EMERGING TECHNOLOGIES:

Understanding Cybersecurity: Challenges and Solutions

LEADER

Frencillo, Francine Lia T.

MEMBERS

Barbosa, Shanika Maureen D.

Galang, Alliah Gabrielle S. R

Salanatin, Nathaly Pearl F.

I. Introduction and Background

Technology refers to the tools, systems, and processes that are developed to solve problems or meet human needs. Its benefits have become a vital part of our life. It has improved and is still improving the efficiency of medicine, transportation, education, entertainment, and more. Technology has minimized both time and labor while increasing the efficiency of production needs. Technology has made our lives easier, more comfortable, healthier, and more pleasurable. The time before the late 20th century gathering information was long and tedious. To get a book that the library did not own would take at least a couple of weeks depending on the time or it may not have been possible to obtain that book. But now people can access a vast amount of information in a matter of minutes.

In today's world, the advancement of technology, along with science, has helped us to become self-reliant in all spheres of life. With the innovation of a particular technology, it becomes part of society and integral to human lives after a point in time. As technology continues to evolve and become more intertwined with our daily lives, technology has also brought along a variety of negative effects that we cannot overlook. Cybersecurity, on the other hand, will continue to play a critical role in ensuring that it is used safely and ethically.

Cyber security is the use of technology, practices, and policies to defend against cyber assaults on systems, networks, programs, devices, and data (National Institute of Standards and Technology, 2020). It aims to reduce the risk of cyber assaults and safeguard against unauthorized use of systems, networks, and technology. It is an essential component of modern civilization, and there has never been a greater need for robust cybersecurity measures (Marsden, 2021). Without cybersecurity, technology could be vulnerable to cyber-attacks such as hacking, malware, and phishing frauds. The consequences of a cyber-attack can be severe, including financial losses, damage to reputation, and potential harm to individuals or society at large (Boyd & Crawford, 2012).

II. Objectives

We cannot escape technology; it has improved the quality of life and brought about revolutions in various fields of modern-day society. It is important to distinguish between unanticipated and undesired consequences when using modern technology. Cybersecurity Technology is designed to ensure the confidentiality, integrity, protecting sensitive information, such as personal data, financial information, trade secrets, and intellectual property, from cyber threats such as hackers, viruses, and malware, which are essential for businesses, governments, and individuals to function in today's interconnected world.

The researcher wants a good environment to implement a user awareness and training to cybersecurity to protect private and personal digital assets: As people's reliance on technology grows, cyber assaults on personal and organizational data have become a significant threat. Those who learn cybersecurity get the knowledge and skills necessary to secure digital assets (Private accounts, Emails, Banks, and their Devices.) from cyber-attacks. Learning cybersecurity can promote a culture of cybersecurity awareness and best practices on staying ahead of evolving cyber threats. Overall, learning and as well implementing cybersecurity provides benefits.

The purpose of this paper is to give awareness how the changing nature of security dangers is one of the most difficult aspects of cybersecurity. As modern technologies emerge, new attack avenues are developed. To keep up with changing security risks, a more initiative-taking and adaptive approach is necessary. It can also help individuals and organizations develop a comprehensive cybersecurity strategy that addresses both technical and non-technical aspects of security.

III. Scope

The study of cyber security titled "Understanding Cybersecurity: Challenges and Solutions" will only review the most commonly known different types of cyber threats, providing its solution and prevention from the threat, including an example for each threat to further understand its work. The study will also discuss the enforced cyber laws of the Philippines and its purpose. The study also acknowledges the cyber threats encountered by the Filipino citizens currently.

IV. Cybersecurity

Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies. Cybersecurity is continually challenged by hackers, data loss, privacy, risk management and changing cybersecurity strategies. What are the top cybersecurity challenges? Cybersecurity is continually challenged by hackers, data loss, privacy, risk management and changing cybersecurity strategies. The number of cyberattacks is not expected to decrease in the near future. The following are commonly known cyber threats and its solutions and prevention:

1. Malware short for "Malicious Software" and used to describe software that enables an attacker to hack, damage, or exploit one or more systems or computer networks.

