CS2107
Introduction to Information Security

Lecture 0

Admin + Overview

0.1 What is CS2107?

Module Description

Objective

This module serves as an introductory module on information security. It ***illustrates*** the ***fundamentals of how systems fail*** due to malicious activities ***and how they can be protected***. The module also places emphasis on the practices of secure programming and implementation. Topics covered include **classical/historical ciphers**, **introduction to modern ciphers** and cryptosystems, ethical, legal and organisational aspects, classic examples of direct attacks on computer systems such as **input validation vulnerability**, examples of other forms of attack such as **social engineering/phishing attacks**, and the **practice of secure programming**.

Outcomes

- Awareness of common and well-known attacks (e.g. phishing, XSS, SQLI, ...)
- Understand basic concepts of security (e.g. confidentiality, availability, ...)
- Understand basic mechanisms & practice of protections (e.g. crypto, PKI, access control, ...)
- Awareness of common pitfalls in implementation (Secure programming)

More Specific Intended Learning Outcome (ILO)

After completing the module, you will be expected to be able to:

1. Explain *the C-I-A security requirements* and recognize their breaches in recent security incident news
2. Describe *key concepts and basic mechanisms* of principal protection mechanisms in information security, such as encryption, authentication, and secure channel
3. Identify the *limitations* of classical cryptographic schemes, and recognize *well-known attacks* on vulnerable hosts, networks, and Web servers

More Specific Intended Learning Outcome (ILO)

4. Utilize some *basic security tools* (e.g. OpenSSL, Wireshark) and security-related *Linux commands* to perform encryption and network traffic analysis
5. Pinpoint flaws in programs due to common *insecure programming practices*, and suggest improvements using more secure practices instead

[Who Need to Take]

- All IT professionals
- Preparation for in-depth studies in cybersecurity

Modular Credits (MCs)

4

Prerequisite(s)

CS1010 or its equivalence

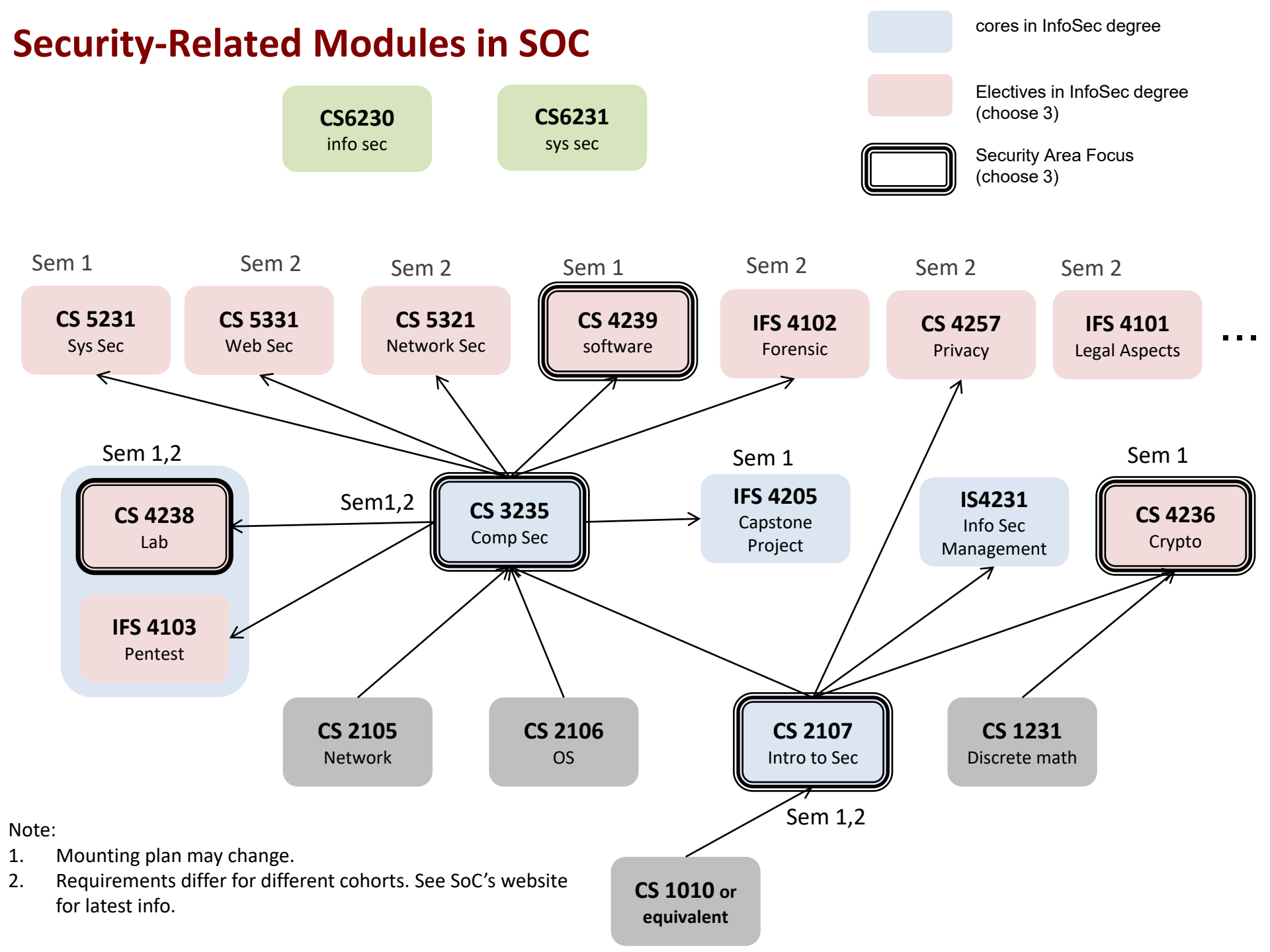
Preclusion(s)

Nil

Weekly Workload

- Lecture: 2 hrs
- Tutorial: 1 hrs
- Project: 3 hrs
- Preparation: 4 hrs

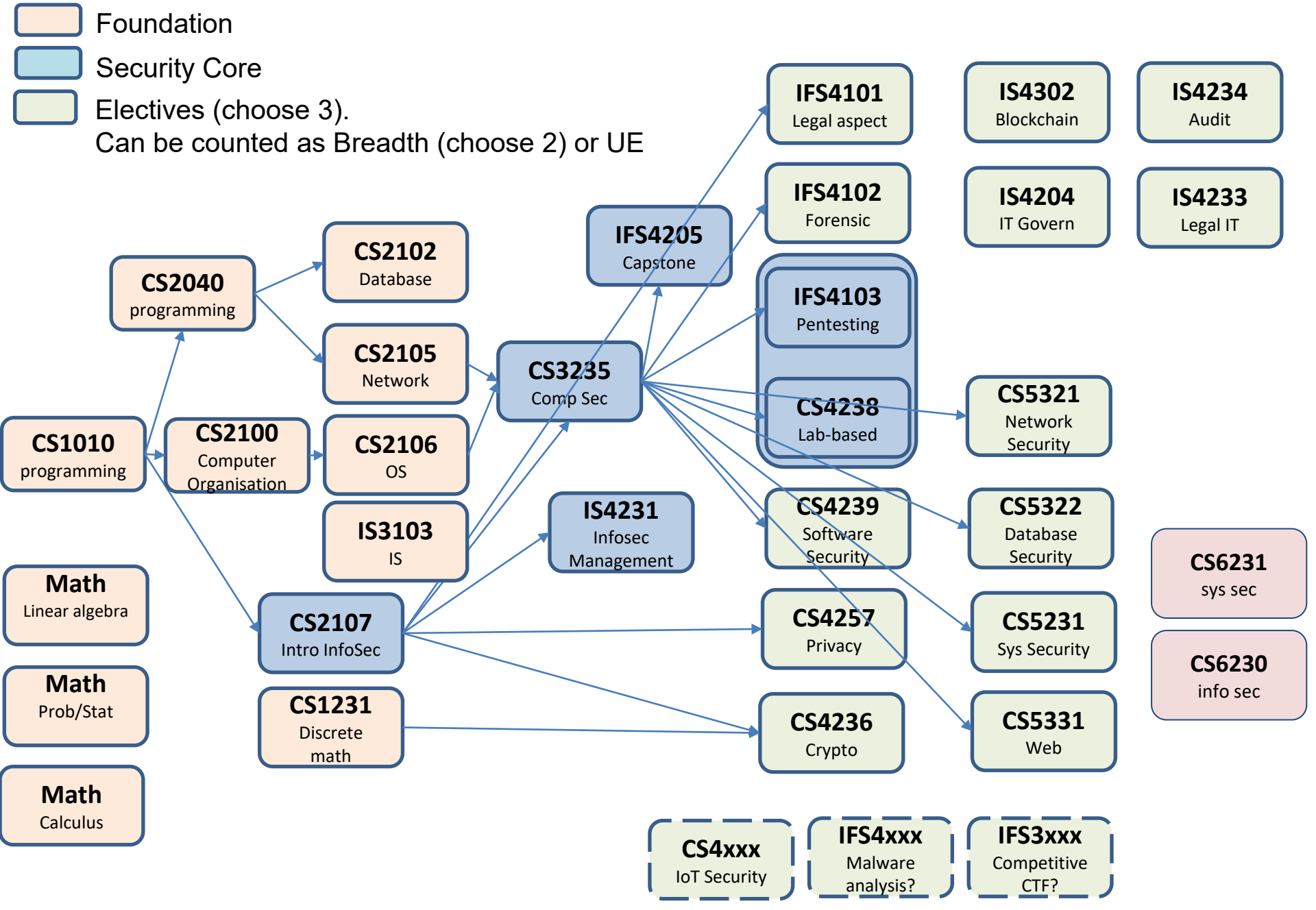
Security-Related Modules in SOC



Note:

