



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

BITS 2523

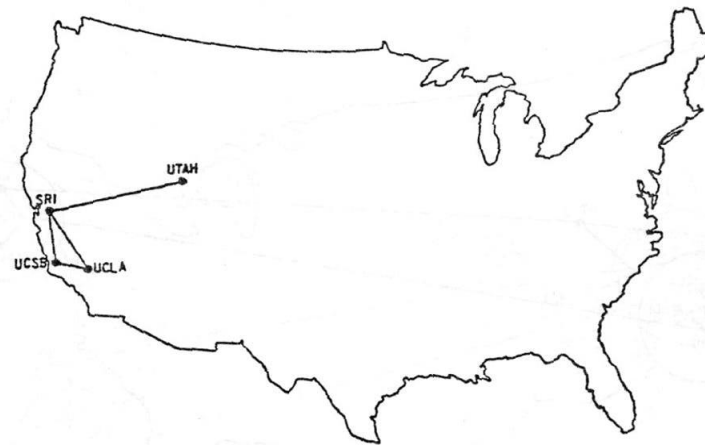
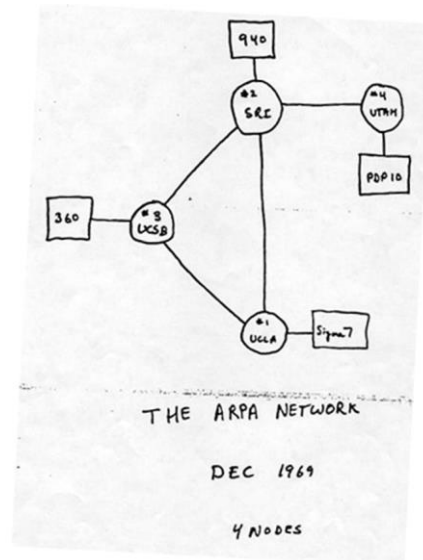
Cyberlaw & Security Policy

Lecture 1

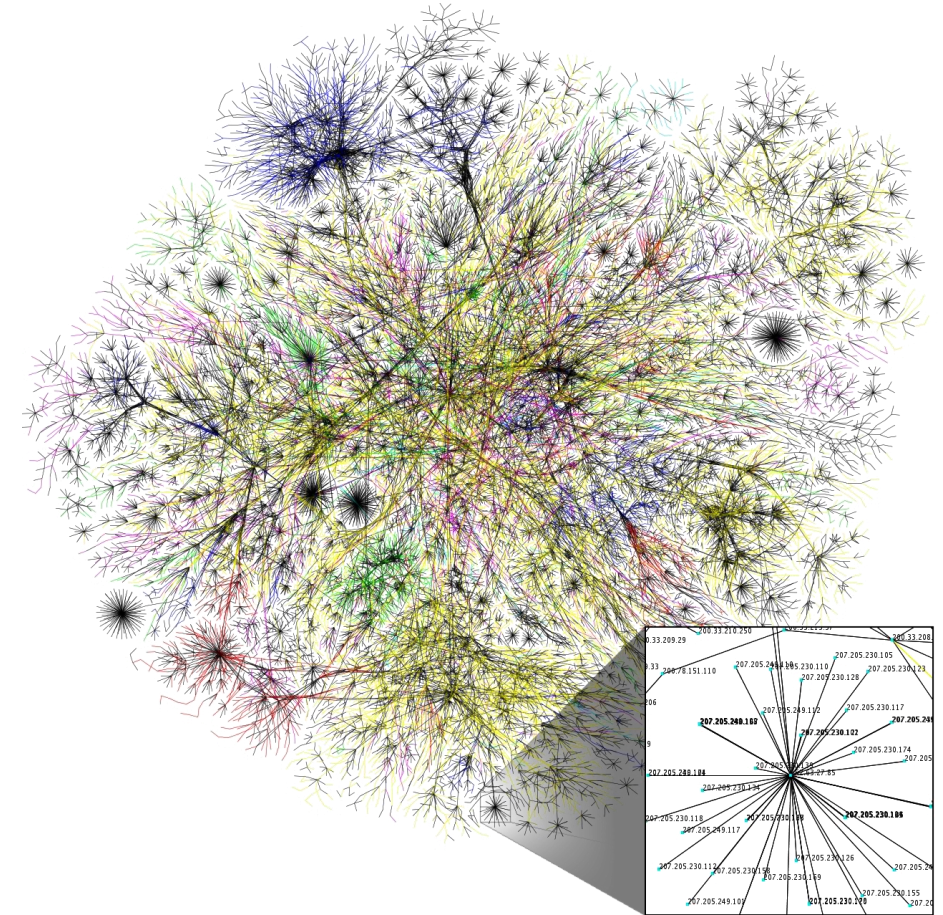
By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

