OULU UNIVERSITY OF
APPLIED SCIENCES

Muhammad Faheem Khan

END USER AWARENESS OF CYBERSECURITY CHALLENGES

END USER AWARENESS OF CYBERSECURITY CHALLENGES

Muhammad Faheem Khan

Bachelor's thesis

Spring 2013

Degree Programme in

Business Information Technology

Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences

Degree Program: Business Information Technology

Author(s): Muhammad Faheem Khan

Title of Bachelor's thesis: End user awareness of cybersecurity challenges

Supervisor(s): Teppo Räisänen

Term and year of completion: Spring 2013

Number of pages: 43+1

The purpose of this Bachelor's thesis was to explore the challenges and threats intend to affect Cyber World. The ever increasing use of internet around the world has without doubt increased the usage of internet based services, easier ways of communication and information sharing. Such drastic increase in usage of network based systems has made the current cybersecurity systems old dated as the hackers and attackers of networked systems is on the rise with new and modern attack methodologies.

The objective of the thesis is to find out the countermeasures of the threats formed by cyber criminals. The use of a computer as an instrument to illegal ends, such as committing fraud, stealing identities, or violating privacy. Another objective of the thesis is awareness of the end user of computer and internet about cybercrimes and threats imposed to the user while using internet.

To find fact and figures about cyber threats, different printed and electronic media were used. An interview was conducted with a network administrator of a university to get real life scenario of the topic and to analyze the preventive measures adopted by the organizations to protect the network from internal and external threats.

As a result, it is important to adopt safety measures against cybercrimes and protect the organization network by installing hardware devices. It is also important to train the computer user about cyber threats and educate them that how to use the computer and peripherals in school and office.

Keywords: cybercrime, cybersecurity, end user awareness

Table of Contents

1. INTRODUCTION 6
2. THEORETICAL BACKGROUND 8
   - 2.1 Networking 8
   - 2.2 TCP/IP 8
   - 2.3 Computer Platforms 9
   - 2.4 Computer Virus 9

3. CYBERCRIME 10
   - 3.1 Cybercrime via Social Media 10
   - 3.2 Cybercrime via Mobile/Smartphone 11
   - 3.3 Hackers 15
   - 3.4 Crakcers 15
   - 3.5 Network Sniffers 17

4. TOOLS & TECHNOLOGIES FOR CYBERCRIME 18
   - 4.1 Email Bomb 18
   - 4.2 Monitor Simple Mail Transfer Protocol (SMTP) 19
   - 4.3 Spam 19
   - 4.4 Password Crackers 21
   - 4.5 Botnets 22
     - 4.5.1. Types of Botnet 23
     - 4.5.2. Botnet Attacks 25

5. CYBERSECURITY THREATS 27
   - 5.1 Distributed Denial of Service (DDoS) 27
   - 5.2 Spoofing 28
   - 5.3 Phishing 28
   - 5.4 Malicious Code 29
   - 5.5 Removable Meida 29

6. CASE STUDY: INTERVIEW WITH IT SUPPORT OFFICER OF A UNIVERSITY 31
6.1 Methodology 31
6.2 Summary of the interview 31
6.3 Analysis 33

7. COMPUTER USER AWARENESS FOR CYBERSECURITY 35
7.1 Update software 35
7.2 Installation of security software to computers 36
7.3 Use strong password 36
7.4 Limited use of privileged accounts 37
7.5 Make backups of important files and folders 37
7.6 Secure physical environment 38
7.7 Always use secure wireless 38
7.8 Understanding peer to peer technology and social networking 39
7.9 Secure messaging 39

8. CONCLUSION AND DISCUSSION 41

9. REFERENCES 42

10. APPENDIX-I 44

1. INTRODUCTION

The theme of thesis is to research that how much cybersecurity is beneficial for internet users and how it affects users in real life. Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies cybersecurity. According to a December 2010 analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years.

It can also be defined as the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning

Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize the likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data. (B., 2012)

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

In 2002, Donn Parker presented an alternative model for the classic CIA term (Confidentiality, Integrity and Availability) that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability and utility.

A specialized field in computer networking that involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.

A disaster recovery plan (DRP) - sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organization manages potential disasters. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention. Disaster recovery is becoming an increasingly important aspect of enterprise computing. As devices, systems, and networks become ever more complex, there are simply more things that can go wrong. As a consequence, recovery plans have also become more complex. (c5franey, 2011)

2. THEORETICAL BACKGROUND

2.1 Networking

A network is a collection of computers and devices connected to each other. The network allows computers to communicate with each other and share resources and information. In other words networking can be defined as inter-connection of two or more computers for sharing the resources (hardware and software).

Computer networks can be classified into two types of communication media:

i. Wired Technologies: It is known as transmission of data over a wire-based communication technology. For example; telephone networks, cable television, internet access and fiber optic communication.
ii. Wireless Technologies: It can be described as communication with electromagnetic waves which are used for communication purpose. It can be used for different purposes. For example; Cellular phones, Wireless computer peripherals and Global positioning system (GPS).

2.2 Transmission Control Protocol/Internet Protocol (TCP/IP)

All communication, whether face-to-face or over a network is governed by predetermined rules called protocols. Successful communication between hosts on a network requires the interaction of many different protocols. A group of inter-related protocols that are necessary to perform a communication function is called a protocol suite.