1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

Security-Related Modules and BCOMP InfoSec Requirements



Some of the Terms Encountered in This Module

Alice, Bob, Eve, Encryption, Decryption, Key-space, Known-plaintext attack, Ciphertext-only attack, Confidentiality, Integrity, Availability, Authenticity, Passwords, Random IV, Multi-factor authentication, Kerckhoff's principle

Digital signature, RSA, Certificate, Public Key Infrastructure, Authentication protocol, Secure channel, SSL, HTTPS, WPA, Wireshark

Dictionary attack, Side-channel attack, Timing attack, Key logger, ATM skimmer, Social engineering attack, Man-in-the-middle attack

DDOS, Syn flood, Botnet, Spoofing, Sniffing, Poisoning

Access Control List, Capabilities, UNIX's rwx permission triplet, superuser, root, Least privilege, Privilege escalation, Reference monitor

Input validation, SQL injection, Secure programming, Buffer overflow, Stack smashing, Integer overflow, CVE

Web cookies, Same-Origin Policy, Session ID

Virus, Worm, Rootkit, Cross Site Scripting attack, Cross Site Request Forgery

0.2 Module Admin

Teaching Mode

- 13 Lectures
- 9 Tutorials (from Week 3): the last 2 tutorials for group presentation
- **Continuous Assessment** (55%):
  - 2 Assignments (25%)
  - 1 Mid-term exam/quiz (15%): after the recess week **(1 Oct)**
  - 1 LumiNUS online quiz (5%): 1 week before reading week
  - 1 Group presentation on open-ended topic (5%)
  - Tutorial attendance (5%): 5 out of 9 tutorials, ≥25 mins/session, based on Zoom's meeting-attendance reports
- **Final Exam** (45%): open-book, no Internet

Teaching Staff

Lecturer: Sufatrio (Rio)

TAs (tutorials): Wesley Joon-Wie Tann, Brian Yen, Goh Rui Zhi, Charmaine Koh, Ryo Chandra Putra Armanda, Fabian Chia Hup Peng

TAs (assignments): Loh Fah Yao Jaryl, Ye Guoquan, Chan Jian Hao

Slides:

- Based on A/P Chang Ee-Chien's
- Extended with additional explanations and illustrations

NUS Resources for Our Module

CS2107 on **LumiNUS**: *check it regularly*!

- Files: for lecture notes, tutorial notes, assignment briefs
- Forum: for discussions and project arrangements
- Multimedia: for lecture recordings, video demos
- Quiz: for your online quiz

CS2107 team on **Microsoft Teams**:

- With general, tutorial-group channels

CS2107 **Assignment server**:

- For assignment submissions

ExamSoft's Examplify + Zoom:

- For mid-term and final e-exams & proctoring

What's New in CS2107 (Since AY20-21)

- More crypto!
  - More in-depth coverage: gives a *deeper understanding* of crypto
  - More rigorous definition & analysis: for *firmer foundations*
  - Develop a *stronger basis* for important "secure communication channel": secure communications & transactions over insecure public network
- Parts of software security are shifted to CS3235:
  - OS security (access control), deeper aspects of network & web security
  - Can be covered better after CS2105 and CS2106
- Main goals of the module enhancement:
  - To better understand how crypto is used in practice (real world)
  - To minimize overlap with CS3235
- Crypto analysis coverage and approach:
  - Basic threat modeling, cryptographic goals, cryptosystem security
  - Not so formal, intuitive explanation is also given

Main References

- "**Security in Computing**" (5th ed), Charles P. Pfleeger et al., Prentice Hall

  Customized version (Chapter 1 to 6) from Pearson is available in NUS Co-ops

  Notation: Throughout the slides, the reference **[PF*x*.*y*]** refer to Chapter *x* Section *y*

- "**Serious Cryptography: A Practical Introduction to Modern Encryption**", Jean-Philippe Aumasson, No Starch Press, 2017

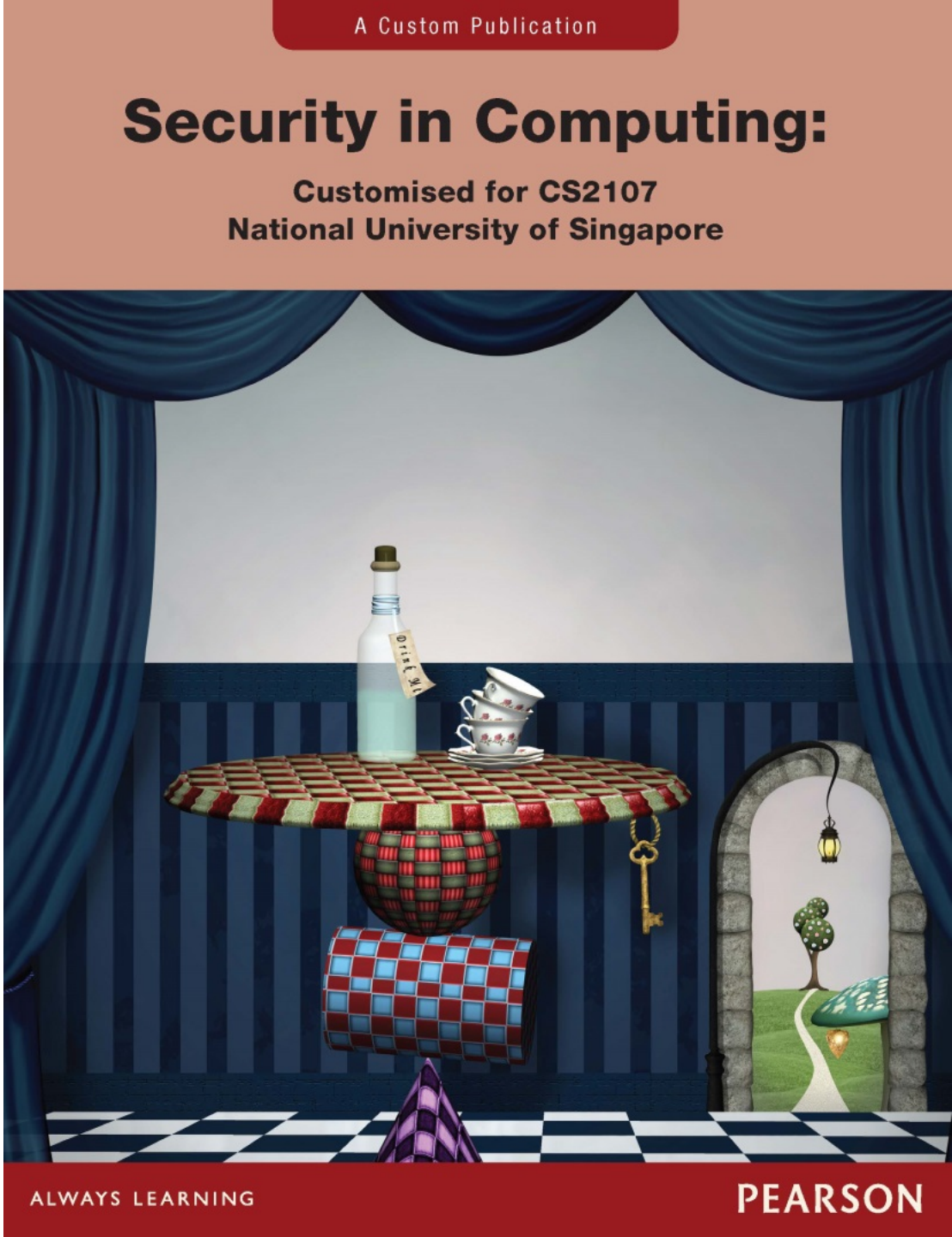
- "**Security Engineering**" (2nd ed), Ross Anderson, Wiley