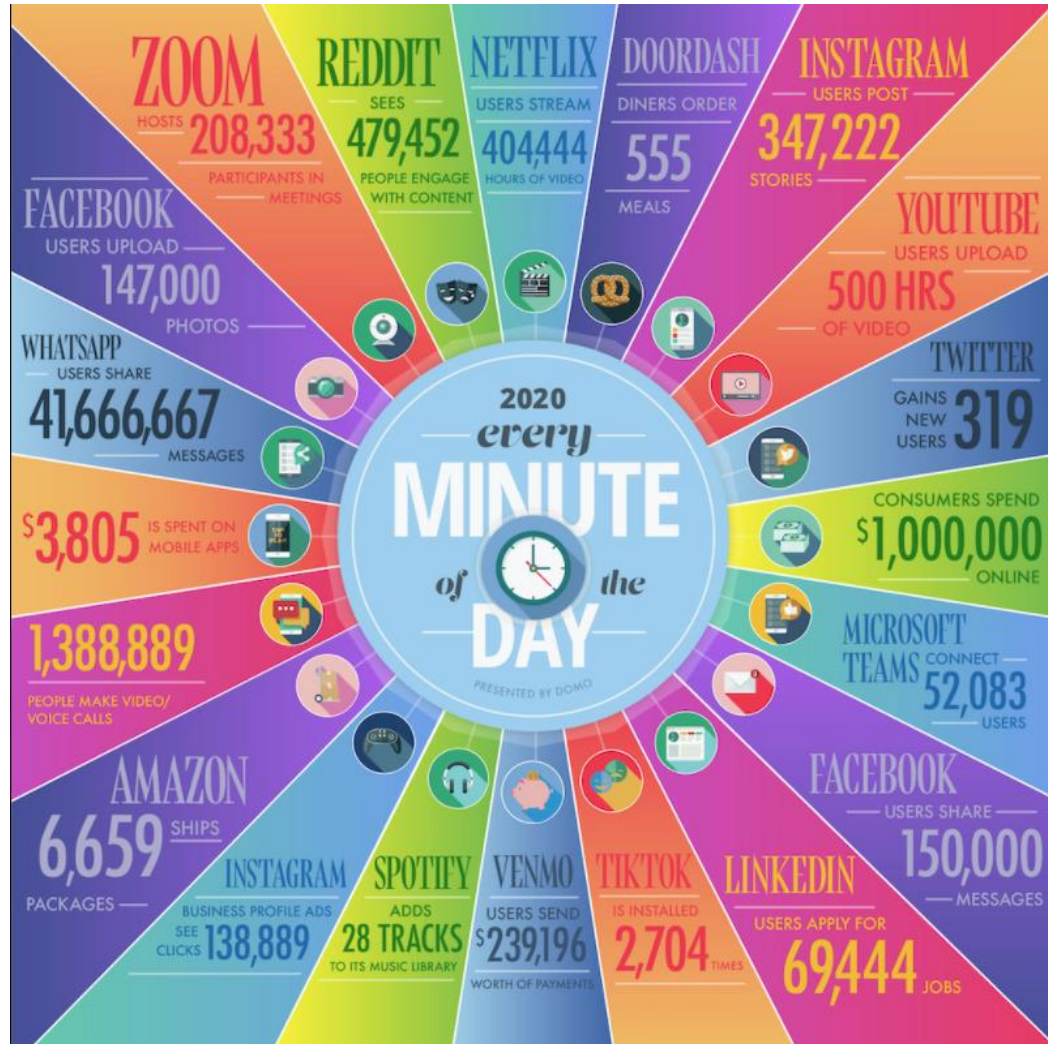


The ARPANET in December 1969












Data Never Sleeps

Always A Pioneer, Always Ahead



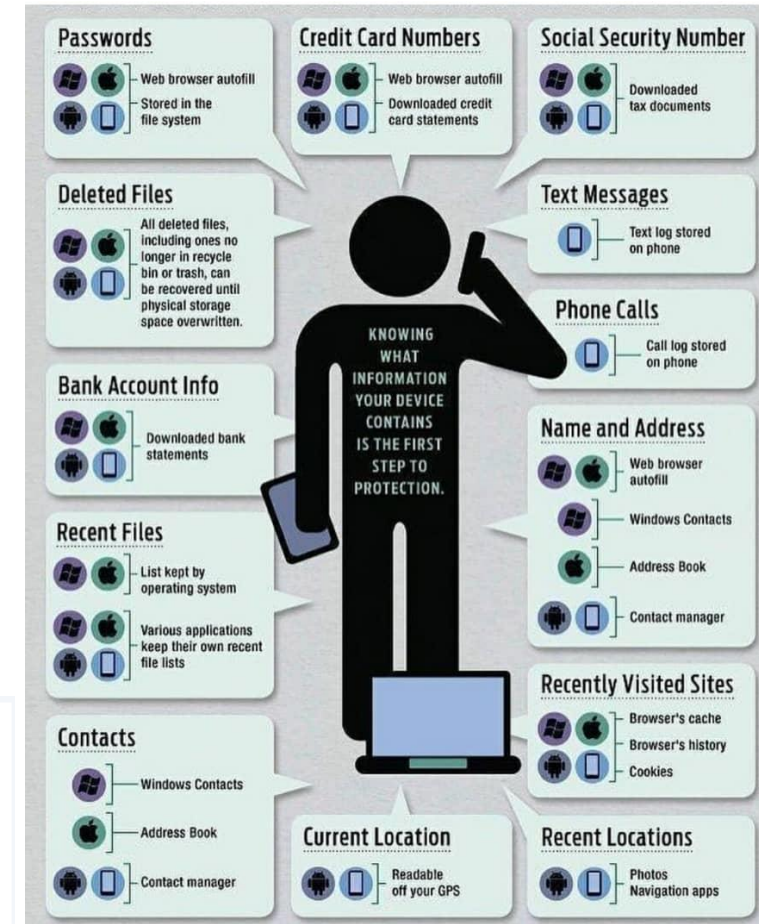
Dependency on the Internet

Always A Pioneer, Always Ahead

Country	Internet Users (2020 Q1)	Internet penetration
 China	854,000,000	59%
 India	560,000,000	41%
 United States	313,322,868	95%
 Indonesia	171,260,000	62%
 Brazil	149,057,635	70%
 Nigeria	126,078,999	61%
 Japan	118,626,672	94%
 Russia	116,353,942	79%
 Bangladesh	94,199,000	57%

<https://www.visualcapitalist.com/countries-with-most-internet-users/>

The average internet user spends **6 hours and 43 minutes** online every day. That's more than 100 days online this year.



Introduction: why cyber laws are needed

Always A Pioneer, Always Ahead

- Cyberspace is a virtual place that has become as important as physical space for social, economic and political activities.
- Many countries in the world are increasing their dependency on cyberspace when they use ICT.
- We rely heavily on the internet and various other online applications day in and out, to deal with our finances, shopping, corresponding, news reading and many other activities, it is no wonder that criminals or misusers would be tempted to seek for their target in the cyber world, and such misdemeanors are often motivated by financial gains, revenge, or even curiosity or apathy.

