CYBERCRIME AND SECURITY

Various Cybercrime Offenses

Cybercrime is committed in *cyberspace* using information and communication technologies such as televisions, smartphones, computers, networks, and other communication devices.

Cybercrime Categories

These are the four categories fitting the definition of cybercrime:

- Cyber-enabled offenses.
- Cyber-dependent offenses.
- Computer/cyber-supported offenses; and
- national security offenses or cyberterrorism.

Every category can be broken down into specific subtypes of criminal activities which fall under each one.

Cyber-Enabled Offenses

These are offenses committed with or without technology but increased their reach using such technologies. These cybercrimes are also described as "*technology-as-instrument*" offenses.

- ***Identity theft*** – refers to obtaining or possessing another's identity and information to commit a legal offense.
- ***Identity fraud –*** refers to the fraudulent impersonation of someone to gain an advantage, obtain property, cause a disadvantage, or avoid prosecution.
- ***Phishing*** – refers to luring users to log onto a fake website that appears real to gather sensitive information, such as the user's password, account number, ATM PIN, and credit card.
- ***Cyberbullying and Online Harassment**:* Online tools and social media applications are used to harass, intimidate, or embarrass another person or other identifiable groups.

Cyber-Dependent Offenses

These are offenses that are strictly committed using information and communication technologies. Cyber-dependent crimes target network systems and data confidentiality, integrity, and availability.

- ***Hacking* –** refers to someone manipulating a computer system or private network to access digital files or systems without proper authorization. Hacking can be classified into five categories:

  1. **Unauthorized access** – refers to gaining logical or physical entry to a network, data, website, program, or another system, without proper authorization or credentials
  2. **Modification of data** – refers to inserting, removing, or altering data without proper authorization.
  3. **Impairment of data** – refers to disrupting the transmission or communication of data.
  4. **Interception of data** – refers to the unauthorized access and alteration in the data transmission between machines for personal or financial gain.
  5. **Misuse of assets** – refers to the unauthorized use of company files, systems, computers, and networks to damage the company's properties.

- ***Cyber-attack**:* These are attacks that use computers against other computers or networks to modify, steal, or gain information through unauthorized access. An insider or an outsider can initiate an attack.

  1. **Inside attack** – an attack from inside the security perimeter, also called "*insider*."
  2. **Outside attack** – an attack from outside the security perimeter or the system, also called *"outsider*."

- ***Malware*** – or *malicious software- is* software-based hacking and cyber-attacking tools. The difference between malware and software is that malware is intentionally malicious.

  These are some of the usual types of malware:

  1. **Virus**: This is designed to spread from one program to another, which can self-replicate. When a virus is executed, it replicates itself by changing other computer programs, documents, or boot sectors.
  2. **Worm:** Unlike viruses, this standalone malware replicates itself without human intervention. It uses a computer network to spread itself by depending on the security failures of the targeted computer to access it.
  3. **Trojan –** *trojan horse* or *trojan virus*, appears as a legitimate program when downloaded to a computer. It can be found on file-sharing sites, email attachments, sketchy websites, and hacked Wi-Fi networks.
  4. **Spammer –** sends massive amounts of unsolicited commercial emails to illegally acquired email addresses. While this is illegal, these programs are not fundamentally destructive.
  5. **Spyware –** used to perform illegal activities such as creating malicious pop-up advertisements, capturing banking login details, and taking screenshots of the visited websites.

Computer/Cyber-Supported Offenses

These offenses deal with the illegal use of computers for data storage, documentation, and communication. Computer/cyber-supported offenses are instances wherein the use of the computer or network is not vital to the actual crime but may still be legally relevant to be considered as evidence or as an accessory to the crime.

National Security Offenses

These are considered **cyberterrorism**, an umbrella term for unlawful offenses that commit terrorist activities or engage in terrorism against computers, networks, and the information stored therein. It is the conjunction of terrorism and cyberspace.

Categories of Cyberterrorism

1. **Incursion** – sudden invasive attacks targeting computer information systems, networks, infrastructure, or personal electronic devices.
2. **Destruction** – an umbrella term for destroying digital data where it becomes unreadable, inaccessible, or susceptible to unauthorized purposes
3. **Disinformation** – refers to the intentional dissemination of false information to mislead, confuse, or manipulate an audience.
4. **Distributed Denial of Service (DDoS)** – refers to malicious attempts from multiple machines to disrupt computer networks by temporarily or indefinitely making them inaccessible.
5. **Defacement of Websites** – refers to malicious attacks targeting websites to replace their content with the attacker's message. These offenses convey political or religious messages, profanity, and other inappropriate content.

Penalties

Any person or group found liable for any of the offenses in **Cyber-enabled,** and **Cyber-enabled offenses** are punished with ***prision mayor*** which is six (6) years and one (1) day to 12 years of imprisonment or a fine of at least P200,000.

Specifically, any person found liable for offenses of **Misuse of Assets** is punished with *prision mayor* or a fine of not more than P500,000 or both.

If offenses in **Cyber-enabled offenses** are committed against critical infrastructure, ***reclusion temporal*** which is 12 years and 1 day to 20 years of imprisonment, or a fine of at least P500,000 up to the equal amount of the damages is imposed.

