of the vulnerability
- ▶ Inputs
 - ▶ AV = Asset Value
 - ▶ EF = Exposure Factor
 - ▶ Expected percentage loss that would occur from a given vulnerability being exploited

$$\mathbf{SLE = AV \times EF}$$

Step 2: Calculate Annualized Loss Expectancy for the Vulnerability

- ▶ Overall loss potential of the risk on an annual basis
 - ▶ Inputs
 - ▶ SLE (from Step 1)
 - ▶ ARO (Annualized Rate of Occurrence)
 - Indicates how often a *successful* attack (that exploits the vulnerability) is expected to occur in a year
 - ▶ Examples
 - If a successful attack occurs once every 2 years $\Rightarrow \text{ARO}=0.5$
 - If an attack happens several times a second but succeeds once each month $\Rightarrow \text{ARO}=12$.
 - ▶ **ALE (Annualized Loss Expectancy)=SLE*ARO**

Example: Website

- ▶ Estimated value of website AV = \$1,000,000
 - ▶ Sabotage/vandalism would damage or destroy 10% of website
 - ▶ Annualized rate of occurrence ARO=0.5

So SLE=?ALE=?

$$SLE = 1000000 \times 0.1 = 100\ 000$$

$$ALE = 100\ 000 \times 0.5 = 50\ 000$$



thus the selected control should cost less than 50k

More Examples

Asset	Risk	AV	EF	SLE	ARO	ALE
Customer database	Hacked	\$432,000	0.74	\$320,000	0.25	\$80,000
Word documents and data files	Virus	\$9,450	0.17	\$1,650	0.9	\$1,485
Domain controller	Server failure	\$82,500	0.88	\$72,500	0.25	\$18,125
E-commerce website	DDoS	\$250,000	0.44	\$110,000	0.45	\$49,500

What is the ALE good for?

- ▶ Indicates how much the organization could benefit from addressing a specific vulnerability
- ▶ A clear, easily understood value that can be used for budgetary purposes
- ▶ Can be used to test economic feasibility of every control alternative for a specific vulnerability
 - ▶ Using the **cost-benefit analysis formula**

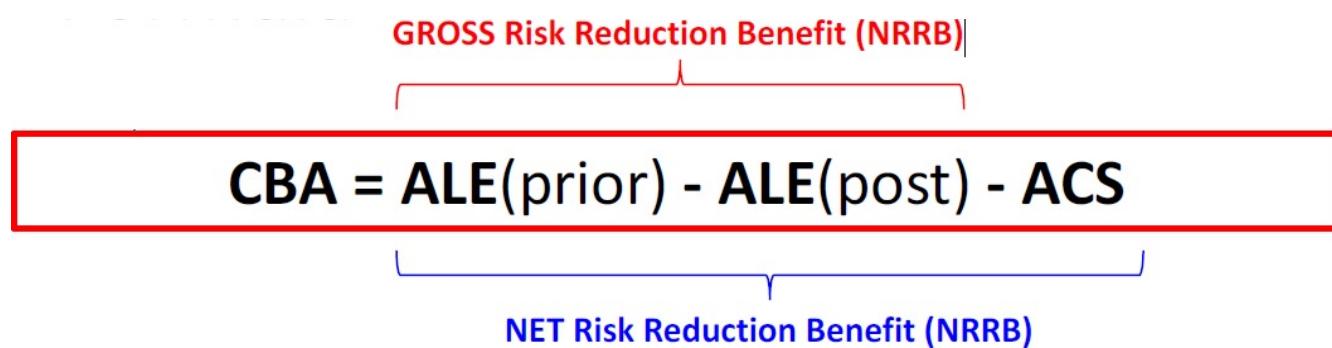
Feasibility Analysis (cont.)

- ▶ When is a feasibility analysis done?
 - ▶ Before a risk control is implemented, to decide if the control is worth implementing
 - ▶ After a risk control has been implemented and been functioning for some time, to assess if the control was worth implementing

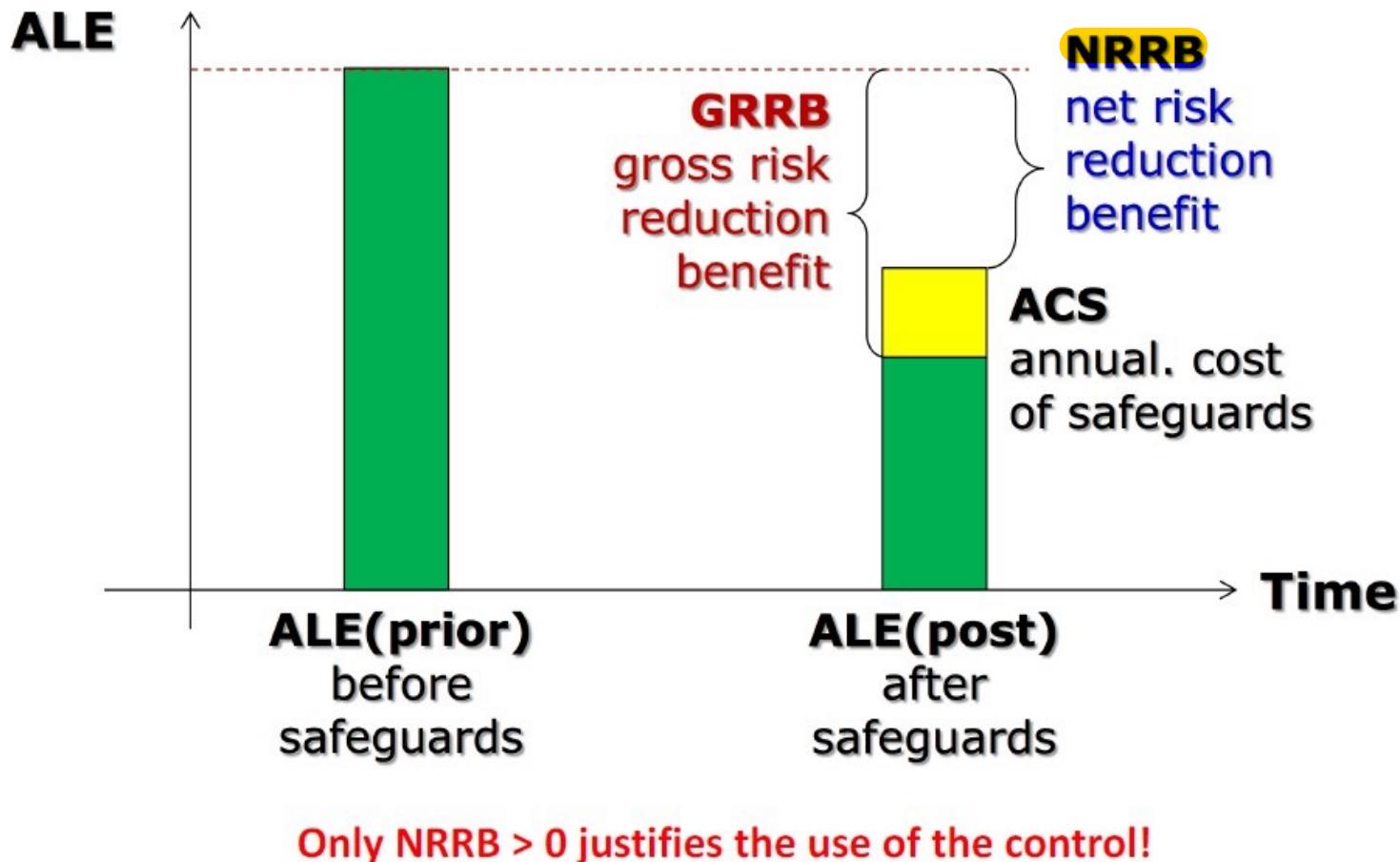
Organization should not spend more to protect an asset than the asset is worth!

Cost-Benefit Analysis (CBA) Formula

- ▶ **ALE(prior)**
 - ▶ Annualized loss expectancy *before* implementing the control
- ▶ **ALE(post)**
 - ▶ Annualized loss expectancy *after* implementing the control
- ▶ **ACS**
 - ▶ Annual cost of **implementing the safeguard** (i.e., control)



Cost-Benefit Analysis (CBA) Formula (cont.)



Example: Determining NRRB

Your organization has decided to centralize anti-virus support on a server which automatically updates virus signatures on user's PCs.

When calculating risk due to viruses, the annualized loss expected (ALE) is \$145,000.

The cost of this anti-virus countermeasure is estimated to \$24,000 per year, and it will lower the ALE to \$65,000.