Transmission Control Protocol (TCP) is the transport protocol that manages the individual conversations between web servers and web clients. TCP divides the HTTP messages into smaller pieces, called segments, to be sent to the destination client. It is also responsible for controlling the size and rate at which messages are exchanged between the server and the client. (Anonymous, 1998)

The most common internetwork protocol is Internet Protocol (IP). IP is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning the appropriate addresses, and selecting the best path to the destination host.

2.3 Computer Platforms

In personal computing, a platform is the basic hardware (computer) and software (operating system) on which software applications can be run. Computers use specific Central Processing Units (CPUs) that are designed to run specific machine language code. In order for the computer to run software applications, the applications must be in that CPU's binary-coded machine language. Thus, historically, application programs written for one platform would not work on a different platform.

There are different types of platforms, for example; Microsoft Windows, Mac OS, Linux, Solaris etc. (Viega, 2009)

2.4 Computer Virus

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Viruses have the capability of infecting any file; however, will infect executable files or data files, such as word or excel documents that are opened frequently and allow the virus to try infecting other files more often.

There are different types of virus; most popular and common viruses are Trojan Horse, Worms, Boot sector Virus, Macro Virus and Memory Resident Virus.

3. CYBERCRIME

Cybercrime is a term for any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. These include attacks against computer data and systems, identity theft, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, Botnets, and various email scams.

3.1 Cybercrime via Social Media

Cyber criminals are enjoying greater degrees of success on social networks because they are easier to target and users are more likely to fall for scams. Social networking sites are becoming more and more prone to online attacks as users continue to grow by the day. The growing commercialization of social media through links to online trading such "buy, swap and sell" sites means cyber crooks now have a strong motivation to hack people's account details. These included vicious "form-grabbing malware" that can steal large amounts of personal data, as well as complacency about the security of mobile devices, which most people do not protect with anti-virus software, even while using their phones to do banking. Attackers go where the people go. Facebook is the social networking website. One of the most insidious threats is Koobface, a virus that takes over PCs when users click on links in spam messages. The virus turned up on MySpace about a year ago, but the unknown authors now focus on spreading it through Facebook. Many people have to pay the price after being the victim of cyber crime at different social media platforms. Many people even terminate and deactivate their social media account after such bad experiences.

Security attacks through social networks are becoming more prevalent.

- In the US the number of social networkers who experienced Koobface infections and other social network attacks climbed from 8% in 2009 to 13% in 2010 to 18% in 2011.
- In the United Kingdom the number of social networkers who experienced attacks on social networks jumped from 6% in 2009 to 12% in 2010 to 15% in 2011.
- Friend in distress scams jumped from 2% in 2009 to 14% in 2011 in the US; in the UK these scams increased from 6% in 2009 to 11% in 2011.

Countermeasures

- Maintain current anti-virus software that is obtained from a reputable source and is regularly updated.
- Make sure operating system is updated to ensure any security vulnerabilities are mitigated.
- Use strong passwords to protect personal information.
- Passwords should also be kept secret and changed regularly.
- Limit the amount of personal information placed on the internet.
- Do not provide financial or other personal information to unknown people.
- Never click on links contained within spam or unexpected emails.

3.2 Cybercrime via Mobile/Smartphones

Cyber criminals who are experts at hijacking computers with viruses and malware are looking elsewhere for their next efforts. They see major potential with smartphone. Addiction to smartphones has led to a spike in the number of people falling victim to cybercrime. Around 5.4 million people were targeted by online criminals over the past 12 months, according to Norton's annual Cybercrime report. Smartphone applications have inherent vulnerabilities allowing it to be compromised by hackers and security threats. For instance a mere popular game which is known to many appears to be harmless but once it is downloaded it activates the phone's GPS and then relays the information of the activities on the phone to a cyber criminal.

Survey says that forty percent (40%) of mobiles sold in the year 2012 were Smartphones. It has already become a gateway for cyber criminals but once a person has access to computer, e-mails, and social media by only a touch it is probably impossible to switch down to an older version of phone. Though the cybersecurity has warned that the world will be facing a wave of cybercrime with the usage of Smartphones, people can never overcome their addiction to latest gadgets.

Mobile applications are the new frontier for cybercrimes. The demand for mobile applications increases with the growth in mobile device usage. Mobile applications, or mobile apps, are software created for smartphones and tablets. Due to the growing usage of mobile devices worldwide, web threats are no longer limited to conventional PCs. App stores now serve as the sites for software download, while mobile apps serve

as programs we download onto our mobile devices. It's a shift in platform but with the same threat scenario. Users who download from app stores may end up downloading malware instead. Because of this, mobile apps have become the new frontier for threats. Malware, short for malicious software, has become the latest attacking tool of cyber crime.

Many people do not realize that there are still some security risks despite downloading apps from their official sites.

The Android platform has become the target of continuous cyber attacks due to its app distribution model that makes it open to any developing parties. But this does not mean that other mobile platform users should take security issues lightly.

There are also third-party sites that provide alternative apps for users. However, downloading from these unofficial channels can be as risky as downloading programs from unverified and peer-to-peer sites. While third-party app stores are not malicious in nature, they do not have the resources to adequately curate app submissions. As a result, malicious, repackaged, and pirated applications may be found in these independent app stores. Thus, it is important to know the business model that these app stores use to understand the possible risks and threats when downloading mobile apps.

