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?

1. Background

2021 Colonial Pipeline Ransomware Attack

Search **Bloomberg** Sig

Schools Brace for More Cyberattacks After Record in 2020 | Apple Says Feature to Find Child Images Doesn't Create Backd... | Microsoft Exchange Used to Hack Diplomats Before 2021 Breach

Photographer: Samue

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

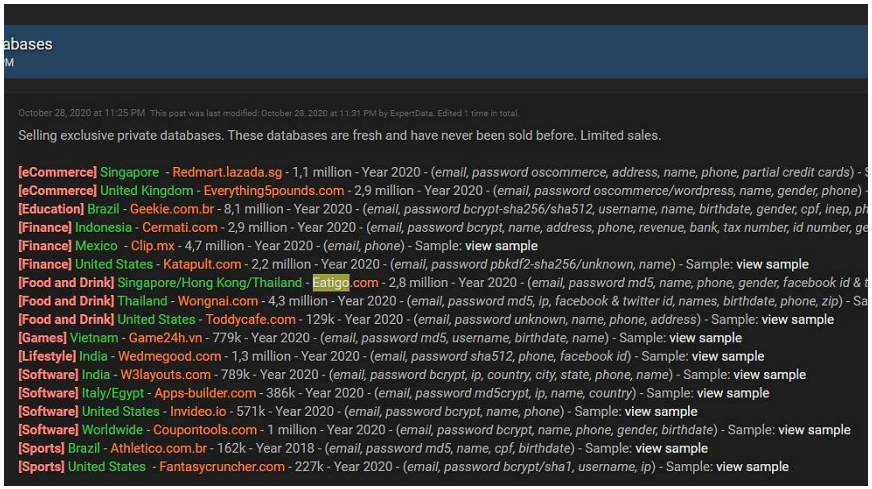
2020 Lazada Data Breach

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)



"This RedMart-only information is more than 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

Lazada is investigating the data breach and has informed the Personal Data Protection Commission.

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.

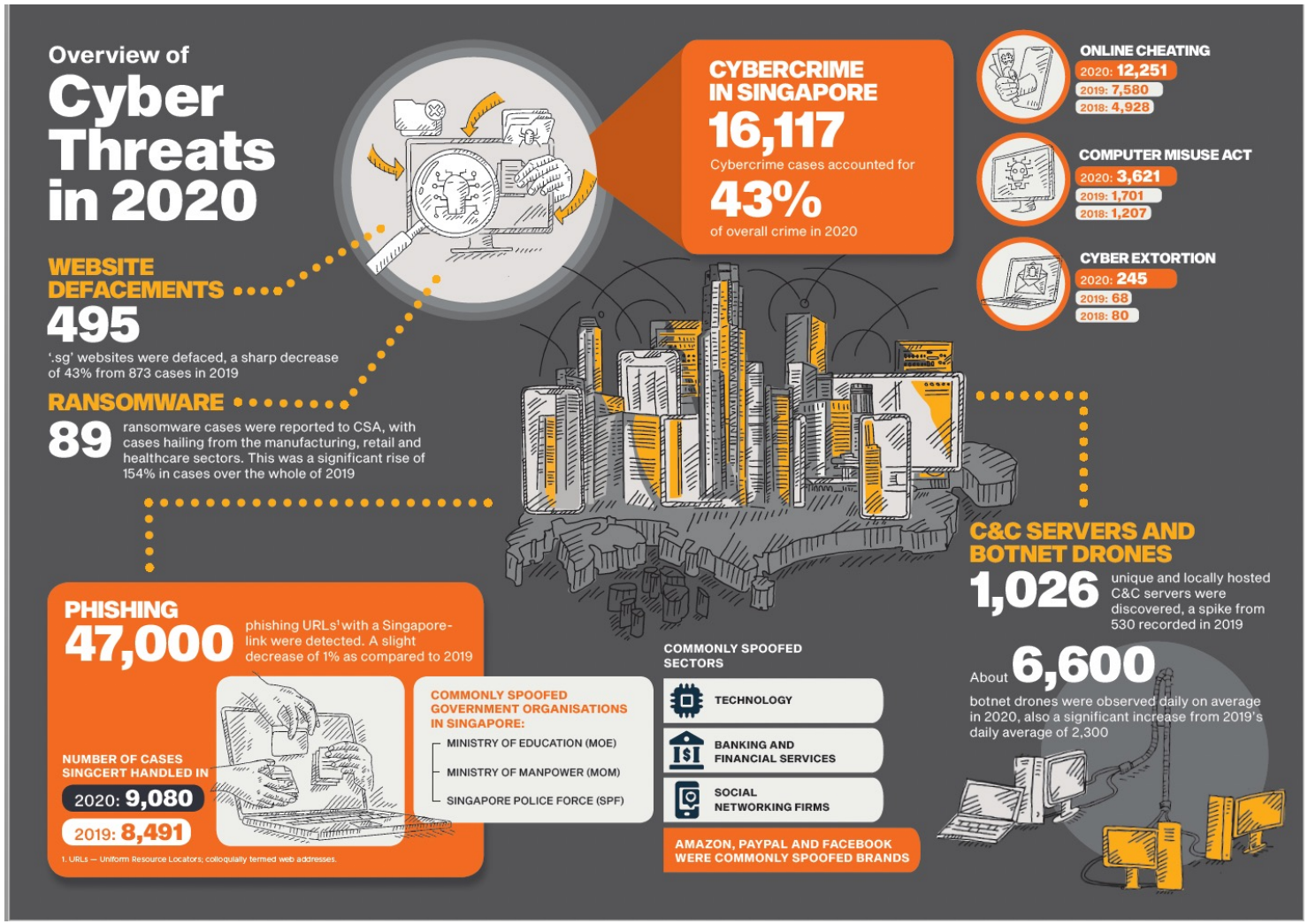
The "most serious breach of personal data" in Singapore's history took place last month, with 1.5 million SingHealth patients' records accessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken, according to the Ministry of Health and Ministry of Communications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

