



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

BITS 2523

Cyberlaw & Security Policy

Lecture 4

By

Mohd Fairuz Iskandar Othman, Phd

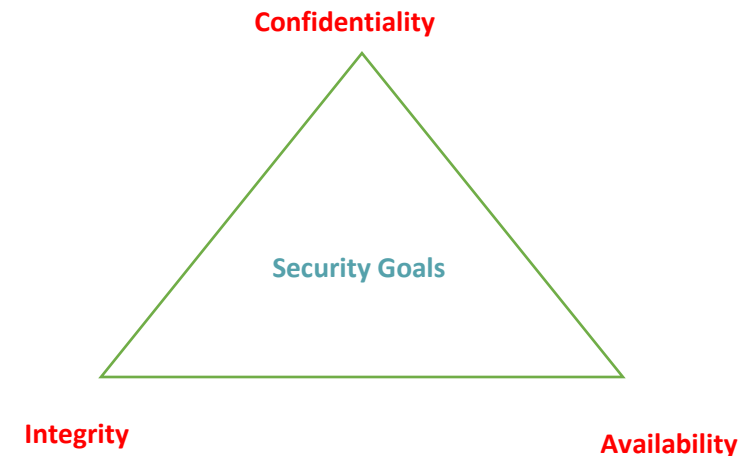
mohdfairuz@utem.edu.my

Topics covered:

- What is information security?
- The goals of Internet & Information Security
- Why is information security an issue?
- Basic concepts of information security
- Common information security concerns
- Mechanisms that ensure information security
- The challenges of Internet & Information Security
- Malaysia Cybersecurity Law?

What is information security?

- Information security is the study and practice of protecting information. Its main goal is to protect the confidentiality, integrity, and availability of information.
- Professionals usually refer to this as the C-I-A triad, (A triad is a group of three things considered to be a single unit.)
- All information security measures try to address at least one of the three goals:
 - Confidentiality
 - Integrity
 - Availability



- Protect the *confidentiality* of data
 - Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible
- Preserve the *integrity* of data
 - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
- Promote the *availability* of data for authorized use
 - Availability models keep data and resources available for authorized use during denial-of-service attacks, natural disasters, and equipment failures

Why is information security an issue?

Always A Pioneer, Always Ahead

The average cost of a data breach is \$3.86 million as of 2020. (IBM)

Total cost for cybercrime committed globally will reach \$6 trillion by 2021 (Forbes)

Share prices fall 7.27% on average after a breach (Comparitech)

In 2020, a Twitter breach targeted 130 accounts, including those of past presidents and Elon Musk, resulted in attackers swindling \$121,000 in Bitcoin through nearly 300 transactions. (CNBC)

Supply chain attacks were up 78% in 2019. (Symantec)

Ransomware damage costs will rise to \$20 billion by 2021 and a business will fall victim to a ransomware attack every 11 seconds at that time. (Cybersecurity Ventures)

After declining in 2019, phishing increased in 2020 to account for 1 in every 4,200 emails. (Symantec)

Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes (HIPAA Journal)

27% of COVID-19 cyberattacks target banks or healthcare organizations and COVID-19 is credited for a 238% rise in cyberattacks on banks in 2020. (Fintech News)

9.7 Million Records healthcare records were compromised in September 2020 alone (CNBC)

15% of breaches involved healthcare organizations, 10% in the financial industry and 16% in the public Sector. (Verizon)

More than 77% of organizations do not have a Cyber Security Incident Response plan (Cybint)

Connected IoT devices will reach 75 billion by 2025 (Prnewswire)

95% of cybersecurity breaches are due to human error (Cybint)

Remote workers have caused a security breach in 20% of organizations. (Malwarebytes)

86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)

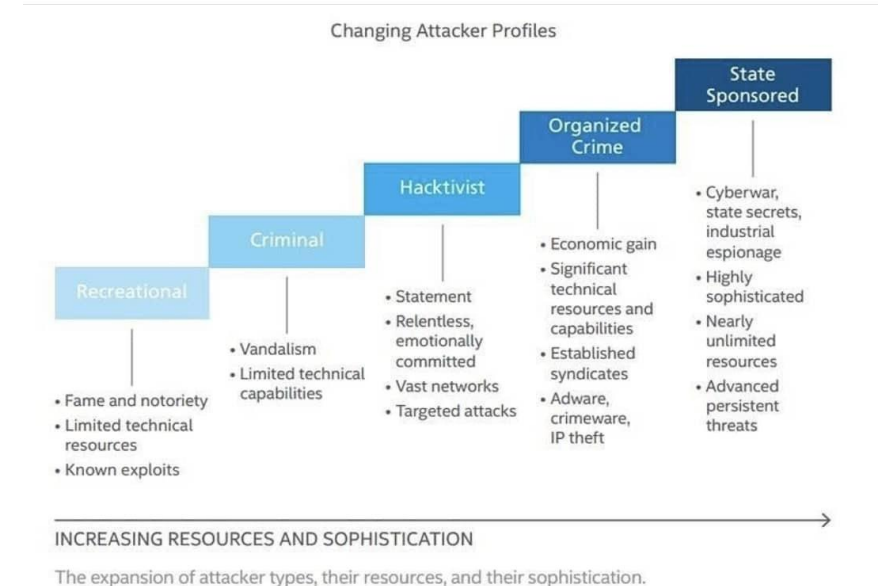
Why is information security an issue?