Is this a cost-effective control? Why or why not?

$$145 - 65 - 24 = 56k$$

This control is cost-effective = Net Risk Reduction Benefit is 56k which is a positive number
- plus it is around 50% of the original ALE (prior) thus it is very cost effective

Other Feasibility Measures

- ▶ Cost-benefit analysis determines whether a security control measure is economically feasible
- ▶ Other ‘measures of feasibility’ when evaluating a security control, include
 - ▶ Organizational feasibility
 - ▶ Operational (or behavioural feasibility)
 - ▶ Technical feasibility
 - ▶ Political feasibility

Organizational Feasibility

- ▶ Examines how well a proposed information security control will contribute to organization's **strategic objectives**

to measure organisational feasibility - can just arrange a meeting with governance & senior manager team to check

Operational Feasibility

- ▶ Known as behavioral feasibility
- ▶ Examines users' and management's acceptance & support of a proposed security control
 - ▶ e.g., A new policy / technology / programme will fail if users do not accept and support it
 - ▶ Most common methods for getting user acceptance
 - ▶ Communication
 - Affected parties must know the purpose and benefits of the proposed change
 - ▶ Education
 - Affected parties must be educated on how to work under the new constraints
 - ▶ Involvement
 - Affected parties must be given a chance to express what they want and what they will tolerate from the system



best way to detect/measure behavioral feasibility

= anonymous survey for pilot programmes

= focus group discussions

= workshops to interact with different employees

= adoption rate / usage time

Technical Feasibility

- ▶ Determine whether organization has or can acquire the technology and/or tech expertise to implement and support the proposed controls
 - ▶ e.g., a firewall may require special software/hardware support/installation on all computers

Political Feasibility

- ▶ Determines what can or cannot be done based on the consensus and relationships between the communities of interest
- ▶ e.g., IT and infosec departments may have to compete for same or limited resources this might be because CISO is lower than CIO

or some privacy issue - since there are so many policy measures

- to monitor employee behaviour
- or to collect employee bio data or extra data

Alternatives to Feasibility Analysis

- ▶ **Benchmarking**
- ▶ **Due care and due diligence**
- ▶ Best business practices
- ▶ Gold standard
 - ▶ Organizations aspire to set the standard for their industry.
- ▶ Government recommendations and best practices
- ▶ **Baseline**

Documenting the Results of Risk Assessment

- ▶ What to document
 - ▶ Risk Scenario
 - ▶ Threat event, vulnerability, asset, consequence
 - E.g., Malware installed on POS terminals with no white-list application installation rule applied, makes credit card data stolen.
 - ▶ Identification date
 - ▶ Existing measures
 - ▶ Current risk
 - ▶ Treatment plan
 - ▶ Progress status
 - ▶ Residual risk
 - ▶ Risk Owner

Recommended Risk Control Practices

Qualitative and Hybrid Measures

- ▶ Use if quantitative methods don't work or are too inaccurate
- ▶ Use *labels* for values
 - ▶ E.g., for ARO, list all the attacks possible on a particular information asset, then rate the attacks on low/medium/high probability of occurrence for annual risk of occurrence

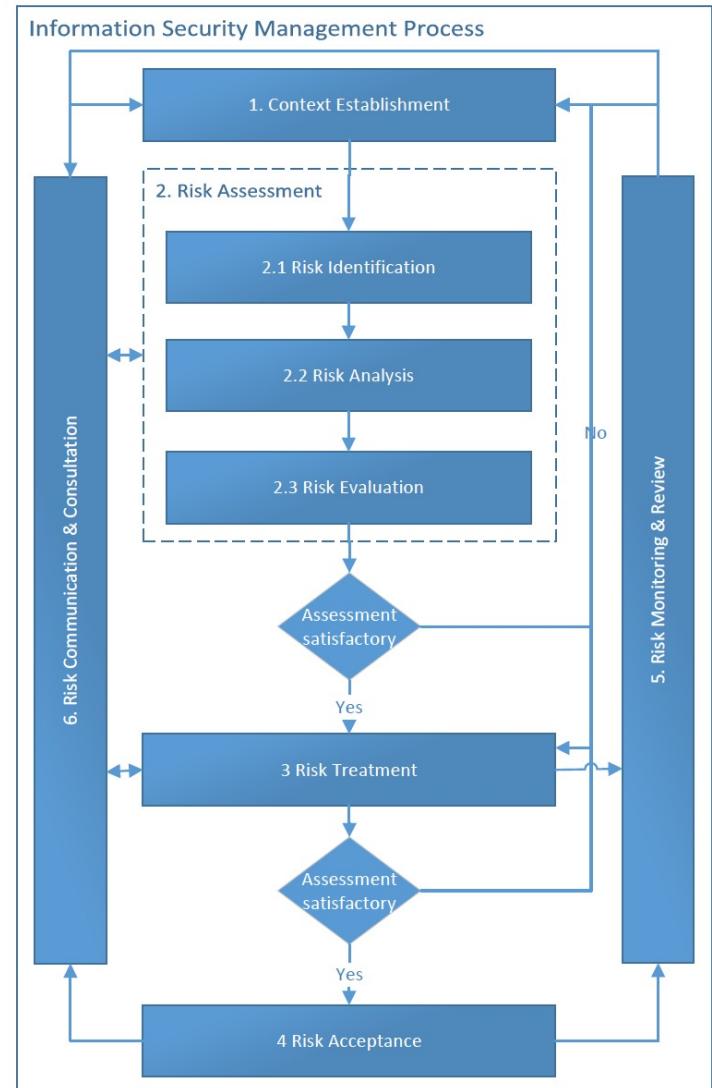
	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

Hybrid Assessment

- ▶ Try to improve on ambiguity of qualitative measures by using ranges of values instead of specific ‘single number’ values
- ▶ Examples
 - ▶ Chance of occurrence of a threat
 - ▶ Scale of 0 - 10, where
 - 0 = no chance of occurrence
 - 10 = almost certain occurrence
 - ▶ Value of information asset
 - ▶ Scale of 1 - 10, where
 - 1 = relatively worthless
 - 10 = extremely critical

ISO27005 InfoSec Risk Management

- ▶ ISO27005: Risk Management
 - ▶ ISMS risk management process
 - ▶ 1. Context Establishment
 - ▶ 2. Risk Assessment
 - 2.1 risk identification
 - 2.2 risk analysis
 - 2.3 risk evaluation
 - ▶ 3. Risk Treatment
 - ▶ 4. Risk Acceptance
 - ▶ 5. Risk Monitoring & Review
 - ▶ 6. Risk Communication & Consultation



ISO 31000 Risk Management

- ▶ ISO 31000 Risk Management
 - ▶ <https://www.iso.org/iso-31000-risk-management.html>
- ▶ It targeted towards any type of risk management
 - ▶ Enterprise risk management
 - ▶ Financial risk management
 - ▶ Environmental risk management
 - ▶ etc

ISO 31000 Risk Management

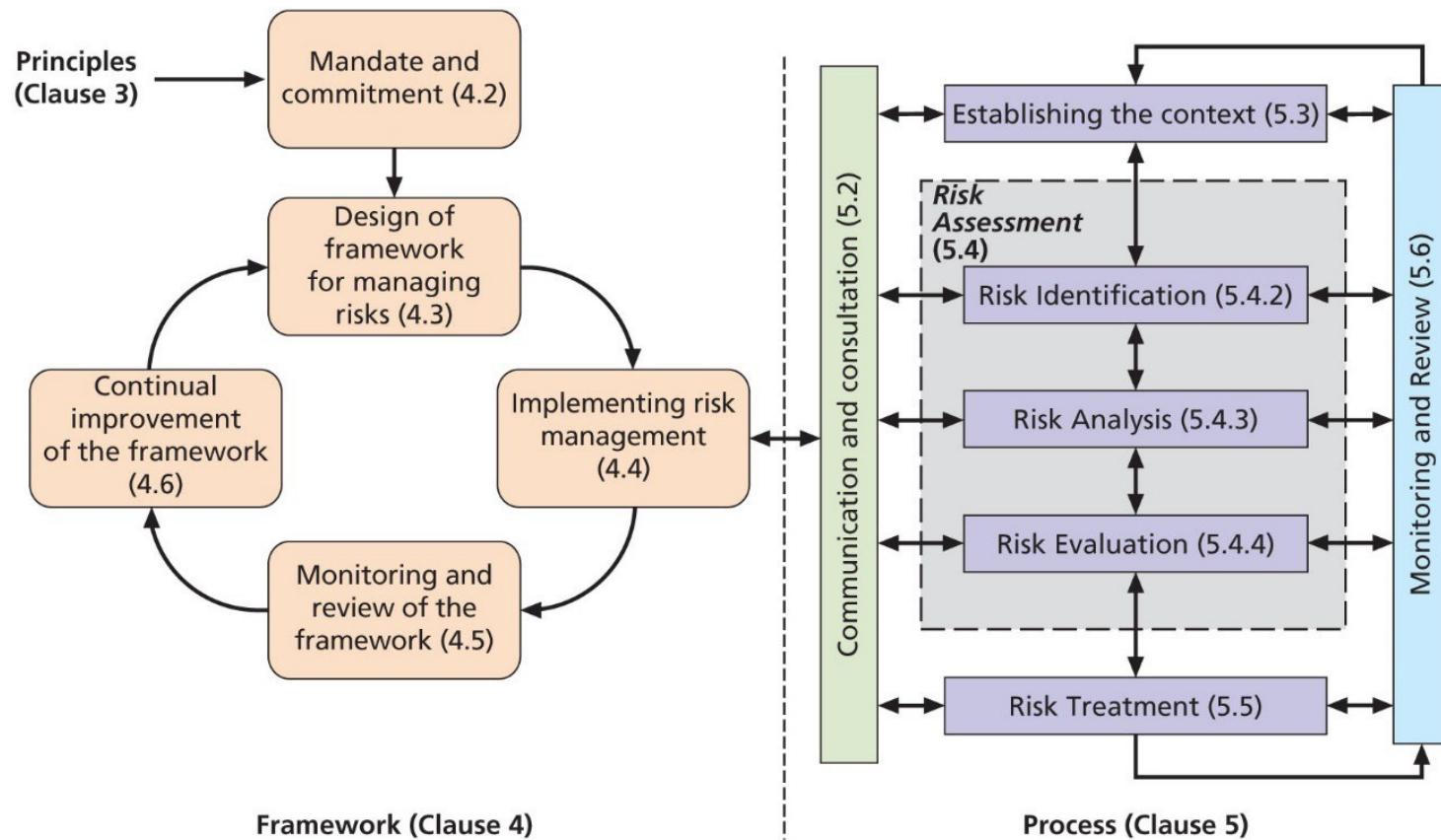


Figure 7-11 ISO 31000 risk management framework and process

Source: ISO 31000: 2009.¹⁵

NIST Risk Management Framework

- ▶ “Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information SystemView”