  Free online version at:

  http://www.cl.cam.ac.uk/~rja14/book.html

Available at
NUS Co-op @ Forum

Or via **NUS Coop website**:
https://www.nuscoop.sg/books



Tentative Schedule

Week	Topic & Covered Attacks		Tutorial	HW
1	Introduction, Cryptography/Encryption	Cryptanalysis on classical ciphers	-	
2	Cryptography/Encryption	Cryptanalysis on classical ciphers	-	
3	Cryptography/Encryption (modern ciphers)	Cryptanalysis on modern ciphers	1. Intro, Encryption	
4	Authentication/Password, Multi-factor authentication, Phishing	Dictionary attacks, Phishing	2. Password, 2FA	A1
5	Authenticity: Data origin, Hash, MAC, Signature	Birthday attacks, Email/SMS spoofing	3. Authenticity: birthday attacks, hash	
6	PKI, Certificate, Authentication protocol	Proxy re-encryption, Protocol attacks	4. PKI, PKI attacks	
7	*Mid-term quiz*		Past mid-term discussion	
8	Secure channel, Key-exchange, SSL/TLS, HTTPS	TLS/HTTPS usage attacks	Mid-term quiz discussion	A2
9	Network Security, DNS, DDOS, Firewall	DNS attack, ARP attacks, DDoS attacks	5. Renegotiation attack	
10	Secure programming: Background, Data representation, Call stack	Heartbleed bug	6. Network security	
11	Secure programming: Buffer overflow attacks, Integer overflow attacks, Malware	Buffer overflow attacks, Integer overflow attacks	7. Secure programming	
12	Web security	XSS, CSRF, SQLI	Project presentations	OQ
13	Guest lecture (TBD), Review		Project presentations	

Notes on Lectures and Tutorials

- Attendance will *not* be taken during **lectures**:
  - But please attend them still if possible
  - Otherwise, check the uploaded recordings
  - Pay attention and participate in class and tutorials
- Do attend your **tutorials** with your assigned tutorial group: claim your **5% participation marks**
- Do *not* disturb/distract others and … yourself!
  - No chatting
  - No Pokemon or games
  - No watching videos

Plagiarism Policy and Guidance Note Changes

"I. The University is taking a tougher stance against academic dishonesty. As such, for cases of plagiarism and cheating in **tests/examinations/graded assignments that have been assessed to be 'Moderate' in severity, the minimum penalty would be a 'Fail' grade for the affected module**.

II. The online version of the revised NUS Plagiarism Policy and Guidance Note can be accessed via the Student Portal.

2 NUS students are expected to uphold the highest standards of academic integrity and honesty at all times, as well as embrace diversity and show mutual respect for one another, both within the University and the wider Singapore community. Students who do not comply with the NUS Statutes and Regulations will face disciplinary action.

3 If you have any queries, suggestions or feedback, please email us at studentconduct@nus.edu.sg."

Reminders on Assignments

- Avoid plagiarism:
  - Importance of *academic honesty*
  - Group study is fine, but do not copy answers
  - Your TAs may ask you to *satisfactorily explain* your answers (before granting marks of correct answers)
- LumiNUS forum for discussing assignments:
  - You can ask questions and share ideas
  - *But* don't reveal your answers!
  - Also, please be courteous,
    even when disagreeing with others

0.3 Why CS2107 and Information Security

Rampant Security Attacks: Internet is a Dangerous Place

Chaos as hospitals, telcos and schools hit

1 of 2 A window announcing the encryption of data including a requirement to pay appears on an electronic timetable display at the railway station in Chemnitz, eastern Germany, last Friday. PHOTOS: AGENCE FRANCE-PRESSE

The Straits Times, May 14, 2017

PUBLISHED MAY 14, 2017, 5:00 AM SGT

Including in Singapore!

www.straitstimes.com/singapore/global-ransomware-attack-hits-digital-directory-at-tiong-ba

ST SINGAPORE POLITICS ASIA WORLD VIDEOS LIFESTYLE FOOD MORE

SINGAPORE › Courts & Crime Education Housing Transport Health Manpower Environm

Singapore malls, users hit in cyber attack

A digital display at Tiong Bahru Plaza shows a ransomware message. PHOTO: REDDIT

PUBLISHED MAY 14, 2017, 7:20 PM SGT

The Straits Times, May 14, 2017

Including in Singapore!

We set you thinking
TODAY
WEDNESDAY 14 AUGUST 2019

SingHealth cyber attack a result of human lapses, IT system weaknesses: COI report

By CYNTHIA CHOO

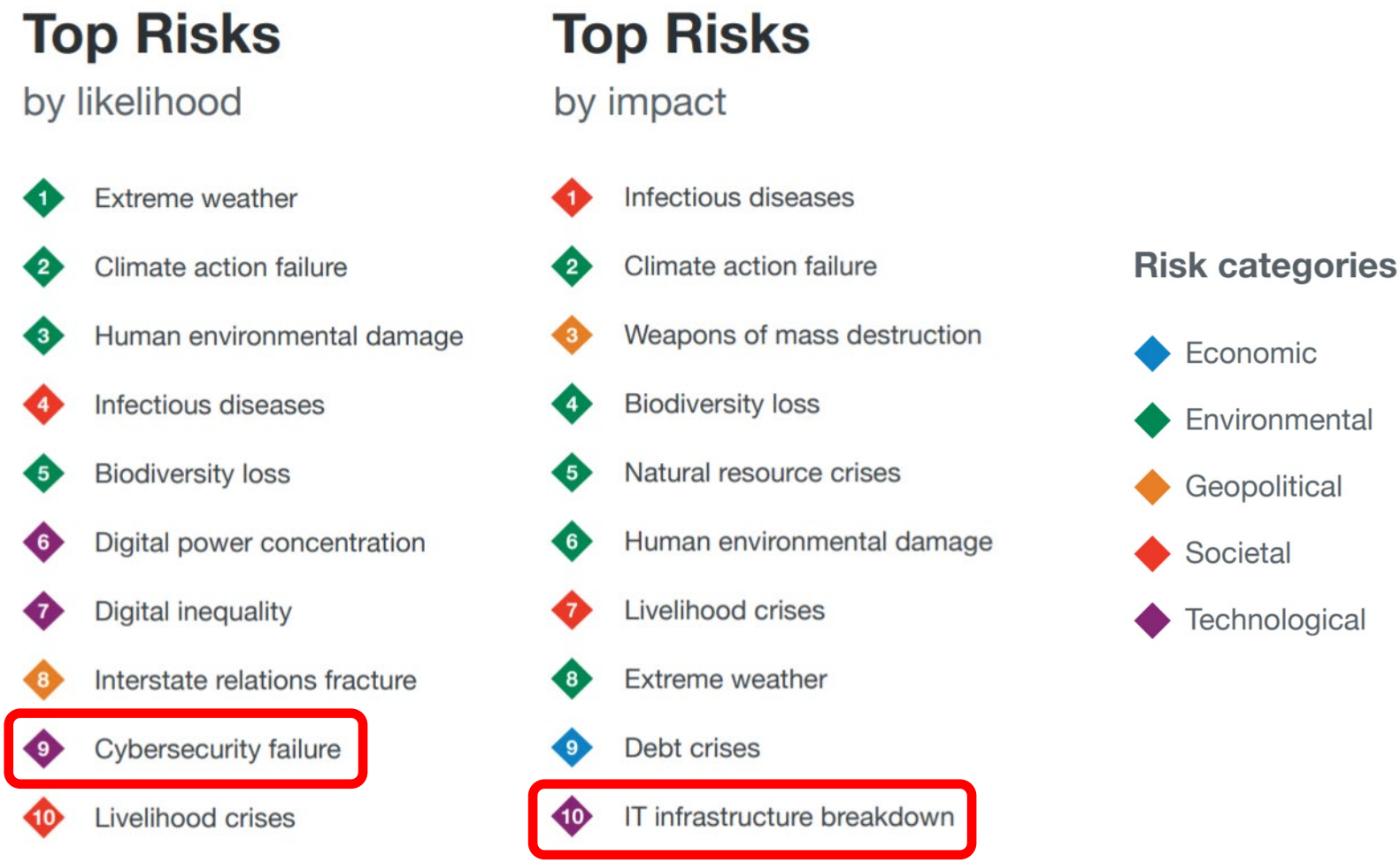
Reuters file photo

The SingHealth cyber attack happened because of lapses by employees and vulnerabilities with the system.