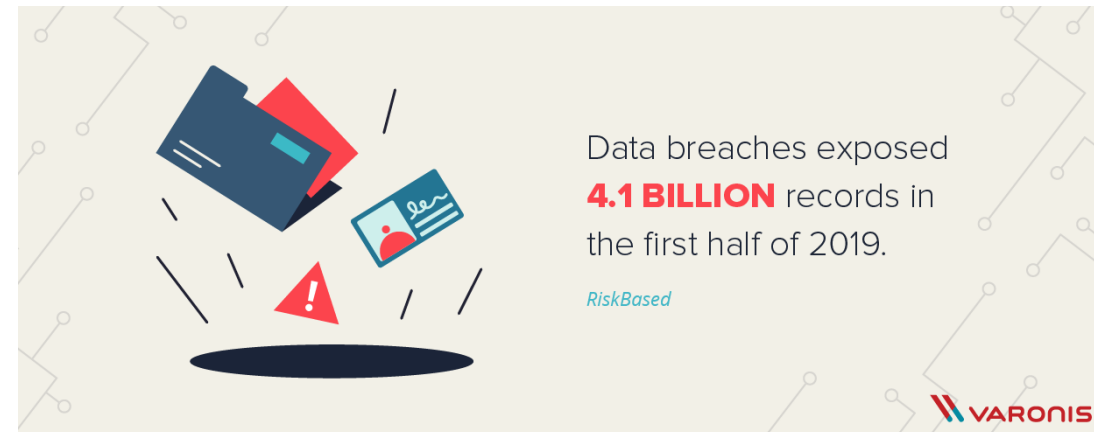
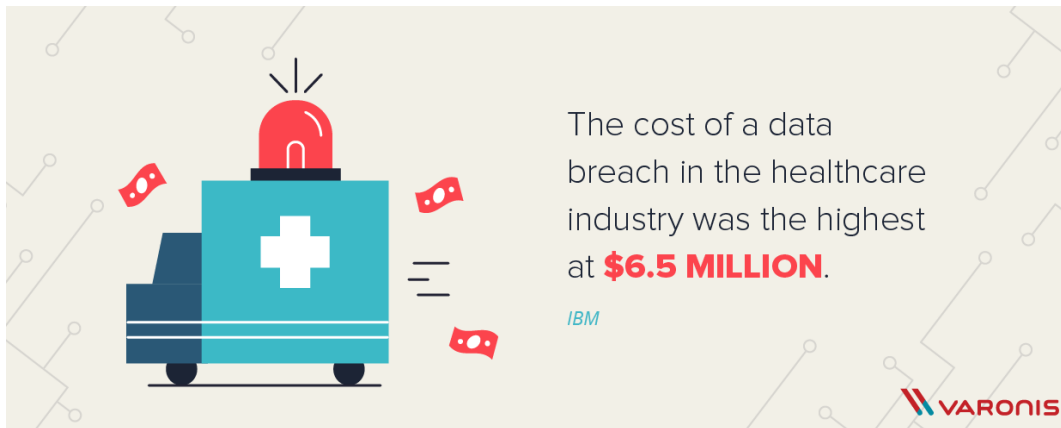
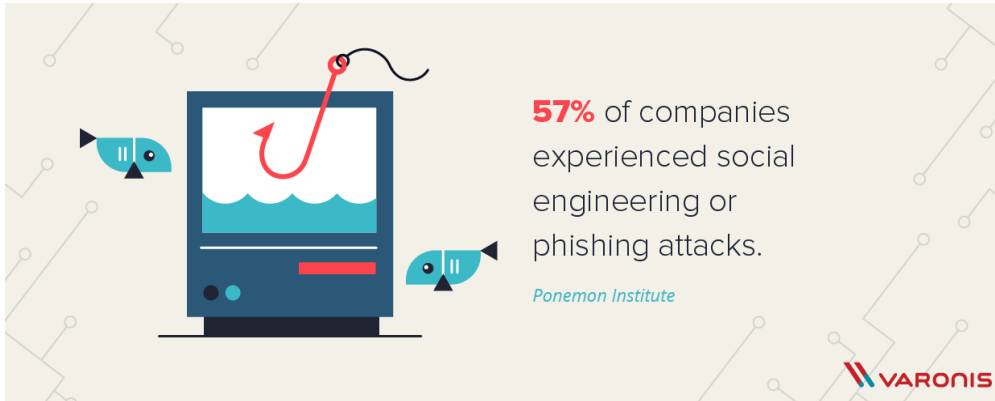
Introduction: why cyber laws are needed