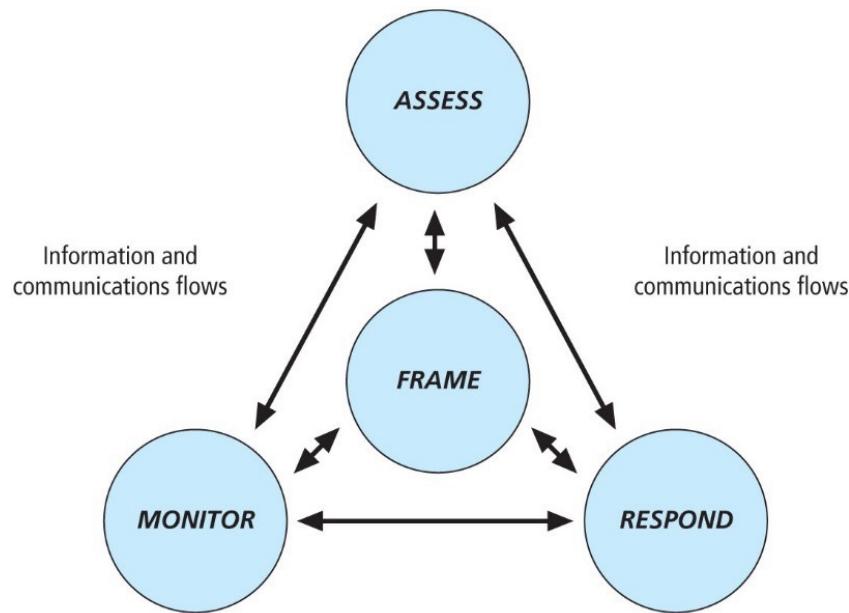


Figure 7-12 NIST risk management framework overview

Microsoft Risk Management Approach

- ▶ Four phases in the MS InfoSec risk management process:
 1. Assessing risk
 2. Conducting decision support
 3. Implementing controls
 4. Measuring program effectiveness

Microsoft Risk Management Approach

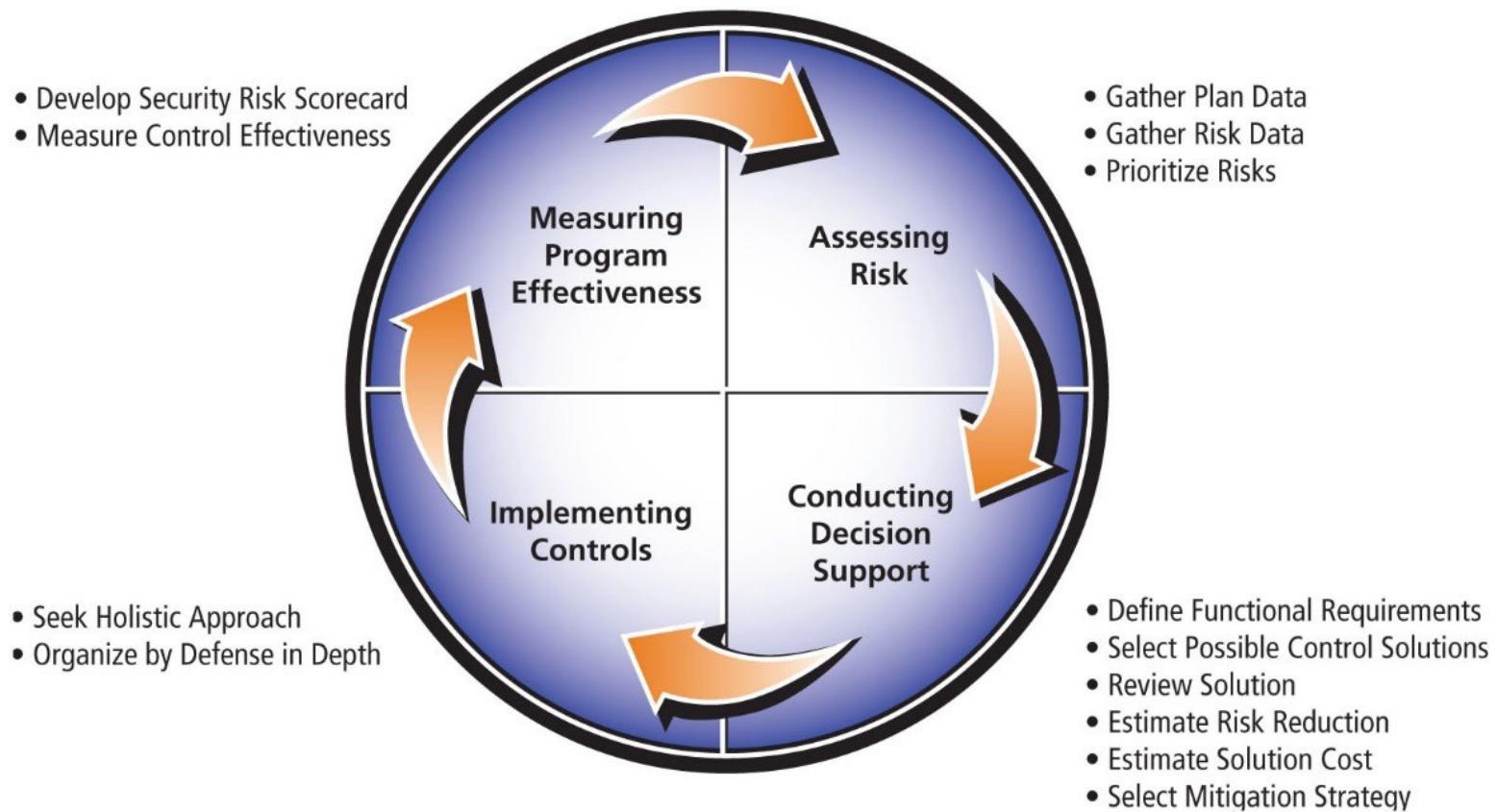


Figure 7-8 Microsoft's security risk management guide

Next Week

- ▶ L10 Planning for Contingencies
- ▶ Ch10

IS4231

Information Security Management

Lecture 10

Planning for Contingencies

AY 2021/2022 Semester 1

Lecturer: Dr. YANG Lu

Reading: Chapter 10

Learning Objectives

- ▶ Describe the major components of incident response, disaster recovery, business continuity and crisis management
- ▶ Discuss how the organization would prepare and execute a test of contingency plans



Topics

- ▶ Business Impact Analysis
- ▶ Incident Response Planning
- ▶ Disaster Recovery Planning
- ▶ Business Continuity Planning
- ▶ Crisis Management
- ▶ Timing & Sequence of CP Elements
- ▶ Testing Contingency Plans

Introduction to Contingency Planning

What is Contingency Planning?

- ▶ **Contingency Planning (CP)**
 - ▶ The overall process of preparing for *unexpected adverse events*
 - ▶ Main goal
 - ▶ Restore normal modes of operation with minimal cost asap
 - ▶ Involves IT and InfoSec managers, supported by all other communities of interest or stakeholders

 due to limited resources, usually it is not possible to react to adverse event in the most ideal way
- typically, there is a need to balance and compromise

Four Major Components

- ▶ **Business Impact Analysis (BIA)**
 - ▶ Help the organization identify which business functions and information systems are the most critical to the success of the organization
- ▶ **Incident Response Plan (IRP)**
 - ▶ Focus on the immediate responses to unexpected adverse event
- ▶ **Disaster Recovery Plan (DRP)**
 - ▶ Focuses on restoring operations at the primary site after disasters occur
- ▶ **Business Continuity Plan (BCP)**
 - ▶ Facilitates establishment of operations at an alternate site

Components of Contingency Planning

- ▶ CP major components:
 - ▶ BIA, IR plan, DR plan, BC plan, CR plan

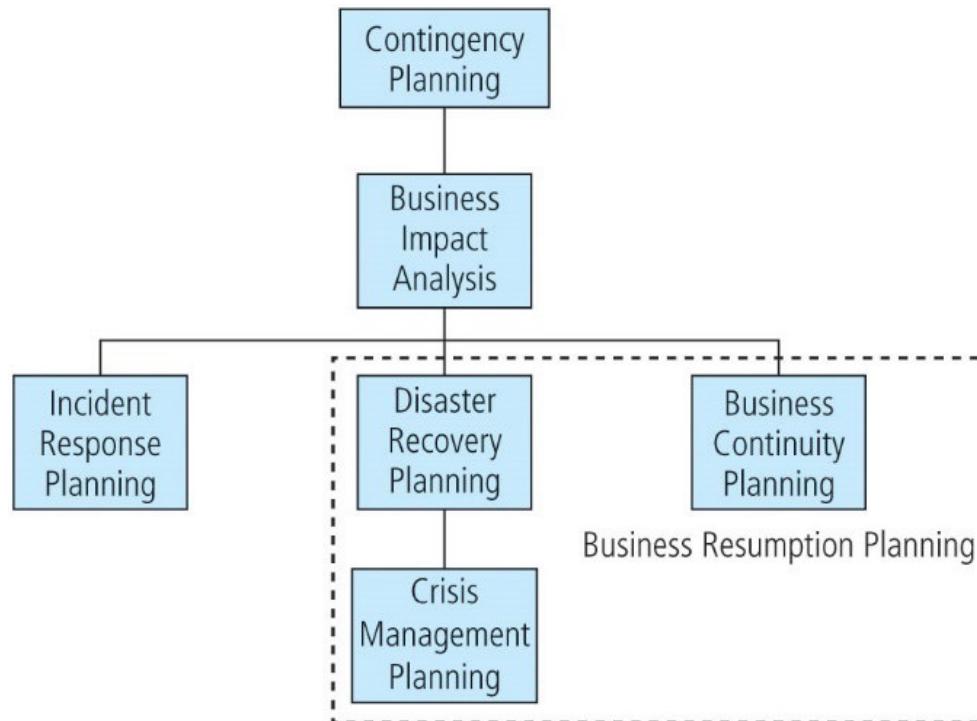


Figure 10-1 Contingency planning hierarchies

Fundamentals of Contingency Planning (cont.)