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 trajectory[2].

Global Observations

Dec 2019 - Mar 2020

- Customisation of lures.
- Healthcare sector a key target.

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

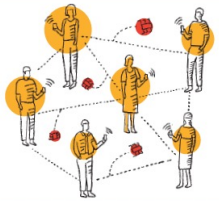
Mar - May 2020

- 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.

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

Jun - Jul 2020

- Pivot to exploit vulnerabilities in contact tracing app technology.
- Telecommuting workforce and online users constantly targeted by social engineering lures.



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

Aug - Dec 2020

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.

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

Local Observations

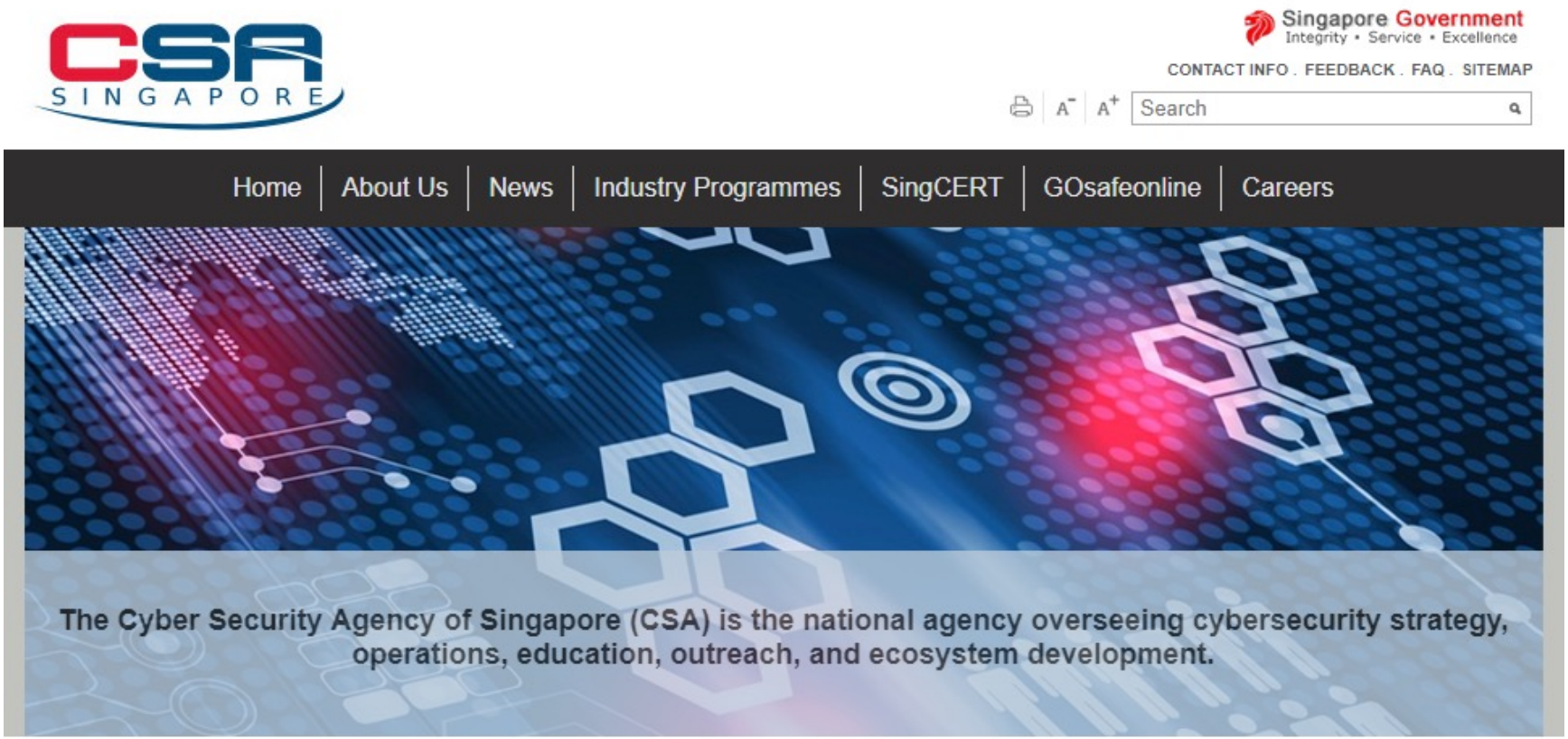
- Spike in COVID-19-related phishing, scams and ransomware cases.
- Key targets: Healthcare, Education.
- Zoom for home-based teaching suspended after lesson hijacking incident.
- ake COVID-19 contact cing apps, including ake TraceTogether app, with the ability to deliver malware detected.
- Singapore a target of global phishing campaign on government support.