Always A Pioneer, Always Ahead

thecybersecurityhub The City of Johannesburg shut down its website and billing systems after a group hacked into the authority's system and demanded a ransom of four bitcoins worth about \$30 000. The call center, cashiers and other digital platforms were also taken offline as a precaution following the breach, the City said on its Twitter account. A group called Shadow Kill Hackers advertised the hack on the City's website before it was shut down, local broadcaster eNCA reported. The cyber extortionists then threatened to upload all hijacked data on the internet by October 28 if their crypto-currency ransom isn't met, the news agency said. The incident is being investigated by security experts who are striving to limit the impact, the City said. The investigation will take 24 hours. Multiple banks were hit by online attacks that affected public-facing services earlier this week, though they don't constitute a hack or a data breach and no customer data was put at risk, according to the South African Banking Risk Information Centre. In July, Johannesburg's City Power was hit by a virus that restricted the ability of customers to buy electricity online. #cybersecurity

thecybersecurityhub Two former employees of Twitter were charged with spying for Saudi Arabia by snooping into thousands of private accounts seeking personal information about critics of the Riyadh government. The case represents the first time that federal prosecutor have charged Saudis with deploying agents inside the United States. Ahmad Abouammo, a U.S. citizen, was a media partnerships manager at Twitter who was not authorized to access Twitter users' private information. He allegedly did exactly that for which he received payments of up to \$300,000 from a Saudi source. Abouammo also received a Hublot watch with a value of about \$20,000. Last year, Abouammo was interviewed by the FBI about the watch and the payments he had received. During the interview he created a false invoice on his home computer to try to justify the payments as compensation for media consulting he said totaled no more than \$100,000. Abouammo is charged with acting as a foreign agent and falsifying records to obstruct a federal investigation. Ali Alzabarah, a Saudi citizen worked at Twitter beginning in August 2013 as a "site reliability engineer." Between May 21, 2015, and November 18, 2015, Alzabarah, without authorization, accessed the Twitter data of over 6,000 Twitter users, including at least 33 usernames for which Saudi Arabian law enforcement had submitted emergency disclosure requests to Twitter. Among the accounts he accessed were those belonging to well-known critics of the Saudi government. #cybersecurity #infosec

thecybersecurityhub The University of Northampton has confirmed a cyber attack interrupted IT services and telephones on campus on 17 March. Northamptonshire Police and experts consultants have been brought to investigate the breach, which is still causing problems although the university says it has implemented 'work around solutions.' A spokesperson for the University of Northamptonshire said: "We are working with expert consultants to investigate and resolve this issue as quickly as possible, including legal counsel and IT forensics investigators, who are assessing the impact and advising on the appropriate remedial actions." "The full facts of the situation have not yet been established and we will provide further information as soon as we can." The university added: "We have notified the Information Commissioner's Office (ICO) as a precaution and are liaising with the police as we investigate this attack further." "A number of temporary work around solutions are being rolled out to support students and staff. "At the University of Northampton, we take the safety and security of our information as well as the continuity of our systems and services extremely seriously - and will continue to take every action to protect the organisation against cyber attacks " #computerscience



- Some of the concepts include:
 - Vulnerabilities
 - Threats
 - Risks
 - Safeguards
 - Choosing a safeguard

- Vulnerability – a weakness or flaw in an information system. Vulnerabilities can be exploited to harm information security.
- 4 classification of vulnerabilities:
 - People
 - Process
 - Facility
 - Technology
- Exploits – are successful attacks against vulnerabilities. They take place in a period known as window of vulnerability

