Tutorial 6: Online Crime and Real Punishment

Part 1

1. Explain how satellite technology helps in military warfare? How can the terrorists misuse the satellite technology in warfare? (PIC: Yit Wee)

Helps:

It can help for **early warning** related to movements and redeployment by enemy forces, **gathering of and communicating** to the appropriate agency all the intelligence information obtained on enemy forces both through electronic and signal intelligence, **provide speedy and efficient communication** links to own and other friendly forces deployed against the enemy in the remotest.

- Reconnaissance - can help the army with intelligence gathering and surveillance because of the view from space.
- Navigation - help many precision-guided weapons use the global positioning system (GPS) satellite constellation or laser guidance, some weapons such as unmanned Predator drones
- Military communications - They are deployed in geostationary orbit and provide wideband, narrowband and protected military communication systems. Protected systems offer more sophisticated security protection like antijam features and nuclear survivability.
- Potential delivery of offensive systems (attack)- cruise missiles may also transmit live video footage or receive updated target information via satellite, ballistic missiles attack

Misuse:

Terrorist may **steal the important data** from the country they want and sell to other country. Next, terrorist may **become spy** in the country they want. Example satellite-data-driven tools such as Google Earth are also now being used by terrorists to help plan their attacks.

2. Compare the advancement of computing and communication technologies between today's war news reporter and the previous generation. (PIC: Chia Chung)

Previous Generation:

- We took time to process the photos and films.
- Propagated via offline methods such as fax, call, wait for war reporters to come back and report as well as be told on the radio.
- Printed out the newspapers and sent it out.
- Delay information delivery to people compared to nowadays.
- Professional training is needed to be gone through for the war reporters.

Today:

- Digital cameras allow war reporters to capture and send out immediately as well as upload the photos and videos to the cloud.
- Drone shooting to prevent war reporters from accidents on the battlefield.
- Live streams on multiple platforms such as social media allow citizens to report war news instantly.
- The emergence of "amateur reporter / citizen reporter" ---public/citizen reporter who reports the war news (everyone can be the news reporter provided there have the gadget/devices and access to the Internet, post the news onto the internet immediately such as live broadcast, tv news and so on).

3. In your opinion, what are the three factors that contribute to a system's security weaknesses? Do you agree that hiring a white hat hacker can help to improve a company's security? Justify your answer. (PIC: Jun Rong)

Weak user authentication

- User authentication weaknesses in legacy control systems often include hard-coded passwords, easily cracked passwords, passwords stored in easily recoverable formats, and passwords sent in clear text. An attacker who obtains these passwords can often interact with the controlled process whenever they want.

Operating System Vulnerabilities

- These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on or to cause damage to it. Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.

Network Vulnerabilities

- These are issues with a network's hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.

Outdated hardware which are unable to handle modern network security threats

- This hardware may operate too simplistically or lack the processing power and memory to handle the threat environment presented by modern network technology.

Human nature

- An employee that has been working in the company for years already got familiar with the operation of the system and they can simply atack or steal the data from the system without anyone knowing.
- An employee who always sticks to the same password instead of changing it frequently may be the target of a hacker or other individuals. Since the same password is used for multiple accounts or systems, once the other individuals get to know the password, they can simply gain access to the system and perform some unethical and illegal actions.

Complexity of the computer system

- It is hard to manage the system if the system is having some error and make it easy for the hacker to hack into the system.

Speed at which new applications develop

e.g. whenever the new application/the new “version” of such application release into the market too often/too frequent (in which such a short time gap between the 2 similar product/ prior and later version of the same product) may invite user doubt/confusion in which user may worry that there may be some hidden bugs/error since insufficient time to undergo testing/insufficient testing/insufficient R&D carried out before such new feature/function had been launched to the market

Yes, I do agree that hiring a white hat hacker can help to improve a company’s security. It is because the white hat hacker would build new attack techniques much like their black hat counterparts. By using these techniques, they can root out any vulnerabilities that could be exploited by someone, especially those with malicious intentions.