- ▶ **Contingency planning management team (CPMT)**
 - ▶ CIO, system administrators, CISO, key IT and business managers should be actively involved
- ▶ **Developing a CP document**
 - ▶ Develops the CP policy statement
 - ▶ Conducts the BIA
 - ▶ Identifies preventative controls
 - ▶ Creates contingency strategies
 - ▶ **Develops a contingency plan**
 - ▶ Ensures plan testing, training, and exercises
 - ▶ Ensures plan maintenance

Fundamentals of Contingency Planning (cont.)

- ▶ Individuals and teams involved in CP
 - ▶ CPMT should include:
 - ▶ Champion
 - ▶ Project Manager
 - ▶ Team Members
 - Business managers
 - Information technology managers
 - Information security managers
 - ▶ Incident response team - manages and executes the IR plan
 - ▶ Disaster recovery team - manages and executes the DR plan
 - ▶ Business continuity team - manages and executes the BC plan

Since the ITSec team is usually very small, it is very normal for overlapping to occur between the different teams

Business Impact Analysis

What is Business Impact Analysis?

- ▶ BIA investigates and assesses the impact that identified adverse events can have on the organization
 - ▶ By assuming that attack succeeded, the worst has happened, then assessing how that adversity will impact the organization.
- ▶ The CPMT conducts the BIA in three stages:
 1. Determine mission/business processes and recovery criticality
 2. Identify resource requirements
 3. Identify recovery priorities for system resources

1. Determine Mission/Business Processes and Recovery Criticality

- ▶ A BIA  questionnaire is an instrument used to collect relevant business impact information for analysis, It can allow functional managers to enter:
 - ▶ Information about their functions  by default, CISO/CIO should already know about the  own jewels of the business
 - ▶ Impacts the functions have on the business
 - ▶ Dependencies that exist for the functions from specific resources and outside service providers
- ▶ Then a weighted table analysis (WTA) could be used to decide which business processes and functions are most critical

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

▶ Key recovery measures affecting B.I.A

- ▶ **Maximum Tolerable Downtime (MTD)** - “the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations
- ▶ **Recovery time objective (RTO)** - maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and processes
- ▶ **Recovery point objective (RPO)** - the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered from backups after an outage

however most of the time there has to be hard requirements set which will come from external forces- these will come from external organisations (compliance agency)

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

- ▶ Key recovery measures affecting B.I.A
 - ▶ **Work Recovery Time (WRT)** - the amount of effort (expressed as elapsed time) that is necessary to get the business function operational AFTER the technology element is recovered (as identified with RTO).
 - ▶ It typically involves the addition of **nontechnical tasks required** for the organization to make the particular information asset usable for its intended business function again

RTO, RPO, MTD and WRT

RTO RPO MTD graph

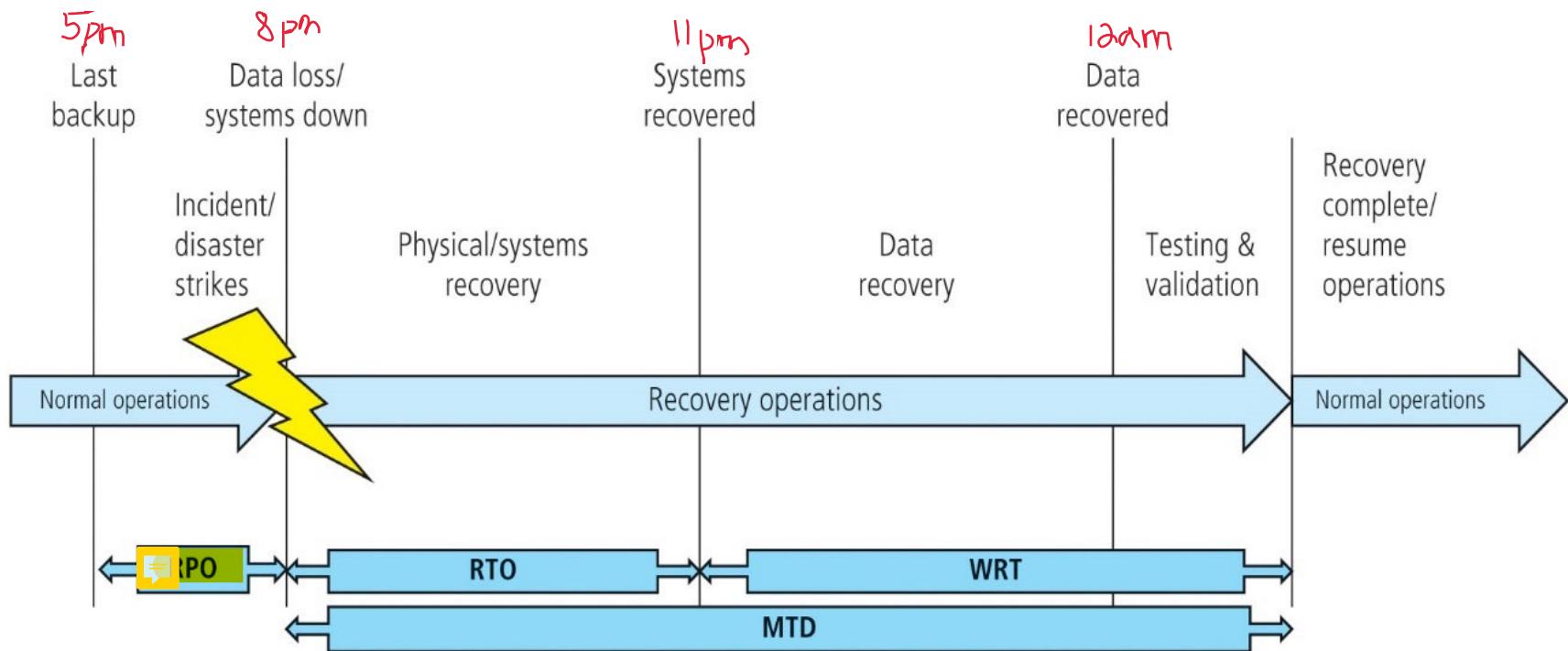


Figure 10-4 RTO, RPO, MTD, and WRT

Source: <http://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html>.

MTD = 4h

RPO = 3h

RTO = 3h

WRT = 1h

1. Determine Mission/Business Processes and Recovery Criticality (cont.)

- ▶ Must balance the cost of system inoperability against the cost of recovery

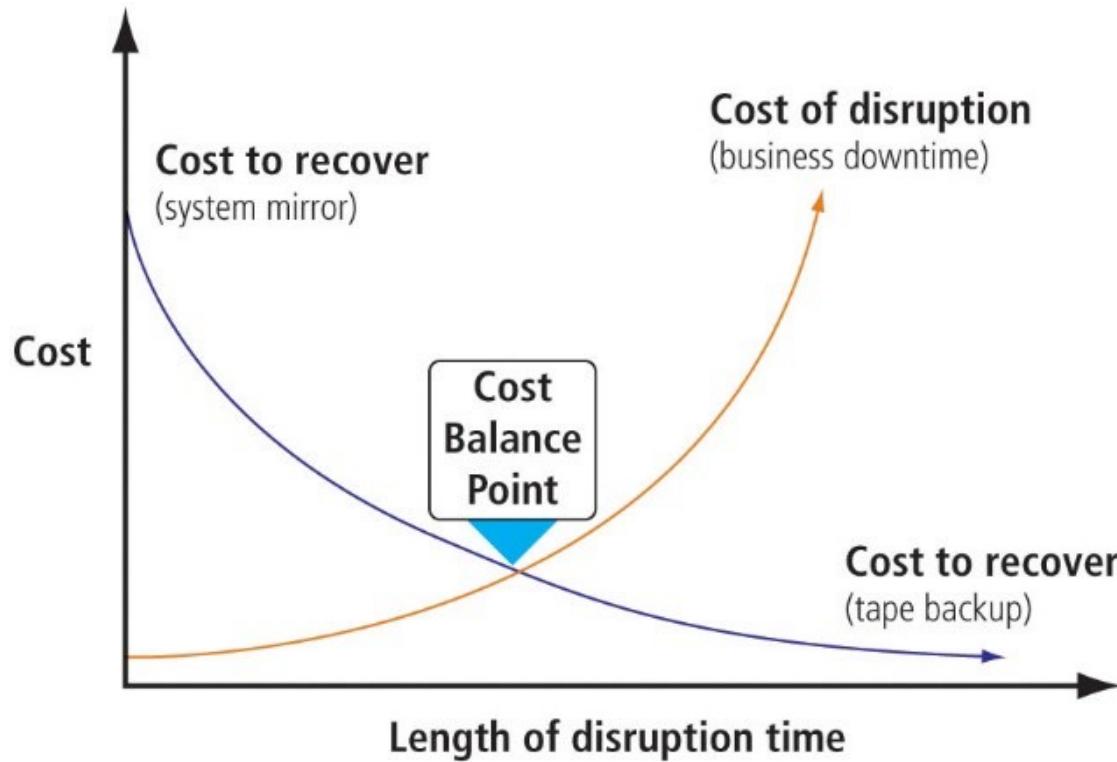


Figure 10-5 Cost balancing

Example: MAS requirements

► 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.