Always A Pioneer, Always Ahead

- This dependency places us in a precarious position because cyberspace is borderless and vulnerable to cyber attacks.
- Individuals and groups have the ability and capability to cause damage and harm to an individual, group and even a nation through cyberspace.
- Cyber attacks are also attractive because it is a cheap in relation to the costs of developing, maintaining and using advanced as well as sophisticated tools.
- Cyberlaw is needed to properly prosecute criminals of this nature.

Cyberattacks: Worrying statistics

Always A Pioneer, Always Ahead



More worrying statistics...

Always A Pioneer, Always Ahead

“ CYBER CRIME IS QUICKLY BECOMING MORE PROFITABLE THAN THE ILLEGAL DRUG TRADE

Source: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

“ RANSOMWARE IS THE #1 CYBERSECURITY THREAT IN 2021

Source: <https://purplesec.us/cyber-security-trends-2021/>

“ THE COSTS OF GLOBAL CYBERCRIME ARE SET TO REACH \$10.5 TRILLION ANNUALLY BY 2025

Source: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report>

“ PERSONAL DATA CAN BE PURCHASED WITHIN THE RANGE OF \$0.20 TO \$15.00

Source: <https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf>

“ IF THEY HAVE A DATA BREACH, IT TYPICALLY TAKES COMPANIES OVER 6 MONTHS TO NOTICE.

Source: <https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/>

“ AROUND 95 PERCENT OF CLOUD SECURITY FAILURES ARE PREDICTED TO BE THE CUSTOMER'S FAULT

Source: <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>

More worrying statistics...

Always A Pioneer, Always Ahead

“ THE AVERAGE COST OF A DATA BREACH FOR A COMPANY IS \$3.86 MILLION.

Source: <https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/>

“ COMPANIES ARE UNPREPARED – AND ONLY AROUND 38 PERCENT OF GLOBAL COMPANIES THINK THEY COULD HANDLE A BIG CYBER-ATTACK SHOULD IT HAPPEN.

Source: <https://www.cybintsolutions.com/cyber-security-facts-stats/>

“ A HACKER ATTACK OCCURS EVERY 39 SECONDS

Source: <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>

“ IN 2019 IOT (INTERNET OF THINGS) DEVICES WILL BECOME MAJOR TARGETS FOR MALWARE ATTACKS

Source: <https://www.beyondtrust.com/blog/entry/beyondtrust-2019-security-predictions>

“ IT'S ESTIMATED THAT 2020 WILL SEE 200 BILLION CONNECTED DEVICES

Source: <https://www.symantec.com/security-center/threat-report>

<https://www.websitehostingrating.com/cybersecurity-statistics-facts/>

Types of cybercrime

Examples of different types of cybercrime:

- Email and internet **fraud**.
- Identity **fraud** (where personal information is stolen and used).
- **Theft** of financial or card payment data.
- **Theft** and sale of corporate data.
- Cyber**extortion** (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyber**extortion**).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyber**espionage** (where hackers access government or company data).

<https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>

Definition: Cyberspace

Always A Pioneer, Always Ahead

- systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks.

(ITU National Cybersecurity Strategy Guide)

- one of five interdependent domains, the remaining four being land, air, maritime, and space.

(United States Cyber Command)

Definition: Computer crime

Always A Pioneer, Always Ahead

- computer-related crime - the use of a computer is integral to committing the offence; examples are offences such as computer-related forgery (where false data are put forward as authentic) and computer-related fraud (the fraudulent interference with or manipulation of data to cause property loss);
- computer crime - this is a general label for offences in which a computer is the object of the offence or the tool for its commission;

(Australian Institute of Criminology)

Definition: Computer crime

Always A Pioneer, Always Ahead

- Internet crime - refers to crimes in which the use of the internet is a key feature and includes content-related offences such as possession of child pornography, or in some countries, the dissemination of hate or racist material;
- e-crime - a general label for offences committed using an electronic data storage or communications device.