Published 10 JANUARY, 2019 UPDATED 10 JANUARY, 2019

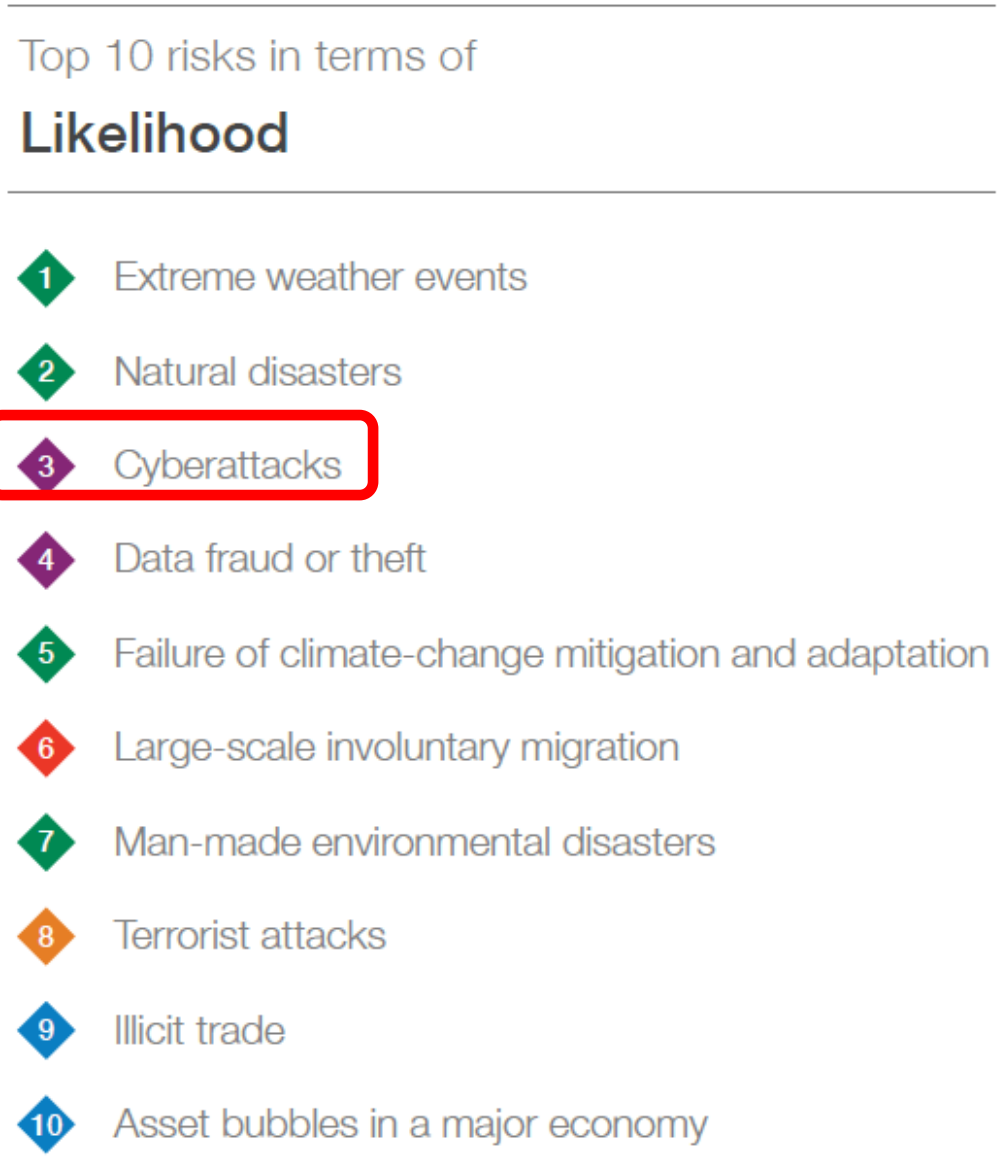
Ref:
https://www.todayonline.com/singapore/singhealth-cyber-attack-result-human-lapses-it-system-weaknesses-coi-report

WEF Global Risks Report 2021



From: "The Global Risks Report 2021, 16th Edition", World Economic Forum, 2021.