There are different online app stores for mobile users, for example: iTunes app store, Android market, Blackberry app world and Nokia's Ovi store etc. (ll, 2011)

The techniques and payload for targeting Android OS can be categorized in different ways. See Table 1:

Table 1. Types and Techniques to target Android OS (New Frontier for Cybercrime, 2013)

Category	**Method**	**User Suggestion**
Data Stealer	Steals information stored in the mobile device and sends it to a remote user	Stolen information may be used for malicious purposes
Premium Service Abuser	Subscribes the infected phone to premium services without user consent	Unnecessary charges for services not authorized by user
Click Fraudster	Mobile devices are abused via clicking online ads without users' knowledge (pay-per-click)	Cybercriminals gain profit from these clicks
Malicious Downloader	Downloads other malicious files and apps	Mobile device is vulnerable to more infection
Spying Tools	Tracks user's location via monitoring GPS data and sends this to third party	Cybercriminals track down location of users
Rooter	Gains complete control of the phone, including their functions	Users' mobile devices are exposed to more threats

Countermeaures

The countermeasures against cybercrime via smartphone are presented in Table 2.

Table 2. Countermeasures against cybercrime via smartphone

Maximize the security features installed on your mobile devices	Users should properly configure their smartphones location and security settings. For additional protection, use the PIN (numeric) and password lock features of your smartphones. Other devices have fingerprint lock, which is also a great option, as it ensures that you are the only one who can access your smartphone. Don't leave your phone unattended at work or at play. Keep your smartphone locked if not in use, keep it where you can see it or safely put it away from prying eyes. Always log out of mobile apps or mobile websites and do not store mobile app passwords for easy log in.
Think before you download	Consider downloading exclusively from official app stores like the *Android* Market. Not all the apps are guaranteed as secure but the Android Market is still your best bet, security-wise. Before downloading a mobile app learn about who created it.
Scrutinize permissions asked by apps	It is noticed that malicious apps ask for access to a long list of information stored in your device. Be careful in accepting requests for personal or device information.
Treat your mobile device like your PC	Today's smartphones act like mini-PCs. They are designed to handle multiple tasks, like web browsing. Just the same, they are also open to the same threats. Think twice before browsing the Internet via smartphones.

3.3 Hackers

Computer hackers are unauthorized users who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without user knowledge or consent. Their clever tactics and detailed technical knowledge help them access information.

A hacker commonly known as “White hat” is a person intensely interested in the arcane and obscure workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

Dennis Ritchie, Ken Thompson, Linus Torvalds, Paul Baran and Brian Kernighan are well known hackers. (Anonymous, 1998)

3.4 Crackers

A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

Crackers known as “Black hat” is someone who breaks computer security without authorization or uses technology (usually a computer, phone system or network) for vandalism, credit card fraud, identity theft, piracy, or other types of illegal activity.

A common method used by crackers for harming networks or stealing important information, such as passwords or credit card numbers, is through a Trojan horse. A Trojan horse is able to recognize and record every keystroke that a user makes. Another method is password cracking, which is the process of gaining passwords from data, which has been stored in a computer system. There are three types of password cracking, which are commonly used; these include Dictionary, Hybrid, and Brute Force.

Crackers can also refer to those who reverse engineer software and modify it for their own amusement. The most common way crackers gain access to networks or systems is through social engineering, whereby the cracker contacts employees at a company and

tricks them into divulging passwords and other information that allows a cracker to gain access.

Indicators for being hacked

- Inbox contains mailing errors or mailer-daemon messages for email didn't send.
- People you know are getting emails from you that you didn't send.
- There are outgoing messages in your Sent, Drafts or Outbox folder that you didn't create or send.
- Account folders (Sent, Deleted, Spam, Inbox, etc.) have been emptied or deleted.
- Address Book contacts have been erased.
- During sign-in or when sending a message, you're asked to pass an image challenge.
- Emails try to send are suddenly getting refused and returned to you.
- There are contacts in Address Book you didn't add.
- Keep getting bumped offline when you're signed into your account.
- Email signature suddenly has a link you didn't put there.
- Stop getting new mail.

Countermeasures

Create a strong password: For the most up-to-date recommendations for making a strong password, Note that passwords should be at least six characters long and include at least one number, letter (combination of upper and lower cases) and special character ($, *, &, !, etc.). Make sure your new password is different from any other passwords you have used. Also, if you use the same password for other online accounts such as social media and financial services, change those passwords as well. It is strongly advised that you use different passwords for different social media accounts.

Make sure you have antivirus software installed and updated: Virus scans search for any spyware, viruses or other malware that may have found their way onto your computer. Run scans frequently to make sure your computer is free of all malware.

Don't download attachments (e.g., pictures, games, electronic greetings) unless it's from someone you know.

3.5 Network Sniffers

Network sniffer is a program or device that monitors data traveling over a network. Packet sniffers or protocol analyzers are tools that are commonly used by network technicians to diagnose network-related problems. Packet sniffers can also be used by hackers for less than noble purposes such as spying on network user traffic and collecting passwords. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal.

On TCP/IP networks, where they sniff packets, they're often called *packet sniffers*.

Strategy for Network Sniffing

Network/Packet sniffers perform by intercepting and logging network traffic that they can see via the wired or wireless network interface that the packet sniffing software has access to on its host computer.

On a wired network, what can be captured depends on the structure of the network. A packet sniffer might be able to see traffic on an entire network or only a certain segment of it, depending on how the network switches are configured, placed, etc. On wireless networks, packet sniffers can usually only capture one channel at a time unless the host computer has multiple wireless interfaces that allow for multichannel capture.