(Australian Institute of Criminology)

Definition: Cybercrime

Always A Pioneer, Always Ahead

- “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution”.

(US Department of Justice)

- the “use of networked computers, telephony or internet technology to commit or facilitate the commission of crime”.

(UK Association of Chief Police Officers (ACPO))

Definition: Cybercrime

- “any crime that is committed using a computer or network or hardware device”.

(Symantec Corporation)

- “offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence”.

(Australian Centre for Police Research (ACPR))

Definition Conundrum

- In Australia, cybercrime has a narrow statutory meaning as used in the *Cybercrime Act 2001* (Cwlth), which details offences against computer data and systems.
- However, a broad meaning is given to cybercrime at an international level.
- In the Council of Europe's *Convention on Cybercrime* (EST no. 185), cybercrime is used as an *umbrella term* to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences and copyright offences.

(Australian Institute of Criminology)

Definition Conundrum

- As shown, there are considerable difficulties in defining the term “cybercrime”. The term “cybercrime” is used to describe a range of offences including traditional computer crimes, as well as network crimes.
- As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the Stanford Draft Convention and the Convention on Cybercrime, whilst excluding traditional crimes that are just committed using hardware.
- The fact that there is no single definition of “cybercrime” need not be important, as long as the term is not used as a legal term.

(Cybercrime: A Guide for Developing Countries)

Definition: Cybersecurity

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
- An ongoing evaluation and monitoring of the above policies and actions in order to ensure the continued quality of security in face of the changing nature of threats.

(ITU-T Overview of Cybersecurity)

Definition: Cyberlaw

- Cyberlaw is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.
- Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law is referred to as the Law of the Internet.
- a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order.
- If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Definition: Critical Infrastructure

Always A Pioneer, Always Ahead

- “the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these
- Whilst what comprises CI varies across States, in this Guide we regard typical infrastructure sectors as including health, water, transport, communications, government, energy, food, finance and emergency services sectors.

(ITU National Cybersecurity Strategy Guide)

Definition: Critical Information Infrastructure

Always A Pioneer, Always Ahead

- Increasingly, the critical sectors also rely on cyberspace and the information and communication technologies (ICTs) that enable it.
- The Study Group classifies cyberspace and its supporting ICTs as critical information infrastructure (CII).

(ITU National Cybersecurity Strategy Guide)

Malaysia has identified the following as its Critical National Information Infrastructure (CNII):

- National Defense & Security
- Banking & Finance
- Information & Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food & Agriculture

Computer Crime / cybercrime

- “Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.”
- These categories are not exclusive, and many activities can be characterized as falling in one or more categories. The term *cybercrime* has a connotation of the use of networks specifically, whereas *computer crime* may or may not involve networks.

Computer Crime: Hard to define?

Always A Pioneer, Always Ahead

1. Creating and changing laws are slow processes
 - Which is very much out of pace with a technology that is progressing as fast as computing.
2. A computer can perform many roles in a crime
 - Computer can be the subject, object or a medium of a crime:
 - A computer can be attacked (attempted unauthorized access)
 - Used to attack (impersonating a legitimate node on a network)
 - Used as a means to commit crime (Trojan horse or fake login)

Computer Crime: Hard to prosecute?

Always A Pioneer, Always Ahead

- Why computer crime is hard to prosecute?
 - Lack of understanding
 - Lack of physical evidence
 - Lack of recognition of assets
 - Lack of political impact
 - Complexity of case
 - Juveniles

Types of Computer Crime

- the U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:

computers as targets

involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

computers as storage devices

using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

computers as communications tools

crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Article 2 Illegal access

The access to the whole or any part of a computer system without right.

Article 3 Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices

- a The production, sale, procurement for use, import, distribution or otherwise making available of:
 - i A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and
- b The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

- a Any input, alteration, deletion or suppression of computer data;
- b Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

- The Convention on Cybercrime represents an international consensus on what constitutes computer crime, or cybercrime, and what crimes are considered important.