7 A bank shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

Incident Contingency Planning

Incident

- ▶ Adverse event: An event with negative consequences that could threaten the organization's information assets or operations. Sometimes referred to as an incident candidate
- ▶ Incident: An adverse event that could result in a loss of information assets, but *does not threaten the viability of the entire organization*
severity of situation is manageable/controlled = then will be called an incident
- ▶ It is important to understand that IR is a *reactive measure, not a preventative one*

Getting Started

- ▶ An early task for the CPMT is to form a computer security incident response team (IRT)
 - ▶ An IR team composed of technical IT, managerial IT, and InfoSec professionals who are prepared to detect, react to, and recover from an incident
- ▶ Key members of the IRT become the IR planning committee and begin work by
 - ▶ Developing policy to define the operations of the team,
 - ▶ Articulating the organizational response to various types of incidents
 - ▶ Advising end users on how to contribute to the effective response of the organization

Incident Response Policy

- ▶ The policy statement that guides the development and implementation of IR plans and the formulation and performance of IR teams
- ▶ Key Components
 - ▶ Statement of management commitment
 - ▶ Purpose and objectives of the policy
 - ▶ Scope of the policy
 - ▶ Definition of InfoSec incidents and related terms
 - ▶ Organizational structure and definition of rules, responsibilities, and levels of authority
 - ▶ Prioritization or severity ratings of incidents
 - ▶ Performance measures
 - ▶ Reporting and contact forms

Incident Response Planning

- ▶ For every incident scenario, the CP team creates three sets of incident-handling procedures:
 - ▶ Before the incident
 - ▶ Details of data backup schedules
 - ▶ Disaster recovery preparation
 - ▶ Training schedules
 - ▶ Testing plans
 - ▶ Copies of service agreements
 - ▶ During the incident
 - ▶ After the incident

Example of IRP Incident-handling procedures

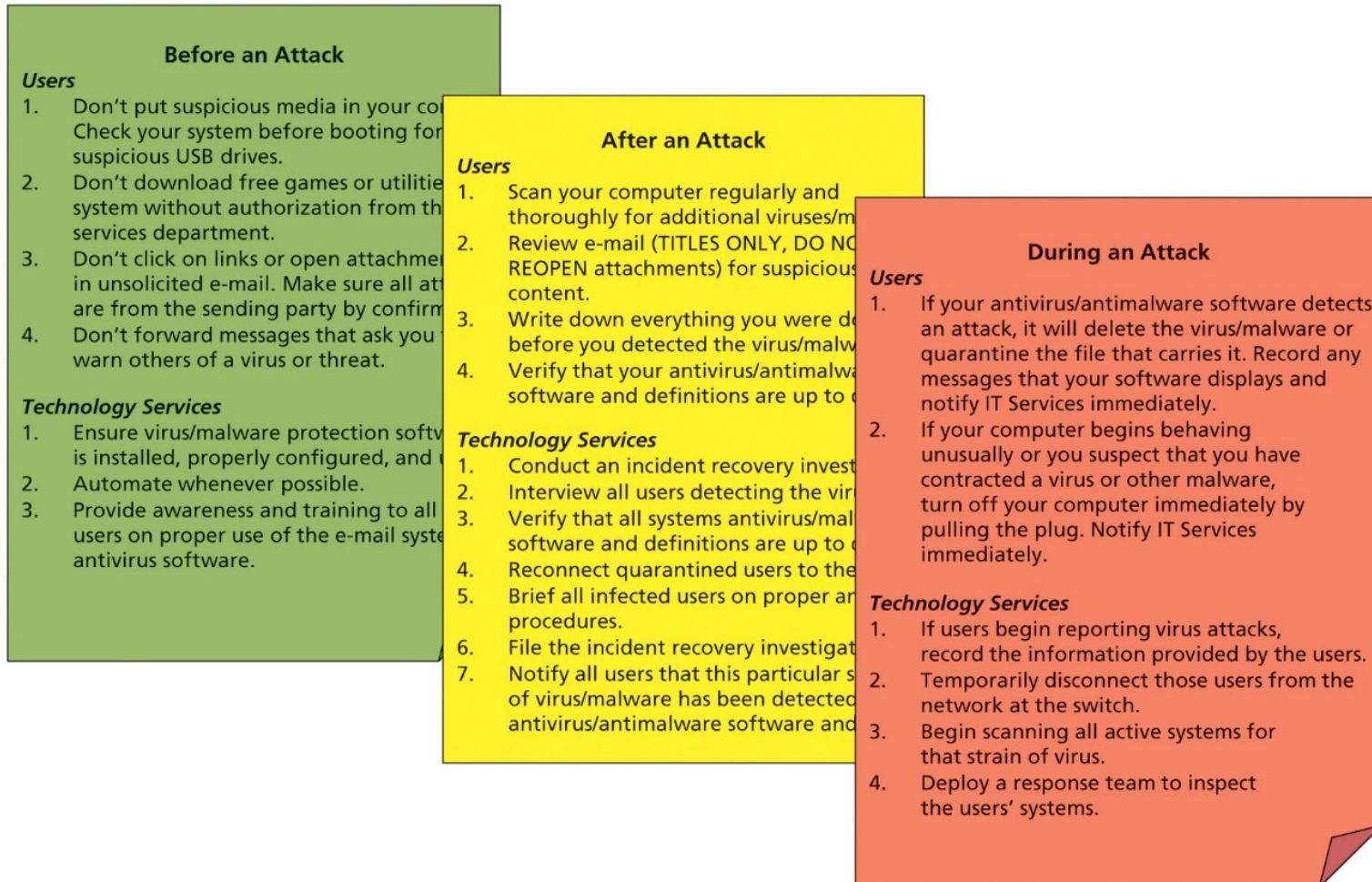


Figure 10-8 Example of IRP incident-handling procedures

Incident Response Actions

- ▶ Incident response actions can be organized into three basic phases:
 1. Detection—Recognition that an incident is under way
 2. Reaction—Responding to the incident in a predetermined fashion to contain and mitigate its potential damage
 3. Recovery—Returning all systems and data to their state before the incident

1.Detecting Incidents

- ▶ Incident classification is the process of examining an adverse event or incident candidate and determining whether it constitutes an actual incident
- ▶ Three categories of incident indicators:
 - ▶ Possible indicators
 - ▶ *Presence of unfamiliar files*
 - ▶ *Presence or execution of unknown programs or processes*
 - ▶ *Unusual consumption of computing resources*
 - ▶ *Unusual system crashes*

1.Detecting Incidents (cont.)

- ▶ Three categories of incident indicators (cont.):
 - ▶ Probable indicators
 - ▶ *Activities at unexpected times*
 - ▶ *Presence of new accounts*
 - ▶ *Reported attacks*
 - ▶ *Notification from an Intrusion Detection and Prevention System (IPDS)*
 - ▶ Definite indicators
 - ▶ *Use of dormant accounts*
 - ▶ *Changes to logs*
 - ▶ *Presence of hacker tools*
 - ▶ *Notifications by partner or peer*
 - ▶ *Notification by hacker*

Indicators of Compromise (IOC)