WEF Global Risks Report 2018

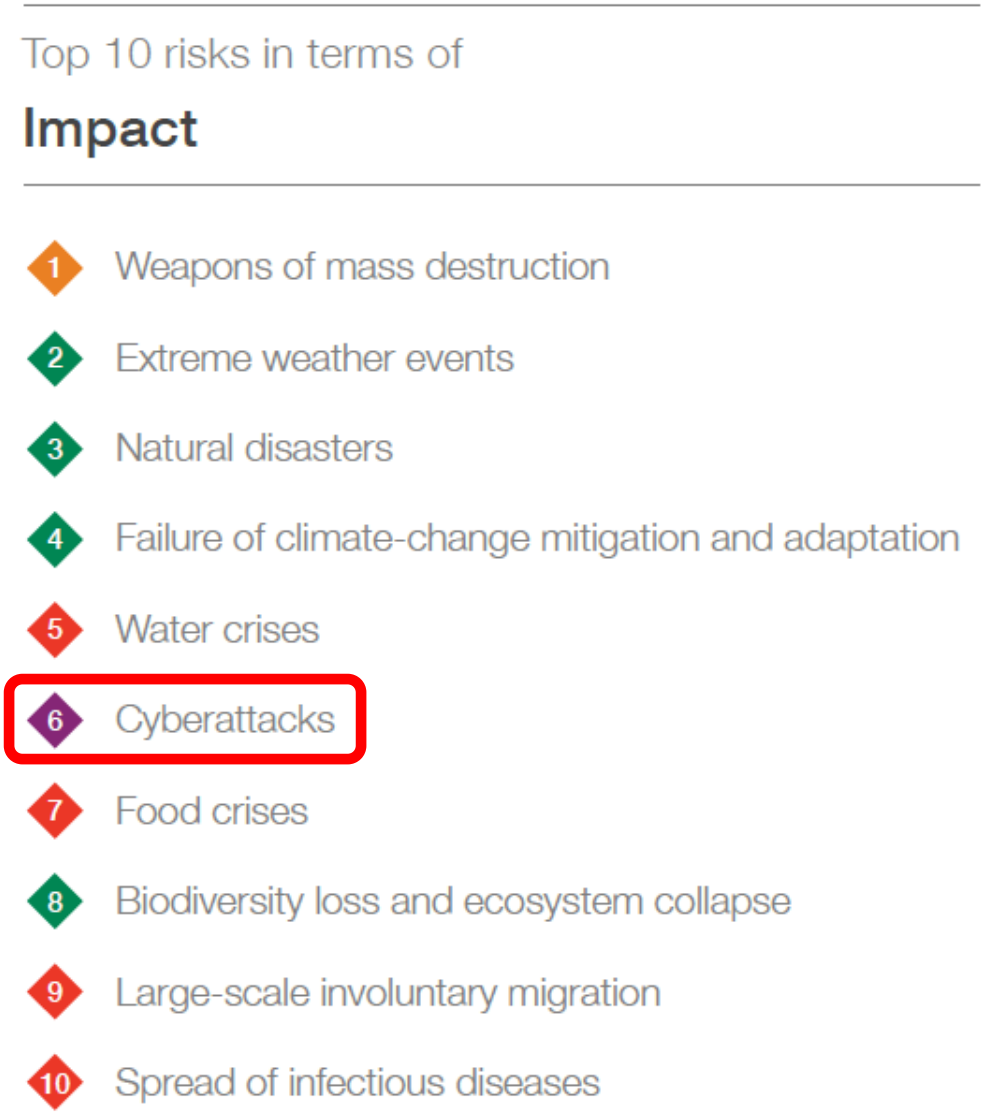


WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

WEF Global Risks Report 2018



From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

WEF Global Risks Report 2018: From Executive Summary

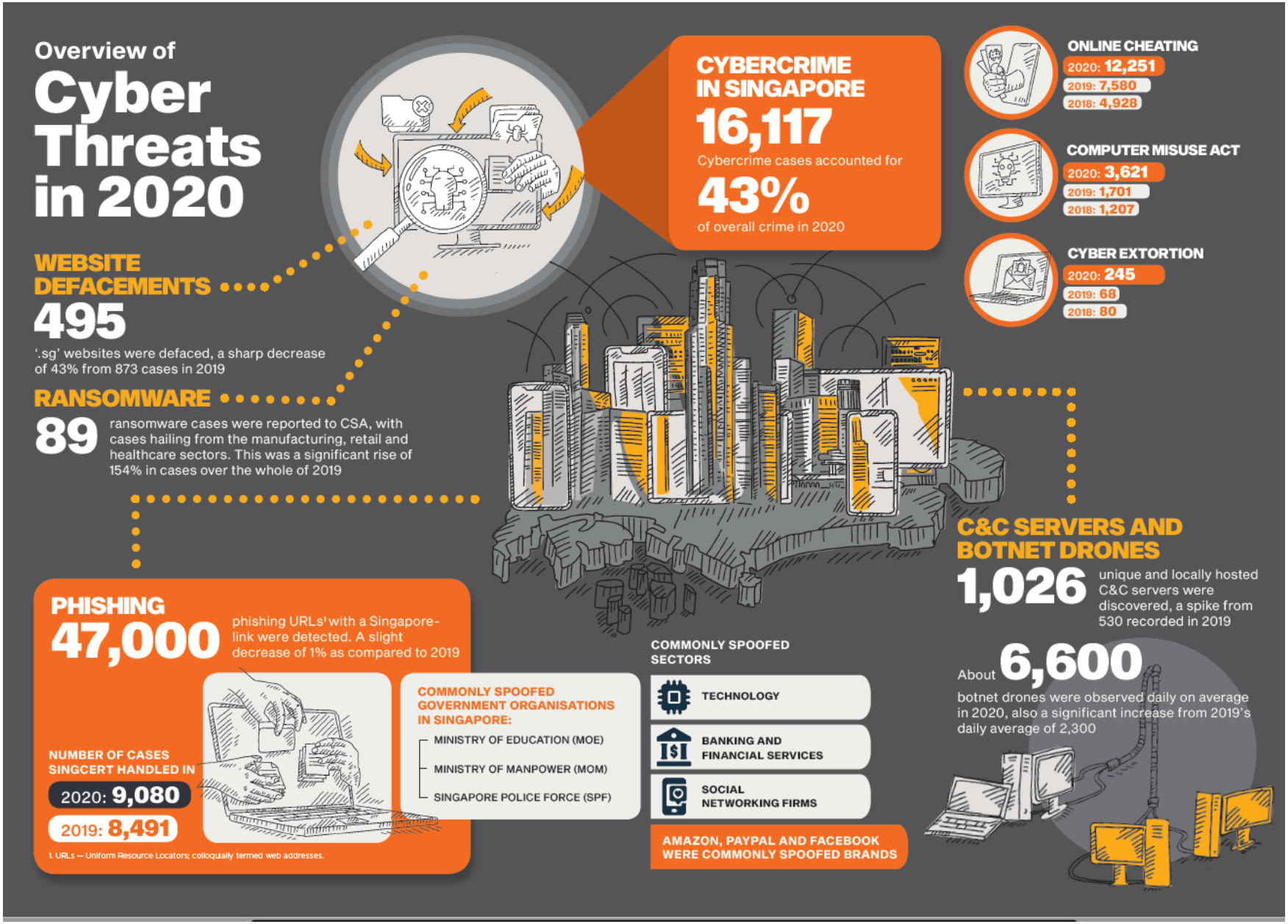
Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses. Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.

From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

Singapore Cyber Landscape Report

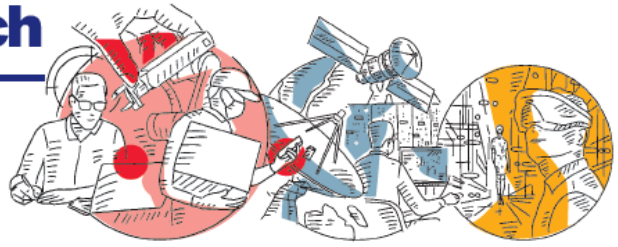
- Annual snapshot of **cyber landscape** in Singapore
- The latest: "*Singapore Cyber Landscape 2020*", by Cyber Security Agency of Singapore, 2021:
  - Spotlight on cyber threats
  - Local case studies
  - A retrospective look
  - Looking back to look forward
- See: https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020

Cyber Threats in 2020



Cybersecurity Trends to Watch

Cybersecurity Trends to Watch



NEAR TERM
Risk of Remote Workforce, Increased Risk of Supply-chain Attacks and the Ransomware Threat

MEDIUM TERM
Cybersecurity of Space Infrastructure

LONG TERM
Hyper-Connectivity and the Metaverse

NEAR TERM: Risk of Remote Workforce

What Is It?

Social distancing measures during the COVID-19 pandemic have led to the rapid adoption of remote working. Overnight, many organisations had to implement new processes and systems to facilitate business continuity. Threat actors were quick to capitalise on this expanded – and often more vulnerable – attack surface brought about by these new work-from-home ecosystems.

Why Does It Matter?

Remote working is here to stay, even after the pandemic. It has become an increasingly attractive alternative to working from the office[41]. Companies have found that remote working reduces overheads, without reducing employee efficiency.

Poorly configured network and software systems to facilitate remote work can expose organisations to greater risk of cyber-attacks. Defending the infrastructure needed to sustain a large remote workforce against malicious threat actors will present a daunting challenge for organisations moving forward.

NEAR TERM: Increased Risk of Supply-chain Attacks

What Is It?

Organisations often rely on vendors, such as technology firms and managed service providers, for products and services to support their business operations. Cyber threat actors have exploited such interdependencies to carry out supply-chain attacks. Supply-chain attacks involve targeting an organisation by exploiting weak links and trusted relationships in the supply network.

Why Does It Matter?

A successful breach in the supply chain, as seen in the SolarWinds incident, provides cyber threat actors a single pivoting point to multiple victims. The compromise of a trusted supplier – or a popular and widely-used product – can result in massive and widespread

41. The Straits Times article published on 24 March 2021 said that 9 in 10 employees in Singapore wanted to continue working from home for reasons such as flexibility and cost savings.

LOOKING BACK TO LOOK FORWARD

repercussions worldwide, as victims could include major vendors with huge customer bases. The supply-chain attack also highlighted the level of sophistication, patience and operational security that determined threat actors can be capable of. Cyber threat actors of all stripes, whether motivated by financial rewards or privileged access to information and systems, are likely to emulate such methods and attempt propagating to as many victims as possible by targeting and compromising supply chains.

NEAR TERM: The Ransomware Threat – From Sporadic and Isolated, to Massive and Systemic

What Is It?

From sporadic and isolated incidents, which targeted a handful of machines and caused nuisance to individuals and small businesses, ransomware has evolved into a massive and systemic threat. Today, ransomware attacks target large organisations and even government agencies, disrupting not just IT operations but also the provision of essential services, with the potential to inflict severe cyber-physical impact. Threat actors have become more operationally sophisticated, exploiting loopholes in victims' business processes, or dependencies between victims' operations and business flows, to maximise the likelihood of success and impact of their attacks. Compounding the problem, threat actors have also become more directed in their targeting, striking key assets such as the Active Directory[42] to launch commands that lock up hundreds – if not thousands – of machines and entire networks almost simultaneously.

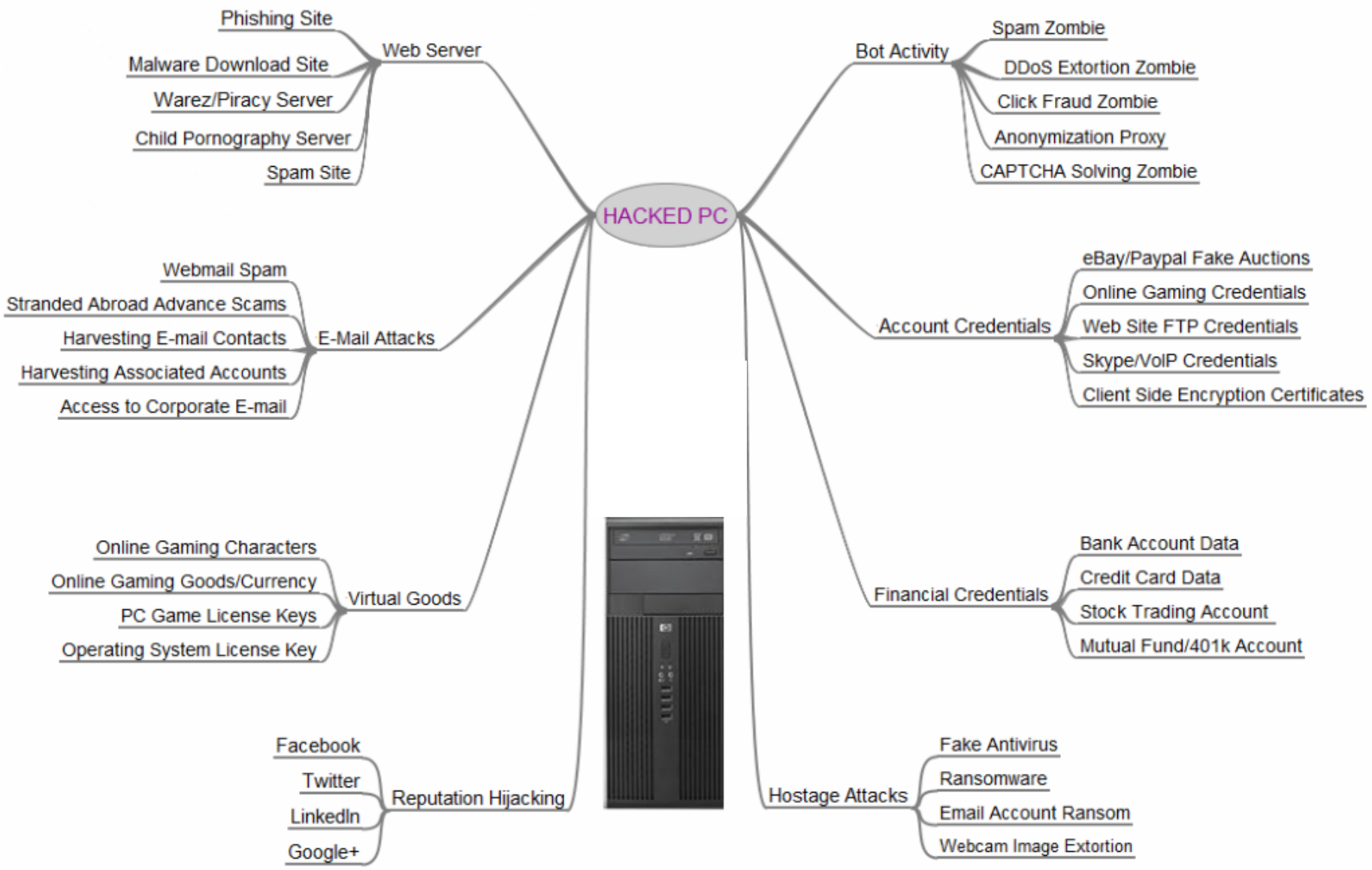
Why Does It Matter?