One method white hat hackers utilize is called **penetration testing**. This is a simulated attack on a company’s network either manually or through the use of a computer program whereby the hacker will find a way in, scan the network, steal as much data as possible, and then leave without a trace. The hacker will note how they achieved each goal. In other words, they’ll point out each fault in the network and pass those vulnerabilities along to the network administrator.

White hat hackers can also use other attack methods, such as social engineering tactics like phishing, in which they will email a company’s staff in an attempt to gather passwords or any other sensitive data.

In conclusion, white hat hackers can and will find the holes in your security you and your staff may not be able to see.

Part 2

1. Businesses are becoming increasingly aware of cybercrime threats and are boosting investment to protect themselves. However, employees are also playing a very important role in combating cyber attacks. Discuss FOUR (4) ways you, as an employee, can help to protect your company from cybercrime. (PIC: Ming Jun)

1. **Teach employees to spot suspicious emails**

   Train employees to identify phishing scams and teach them not to open the email if the sender has an unfamiliar email address even if it appears to be from a reputable source. They should also be leery of emails that contain grammatical or spelling errors.

2. **Communicate best practices for selecting passwords**

   Simply having employees pick better passwords can prevent many cybercrimes. Employees are highly encouraged to make their passwords a little more complex than usual as it is very helpful to prevent cyber attacks. The password should include punctuations, uppercases, lowercases, and numbers. Employees are also encouraged to change their passwords regularly. For example, once per month.

3. **Set policies for guarding sensitive business information**

   Craft and communicate protocols for protecting user names and passwords. The company should institute a policy that no employee can use a company computer or specific systems without first getting security training.

4. **Maintain physical security of the company and personal devices**

   Employees are encouraged to keep external doors and file server rooms locked, and to refuse unauthorized entry to strangers. If a hacker can get into the business and sit down at a terminal, it’s much easier to break into a network.

5. **Always Back-up the company data**

   Employees should be taught to always back up their data so that the company will not face big challenges when the company is facing ransomware attacks as the company can just load all the backup data back into the company's systems.

6. **Never connect to unknown/public connection points**

   Some connection points at the public area have been configured manually by the individual with malicious intention to steal personal information, such as account number, and password.

7. **Encrypt important information before sending online**

   Encryption the document into a secret code before sending it out over the internet because it can reduce the risk of theft, destruction by third parties. For example, turn on the network encryption through the router setting or install the virtual private network (VPN) on the device when using the public network.

8. **Avoid jailbreaking and rooting**

   By rooting the smart gadgets, especially smartphones, the privilege of having full access to the handset is not only limited to the owner, but also certain viruses. The viruses can gain unlimited access to all the private information managed through the phone. As a result, the device becomes much more vulnerable to malware which may cause a lot of problems to the user.

https://www.spectrum.com/business/insights/management/5-ways-your-employees-can-help-prevent-cyberattacks/

==

2. Propose ways to avoid being a victim of cybercrime? (PIC: Yih Feng)

1.**Keep software and operating system updated**

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

2.**Use anti-virus software and keep it updated**

Using anti-virus or a comprehensive internet security solution like Kaspersky Total Security is a smart way to protect your system from attacks.

Anti-virus software allows you to **scan, detect and remove threats** before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you peace of mind.

If you use anti-virus software, make sure you keep it updated to get the best level of protection.

3.**Use strong passwords & regular update of password**

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

4.**Never open attachments in spam emails**

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

Hands typing on laptop keyboard

5.**Do not click on links in spam emails or untrusted websites**

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

6.**Do not give out personal information unless secure**
Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

7.**Contact companies directly about suspicious requests**
If you get asked for data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal.

Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialed, they can pretend to be from the bank or other organization that you think you're speaking to.