Malware comes in a variety of forms, each with unique traits and objectives.

Typical forms of malware include:

1.1 Viruses: Virus is a form of malware that links to another program and multiplies and spreads once it has been launched on a system. The first known computer virus, called "Creeper," was created by Bob Thomas in 1971.

Viruses come from these sources:

1. Opening suspicious email attachments.
2. Attaching unsecured removable or external storage devices (e.g., flash drives, external hard drives, memory cards)
3. visiting a malicious web page

(e.g., you could receive a random email with malicious attachment to it, open the file unknowingly, and then the computer virus runs on your computer.)

Here are some common types of viruses:

1. **File Infector Viruses**: It attach themselves to files such as .exe or .dll files, and modify the host files to include their own code. When the infected file is executed, the virus activates and may further spread to other files on the system.
2. **Macro Viruses**: It primarily target productivity software, such as word processors or spreadsheet applications. They infect documents or templates that contain macros and use the macro scripting capabilities to execute malicious actions when the document is opened, or macros are enabled.
3. **Multipartite Viruses**: It can infect both files and the boot sectors of storage devices. It combine the characteristics of file infectors and boot sector viruses, enabling them to spread through multiple attack vectors and making them more challenging to detect and remove.

Prevention:

1. Install antivirus or anti-malware software - It's essential to keep your PC virus free.
2. Run antivirus scans regularly.
3. Exercise Caution with Email Attachments
4. Practice Safe Browsing Habits

Solution

1. Download and install a virus scanner
2. .Disconnect from internet
3. Reboot your computer into safe mode
4. Delete any temporary files
5. Run a virus scan
6. Reboot your computer
7. Change all your passwords
8. .Update your software, browser and operating system)

1.2 **Trojans**: Trojan is a form of malware that pretends to be legitimate software but can take control of your computer and perform to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. John Walker is commonly credited for inventing the first trojan virus, back in 1975.

Trojans come from these sources:

1. Infected websites
2. Hacked Wi-Fi
3. File-sharing sites
4. Email attachments

(e.g., you click a banking website that looks legitimate; enter your info and such. With the stolen banking credentials, the attacker can initiate fraudulent transactions, transfer funds, or compromise online banking accounts, resulting in financial loss for the victims.)

Common types of Trojan

1. **Backdoor Trojan**: A backdoor Trojan installs a backdoor program without your knowledge. The program then gives the malware creator remote access to your device.

2. **Banker Trojan**: A banker Trojan is any Trojan that steals financial information or online banking credentials.
3. **FakeAV Trojans**: FakeAV Trojans masquerade as legitimate antivirus software. It don't actually protect your devices from malware, of course; they fake the detection of malware and extort money in exchange for its deletion.
4. **Trojan-PSW**: In malware terms, "PSW" stands for "password stealer," which is exactly what Trojan-PSW is. It steals passwords and login credentials from infected computers.
5. **Trojan-Notifier**: Trojan-Notifier usually accompanies another malware program. Its purpose is to alert the attacker of events related to the malware. For example, when a user installs a backdoor program, the Trojan-Notifier tells the attacker to begin the attack.

Prevention:

1. Educate Employees - Arming your staff with the necessary knowledge they need to practice secure browsing and email habits can prevent a lot of malware attacks.
2. Never download or install software from a source you don't trust completely.
3. Never open an attachment or run a program sent to you in an email from someone you don't know.
4. Always remember to legit check.

Solution:

1. Reboot your computer in Safe Mode
2. Install your antivirus and make sure it updates to the latest version.
3. Run a full system sweep.
4. Safe backup.
5. Format everything & reinstall

1.3 Spyware: Spyware is a form of malware that is installed on user computer device without consent. The device is invaded, sensitive data and internet usage statistics can be stolen, and they are then relayed to advertising, data companies, or outside users. The origins of spyware can be traced back to the late 1990s and early 2000s when the internet became more widely accessible, and online advertising started to gain traction.