Ransomware attacks are financially-driven ventures. The higher the stakes, the more likely the victims are to be cowed into paying larger ransoms. Attackers are deliberately causing extensive disruptions to victims' operations, putting the latter under ever-greater pressure to accede to the ransom demands. The proliferation of Ransomware-as-a-Service affiliate models[43] means attacks now occur at scale, and at a growing intensity. We can therefore expect ransomware operators to be increasingly audacious and savvy at hitting targets which are "too important to fail". These attacks have already caused real-world effects and harm, and may have the potential to become national security concerns.

These developments underscore an urgency for organisations to regularly review their cyber hygiene, network connections, and operational dependencies. First, ransomware typically enters via relatively unsophisticated means. So organisations can protect themselves if they maintain good cyber hygiene. This includes keeping systems and software updated, raising employees' awareness of threats, and detecting intrusions quickly. Second, organisations must ensure that crucial systems' linkages are adequately protected, especially any connections or linkages between Internet-connected systems and OT systems. Thirdly, organisations must understand their dependencies. These include operational and business-type flows. Key dependencies must be mapped and protected. And last, organisations must develop and practise contingency plans, including business continuity, technical recovery and disaster recovery plans, involving appropriate key decision makers and stakeholders from both operations and business functions.

42. Active Directory is a Windows OS directory service that allows admins and users to search for resources stored anywhere on the network.
43. Ransomware-as-a-Service (RaaS) affiliate models grant cybercriminals access to shared infrastructure to conduct ransomware attacks without the need to develop native capabilities, lowering barriers to entry for even technically unsophisticated hackers.

The Value a Hacked PC: (Yes) The Stakes are Very High



https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Availability of Various Offensive Tools

A video demo (perhaps to scare you off a bit?):

Yet, Some Possible Excuses

- Still some famous *last words* out there:
  - “Nobody would bother to hack us”
  - “Our expensive network firewall will keep us safe”
  - “Our users have completed their acceptance tests”
  - “We are now adding good security measures into our system”
  - “*What's the worst that could happen*?”
  - …

Yet, *Defense Mechanisms* are Available Too!

21 Jun 2021 11:05PM
(Updated: 21 Jun 2021 11:41PM)

Bookmark

Business

SolarWinds hackers could have been waylaid by simple countermeasure: US officials

FILE PHOTO: A man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel

Source: Channel News Asia, 21 June 2021

Yet, *Defense Mechanisms* are Available Too!

The hackers - alleged to be Russian operatives - pulled off the intelligence coup by subverting SolarWinds' widely deployed networking monitoring program and using it to plant malicious software on thousands of clients' servers, eventually singling out a smaller number for in-depth exploitation.

CISA said that had those victims configured their firewalls so that they blocked all outbound connections from the servers running SolarWinds, it "would have neutralised the malware".

The agency said that several targets who did set up their firewalls that way "successfully blocked connection attempts" and had no "follow-on exploitation".

Source: Channel News Asia,
21 June 2021

0.4 What is Computer/Information/ Cyber Security?

Some Background

- System may fail, which could due to:
  - Operator mistakes: e.g. a system file is accidentally deleted, which later leads to a system crash
  - Hardware failures
  - Poor implementation: e.g. Year 2000 (Y2K) problem
- Some failure are inflicted by *deliberate human actions* that are designed to cause failure
- Cyber security is concerned with such intentional failures

Some Background

- Examples:
  1. An attacker carries out a particular combination of steps on the ATM to withdraw money without being recorded www.wired.com/2014/11/nashville/.
     (Such combination of steps is extremely unlikely to occur by mistake.)
  2. An attacker who uses objects resembling valid coins to buy drinks from vending machines.

See [PF3.1 page157]
Undocumented Access Point (a form of *back door*)

In this module,
"read": Part of the teaching materials. Read it.
"see": Information that is good to know.
"optional": Optional information.

Some Background

You may have seen similar "clueless" advertisement *:

> *"Studies have shown that there is a growing threat of mobile malwares and growing concern of privacy. Our secure contacts management system ensures that the contacts list in your mobile phone is securely protected, even under hostile environment. Our secure cloud service employs state-of-the-art Advanced Encryption Standard (AES), together with defense-grade secure mobile platform, to provide a practical and secure BYOD (Bring Your Own Device) solution to secure your valuable client list."*

The term "secure" appears many times, but what does it mean?

We need more refine and precise definitions of "security".

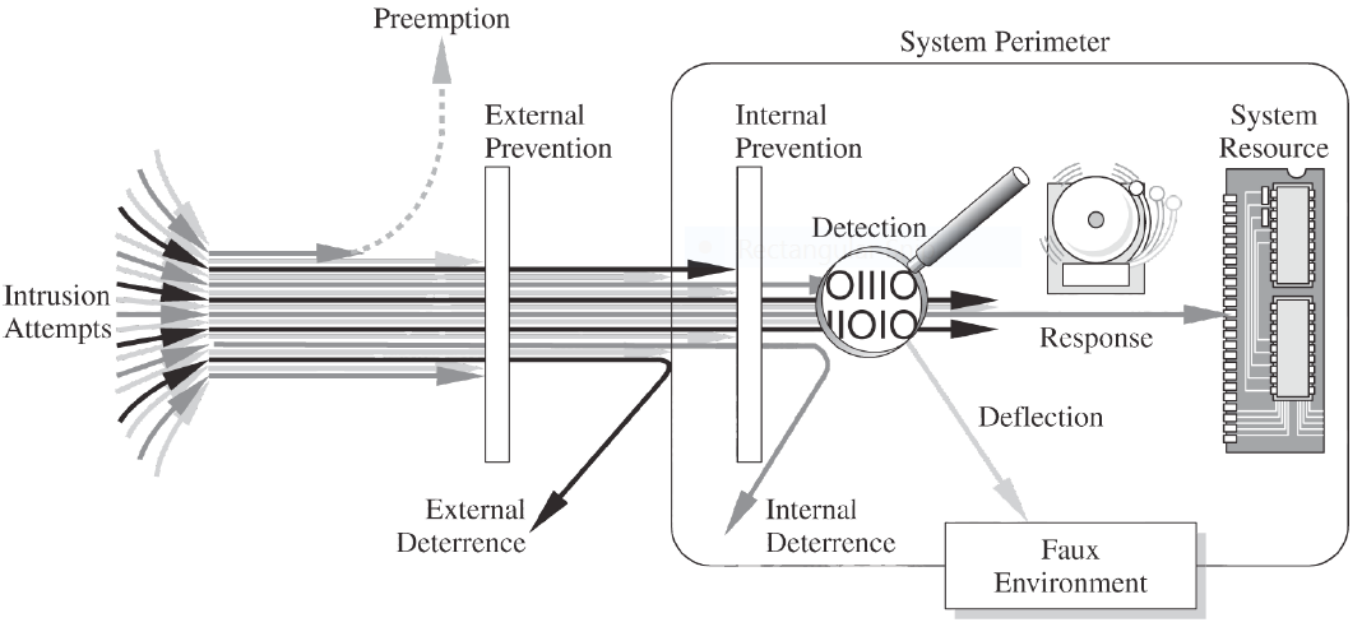
* I make this up. This advertisement is not real.