- Increasing trend of Business Email Compromise (BEC) and data breaches/leaks.
- Alert by Singapore Police Force warning of vaccination scams.

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

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

Attacks can also have different motivations such as monetary and politcal

Singapore Cybersecurity Agency



Singapore Cybersecurity Strategy

- Pillar One:
  - Building a Resilient Infrastructure
- Pillar Two:
  - Creating a Safer Cyberspace
- Pillar Three:
  - Vibrant Cybersecurity Ecosystem
- Pillar Four:
  - Strengthening International Partnerships

These national level strategies are also similar to organisation level strategies

- 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
    - Singapore's Operational Technology (OT) Cybersecurity Masterplan 2019

Recent moves to protect essential services / CII

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
    - PDPC 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

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*.

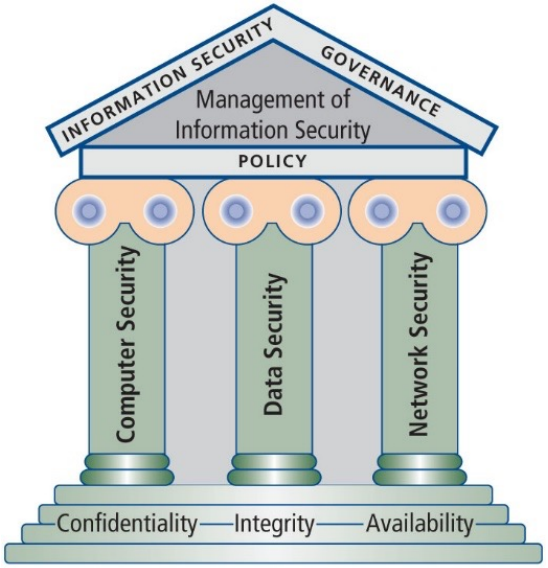


Figure 1-1 Components of information security

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.)