Spyware come from these sources:

1. Freeware and Shareware
2. Malicious Ads and Pop-ups
3. Infected Removable Media
4. Malicious Websites

(e.g., one of the known example of spyware is the Kdrama movie named "UNLOCKED" it was released this last February 2023, the movie shows when the main character lee na-mi losses her phone, but she luckily gets her phone back allowing Jun-yeong (Yim Si-wan) the one who found her phone to destroy her life through spyware without permission)

Common types of spyware:

1. **Mobile spyware** - When a smartphone or tablet gets infected with mobile spyware that is side loaded with a third-party app, the phone's camera and microphone can be used to spy on nearby activity, record phone calls, and log browsing activity and keystrokes. The device owner's location can also be monitored through GPS.
2. **Keyloggers** – It is designed to capture computer activity, including keystrokes, websites visited, search history, email discussions, chat-room dialogue, and system credentials.

3. **Remote Access Trojans** (**RATs**) - RATs are potent spyware tools that provide attackers remote access to a compromised device. They can record audio, take screenshots, keep track on user activity, and even operate the webcam or microphone.

Prevention:

1. Don't download files unless they come from a trusted source.
2. Use a reputable cyber security program to counter advanced spyware. In particular, look for cyber security that includes real-time protection.
3. Mouse-over links before clicking on them and make sure you're being sent to the right webpage.
4. Be Cautious with Pop-ups and Advertisements

Solution

1. Make sure your system has been cleaned of any infection so that new passwords are not compromised.
2. Get yourself a robust cyber security program with a reputation for aggressive spyware removal technology
3. Think about contacting law enforcement and/or make a public disclosure.
4. Activating a credit freeze is definitely a good idea.

1.4 Ransomware: Ransomware is a form of malware that is used by hackers for cyber extortion.

Ransomware come from these sources:

1. **Phishing Emails** - These emails often contain malicious attachments or links that, when clicked, initiate the ransomware download or installation.
2. **Malvertising** - These advertisements may lead users to websites that contain malware or may cause their computers to download ransomware without their knowledge.

3. **Exploit Kits** - Exploit kits can use these vulnerabilities to distribute and install ransomware on your machine if your software is out of current with the most recent security updates.

(e.g., The hackers hold the files or computers of the victims' hostage through encryption while demanding ransom in exchange for releasing the devices or decrypting the files.) TeslaCrypt was a Trojan Horse Cryptovirus that targeted 185 game files of 40 popular games like the Call of Duty series, World of Warcraft, Minecraft, World of Tanks, etc. The ransomware targets save data, player profiles, custom maps, and game modifications stored on the target's hard drive. The later versions of TeslaCrypt also encrypted Word, PDF, JPEG, and other file types. It prompted the victims to pay a $500 ransom to get the decryption key.

Prevention:

1. Control access to essential data - Enforcing Identity and access management in ransomware attacks can easily protect your company assets against the growing threats of hacking, phishing, and malware attacks.
2. Backup your systems - Backing up your systems will keep your data safe in a place where cybercriminals are less likely to access, but it'll also make it pretty easy to wipe out your old files and repair using backup data in the event of an attack.

Solution:

1. Take a Photo of the Ransomware Note
2. Quarantine Affected Systems
3. Look for Decryption Tools
4. Disable Maintenance Tasks
5. Disconnect Backups
6. Identify the Attack Variant
7. Reset Passwords

8. Report the Ransomware
9. Decide Whether to Pay or Not

1.5 Adware - It displays unwanted advertisements on a user's device. It often collects browsing habits and personal information to deliver targeted advertisements.

Adware come from these sources:

1. Software Download Sites - Certain software download sites may host modified or repackaged versions of legitimate software applications that include adware. It's advisable to download software only from reputable sources and official websites.

(e.g.,The perfect example for adware is that when a user tried to install something in web, and we all know that the Lazada ad kept popping up and we accidentally click it without knowing it's a malware.)

Common types of Adware:

1. **Legal abusive adware PUA** - designed to bombard you with ads. Without any malware, this is also legal. Ads for things like pornography or fitness pills frequently appear in adware like this.
2. **Legal deceptive adware PUA** - it tricky to opt-out of installing harmless third-party software. While frustrating, legitimate adware sometimes uses this method. It is legal if the creator has not knowingly included malware-tainted ads or software.
3. **Illegal malicious adware PUA** - from malicious third parties who want to distribute malicious software like spyware, viruses, or other malware onto devices. This malware may be intentionally masked within the adware itself.