Assets, Threat, Vulnerability and Control

- Security is about the protection of **assets** (objects of value):
  - Hardware
  - Software
  - Data and information
  - Reputation: which is intangible
- (See [PF1], which gives detailed elaboration on *Threat-Vulnerability-Control*)
- ***Threat***: A set of circumstances that has the potential to cause loss or harm
  - E.g. an attacker who controls the workstation in the lecture room could maliciously gather sensitive information such as passwords
- ***Vulnerability***: a weakness in the system
  - E.g. anyone can reboot the system from USB or disk to gain control

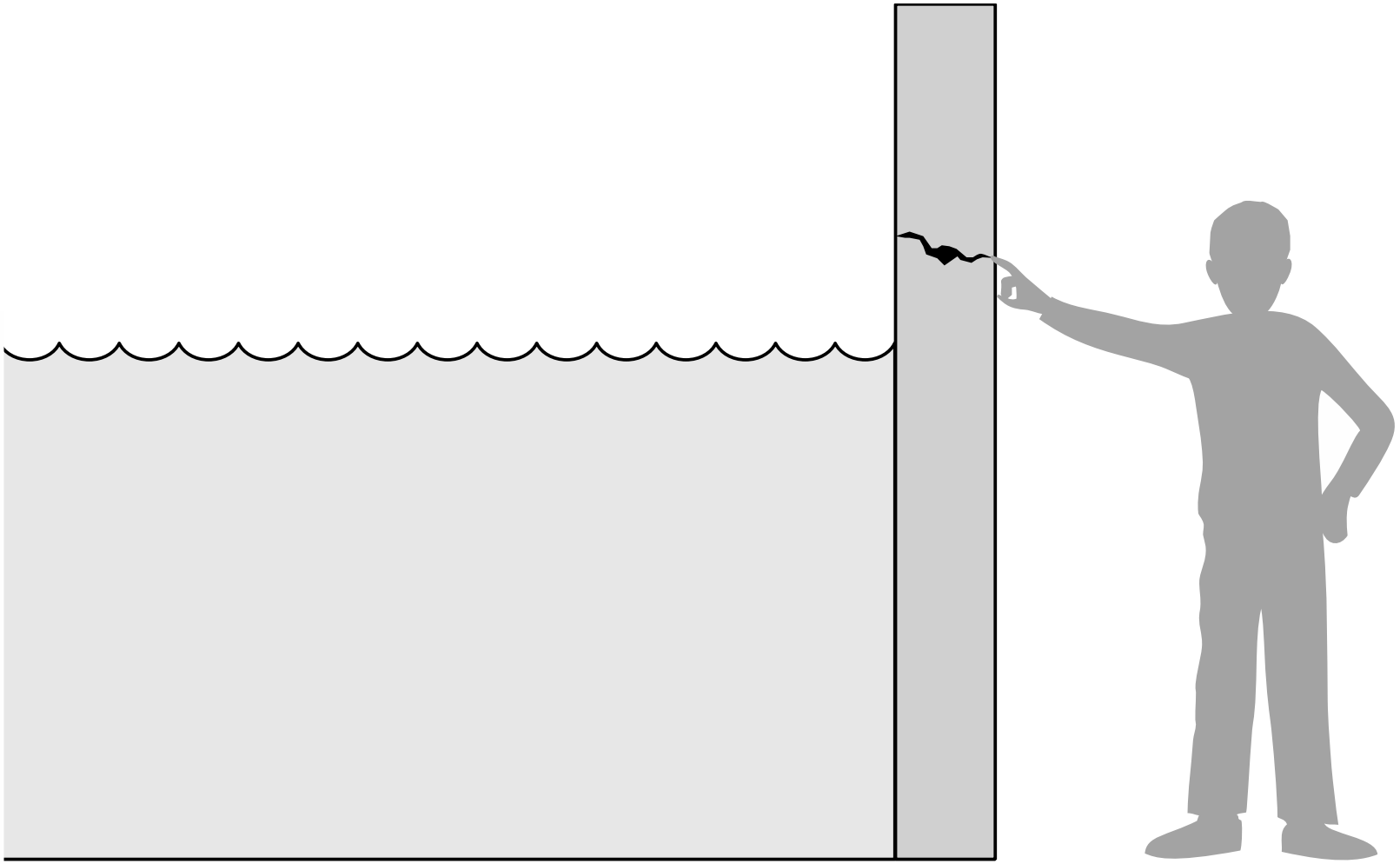
Assets, Threat, Vulnerability and Control

- ***Control***: A control, countermeasure, security mechanism is a mean to counter threats
  - E.g. restrict physical access to the workstation, disable USB booting, etc.
  - See [PF1.5] on prevent, deter, deflect, detect, mitigate, recover



A ***threat*** is blocked by ***control*** of a ***vulnerability***

Threat, Vulnerability and Control: Analogy (for Quiz 0-1)



Another Look at Security Terminologies

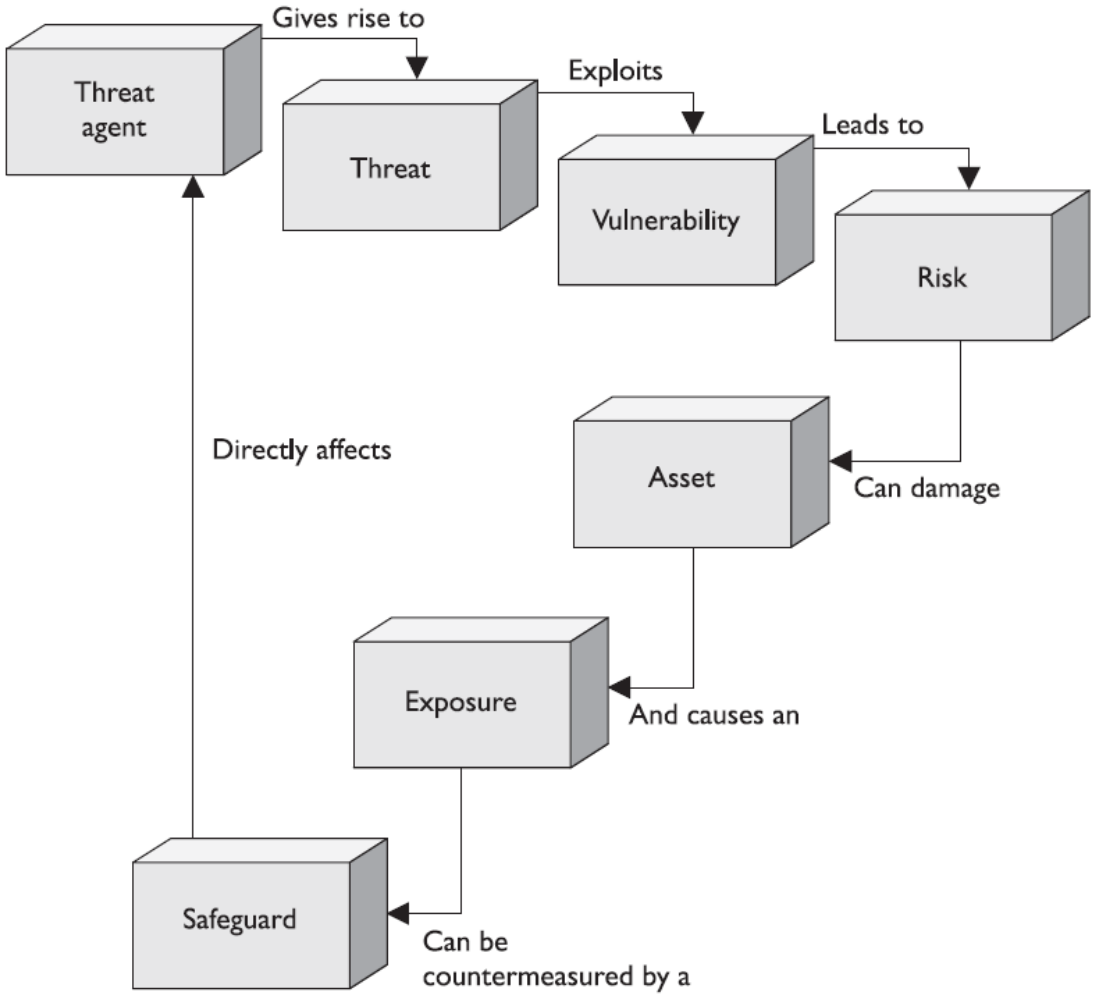


Figure 3-3 The relationships among the different security components

From: Shon Harris, "CISSP All-in-One Exam Guide", 5th Edition, 2010, McGraw-Hill Osborne Media

Note: The term "*safeguard*" is used for "*control*" in the diagram

Different Types of Controls

Figure 3-1 Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets.

From: Shon Harris, "CISSP All-in-One Exam Guide", 5th Edition, 2010, McGraw-Hill Osborne Media

Security Definitions: C-I-A Triad

- **Confidentiality:**
  - + The ability to ensure that an asset is *viewed* only by authorized parties
  - - Prevention of *unauthorized disclosure* of information
- **Integrity:**
  - + The ability to ensure that an asset is *modified* only by authorized parties
  - - Prevention of *unauthorized modification* of information or processes
- **Availability:**
  - + The ability to ensure that an asset can be *used* by any authorized parties
  - - Prevention of *unauthorized withholding* of information or resources

1. Confidentiality

- Edward Snowden leaked classified NSA information.
  From NSA's point of view, this is a breach of ***confidentiality***.
- A student "hacked" into the university system and *downloaded* the examination reports. He now know the marks obtained by each student.

  Confidentiality of the exam result is thus compromised.

2. Integrity

- A student "hacked" into the university system and *modified* his own grade.