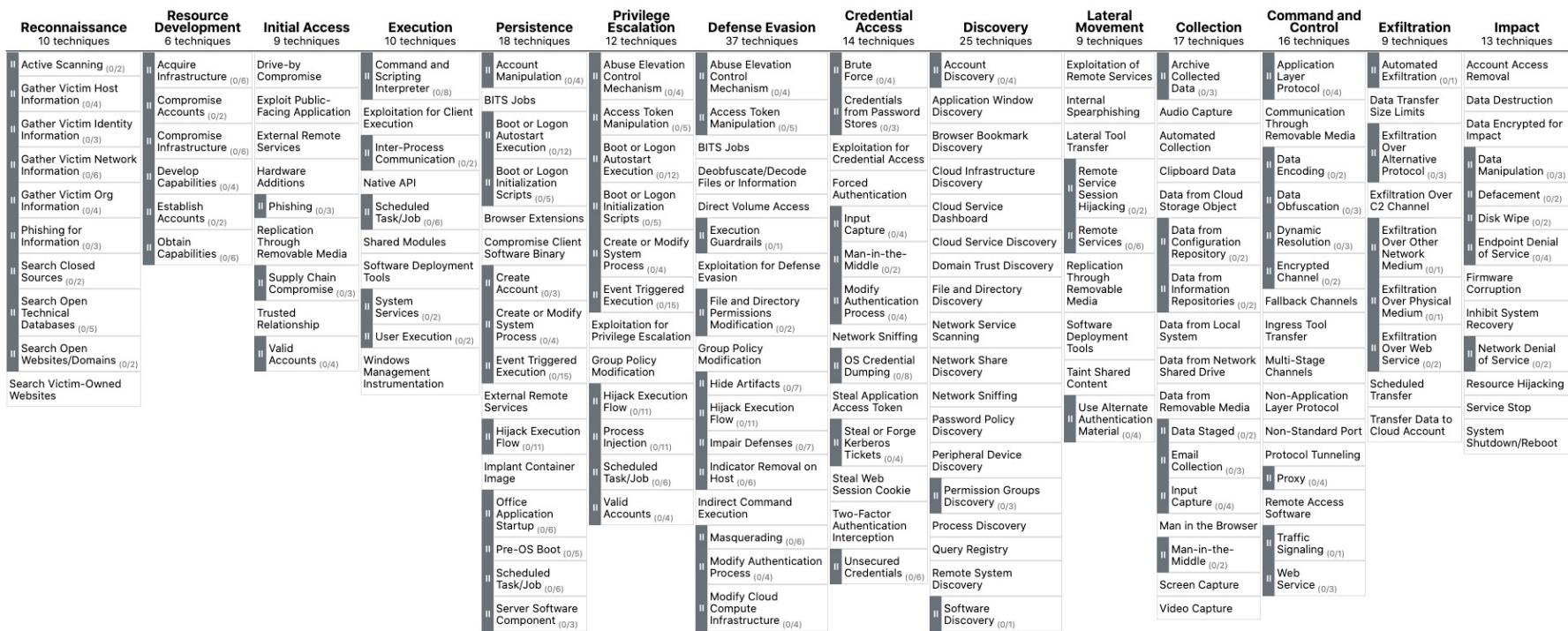
- ▶ Forensic artifacts that are used as signs that, with high confidence, indicates a computer intrusion.
 - ▶ Such as:
 - ▶ Unusual traffic going in and out of the network
 - ▶ Unknown files, applications, and processes in the system
 - ▶ Suspicious activity in administrator or privileged accounts
 - ▶ Irregular activities such as traffic in countries an organization doesn't do business with
 - ▶ Dubious log-ins, access, and other network activities that indicate probing or brute force attacks
 - ▶ Anomalous spikes of requests and read volume in company files
 - ▶ Network traffic that traverses in unusually used ports
 - ▶ Tampered file, Domain Name Servers (DNS) and registry configurations as well as changes in system settings, including those in mobile devices
 - ▶ Large amounts of compressed files and data unexplainably found in locations where they shouldn't be

MITRE ATT&CK Framework

- ▶ It contains a set of techniques used by adversaries to accomplish a specific objective.
 - ▶ **Reconnaissance:** gathering information to plan future adversary operations, i.e., information about the target organization
 - ▶ **Resource Development:** establishing resources to support operations, i.e., setting up command and control infrastructure
 - ▶ **Initial Access:** trying to get into your network, i.e., spear phishing
 - ▶ **Execution:** trying to run malicious code, i.e., running a remote access tool
 - ▶ **Persistence:** trying to maintain their foothold, i.e., changing configurations
 - ▶ **Privilege Escalation:** trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
 - ▶ **Defense Evasion:** trying to avoid being detected, i.e., using trusted processes to hide malware
 - ▶ **Credential Access:** stealing accounts names and passwords, i.e., keylogging
 - ▶ **Discovery:** trying to figure out your environment, i.e., exploring what they can control
 - ▶ **Lateral Movement:** moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
 - ▶ **Collection:** gathering data of interest to the adversary goal, i.e., accessing data in cloud storage
 - ▶ **Command and Control:** communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
 - ▶ **Exfiltration:** stealing data, i.e., transfer data to cloud account
 - ▶ **Impact:** manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

MITRE ATT&CK Framework (cont.)

- ▶ It contains a set of techniques used by adversaries to accomplish a specific objective.



Source: <https://attack.mitre.org/>

2. Reacting to Incidents

- ▶ Once an incident has been confirmed and properly classified
 - ▶ The IR plan moves from the detection phase to the reaction phase
- ▶ An effective IR plan includes the following steps:
 - ▶ **Notification of key personnel**
 - ▶ Alert roster, alert message
 - ▶ Documentation of the incident
 - ▶ It should record the who, what, when, where, why and how of each action taken while the incident is occurring
 - ▶ It serves as a case study after the fact
 - ▶ Assignment of tasks

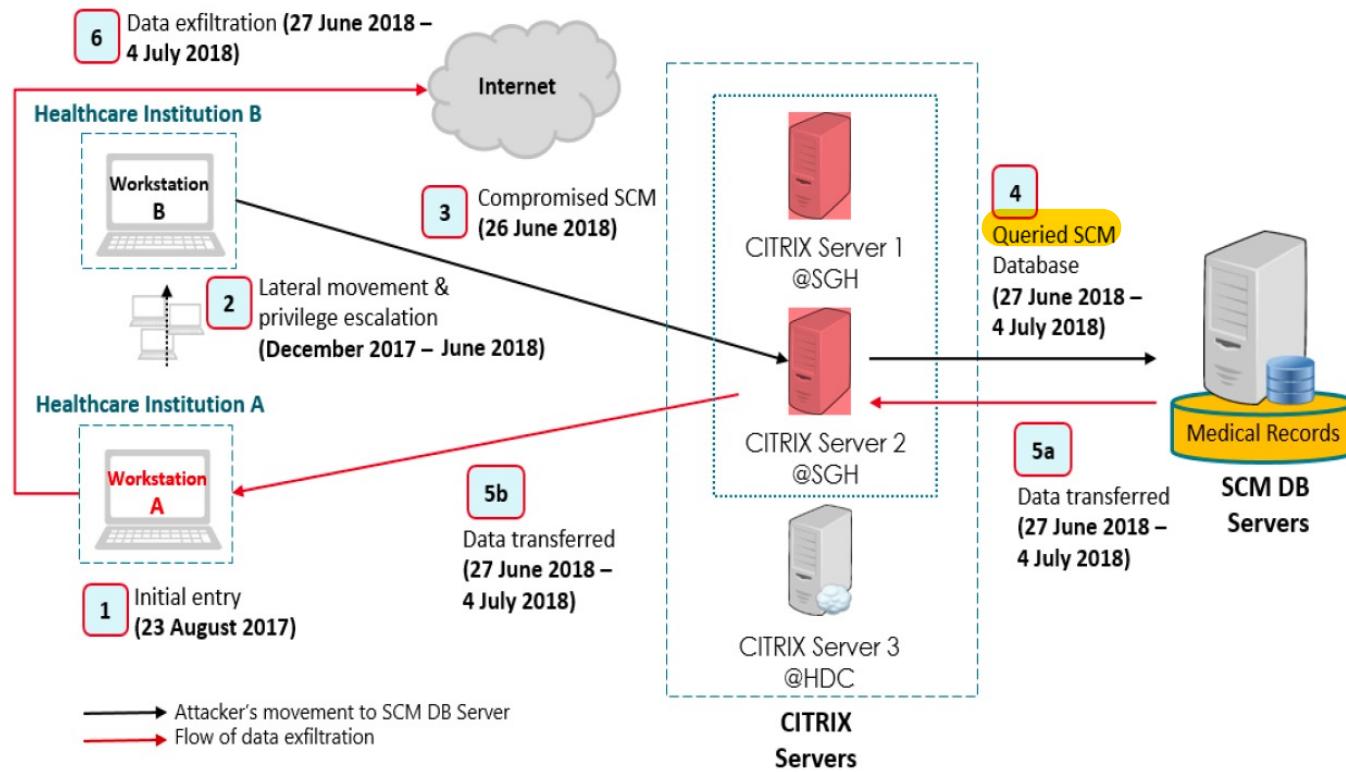
2. Reacting to Incidents (cont.)