Prevention:

1. Be cautious, not curious - Always ask yourself, "what's the worst that can happen if this is malicious," and proceed with caution.
2. Watch for the fine details - Criminals try to mimic trusted URLs, email addresses, and social media profiles to catch you off guard. If you take a moment to examine these, you'll find odd details that are red flags for scams.
3. Always read all terms and checkbox agreements

Solution

1. Remove redirects and pop-up ads from your browser
2. Remove malicious device admin apps
3. Uninstall the malicious apps from your Android phone
4. Use antivirus software for Android to remove viruses, adware, and other malware

1.6 Botnets – is a form of malware that infected malicious group of bots and devices linked together to perform the same task—for distribution and scaling. It is usually used in large-scale cybercrime.

Botnets come from these sources:

1. Infected Computers - Malicious email attachments, drive-by downloads from infected websites, and software exploits are just a few of the ways that these infections can spread.
2. Malicious Downloads – It can be distributed through malicious downloads.

(e.g., One of know example of botnet is the Zeus "Zbot" that targeted the window-based computers. It steals sensitive information on user, such as, bank credentials, personal data etc.)

Common types of botnets:

1. **Information stealing botnets** – It collects personal information from the user and sells it on the black-market exchange for money.
2. **Network-probing botnets** – It infects machines have one purpose – to scan the Internet and find other vulnerable computers in order to infect them with malware that could potentially turn them into bots as well.
3. **Spam-sending botnets** - These types of malware are designed to send out millions (or even billions) of unsolicited messages from infected computers around the world to their potential victims.

Prevention

1. Avoid buying devices with weak security.
2. Be wary of any email attachments.
3. Improve all user passwords for smart devices. Avoid having same password on all your account as much as possible.

Solution

1. The first thing you need to do is remove suspicious programs and files.
2. Implement firewalls and intrusion detection systems
3. Seek professional assistance
4. Educate yourself and others

1.7 Worm - is a form of malware that replicates itself and automatically spreads through a network.

Worm comes from these sources:

1. Email Attachments

2. Link to a Web or FTP Resource
3. Through Network Packets
4. Via Peer-to-Peer (P2P) File-sharing Networks

(e.g., ILOVEYOU, also known as the Love Bug, emerged in 2000 and spread via email as a malicious Visual Basic script. It disguised itself as a love letter or a harmless attachment, such as a text file or an image. Once opened, it infected the system, overwrote files, and spread to the victim's email contacts.)

Common types of worm:

1. **The ILOVEYOU worm** - ILOVEYOU primarily spread when targeted victims opened an email attachment, and the malware re-sent itself to all the victim's contacts in Microsoft Outlook.
2. **WannaCry** - uses a worm to infect Windows computers and encrypt files on PC hard drives.
3. **Net-Worm** - A net-worm refers to a kind of worm that can find new hosts by using shares made over a network.

Prevention

1. Never click on attachments or links in emails or other messaging applications that might expose systems to malicious software.
2. Install operating system updates and software patches.
3. Use encryption to protect sensitive data stored on computers, servers and mobile devices.)

Solution:

1. Update all antivirus.
2. Scan the computer with the up-to-date antivirus software.
3. Use the antivirus software to remove any malware, malicious code and worms it finds, and clean infected files.
4. Use the antivirus software to remove any malware, malicious code and worms it finds, and clean infected files.

Aside from the given steps to solve and prevent the following threats, these are some of ways for your computer to be safe and moderated at all times:

- Firewalls: designed to prevent unauthorized access to the computers network and system
- Multi-factor authentication: requiring users to provide another form of identification to access a computer system.
- Employee training: Cyber security training for employees can help raise awareness of potential threats and teach them how to identify and respond to threats.
- Backups: Frequent backups of important data can help protect against data loss in the event of a data breach.