  Integrity of the exam result is compromised.

3. Availability

- Chewing gum sticking to a car's door lock.
- A *botnet* floods a Web server with HTTP requests.
  A legitimate HTTP request now takes longer time to be processed. Thus, the QoS significantly degraded.
  In the extreme scenarios, the Web service is denied.

  This is a ***distributed denial of service attack*** (DDoS) on the Web server, which compromise ***availability***.

Notes:

There are also other requirements like:

- ***Authenticity***: logins, password checks, message sender/origin.
- ***Accountability***, including ***non-repudiation*** of a prior commitment.

Some literatures treat these as different requirements.
Some group them under C-I-A, e.g., very often,
"authenticity" is treated as "integrity".
(Hence, read the context carefully).

Quiz 0-2

- Which security requirements are compromised below?
  "An application is being modified by an attacker.
  The compromised application carries out key-logging:
  it captures the password entered by the user and sends it to the attackers."
- Answer?
  Please use Quiz 0-2 Zoom poll

Remarks on Security Terminology

- There are many **inconsistent usages** of security terms
- For e.g. the term "privacy" in the following statement "*HTTPS provides privacy, integrity & authenticity for …*" could mean *confidentiality*
- *Why?*
- A sample relevant scenario:
  "If Alice uses a free airport WiFi, and submit a report to LumiNUS via HTTPS, even the airport operator is unable to know the content of the report."

Remarks on Security Terminology

- Whereas the "privacy" in:
  - *"Social networking sites vary in the level of privacy offered."*
  - *"Advocates have raised the issue of privacy in mobile advertisement."*

  could means revelation of **personal information** like age, salary, that the individuals do not intend to share
- Sample scenario: "Alice uses a calculator app on her mobile phone. The app obtains the **GPS location** and contact list, and shares it with another company".
- There is **no single definition** of security:
  Different fields, experts, documents may use different definitions. Hence, do take special note of the context.

Difficulty in Achieving Security

- **Security is not considered** during the early design stage
- It is often **difficult to formulate security requirements**
- There can be **various design constrains**
- It is **difficult to verify** that a design achieves the intended security requirements
- Even if the design is secure, the system **may not be properly implemented**, especially for large, complex systems
- A deployed system is most vulnerable at its **weakest point**
- Even a secure system can still be **difficult to manage**, particularly with *humans in the loop*: configuration errors, mismanagement of patches/credentials/etc.

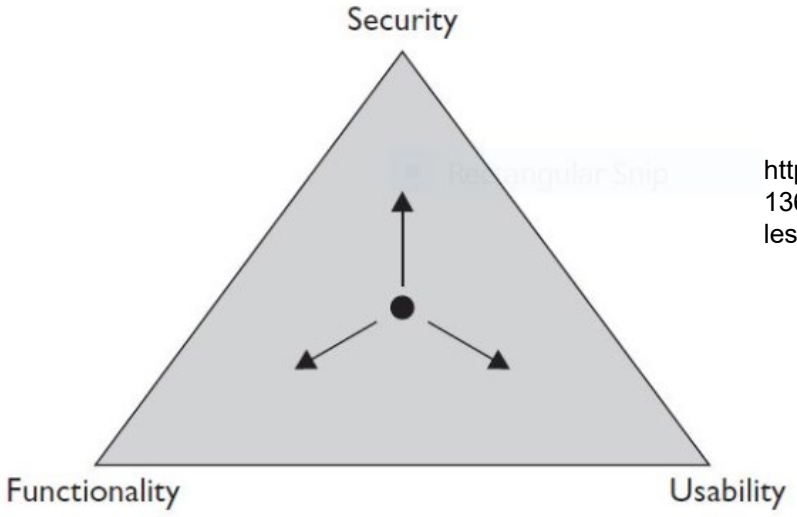
In this module, we will look into examples to illustrate how systems fails, and various protection mechanisms in overcoming the above difficulties

Trade-off in Security

There is a trade-off between security and:

- **Ease-of-use**: Security mechanisms interfere with working patterns users originally familiar with
- **Performance:** Security mechanisms consumes more computing resources
- **Cost:** Security mechanisms are expensive to develop

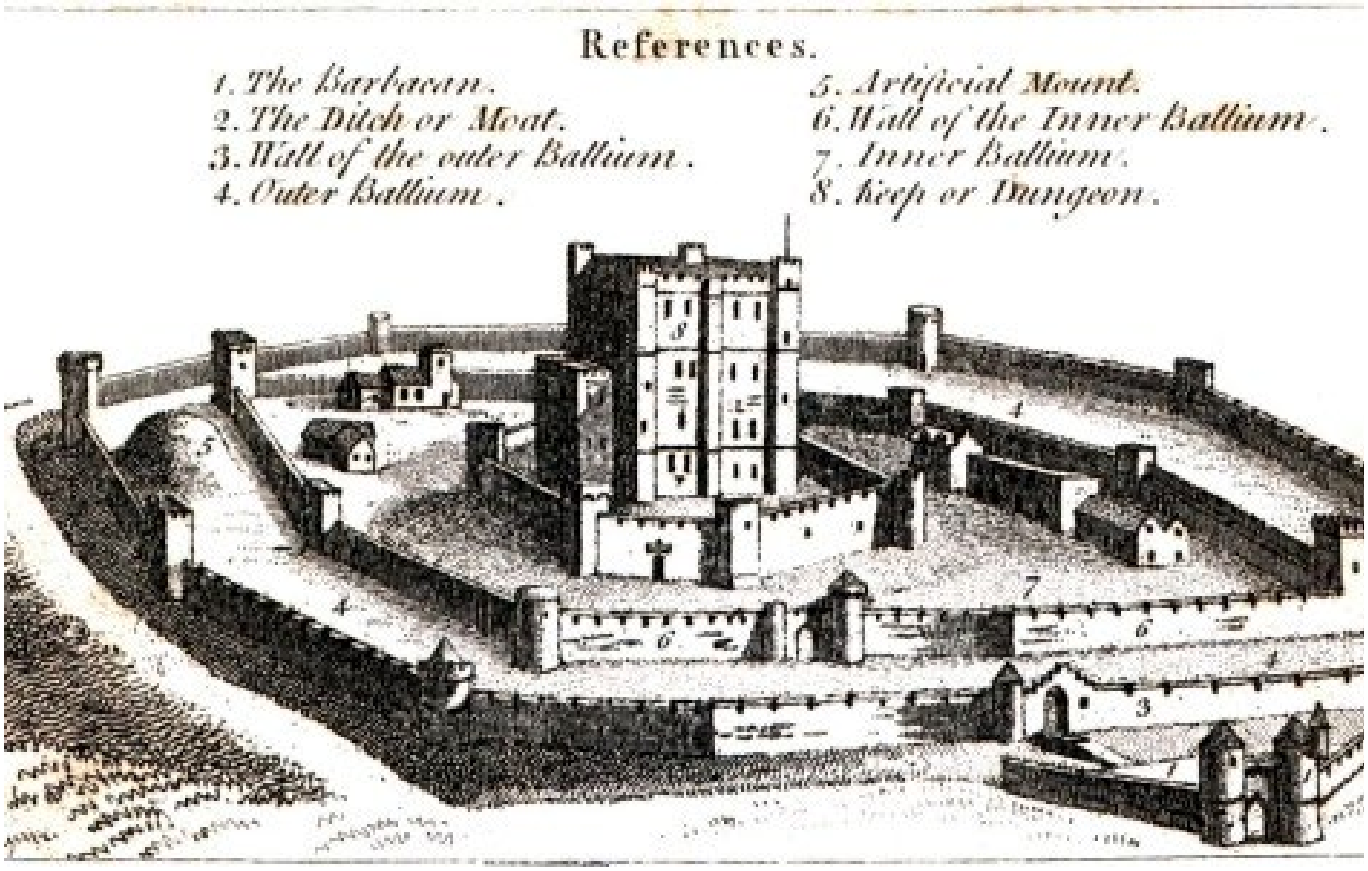
Security, Functionality and Usability Triangle: the more secure something is, the less usable and functional it becomes



https://www.linkedin.com/pulse/20140619200426-136462609-the-more-secure-something-is-the-less-usable-and-functional-it-becomes

“Security: Computing in an *Adversarial* Environment”

We are facing “smart” adversaries who actively look for vulnerabilities



See https://smartbear.com/blog/test-and-monitor/what-medieval-castles-can-teach-you-about-web-secu/

"Security: Computing in an *Adversarial* Environment"

Town-protecting castles:

- **Services:**
  - Markets, admin office, etc.
- **Users:**
  - Citizens, travelers, etc.
- **Attackers' goals:**
  - Capture the whole city, steal info, disrupt services, etc.
- **Protection mechanisms**:
  - All-round defense: "security depends on the weakness point"
  - Layered defense
  - Access control: e.g. castle/door guards
  - Other measures: dummy target, death trap, obscurity, …