- ▶ **Incident containment strategies:**
 - ▶ Disabling compromised user accounts
 - ▶ Reconfiguring a firewall to block problem traffic
 - ▶ Temporarily disabling the compromised process or service
 - ▶ Taking down the conduit application or server
 - ▶ Example: e-mail server
 - ▶ Stopping all computers and network devices
- ▶ **The nature of the attack and the organization's technical capabilities may dictate strategy**

Case: SingHealth Breach

- ▶ *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*

Figure 7: Key events of the Cyber Attack

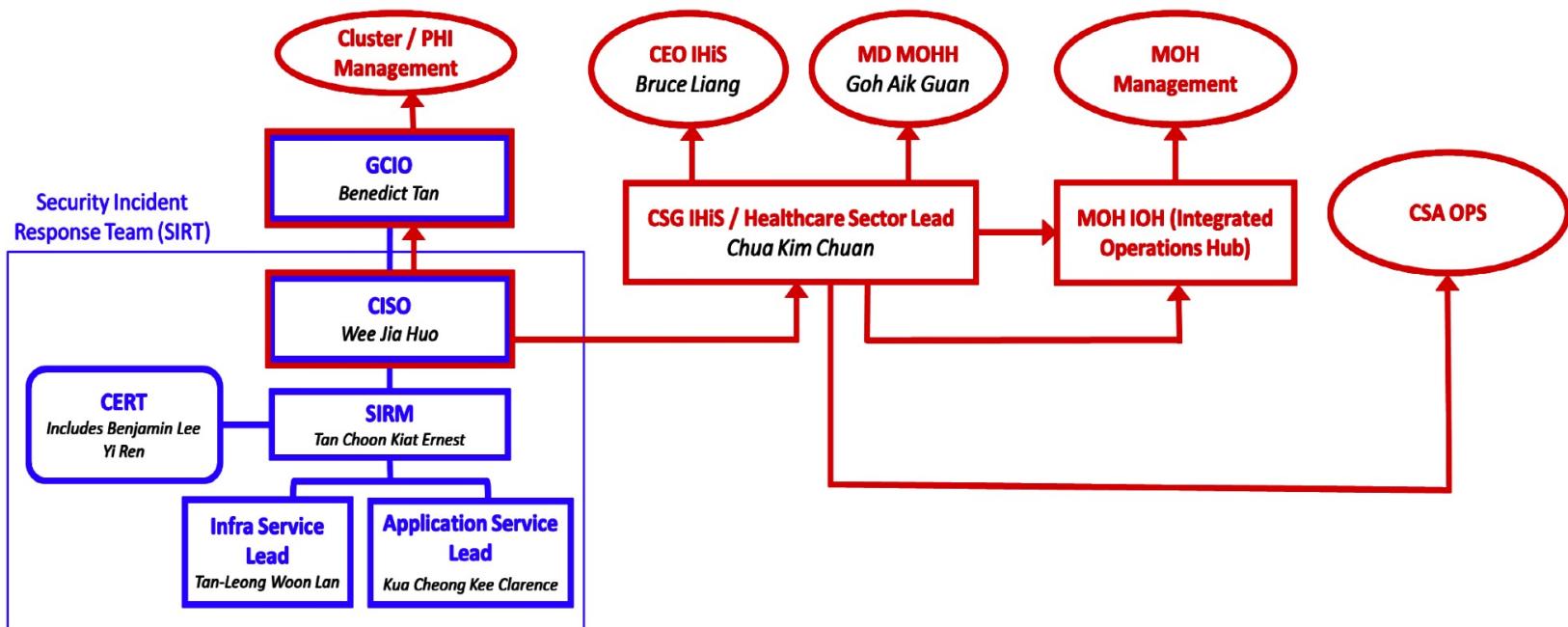


Case: SingHealth Breach (cont.)

- ▶ *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*

In blue – Security Incident Response Team reporting structure (IR-SOP)

In red – Security incident reporting flow (SIRF)



Case: SingHealth Breach (cont.)

- ▶ *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
 - ▶ “The SIRM (Security Incident Response Manager) and the SingHealth CISO were both aware of the suspicion of attack since 13 June 2018 and the remediation efforts of 4 July 2018. They were both copied on emails and were members of a chatgroup created to investigate these incidents. The SingHealth CISO was apprised of the investigations but did not make further enquiries. Instead, he waited passively for updates. The SIRM was overseas until 18 June 2018 without nominating a covering officer. During this time, neither the SIRM nor the SingHealth CISO escalated the matter despite their knowledge of these circumstances through meetings and messages. Also, neither the SIRM nor the SingHealth CISO took any steps to activate the SIRT in accordance with the IR-SOP.”

Source: <https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx>

Case: SingHealth Breach (cont.)

- ▶ *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
 - ▶ Key findings:
 - ▶ “The Security Incident Response Manager (“SIRM”) and Cluster Information Security Officer (“Cluster ISO”) for SingHealth, who were responsible for incident response and reporting, held mistaken understandings of what constituted a ‘security incident’, and when a security incident should be reported.
 - ▶ The SIRM delayed reporting because he felt that additional pressure would be put on him and his team once the situation became known to management.
 - ▶ The evidence also suggests that the reluctance to escalate the matter may have come from a belief that it would not reflect well in the eyes of the organisation if the matter turned out to be a false alarm.
 - ▶ The Cluster ISO did not understand the significance of the information provided to him, and did not take any steps to better understand the information. Instead, he effectively abdicated to the SIRM the responsibility of deciding whether to escalate the incident.”

Case: SingHealth Breach (cont.)

- ▶ *Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack*
 - ▶ 1) the Commissioner finds that it is insufficient for IHiS to have merely informed its non-security staff to alert the relevant personnel through emails, circulars, wallpapers and intranet banners.
 - ▶ 2) IHiS had admitted that while the SIRF and IT-SPS were made available via IHiS' intranet, it had not developed any written policy on IT security incident reporting for its non-security staff. Furthermore, regular training sessions and staff exercises should have been conducted to ensure that all IHiS staff are familiar with the IT security incident reporting and their role in recognising and reporting suspected IT security incidents.

non - security personnels should also be well aware of the SOP of participating in IR work

Source: <https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx>

3. Recovering from Incidents

- ▶ Once the incident has been contained and system control has been regained
 - ▶ Incident recovery can begin
- ▶ First task is to inform the appropriate human resources
- ▶ IRT must assess the full extent of the damage
 - ▶ To determine what must be done to restore the systems
- ▶ Incident damage assessment - determination of the scope of the breach of confidentiality, integrity, and availability of information assets

3. Recovering from Incidents (cont.)

- ▶ Recovery process steps:
 - ▶ Identify vulnerabilities that allowed incident to occur
 - ▶ Address safeguards that failed to stop or limit the incident
 - ▶ Restore data from backups
 - ▶ Restore the services and process in use
 - ▶ Continuously monitor the system
 - ▶ Restore the confidence of the members of the organization's communities of interest
- ▶ **After-action review (AAR):** detailed examination of the events that occurred
 - summarise the whole incident and identify the learning points for everyone

Example: MAS NOTICE 644

- 8 A bank shall submit **a root cause and impact analysis report** to the Authority, within **14 days** or such longer period as the Authority may allow, from the discovery of the relevant incident. The report shall contain—
- (a) an executive summary of the relevant incident;
 - (b) an analysis of the root cause which triggered the relevant incident;
 - (c) a description of the impact of the relevant incident on the bank's—
 - i. compliance with laws and regulations applicable to the bank;
 - ii. operations; and
 - iii. service to its customers; and
 - (d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

Incident Response Planning

► NIST

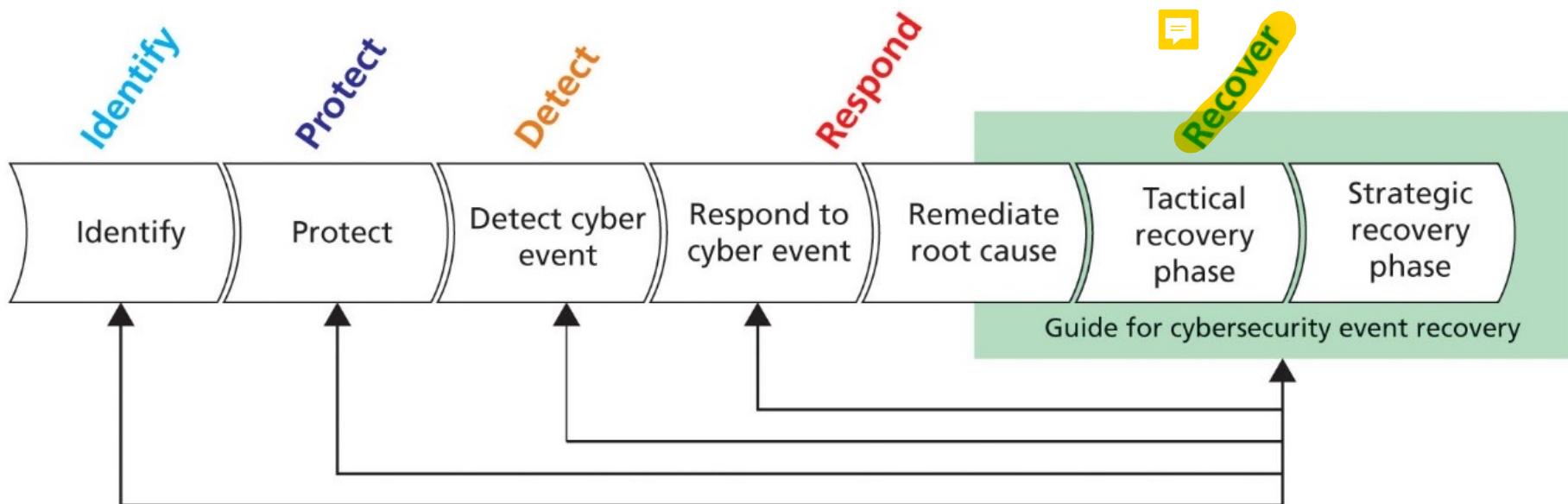


Figure 10-7 NIST Cybersecurity Framework

Disaster Response Planning

What is Disaster Recovery Planning?