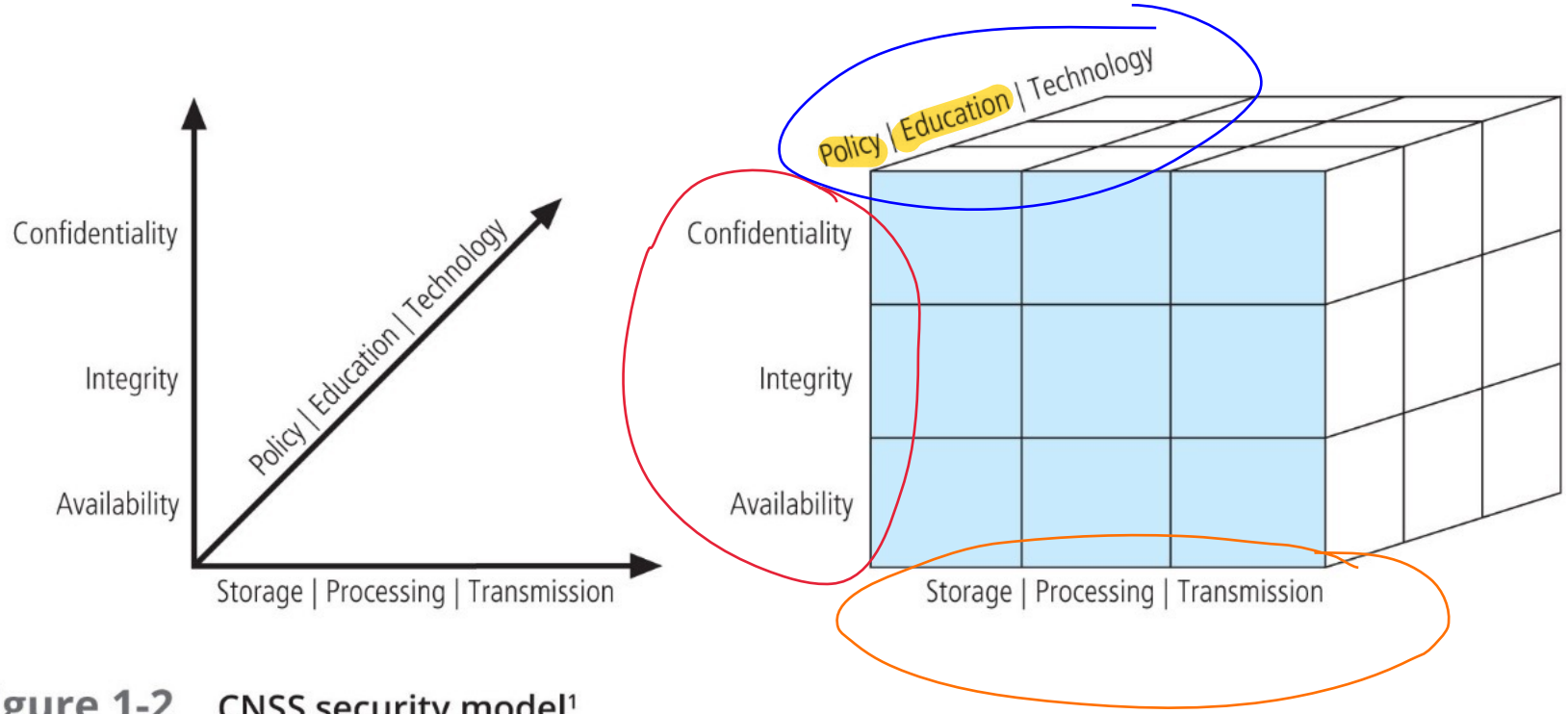


Figure 1-2 CNSS security model[1]

there are 27 cells to focus on individually

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY/
NATIONAL COMPUTER SECURITY CENTER

14TH NATIONAL COMPUTER SECURITY CONFERENCE

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

INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL

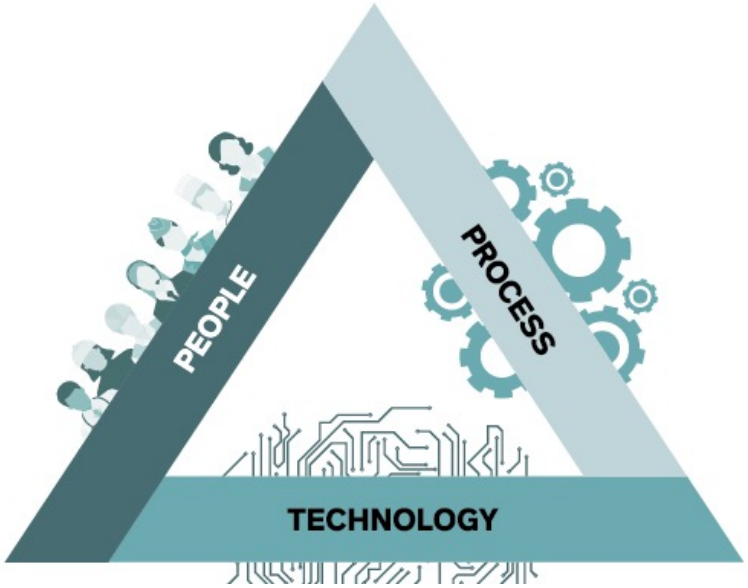
Capt John R. McCumber
Joint Staff/J6K
The Pentagon
Washington, DC 20318-6000