Once the raw packet data is captured, the packet sniffing software must analyze it and present it in human-readable form so that the person using the packet sniffing software can make sense of it. The person analyzing the data can view details of the conversation happening between two or more nodes on the network. (Whitman & Mattord, 2009)

Hackers can use sniffers to unencrypted data in the packets to see what information is being exchanged between two parties. They can also capture information such as passwords and authentication tokens (if they are sent in the clear). “Wireshark”, open source software is commonly used for network sniffing purpose.

4. TOOLS AND TECHNOLOGIES FOR CYBERCRIME

4.1 Email Bomb

Email bombing is the process of sending large number of mails into someone's mailbox, with intention to affect the operating system of a computer or a network. It is also termed as email flooding, as the targeted mailbox is flooded with a barrage of mails. When your mailbox is flooded with unwanted and junk emails, your mailbox capacity will get exhausted and you won't be able to receive any mails further. This action prevents you from reading the legitimate mails. It can even be used to completely overload any company's mail server. It is done intentionally with intent to affect the DOS (Disk Operating System) of a computer. (Sukumar, 2011)

The intensity of email bombing can also result in crashing of the operating system and the mail servers. It has the capacity to consume the whole system. By limiting the user quota to a certain capacity, it can help to restrict its overflow. The hacker aims to shut down the website of a victim, by sending email bombs. The first known incident of email bombing was done by Tamil guerrilla groups against the Sri Lankan government. Tamil guerrillas swamped the system of Sri Lankan embassies with an email containing the message "We are the Internet Black Tigers and we're doing this to disrupt your communications".

The following indications occur during the process:

- Overloading of the network connection
- Loss of connectivity
- Denial of service
- Consumption of all system resources
- Syslog entries

Countermeasures

If the email bombs are incoming from many IP addresses, it's difficult to spam and filter each and every mail from those addresses. In this case, employing proxy servers will help to minimize the problem. The computers in a particular network will be connected to a proxy server, which is another computer. The client computers request for information and resources of other computers, to the proxy server.

The proxy server addresses the request and sends the information, after filtering the messages which is done according to the filtering rules of the proxy. It checks for malware content and filters the messages from suspicious IP addresses and protocols before transmitting it to its clients. In this way, proxy servers, protect the network and also take on the complexity of the computer networks.

4.2 Monitor Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is a method of authenticating the exchange of messages that are transmitted or received across the Internet protocols. The clients in the network use Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP), of their system to access their mailbox. The Mail Submission Agent sends a mail or transfers any information to the Mail Transfer Agent (MTA), through SMTP. The MTA connects to the SMTP and then analyzes the mail exchange record and the IP address of the sender, and then only accepts the message. Security mechanisms such as authentication and negotiation are processed during the exchange of data. Internet Engineering Task Force (IRTF), is working on the authentication process and finding ways to strengthen this system, as the complexity of the system is growing rapidly.

Use Mail Filter Applications Filter packages are exclusionary schemes that are used to filter the mails according to the source addresses. For windows and Mac OS computers, I have listed some filter package tools below.

- EIMS (Mac OS)
- Mail Siphon (Mac OS)
- Musashi (Mac OS)
- SIMS (Mac OS)
- Email Chomper (Windows 95/85/NT)
- Spam Buster (Windows 9x/ ME/ NT/ XP/ 2000)
- SpamKiller (Windows 9x/ ME/ NT/ XP/ 2000)

4.3 Spam

Spam is unsolicited e-mail on the Internet. It is a form of bulk mail, often sent to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail. It refers to

sending email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message that is setup incorrectly.

Unwanted commercial email – also known as "spam" – can be annoying. Worse, it can include bogus offers that could cost you time and money.

Spam is roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message since everyone shares the cost of maintaining the Internet. Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. It has become a major problem for all Internet users. (Goodman, 2004)

Countermeasures

There are several ways to block spam from your e-mail inbox. They say prevention is the best medicine, so avoid giving out your e-mail address to unfamiliar or unknown recipients. This has become very difficult to do, however. Spammers can use software programs that troll the Internet looking for e-mail addresses, much like throwing a net in the ocean and seeing what gets caught in it. Nowadays it's almost impossible to shop online without providing a valid e-mail address. Offline stores are even asking for e-mail addresses in exchange for discounts or free merchandise. Realize that what they are doing is potentially opening the door for a flood of unsolicited e-mails. These organizations will most likely turn around and sell their list to someone else looking for valid e-mails. In these cases, it might be wise to have more than one e-mail address, one for friends, family and colleagues and another for unfamiliar sources. There are many free e-mail services in cyberspace to choose from.

However, also know that even trustworthy sources may be unwittingly shelling out your e-mail address. Ever receive an e-mail greeting card? The sender has given your e-mail to an organization that may very well be compiling e-mail lists to sell to spammers.

A second way to stop spam is to use your e-mail application's filtering features. Most e-mail applications allow you to block specific messages. When an offending e-mail comes in, set the filter to block further incoming mails from that sender.

A more aggressive approach to ridding unwanted e-mail is to report the e-mailer to the spammer's ISP. This is not always an easy task. First you must determine the spam's origins. Many of the bigger and more commercial ISPs forbid spammers from using their services and, once discovered, will actively ban the offending parties from using their services. But there are plenty of smaller ones that do not. To find the spam's origins, instruct your e-mail program to display all of the e-mail's header information. View the "Received" lines, and working from top to bottom you can often pinpoint the origin of spam.