Current State of Cyber Security and Cybercrime in the Philippines

To further elaborate the cyber security, we can take a look at the country's current state in terms of cyber security and threats, outlining some of the cybercrimes Philippines encountered and highlighting the cyber laws that are enacted against these threats.

On January 9, 2023, the PNP issued a statement about cybercrime as one of the 'greatest threats' to Filipinos. According to the police Anti-Cybercrime Group, threats such as (1) malware and (2) ransomware are widespread, as well as (3) unauthorized online lending agencies that humiliates borrowers publicly and harassed them for unpaid loans, (4) fraudulent job listings on Facebook where a number of Filipino's are illegally recruited and trafficked. There is also the issue on the matter of (5) scam text messages in 2022, which led to the mandatory SIM Card Registration. In 2022 other cybercrimes cases

such (6) cyber libel which is an act of spreading false information of a person, company, group or organization with the intent to dishonor, disrespect or humiliate, (7) online scams and (8) identity theft is rampant in Philippines. Criminals would steal another person's identity through social media accounts and force them to send money. Another challenging cybercrime case is called short message service an (9) SMS-phishing wherein a certain link is simply sent through a text message.

As Philippines persevere to develop in the digital industry, more people have come to utilize and benefit from it. Businesses and online jobs have flourished, and organizations have found it very practical. That being so cybercrimes have also increased, according to the data of Kaspersky Security Network, Philippines ranked 2nd worldwide that has experienced cyber-attacks last year because of the pandemic and the increased use of digital platforms. Consequently, as stated in "Cyber security and Cybercrime: Philippine Perspective" by Geronimo L. Sy, the Assistant Secretary, Department of Justice, Republic of Philippines, he points out that "the more you have cyber security shall mean the less you have cybercrime and vice versa". Therefore, to respond to these emerging and developing digital trends and even before these current intelligence threats, cyber laws are enacted with the purpose to prevent these threats and penalize cybercriminals.

The following are some of the cyber laws enacted in accordance with technological related offenses: (1) Republic Act No. 8484 or Access Device Regulation Act of 1998, regulating the use of any means to access account and obtain money, service, goods or any valuable item. (2) Republic Act No. 8792 or Electronic Commerce Act of 2000, this law regulates the electronic industry in the Philippines by ensuring that electronic products manufactured, imported, or exported from the country meet certain standards and requirements. (3) Republic Act No. 9995 or Anti-Photo and Video Voyeurism Act of 2009, penalizing the act of broadcasting or capturing another person's intimate body part without their, the purpose of this law is to punish and prevent the act of voyeurism through the use technology. (4) Republic Act No. 9775 also known as the Anti-Child Pornography Act of 2009, its' purpose is to protect children from all forms of sexual exploitations and abuse by criminalizing the production, distribution, possession, and advertisement of child pornography. (5) Data Privacy Act of 2012 or Republic Act No. 10173, aims to protect personal data providing assurance and security, recognizing personal data as a valuable asset and intends to protect it from unauthorized access or use. (6) Republic Act No. 10175 or Cybercrime Prevention Act (CPA) of 2021, the act aims

to address any computer related offenses such as hacking, system intrusion, cyber bullying, identity theft, and cyber terrorism. Recognizing the act of committing crimes through the use of technology, and providing efficient and effective act to prevent, detect, and prosecute cybercrime in the country. (7) SIM Registration Act or Republic Act No. 11934, law aims to regulate the use of SIM and personal data, to prevent the use of anonymous or pre-registered mobile phones numbers for committing criminal offenses such as fraud, identity theft, and other cybercrimes, it also ensures to identify the user easily in the event of an emergency.