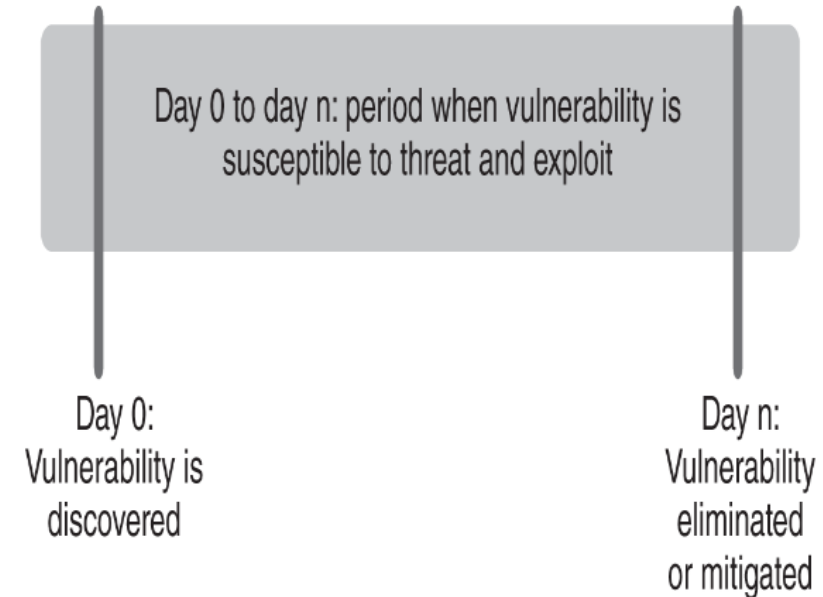


FIGURE 1-2

The window of vulnerability.

NOTE


Some vulnerabilities are exploited almost as soon as they are discovered. The term for this is a **zero-day vulnerability**. It is unique because the vulnerability is exploited before a vendor provides a patch or some other fix.

- Threats are anything that can harm an information system. They are successful exploits against vulnerabilities.
- Example of relation between vulnerability & threat:
 - An organisation may have few controls to prevent an employee from deleting critical computer files. This lack of controls is the vulnerability. A well-meaning employee could delete files by mistake. In this case, the employee is the threat source. The threat is the action of deleting the critical files. If the employee deletes the files, a successful exploit of the vulnerability has taken place. If the files are not recoverable, or recoverable only at great expense, the incident harms the organisation and its security. Therefore, availability and integrity are compromised.

Threats (cont...)

- Threats fall into broad categories:
 - Human – threats carried out by people
 - Natural – uncontrollable events such as earthquakes, flood, fires
 - Technological and operational – threats that operate inside information systems to harm information security goals, like malicious code, hardware and software failures
 - Physical and environmental – facility-based threats like facility breach, loss of cooling within a facility.

- Risks is the likelihood that a threat will exploit a vulnerability and cause harm to the organization.
- These impacts from threats can generally be sorted to 6 categories:
 - **Financial**- risks that affect financial resources or operations
 - **System/services** – risks that impact how an organization provides IT systems and services
 - **Operational** – risks that affect the normal operations of information systems and services
 - **Reputational** – risks that negatively affect an organization's reputation or brand
 - **Compliance** – risks that related to a possible violation of a law, regulations, or organizational policy
 - **Strategic** – risks that may have a lasting impact on an organization's long-term viability

- Organisations have several options for responding to risk. Common response include:
 - Risk avoidance
 - Apply safeguards to avoid a negative impact
 - Risk mitigation
 - Apply safeguards to lower risk to an acceptable level
 - Risk transfer 
 - Pass the risk to another entity, at which point the risk impact is borne by the other entity
 - Risk acceptance
 - Accept the risk if the cost of the risk itself is less than the cost to avoid, mitigate, or transfer the risk

- A safeguard reduces the harm posed by information security vulnerabilities or threats and may eliminate or reduce the risk or harm.
- They are controls or countermeasures, terms that can be used interchangeably.
- Classification of safeguards:
 - Administrative – organizational policies
 - Technical – access control, firewalls
 - Physical – mantraps, fences, locks security cams

Safeguards (cont...)

- Safeguards can also be classified based on how they act:
 - Preventive – keep an incident from happening, like door locks
 - Detective – put in place in order to detect, like system logs
 - Corrective – put in place in order to limit the damage caused by a security incident, like rollback database

Safeguards matrix			
Safeguard type	Preventive	Detective	Corrective
Administrative	Organisation hiring policy	Organisation periodic background checks policy	Discipline policy
Technical	Least privilege principle	Antivirus software	Updating firewall rules to block an attack
Physical	Locks on doors to critical areas	Burglar alarms	Locking a door that was inadvertently left unlocked

Choosing Safeguards

- Organisations may have difficulty choosing suitable safeguards.
- Reference guides provide help for this task:
 - “ISO/IEC 27002:2013, Information Technology—Security Techniques—Code of Practice for Information Security Controls” (2013)
 - “NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations” (2013).