Spammers don't typically just send e-mails from their ISP to yours; that'd be too easy and apparent. Instead, they channel the e-mails through one or more ISPs in order to obfuscate the origin, but each computer that handles the e-mail will attach a "Received" line to the header. There are numerous Internet resources available for help in tracking down the source of spam.

4.4 Password Crackers

A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a humancracker obtain unauthorized access to resources. The easier way to understand how password crackers work is to understand how encrypted passwords are created. Password generators use cryptography, the practice of writing in codes.

Password crackers use two primary methods to identify correct passwords: brute-force and dictionary searches. When a password cracker uses brute-force, it runs through combinations of characters within a predetermined length until it finds the combination accepted by the computer system. When conducting a dictionary search, a password cracker searches each word in the dictionary for the correct password. Password dictionaries exist for a variety of topics and combinations of topics, including politics, movies, and music groups.

Some password cracker programs search for hybrids of dictionary entries and numbers. For example, a password cracker may search for ants01; ants02; ants03, etc. This can be helpful where users have been advised to include a number in their password.

A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able to decrypt it. Or,

by using the same algorithm as the system program, the password cracker creates an encrypted version of the password that matches the original. (Anonymous, 1998)

Countermeasures

There are a few things that can be done on a windows system to prevent your password from being cracked.

Use Complex and Changing Passwords

The most logical way to prevent people from cracking your password is to make it incredibly complex. If password contains lowercase letters, uppercase letters, numbers, special symbols, and is fairly long, it won't be able to be cracked in any reasonable amount of time. In order to given things an added degree of complexity, changing your password frequently means that when an attacker cracks password it will have already been changed. There is no single greater defense than using a strong password that is changed frequently.

Use SYSKEY

SYSKEY is a Windows feature which can be implemented to add an extra 128 bits of encryption to the SAM file. SYSKEY works by the use of a user created key which is used to encrypt the SAM file. Once enabled, SYSKEY cannot be disabled.

It's important to keep in mind that SYSKEY only protects the SAM file (Security Accounts Manager) itself, securing it against being copied. SYSKEY does NOT protect against tools which extract hashes from running memory, such as Cain.

4.5 Botnets

A Bot is an abbreviation for a software robot that can be used for malicious or beneficial purposes. Botnet or Drone-Army, also known as Zombie-Army as well, is an abbreviation for a Ro**botNet**work. Botnet is a network of compromised computers that can be remotely controlled by an attacker, called the BotMaster or BotHerder and each infected computer by a bot can be referred as a Zombie or as a Drone. Bots are remotely controlled through commands sent via the internet by the Botmaster using the C&C server, which stands for Command and Control server (C&C) a remote control & communication channels, for sending and receiving commands between the Botherder and the Zombies. Common botnet actions are Email Spamming, DDoS Attacks and Financial Breach etc. (Rouse, 2012)

Botnets are created when the bot-herder sends the bot from his command and control servers to an unknowing recipient using file sharing, email, or social media application protocols or other bots as an intermediary. Once the recipient opens the malicious file on his computer, the bot reports back to command and control where the bot-herder can dictate commands to infected computers.

As one of the most sophisticated types of modern malware, botnets are an immense cybersecurity concern to governments, enterprises, and individuals. Whereas earlier malware were a swarm of independent agents that simply infected and replicated themselves, botnets are centrally coordinated, networked applications that leverage networks to gain power and resilience. Since infected computers are under the control of the remote bot-herder, a botnet is like having a malicious hacker inside your network as opposed to just a malicious executable program.

4.5.1 Types of Botnet

Agobot/Phatbot/Forbot/XtremBot

This is probably the best known bot. Currently, the AV vendor Sophos lists more than 500 known different versions of Agobot (Sophos virus analyses) and this number is steadily increasing. The bot itself is written in C++ with cross-platform capabilities and the source code is put under the GPL. Agobot was written by Ago alias Wonk, a young German man who was arrested in May 2004 for computer crime. The latest available versions of Agobot are written in tidy C++ and show a really high abstract design. The bot is structured in a very modular way, and it is very easy to add commands or scanners for other vulnerabilities: Simply extend the CCommand Handler or CScanner class and add your feature. Agobot uses libpcap (a packet sniffing library) and Perl Compatible Regular Expressions (PCRE) to sniff and sort traffic. Agobot can use NTFS Alternate Data Stream (ADS) and offers Rootkit capabilities like file and process hiding to hide it's own presence on a compromised host. Furthermore, reverse engineering this malware is harder since it includes functions to detect debuggers (e.g. SoftICEandOllyDbg) and virtual machines (e.g. VMWare and Virtual PC). In addition, Agobot is the only bot that utilized a control protocol other than IRC. A fork using the distributed organized WASTE chat network is available. Furthermore, the Linux version is able to detect the Linux distribution used on the compromised host and sets up a correct initscript. Summarizing: "The code reads like a charm, it's like dating the devil."

SDBot/RBot/UrBot/UrXBot/...