8. **Cookie management** - Turn on cookie management feature to block use of third party cookies that store the user login credentials as well as on-site browsing activities data. In the cases of cookies being allowed, a user should regularly keep track of cookies stored in the browser and remove unknown cookies or cookies from suspicious sites.

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

3. Do online research. Discuss the law in Malaysia that can be used to take legal action against the following offences:

(i) Making obscene/indecent/false/menacing/offensive statements online (PIC: T'nsam)

Communications and Multimedia Act (CMA) 1998 has two main provisions to be used in taking action on content-related matters, namely **Section 211(Prohibition on provision of**

offensive content) and **Section 233(Improper use of network facilities or network service)**. In Malaysia, Section 211 and 233 of the CMA 1998 regulates offensive content on the internet. Section 211 and 233 CMA is very broad to describe the offensive content on the internet, but it's subject to the court's assessment whether the content falls under the types of offensive content on the internet.

Under Section 211, a person who contravenes subsection (1) commits an offense and shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day or part of a day during which the offense is continued after conviction.

Under Section 233, a person who commits an offense under this section shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day during which the offense is continued after conviction.

References: 2. What is MCMC's jurisdiction in addressing complaints about offensive content in the Internet?
(PDF) Offensive Content on The Internet: The Malaysian Legal Approach

(ii) Hacking (PIC: Kai Yuan)

The **Computer Crimes Act 1997 ('CCA')** is the first ever specific legislation enacted in Malaysia to counter cybercrimes. The criminal includes acts of hacking, or, in technical terms, unauthorized access to computer material, whether or not with intent to commit further offence. For example, the case of Basheer Ahmad Maula Sahul Hameed v PP (2016) which involves the use of debit cards belonging to the victim of MH 370 incident by a bank staff to withdraw cash from the ATM and transferring money without authorization.

CCA captures hacking activities such as creating viruses or malware for the purpose of hacking, hacking into Wi-Fi connections or credit card information by using hacking tools, denial of service attacks, electronic theft etc.

Elaborate more Punishment involved ….

Basics of cyber security law in malaysia

(iii) Phishing (PIC: Jun Wai)

There are no specific provisions against crime such as phishing in Malaysia. However, there is **Section 416 of Penal Code** that is provided against such crime such as pretending to be someone else in order to cheat or deceive others. This offense carries the jail term up to five years or with fine (e.g min or max range, how much …), or with both upon conviction, according to **Section 417 of Penal Code**.

Basics of Cyber Security Law in Malaysia

(iv) Online harassment (PIC: Mun Jun)

Internet users who feel they are being harassed online should lodge a complaint against the perpetrator(s) to the operator of the social media platform (Facebook, Instagram and others) and the police so that action can be taken under **Section 233 (1) of the Communications and Multimedia Act.**

This section states that it is deemed an offence if a person "by means of any network facilities or network service or applications service knowingly makes, creates or solicits; and initiates the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person".

Section 233(3) states that those convicted under the Act face a maximum fine of RM50,000 or a maximum one-year jail term or both, as well as a further fine of RM1,000 for every day the offence continues after conviction.

Specific law needed to stem cyberbullying

(v) Online spreading of terrorist propaganda (PIC: Yee Hui)

Online spreading of terrorist propaganda or activities using social media is a serious criminal offence under section **130J Penal code**. In Penal code 130J, any terrorist organization or committing terrorist acts will be punished with imprisonment for life or imprisonment not exceeding 30 years or with fines (RM25,000 to RM150,000). Besides that, the offender's property will be confiscated. Back in 2016, we saw a few Malaysians charged under this provision for spreading Islamic State of Iraq and Syria (a.k.a. ISIS) propaganda.

Penal Code Section 130J (Malaysia) (burgielaw.com)
https://m.akmylaw.com/?ws=services&cid=3103&sid=14520
ISIS Recruitment of Malaysian Youth: Challenge and Response | Middle East Institute (mei.edu)