- Some of the concerns include:
 - **Shoulder surfing** – an attacker looks over the shoulder of another person at a computer to discover sensitive information that the attacker has no right to see.
 - **Social engineering** – an attack that relies heavily on human interaction. Involves tricking other people and taking advantage of their human nature to break normal security procedures and gain sensitive information,
 - **Phishing** - attackers attempt to steal valuable information like credit card numbers, user logon credentials and passwords from their victims via email, instant messages, social media platforms, and etc.

- Some of the concerns include:
 - **Malware** – refers to any type of software that performs some sort of harmful, unauthorized, or unknown activity. The term is a combination of the words malicious and software. Malware is usually a computer virus or worm, or a combination of one or more viruses or worms.
 - **Spyware** and keystroke loggers – also a form of malware. Spyware is **any technology that secretly gathers information** about a person or organization.
 - **Keystroke logger** is a device or program that **records keystrokes made on a keyboard or mouse**. They are able to recover computer keyboard entries and sometimes even mouse clicks.

- Some of the concerns include:
 - **Logic bombs** – harmful code intentionally left on a computer system that lies dormant for a certain period. When specific conditions are met, it “explodes” and carries out its malicious function.
 - **Backdoor** – also called trapdoor, is a way to access a computer program or system that bypasses normal mechanisms. Programmers sometimes install backdoors to access a program quickly during development process to troubleshoot problems.
 - **Denial of service** (DOS) – disrupts systems so they are no longer available to users. Usually by consuming large amounts of bandwidth or processing power, as well as disabling an organization’s website. Distributed denial of service uses multiple systems to attack a targeted system.

- **Laws and legal duties**
 - Organisations are subject to several laws enacted by the state or federal government as well as laws by industry sector
- **Contracts**
 - The action of paying someone to do work on your behalf is called outsourcing. Many organisations outsource IT functions to save money. Functions outsourced can include data centre hosting, email facilities and data storage
- **Organisational governance**
 - An organization's governance documents form the basis for its information security program. These documents include policies, standards, procedures, and guidelines
 - The show the organization's vow to protect its own information and that which is entrusted to it.

Challenge for creating a better Internet Security:

Government Challenges:

- Hiring competent IT professionals (from private sector).
- Providing research funding to private sector for developing Internet Security technologies.
- Providing adequate training for government IT staff.

Educational institutions' Challenges:

- Tailoring the classroom content to the needs of the local industry.
- Recruiting educators in the private sector who have experience in the IT field.

Challenge for creating a better Internet Security (cont...):

Financial industry's challenges:

- Respecting the customer's right to privacy.
- Choosing an Internet service provider (ISP) that supports Internet privacy.
- Using the latest technologies for maximum protection of customer financial data (SSL, SET, SSL, TLS, HTTPS, S-HTTP, 3-D Secure).

Challenge for creating a better Internet Security (cont...):

Service industry's Challenges:

- Using electronic funds transfer (EFT) to secure customer transactions.
- Employing specialized authentication systems to ensure a higher level of security like one time passwords (OTP), behavioral biometrics and behavioral analytics.
- Behavioral biometrics can measure and analyze a variety of user behaviors, from the way they hold their mobile device, to finger pressure, swipe patterns, keystroke dynamics and more. It can look at the user's navigation behavior both within the application and on the device, examining their typical speed of browsing and accuracy of movement.
- Behavioral analytics — a different concept — uses data from multiple sources to understand when and how a user normally interacts with their bank account — such as the time of day they normally log in, the typical transaction amounts and more. Any deviations from the user's typical behavior are detected in real-time by comparing that behavior to historical data.



Malaysia Cybersecurity Law?

Always A Pioneer, Always Ahead

- In June 2017, the then Malaysian Home Minister, Ahmad Zahid Hamidi, announced that a new cybersecurity bill will be drafted and tabled in Parliament, in order to combat cybercrimes, including recruitment and financial sourcing by terrorist groups, money laundering and online gambling.
- In April 2019, the then Deputy Prime Minister Datuk Seri Dr Wan Azizah Wan Ismail said that the government is studying the possibility of introducing an Act on cyber security.
- However, till March 2021, the proposed cybersecurity act or bill has not been tabled in Parliament to date.
- Notwithstanding the above, the current laws which relate to cybersecurity in Malaysia include:
 - **Computer Crimes Act 1997**
 - **Communications and Multimedia Act 1998 (CMA)**
 - **Penal Code**

Thank You



www.utem.edu.my