This family of malware is at the moment the most active one: Sophos lists currently seven derivatives on the "Latest 10 virus alerts". SDBot is written in very poor C and also published under the GPL. It is the father of RBot, RxBot, UrBot, UrXBot, JrBot, and probably many more. The source code of this bot is not very well designed or written. Nevertheless, attackers like it, and it is very often used in the wild. It offers similar features to Agobot, although the command set is not as large, nor the implementation as sophisticated.

mIRC-based Bots - GT-Bots

We subsume all mIRC-based bots as GT-bots, since there are so many different versions of them that it is hard to get an overview of all forks. mIRC itself is a popular IRC client for Windows. GT is an abbreviation for *Global Threat* and this is the common name used for all mIRC-scripted bots. These bots launch an instance of the mIRC chat-client with a set of scripts and other binaries. One binary you will never miss is a *HideWindow* executable used to make the mIRC instance unseen by the user. The other binaries are mainly Dynamic Link Libraries (DLLs) linked to mIRC that add some new features the mIRC scripts can use. The mIRC-scripts, often having the extension ".mrc", are used to control the bot. They can access the scanners in the DLLs and take care of further spreading. GT-Bots spread by exploiting weaknesses on remote computers and uploading themselves to compromised hosts (filesize> 1 MB).

Besides these three types of bots which we find on a nearly daily basis, there are also other bots that we see more seldom. Some of these bots offer "nice" features and are worth mentioning here:

DSNX Bots

The Dataspy Network X (DSNX) bot is written in C++ and has a convenient plugin interface. An attacker can easily write scanners and spreaders as plugins and extend the bot's features. Again, the code is published under the GPL. This bot has one major disadvantage: the default version does not come with any spreaders. But plugins are available to overcome this gap. Furthermore, plugins that offer services like DDoS-attacks, portscan-interface or hidden HTTP-server are available.

Q8 Bots

Q8bot is a very small bot, consisting of only 926 lines of C-code and it has one additional noteworthiness. It is written for Unix/Linux systems. It implements all common features of a bot: Dynamic updating via HTTP-downloads, various DDoS-attacks (e.g. SYN-flood and UDP-flood), execution of arbitrary commands, and many more. In the version we have captured, spreaders are missing. But presumably versions of this bot exist which also include spreaders.

Kaiten

This bot lacks a spreader too, and is also written for Unix/Linux systems. The weak user authentication makes it very easy to hijack a botnet running with kaiten. The bot itself consists of just one file. Thus it is very easy to fetch the source code using wget, and compile it on a vulnerable box using a script. Kaiten offers an easy remote shell, so checking for further vulnerabilities to gain privileged access can be done via IRC.

Perl-based bots

There are many different version of very simple based on the programming language Perl. These bots are very small and contain in most cases only a few hundred lines of code. They offer only a rudimentary set of commands (most often DDoS-attacks) and are used on Unix-based systems.

4.5.2 Botnet Attacks

WordPress Attacked by Botnet

Many WordPress sites are under attack by a botnet using brute-force methods to obtain their passwords. The attacks seem limited to only users who kept the default “Admin” username for their websites, however, these attacks are only the beginning. Analysts and companies fear that the attackers are attempting to build a massive botnet that is much more powerful than any botnet seen before.

Currently, there are over 90,000 IP addresses being used to launch these brute-force attacks. These IP addresses are using thousands of passwords to hack into the WordPress sites. Right now, the botnet is limited to just using home PCs, however, the attackers could soon use the powerful servers that run these WordPress sites to launch a much stronger Botnet. (Stilgherrian, 2013)

Countermeasures regarding prevention measure can be seen in Table 3.

Table 3. Prevention measures against Botnet Attacks

• Use up-to-date anti-virus and anti-spyware software	Look for software that removes viruses and updates itself automatically on a daily basis. Be careful of ads on the Internet offering spyware software, as this might be a plot to get you to download malicious code.
• Set your operating system software to download and install security patches automatically	The security patches released monthly by Microsoft help fix any flaws companies find in their operating system which in turn helps to give your computer the latest protection.
• Insure that your firewall is turned on	Firewalls are designed to prevent hackers from accessing your computer. They help to block incoming communications from unauthorized sources. Many operating systems like Windows and Mac OS have built-in firewalls however you may need to verify if it is enabled. Routers have hardware firewalls. It is especially important to have your firewall enabled if you have a broadband connection.
• Be cautious about opening any attachments, or downloading any files from emails you receive	Even if the email is from a friend or co-worker, be careful about what you choose to open since their computer could be compromised. While sending an email attachment, explain in the email what the attachment is.
• Be careful what you download from the Web	Only visit trusted sites. It is recommended that you use a web browser that has security features or use a program like SiteAdvisor that checks the status of websites to insure that they are safe to visit and use.
• Turn off your computer when you aren't using it	If you are disconnected from the Internet, hackers can't get to you.