Article 9 Offences related to child pornography

- a Producing child pornography for the purpose of its distribution through a computer system;
- b Offering or making available child pornography through a computer system;
- c Distributing or transmitting child pornography through a computer system;
- d Procuring child pornography through a computer system for oneself or for another person;
- e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

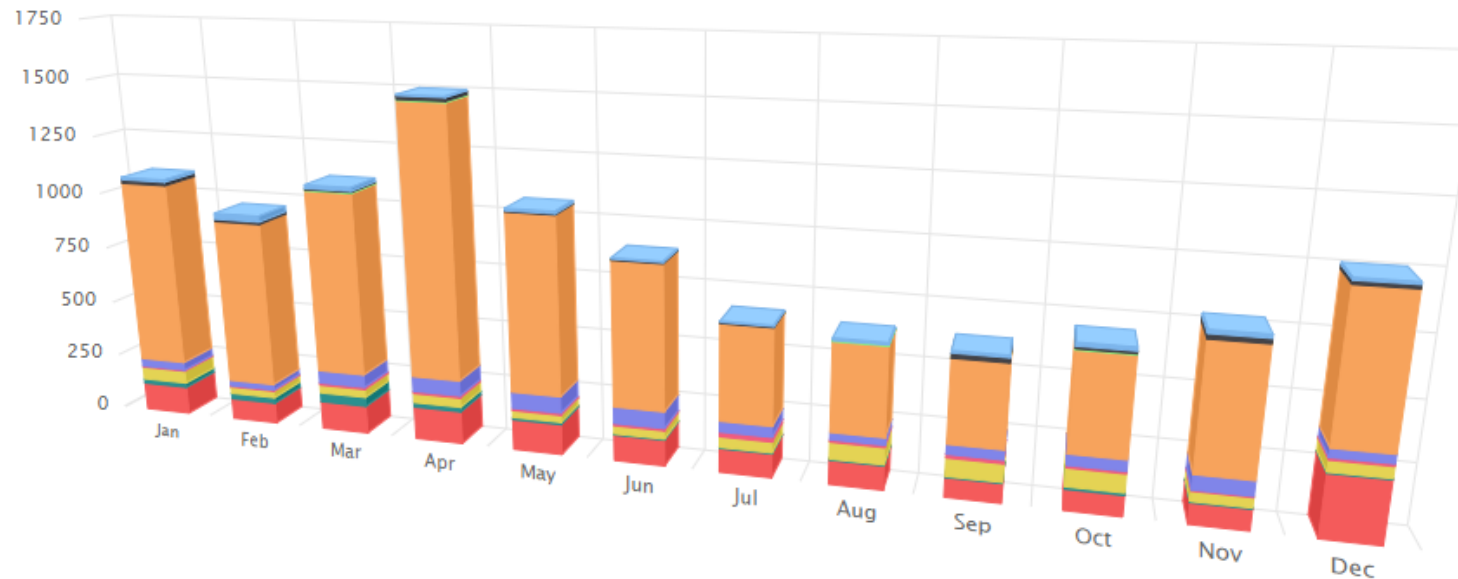
Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

The state of Cybercrime in Malaysia

Always A Pioneer, Always Ahead

Reported Incidents based on General Incident Classification Statistics 2020



Top 3 incidents:

1. Fraud
2. Intrusion
3. Cyber Harassment

Spam (blue), Malicious Codes (yellow), Intrusion Attempt (black), Content Related (teal), Denial of Service (green), Intrusion (red), Fraud (orange), Cyber Harassment (purple), Vulnerabilities Report (pink)

Malicious Codes - 232	Intrusion Attempt - 45	Denial of Service - 12
Fraud - 4,906	Cyber Harassment - 329	Intrusion - 730
Spam - 81	Content Related - 127	Vulnerabilities Report - 50

Total Incidents - 6512

The state of Cyberlaw in Malaysia

Always A Pioneer, Always Ahead

- Malaysia does not yet have a standalone Cybersecurity Law, but several sporadic laws in this area exist to counter cybercrimes:
 - Computer Crimes Act 1997
 - Digital Signature Act 1997
 - Copyright (amendment) Act 1997
 - Communications and Multimedia Act 1998
 - Electronic Commerce Act 2006
 - Electronic Government Activities Act 2007
 - Personal Data Protection Act 2010
 - Penal Code
 - Anti-Fake News Act 2018 (repealed)
 - Telemedicine Act 1997
 - Sedition Act 1948
 - Case laws
 - Other specific guidelines/policies