- ▶ Preparation for and recovery from a disaster
 - ▶ Natural or caused by humans
- ▶ **Disaster recovery (DR) plan:** often activated when the IR plan no longer can handle the effective and efficient recovery from loss
- ▶ In general, an incident is a disaster when:
 - ▶ The organization is unable to contain or control the impact of an incident, or
 - ▶ The level of damage or destruction from an incident is so severe the organization is unable to quickly recover.
- ▶ The key role of a DR Plan is defining how to reestablish operations at the location where the organization is usually located (primary site)

Planning to Recover

- ▶ Key elements of the DR plan:
 - ▶ *Clear delegation of roles and responsibilities*
 - ▶ *Execution of the alert roster and notification of key personnel*
 - ▶ *Clear establishment of priorities*
 - ▶ *Procedures for documentation of the disaster*
 - ▶ *Action steps to mitigate the impact of the disaster on the operations of the organization*
 - ▶ *Alternative implementations for the various system components, should primary versions be unavailable*

Disaster Recovery Response Teams

- ▶ DR Management
- ▶ Communications
- ▶ Computer Recovery
(Hardware) Team
- ▶ Systems Recovery (OS)
- ▶ Network Recovery Team
- ▶ Storage Recovery
- ▶ Applications Recovery
- ▶ Data Management
- ▶ Vendor Contact
- ▶ Damage Assessment and Salvage
- ▶ Business Interface
- ▶ Logistics
- ▶ Others as needed.

Responding to Disaster

- ▶ If physical facilities are intact
 - ▶ DR team should begin restoration of systems and data to work toward full operational capability
- ▶ If facilities are destroyed
 - ▶ Alternative actions must be taken until new facilities can be acquired
- ▶ When disaster threatens the viability of an organization at the primary site, the DR process becomes a business continuity process

Business Continuity Planning

 can see how many companies might not have BCP already prepared since due to the pandemic there are many companies not ready to react with this rare but crucial plan

What is Business Continuity Planning?

- ▶ Disaster makes current business location unusable
 - ▶ **Business Continuity (BC) Plan** allows the business to continue at an alternate location
- ▶ **Most properly managed by the CEO or COO**
- ▶ Activated and executed concurrently with the DR plan when the disaster is major or long term
- ▶ While BCP reestablishes critical functions at alternate site, DRP focuses on reestablishment at the primary site

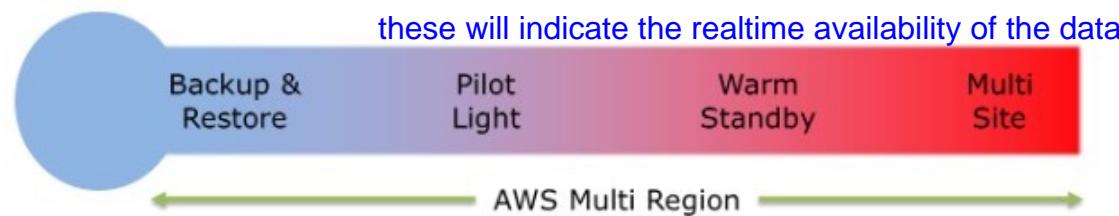
Continuity Strategies

- ▶ Several continuity strategies for business continuity, determining factor is usually
 - ▶ cost there are also non-exclusive
- ▶ Three **exclusive-use** options:
 - ▶ Hot sites
 - ▶ Fully configured computer facility, with all services, communication links, and plant operations
 - ▶ Warm sites
 - ▶ Provides many of the same services as a hot site, but typically software applications are not installed and configured
 - ▶ Cold sites
 - ▶ Provides only rudimentary services and facilities. No computer hardware or peripherals are provided.
only have the room and water/light - nothing else provided

Continuity Strategies

▶ AWS cloud:

- ▶ With multiple regions and availability zones, recover from disaster using different DR approaches.
 - ▶ Backup & Restore
 - ▶ Pilot Light
 - Replicate part of your IT structure for a limited set of core services
 - ▶ Warm standby
 - A scaled-down version of a fully functional environment is always running in the cloud.
 - ▶ Multi-site



Continuity Strategies (cont.)

- ▶ Three shared-use options:
 - ▶ Timeshare
 - ▶ Hot/warm/cold, but is leased in conjunction with a business partner
 - ▶ Service bureaus
 - ▶ Service agency that provides a service for a fee
 - ▶ Mutual agreements
 - ▶ A contract between two organizations in which each party agrees to assist the other in the event of a disaster



NUS - the backup data center is in NUS High School
- they are also who we share mutual agreement with

Crisis Management



maybe something like the data breach of PII - such as the HIV data leak case

Crisis Management

- ▶ Focuses more on the effects that a disaster has on people than its effects on information assets
- ▶ According to Gartner Research, the crisis management team is responsible for managing the event from an enterprise perspective and performs the following roles:
 - ▶ Supporting personnel and their loved ones during the crisis
 - ▶ Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
 - ▶ Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Timing & Sequence of CP Elements

CP Implementation Timeline

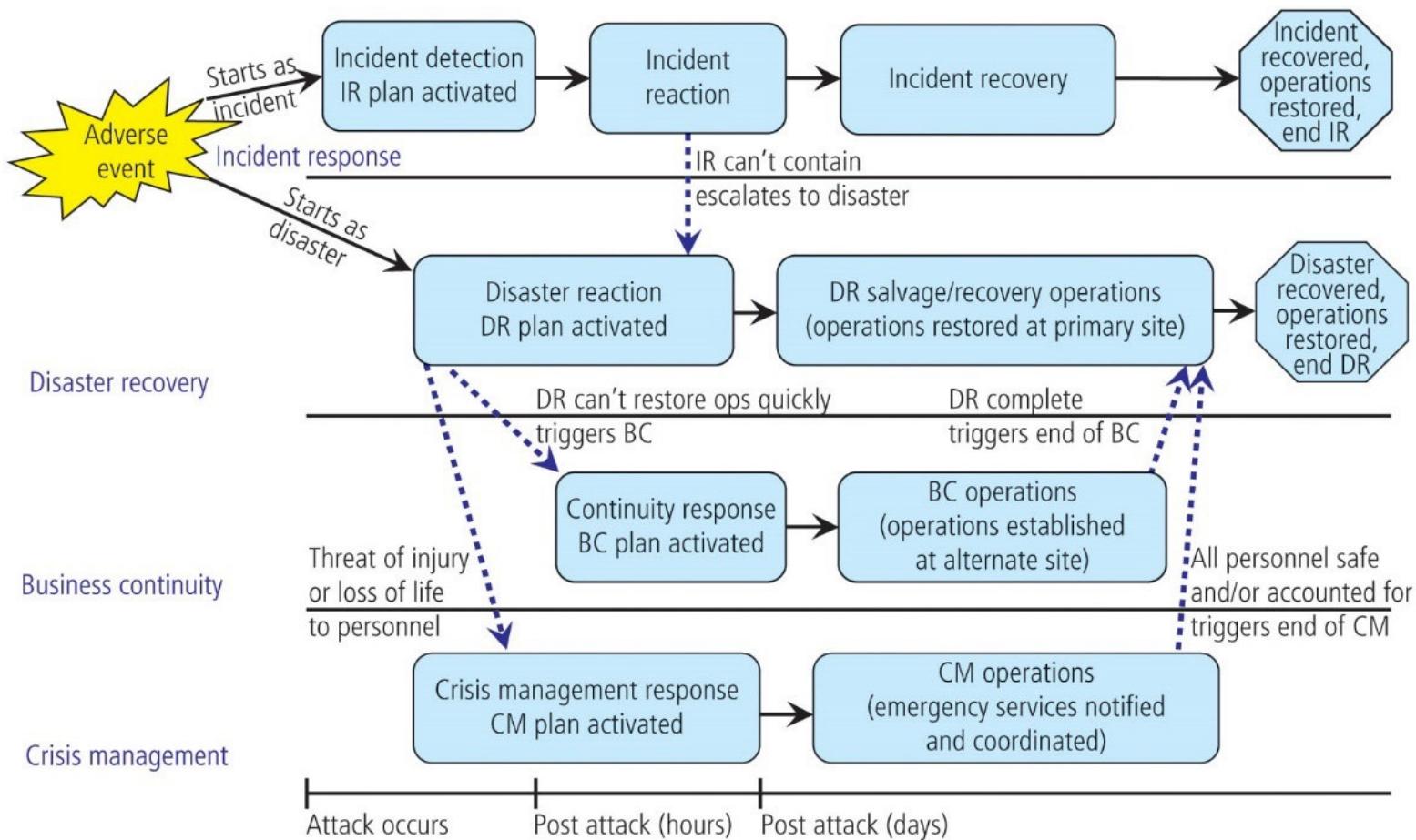


Figure 10-14 Contingency planning implementation timeline

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.

important to have backup for everything - including communication channels



Testing Contingency Plans

Testing Contingency Plans

- ▶ Contingency plans must be tested to identify vulnerabilities and faults
- ▶ Test strategies
 - ▶ **Desk check**
 - ▶ Distribute copies of the appropriate plans to all personnel with assigned incident roles
 - ▶ **Structured walk-through**
 - ▶ All involved personnel walk through the steps they would take during an event
 - ▶ **Simulation**
 - ▶ Each person works individually to simulate the performance of each task
 - ▶ **Full interruption**
 - ▶ Individuals follow each and every procedure, including interruption of service, restoration of data from backups, and notification of appropriate individuals

Next week – Reading week

- ▶ Course review and final exam briefing
 - ▶ Next Wed: 10-11am (attendance: optional)
 - ▶ Recorded.
- ▶ Online exam
 - ▶ Time:
 - Mon, 29 Nov 2021
 - 5-7pm
 - ▶ Channel
 - ▶ LumiNUS-Quiz
 - ▶ Format
 - ▶ Open book
 - ▶ All lecture, tutorial, guest talk content are examinable.
 - ▶ Invigilation
 - ▶ Zoom proctoring
 - ▶ Screen recording