5. CYBERSECURITY THREATS

5.1 Distributed Denial of Service (DDoS)

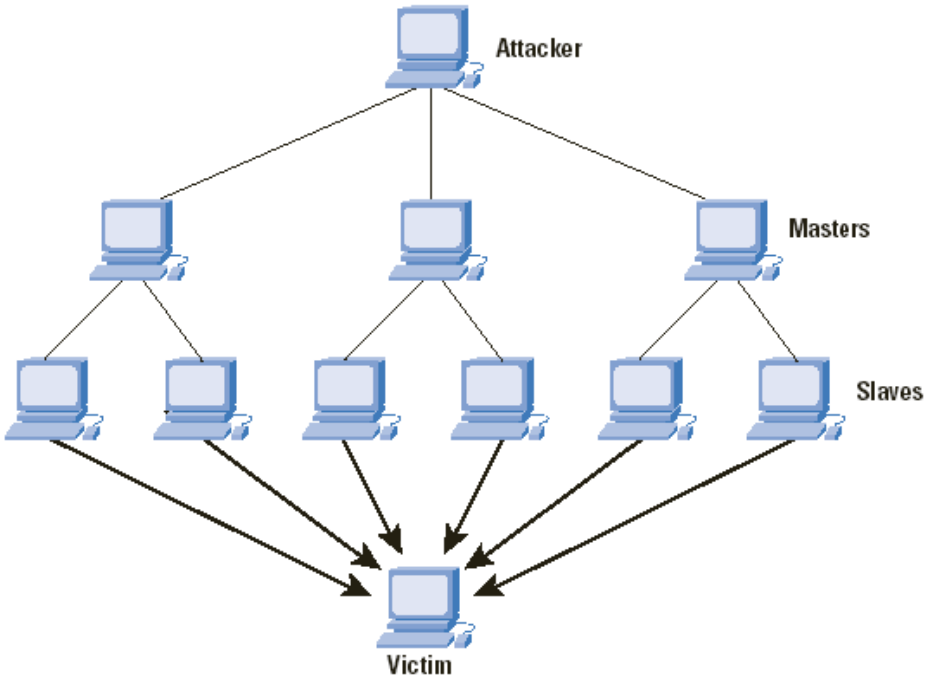

Figure 1. Distributed Denial of Service (cisco, 2013, Retrieved 15.04.2013)

DDoS, Distributed Denial of Service is a type of DoS attack where multiple compromised systems, which are usually infected with a Trojan, used to target a single system causing a Denial of Service (DoS) attack. As shown in figure 1, Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. See figure 1, typical DDoS attack has been shown.

In a typical DDoS attack, a hacker or cracker begins by exploiting vulnerability in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple, sometimes thousands of -- compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. (Douligeris & Serpanos, 2007)

There are many victims in a DDoS attack, the final target and as well the systems controlled by the intruder. Although the owners of co-opted computers are typically unaware that their computers have been compromised, they are nevertheless likely to suffer degradation of service and malfunction. Both owners and users of targeted sites are affected by a denial of service. Yahoo, Buy.com, RIAA and the United States Copyright Office are among the victims of DDoS attacks. DDoS attacks can also create more widespread disruption. In October 2010, for example, a massive DDoS attack took the entire Myanmar offline.

There are a number of DDoS mitigation techniques that organizations can implement to minimize the possibility of an attack. Network security infrastructure should include DDoS detection tools that can identify and block both exploits and tools that attackers use to launch an attack. Additionally, network administrators can create profiles to observe and control specific floods of traffic (i.e. SYN floods, UDP, and ICMP floods). Through looking at all traffic in aggregate, thresholds can be set to monitor and cut behaviors that indicate a possible DDoS attack.

5.2 Spoofing

E-mail spoofing is the imitation of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. It can be used legitimately. However, spoofing anyone other than yourself is illegal in some jurisdictions. (Anonymous, 1998)

5.3 Phishing

Phishing is a high-tech scam that uses e-mail to deceive you into disclosing personal information. It puts your personal information and your organization’s information at risk. Spear phishing is a type of targeted phishing that appears to be directed towards a specific individual or group of individuals.

The suspicious indicators related to phishing and spear phishing are by using e-mails, which include bad grammar, misspellings, and/or generic greetings, maliciously-crafted attachments with varying file extension or links to a malicious website, appear to be from a position of authority or legitimate company, ask you to update or validate information or click on a link.

The user can follow different countermeasures to guard against phishing and spear phishing, for example: watch out for phishing and spear phishing, delete suspicious e-mails, contact system security point of contact with any questions, report any potential incidents, look for digital signatures, configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses and finally ensure anti-virus software are up to date.

5.4 Malicious Code

Malicious code is software that does damage and/or creates unwanted behaviors.

Malicious code includes: Viruses, Trojan horses, Worms, Keyloggers, Spyware, Rootkits and Backdoors.

Indications:

The suspicious indicators related to malicious code are: e-mail attachments, instruction to download files, visiting an infected website and Removable media.

The effects include, but are not limited to corrupt files and destroyed or modified information, compromise and loss of information and hacker access and sabotaged systems.

In respect of countermeasures, a user can take different steps while creating a password, e.g, combine letters, numbers, special characters, do not use personal information, do not use common phrases or words, do not write down your password, memorize it, change password according to your organization's policy, enforce account lockout for end-user accounts after a set number of retry attempts, do not save your passwords or login credentials in your browser and NEVER share your password. (Whitman & Mattord, 2009)

5.5 Removable Media

Removable media is any type of data storage device that can be added to and removed from a computer while the system is running. Hackers may use removable media to gain access to your system. Examples of removable media include:

- Thumb drives
- Flash drives

- CDs
- DVDs
- External hard drives

The indicators which cause problems to user, e.g, leave removable media, such as thumb drives, at locations for personnel to pick up and to send removable media to personnel under the guise of a prize or free product trial

The countermeasures against removable media vulnerabilities are: e.g, contractors: follow your organization’s removable media policy, DoD personnel: do not use flash media unless operationally necessary and government-owned, do not use any personally owned/non-Government removable flash media on DoD systems, do not use Government removable flash media on non-DoD/personal systems, encrypt all data stored on removable media, encrypt in accordance with the data's classification or sensitivity level, use only removable media approved by your organization, store in GSA approved storage containers at the appropriate level of classification

6. CASE STUDY: INTERVIEW WITH IT SUPPORT OFFICER OF A UNIVERSITY

6.1 Methodology

A qualitative research has been done for Bachelor´s Thesis in which an interview is conducted with Head of Network Services of Oulu based university. A questionnaire is designed keeping in mind the network and security issues. The questionnaire contains multiple questions related to some basic information about university IT infrastructure and security measures implemented to protect the university network from external and internal threats.