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.

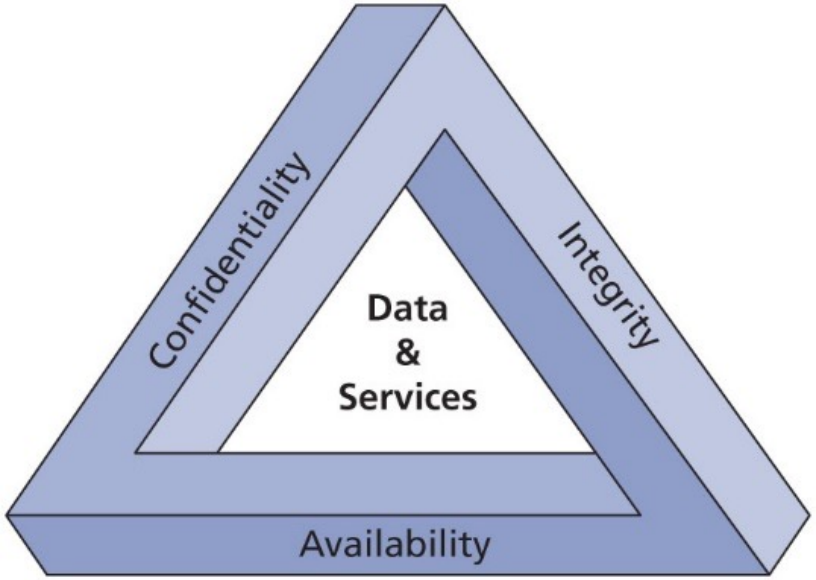


Figure 1-3 The C.I.A. triad

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)