V. Summary

To summarize, the paper discusses the common different types of cyber threats such as a malware and its variety which are virus, Trojan, spyware, adware, ransomeware, Botnet, and worm. It also includes the sources of these viruses and step by step instructions to solve and prevent, generally by having an antivirus software, firewall and keeping a computer system updated. The paper highlights the current state of Philippines on cybercrime, entailing commonly encountered crimes such as malwares, ransomeware, unauthorized online lending, identity theft, cyber libel, online scams, and fraudulent listing. The paper highlights the relevance of cyber security laws such as Access Devices Regulation Act of 1998, Anti-Photo and Video Voyeurism Act of 2009, Anti – Child Pornography Act of 2009, Anti – Child Pornography Act of 2009, Cybercrime Prevention Act (CPA) of 2021, SIM Registration Act, and Electronic Commerce Act of 2000, H. R. 8792, 11th Cong. (2000). Overall, the study highlights the significance of cybersecurity and awareness, the types of cyber threats, solutions and preventions as well as the cybersecurity laws.

VI. Conclusion and Recommendation

In conclusion, we are continuously developing and adapting in in the cyber industry. As more opportunities and benefit the digital space provides the more people are utilizing the cyberspace such as the digitalization of most services, online jobs and more, consequently the higher the threats can be, as cyber criminals also finds it as an opportunity to victimize users. Therefore, having the knowledge and skill

in preventing and solving an attack or threat is highly necessary. The cyber laws were enacted to provide safety, protection, and efficiency in criminalizing if such threats are encountered.

Cyberspace is a broad domain, in which a number of unpredicted events can happen. Despite numerous security applications, programs or cyber laws, it is significantly recommended for users to stay precautious in the cyberspace, no one is certainly safe from these attacks and anyone can be a victim. Despite the elaborated preventions, solutions and law, it should be taken into account that cyber criminals are increasing and their skills continuously develop just as well, therefore their complexity, uncertainty and speed pose as a challenge for the government. Taking into consideration that Philippines is still a developing country and therefore the greater the struggle is to address multiple threats while also establishing a more improved and advantageous cyber security.

Reference

Ayofe, A. N., & Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29(6). https://www.academia.edu/download/62565276/171920200330-53981-1mqgyr5.pdf

Reddy, G. Nikhita. & Reddy, G.J. Ugander. (2014, February 8). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Arxiv. https://arxiv.org/abs/1402.1842?fbclid=IwAR1uIUXUqyOQRQhRQQ0EOwtLBM5_ZX70NijWyajLyofFU_VkGF6g2KSfFlw

Rafter, D. (2021, March 21). How to Protect Your Privacy Online: Tips | Norton. Us. https://us.norton.com/blog/privacy/protecting-your-privacy-online

Know Your Rights » National Privacy Commission. Privacy. https://www.privacy.gov.ph/know-your-rights/#:~:text=Under%20R.A.%2010173%2C%20your%20personal,unless%20otherwise%20provided%20by%20law.

Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

Cavelty, M. D. 2008. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. Journal of Information Technology & Politics, 4(1): 19-36. http://dx.doi.org/10.1300/J516v04n01_03

Sy, G. L. Cybersecurity and Cybercrime: Philippine Perspective

https://doj.gov.ph/files/cybercrime_office/Cybersecurity%20and%20Cybercrime-Philippine%20Perspective.pdf

Tabile, J. D. (2023, March 16) Philippines ranks second on global cyberattack list

https://www.bworldonline.com/technology/2023/03/16/510855/philippines-ranks-second-on-global-cyberattack-list/

Castillo, C. M. PHILIPPINE CYBERSECURITY IN RETROSPECT (2016-2021) https://ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/

Ronda, R. A (2023, March 15) Philippines 2nd most attacked by web threats worldwide last year https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year

Access Devices Regulation Act of 1998, H. R. 8484, 10th Cong. (1998) https://lawphil.net/statutes/repacts/ra1998/ra_8484_1998.html

Anti-Photo and Video Voyeurism Act of 2009, H. R. 9995, 14th Cong. (2009) https://lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html

Anti – Child Pornography Act of 2009, H. R. 9775, 14th Cong. (2009) https://lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html

Data Privacy Act of 2012, H. R. 10173, 15th Cong. (2012) https://lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html

Cybercrime Prevention Act (CPA) of 2021, H. R. 10175, 15th Cong. (2012) https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

SIM Registration Act, H. R. 11934, 15th Cong. (2011) https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html

Electronic Commerce Act of 2000, H. R. 8792, 11th Cong. (2000) https://lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html