Lastly, if the person is found liable for **Computer/Cyber-Supported** and **National Security Offenses**, imprisonment one (1) degree lower than the advised penalty for the offense or a fine of at least P100,000 but not exceeding P500,000 or both is imposed.

Cybersecurity Technologies

Cybersecurity is securing computer systems, networks, and programs from any cyber-attack. It is one of the fastest-growing global challenges that is becoming increasingly important to address, with its enormous implications for government security, economic prosperity, and public safety.

Cybersecurity Technologies

Here are some of the different cybersecurity classifications affecting information systems and technology.

Encryption

It takes plain text, such as a message or an email, and codes it into an unreadable format. It protects the user from illegal and unauthorized access and various malicious attacks.

The technology of encrypting and decrypting information is called **cryptography,** while unencrypted data is called ***plaintext****.* The encrypted data is called ***ciphertext***.

Encryption is encoded using ***encryption keys***, which are part of specific algorithms. The encrypted data appears as a meaningless language only readable by a person with a ***decryption key*** used to decrypt data to make it readable again.

To further understand encryption, think of unencrypted authentication credentials saved in a database. Anyone with authorization can easily access confidential and private information. Encryption allows users' private information to remain safe from hackers and cyber-attacks.

Various technologies are used to encrypt data, such as *RSA* (Rivest–Shamir–Adleman), *Triple Data Encryption Algorithm* (TDEA), *Blowfish* (cipher), and *Twofish* (cipher).

Authentication

It is a technique to validate the identity of an end user or a computer program. Nowadays, personal identification numbers (PINs), driving licenses, and government IDs are used for authentication.

To better understand authentication, think of immigration and customs. When traveling to another country, a valid passport is required. Immigration officers will inspect the passport to ensure it is not forged or falsified. This process is similar to the elements of authentication.

Various authentication technologies include *digital certificates*, *access tokens*, and *security keys.* A combination of PINs and security questions is mainly used these days.

Biometrics

It assures good security as an individual’s physical and behavioral traits are permanent and unique. Unlike security keys and passwords, physical and behavioral traits are harder to lose and duplicate.

Biometrics disregard the use of cards and passwords to open a door but now recognizes the body's eyes, fingerprints, face, and other characteristics. It is also used for banking, education, cars, and health care.

Various biometrics technology includes *optical scanners, ultrasonic scanners, capacitive scanners,* and *voice scann*ers.

Firewall

It is the barrier between networks implemented in software, hardware, or cloud-based applications. It serves as the first line of defense utilized for blocking inbound specific packet types from reaching the protected network and for eliminating unauthorized data access to defend the network.

To better understand the concept of a firewall, imagine a wall around a city that prevents people and merchandise from getting in and out of the town. Inspectors check people and packages that want to get in or out based on city policies. Similarly, a firewall controls the system based on IT professionals' policies.

Sample technologies include *Network Address Translation (NAT)*, *packet-filtering*, and *Virtual Private Networks* (VPNs).

Virus Detection

Antivirus or anti-malware software for computers prevents, detects, and removes any malicious software. It helps users isolate the infected file from cyber-attacks like ransomware, trojan horses, phishing, and DDoS attacks.

Antivirus scans new programs or files as soon as they are installed or entered into the system. The ones that match the virus signatures are flagged as infected programs or files, which are then blacklisted or isolated.

Virus detection technologies include *on-demand scans, on-access scans, boot-time scans,* and *web protection,* depending upon the type of operating system and the platform on which they operate.

Phishing Detection

As phishing models evolve, phishing detection technologies for identifying and preventing attacks now use the same characteristics that attackers use:

- ***Visual Similarity-Based Phishing Detection* –** it targets the visual likeness of the phishing sites. The visual representations of the legitimate websites are stored in a database wherein the malicious website in question crosses the similarity threshold.

  If the extreme similarity between legitimate and malicious websites exists, the malicious website presumably pretends to be a legitimate website to trick users.

- ***Blacklist-Based Phishing Detection*:** Most blacklist-based phishing detection technologies keeps a database of approved and unapproved URLs.

  Suppose a sender's internet protocol or internet service provider has been blacklisted. In that case, users cannot send emails from that email address using various email servers such as Gmail and Hotmail.

- ***Web Crawling-Based Phishing Attack Detection (WC-PAD):*** When the user visits a website, the first thing that WC-PAD checks is whether the website link is in the DNS blacklist.

  If the link is blacklisted, a warning informing the status of the website is sent to the user. But if the website does not match any link, then the software will search the website and check every link present to find faults in the web index. If any links are found wrong, then a warning will be sent to the user.

References:

Department of Justice (2012) *Republic Act No. 10157.* [PDF file]. Retrieved on July 19, 2022, https://www.doj.gov.ph/files/cybercrime_office/RA_10175-Cybercrime_Prevention_Act_of_2012.pdf

Department of Justice (2012) *Rules and regulations implementing Republic Act. No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012."* [PDF file]. Retrieved on July 19, 2022, https://www.doj.gov.ph/files/cybercrime_office/Rules_and_Regulations_Implementing_Republic_Act_10175.pdf

Lukings, M. & Lashkari, A. (2022). *Understanding cybersecurity law and digital privacy: A common law perspective.* Springer.

Moallem, A. (2022). *Understanding cybersecurity technologies: A guide to selecting the right cybersecurity tools*. CRC Press*.*