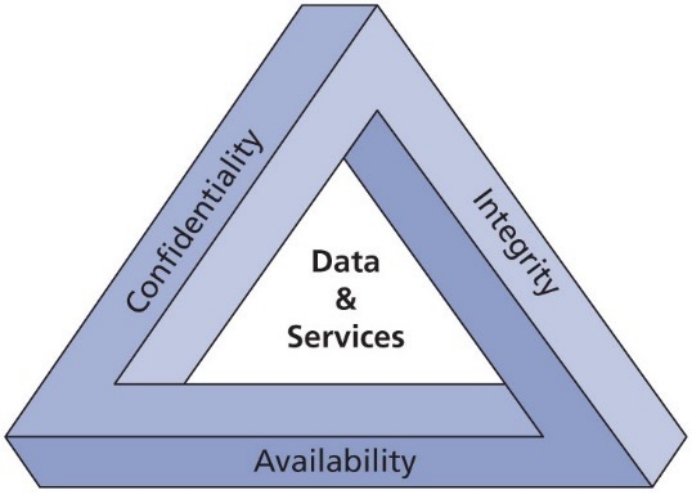


Figure 1-3 The C.I.A. triad

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

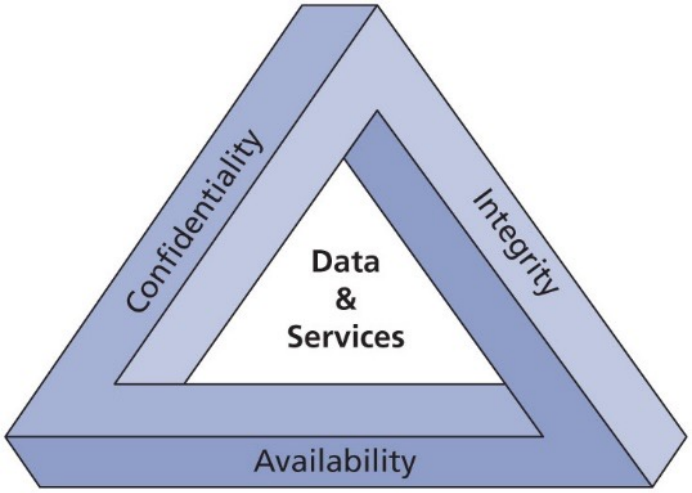


Figure 1-3 The C.I.A. triad

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

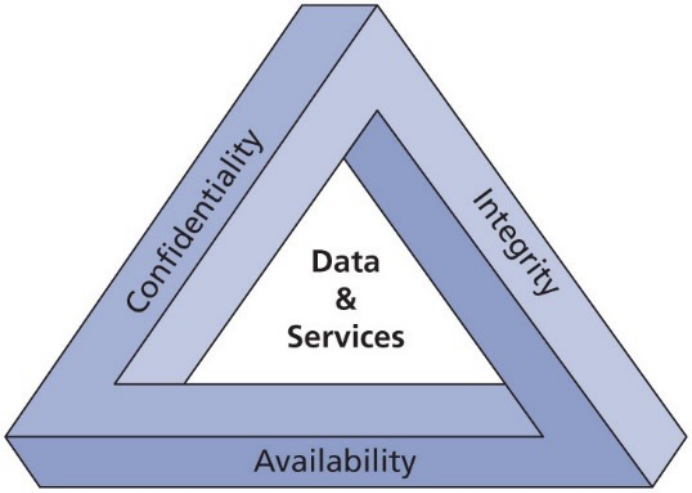


Figure 1-3 The C.I.A. triad

The C.I.A. Triad Extension

- Over time C.I.A. triangle has been expanded to include:
  - Privacy → user
  - Identification
  - Authentication
  - Authorization
  - Accountability

} System

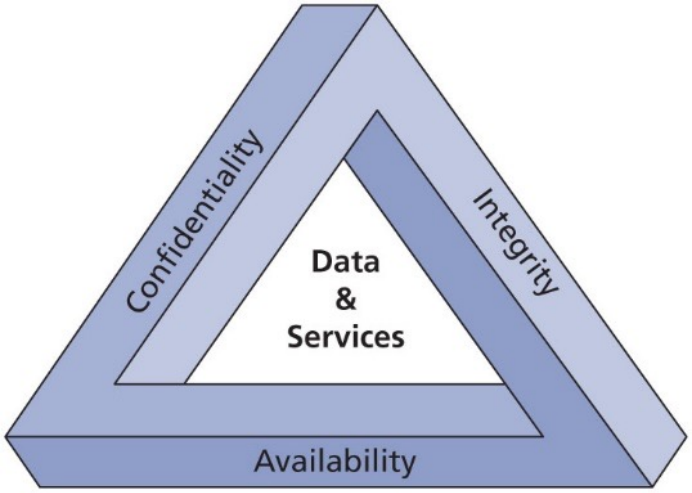


Figure 1-3 The C.I.A. triad

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?

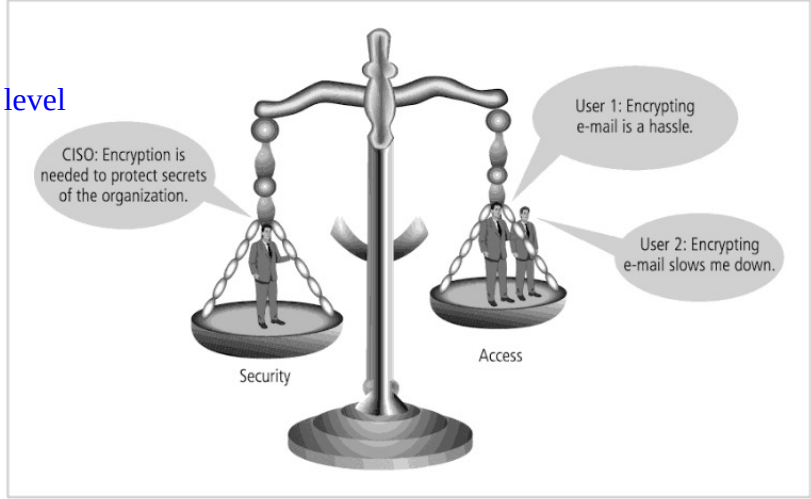
What is Management

- 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


Questions?