Computer Crimes Act 1997

Always A Pioneer, Always Ahead

- Why it exists:
 - As computing becomes more central to people's life and work, computers become both targets and tools of crime. This Act serves to ensure that misuse of computers is an offense.
- What the act is about:
 - The Act makes it an offense to:
 - Enter or attempt to enter into computers and computer systems without authorization;
 - Damage or alter data/information in computers or computer systems by planting viruses or other means;
 - Aid others in committing the above two offences;
 - Give passwords to people who are not authorized to receive it.

Digital Signature Act 1997

Always A Pioneer, Always Ahead

- What the act is about:
 - Provides for the regulation of the public key infrastructure.
 - The Act makes a digital signature as legally valid and enforceable as a traditional signature.

Copyright (amendment) Act 1997

Always A Pioneer, Always Ahead

- Why it exists:
 - Copyright serves to protect the expression of thoughts and ideas from unauthorized copying and/or alteration.
 - With convergence of Information and Communication Technology (ICT), creative expression is now being captured and communicated in new forms (example: multimedia products, broadcast of movies over the Internet and cable TV). These new forms need protection.
- What the act is about:
 - Amends the Copyright Act 1987 to extend copyright law to the new and converged multimedia environment.
 - There is now clear protection accorded to multimedia works.
 - The transmission of copyright works over the Internet now clearly amounts to infringement.
 - Technological methods of ensuring works (and authorship info) are not altered or removed is also protected.

Telemedicine Act 1997

- Why it exists:

- Healthcare systems and providers around the world are becoming interconnected. People and local healthcare providers can thus source quality healthcare advice and consultation from specialists from around the world, independent of geographical location.
- Conversely, interconnectivity also allows for non-quality healthcare advice and consultation from around the world. The Act serves to regulate the practice of tele-consultations in the medical profession.

- What the act is about:

- The Telemedicine Act 1997 is intended to provide a framework to enable licensed medical practitioners to practice medicine using audio, visual and data communications.
- The Act provides that any registered doctor may practice "telemedicine" but other healthcare providers (such as a medical assistant, nurse or midwife) must first obtain a license to do so.
- To date, the Telemedicine Act has yet to be enforced.

- Why it exists:

- Convergence of technologies is driving convergence of telecommunications, broadcasting, computing and content.
- Previously, each of these industries was regulated by several different pieces of legislation.
- The old regulatory framework cannot cope with convergence and inhibits the growth of the new converged industry.

- What the act is about:

- The CMA provides for a restructuring of the converged ICT industry.
- Creates a new system of licenses and defines the roles and responsibilities of those providing communication and multimedia services.
- Provides for the existence of the Communication and Multimedia Commission, the new regulatory authority.

- **Electronic Commerce Act 2006**

- An Act to provide for legal recognition of electronic messages in commercial transactions, the use of the electronic messages to fulfill legal requirements and to enable and facilitate commercial transactions through the use of electronic means and other matters connected therewith.

- **Electronic Government Activities Act 2007**

- An Act to provide for legal recognition of electronic messages in dealings between the Government and the public, the use of electronic messages to fulfill legal requirements and to enable and facilitate the dealings through the use of electronic means and other matters connected therewith.

- **Personal Data Protection Act 2010**

- An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.

Other acts...

Always A Pioneer, Always Ahead

- Penal Code
 - An Act relating to criminal offences.
- Anti-Fake News Act 2018
 - An Act to deal with fake news and related matters.

Enforcement Bodies

Always A Pioneer, Always Ahead

- Malaysian Communications and Multimedia Commission (MCMC)
- Personal Data Protection Commission (PDPC)
- Royal Malaysian Police (RMP)
- Ministry of Domestic Trade, Co-operatives and Consumerism

Thank You



www.utem.edu.my