Based on answers received from IT department of university, an analysis has been done regarding security issues for the users. After the analysis, the conclusion is drawnfor some further observations of how cybersecurity is affective in any organization and how the utilization could be taken even further.

Following are the questions and answers received from IT department of the university:

6.2 Summary of the Interview

Questions can be found at Appendix-I.

An interview was conducted with the Head of Network Services (Internetworking Expert) at an Oulu based university. His area of responsibilities is Management of background systems like active directory, forefront identity manager, Microsoft Exchange, Microsoft Lync-environments etc. As well as to manage all Linux-, Windows- and Solaris servers, making backups and monitoring of network. The university has around 7500 computers and 300 servers. The university mainly using servers like, MySQL, Oracle, Apache/Apache tomcat, Linux servers, Windows servers (Sharepoint, FIM, Exchange, SQL, UAG, TMG, PKI, Hyper-v, Direct access, Active directory, Lync, Remote desktop services and IIS), Solaris servers. The operating systems for end users in the university are Windows Servers 2003 – 2012, Linux Servers (Debian, Ubuntu and Red hat), Solaris servers, Windows XP, Windows 7 and Windows 8.

In response to question about cybersecurity, he told that cybersecurity deals with defending the whole society than one single organization. Cybersecurity can be defined

as securing systems security and making sure that systems are functioning in all situations and it is really helpful for the protection of network. The university protects network from threats by using external and internal firewalls (firewalls contain different programs like IDS (Intrusion Detection System). Computers and servers are equipped with antivirus programs. Different kinds of devices are used for the cybersecurity e.g, Layer ¾ - Switches work as Internal Firewalls and Linux-based operating systems are used as External Firewall.

He also told that they face cybersecurity threats almost every day. Every case is little bit different and they have been taking care of security threats by different methods. Firewalls are really effective and helpful for protection of network from internal and external security threats. To protect the university network from computer viruses, they use anti-virus software to detect or remove malware such as: computer viruses, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, dialers, adware and spyware. But on the other antivirus software might slow the performance of systems. They also cause wrong alarms and malfunctions etc.

In response to the expenditure for protection of network, he mentioned that security systems purchased once during the establishment of computer labs and it costs a lot more than expected. The university allocates funds to update the systems and anti-virus software.

According to him, it is not easy to get rid of spam email. Some spammers find always a way to bypass spam blocking software. Spammers are more active and smarter than spam blocking software developers.

In response to junk emails, he replied that if a user receives junk email, it means that his account has been hijacked or sender spoofed. If account is hijacked, user can change password if it is possible or contact the help desk. To send email by wrong name or other person´s name is quite easy. Individual users cannot influence sender spoofing, this is service provider´s job. The user can prevent hijacker using his account by defining new, longer and more complex password (for example at least 11 characters). A number of measures to address spoofing have been proposed, including: SPF, Sender ID, and DKIM, and these are widely implemented. Password managers play vital role against password hijacking. If password is long and complex it is harder to hack.

In response to emails regarding lottery winnings, he told that these kind of winning are rarely or never informed by email In Finland. People should use common sense in cases like this. There are many ways to explore if message is really a spam. The user should see the sender address, if the message comes from a respected company or well established website, it will not have an email address like support@free email service provider.com or .net etc and also look at the message contents: email asking for personal information, grammatical and spelling errors within the email message etc. The message headers contain tracking information for an individual email, detailing the path a message took as it crossed mail servers and mail servers IP-addresses. The user can check the authenticity of email through Ripe Network Coordination Centre website (http://www.ripe.net) to whom IP-address belongs to.

The level of threats in universities is Medium. Most of the universities are equipped with firewalls and anti-virus software. IT staff in universities keep guard on the campus network. Over preparation and making too tight security policies may complicates normal use of the systems. A network manager can prevent cybersecurity threat by monitoring, controlling and keeping system´s security updated.

If a user wants real computer security, he needs to adopt safe computing practices rather than rely totally on security products to protect him. No security product or combination of products can or ever will provide perfect system security just like no car can provide perfect road safety. With both cars and systems, user needs to be careful in own behavior.

6.3 Analysis

Based on the data received from university, the university is well equipped with 7500 computers and 300 servers. The university installed the most advanced operating systems in server side and end user side. They protect university intranet and internet by installing different kinds of internal, external firewalls and antivirus software. According to System Administrator, they face security threats almost every day. He mentioned that antivirus softwares are quite helpful in detecting and removal of malwares but these softwares also affect the performance of the computers. He also mentioned that it is difficult to stop receiving spam because some spammers are clever to bypass the security barriers. According to him, user must select the strong password which can help user to protect their accounts and prevent receiving junk emails.

In response to promotional emails, system administrator recommends that end user must be educated regarding respond to fake emails. A user can check the authenticity of the email by verifying sender's email address and the content of email.

A network can be protected by regular monitoring, controlling and keeping the security softwares updated.

7. COMPUTER USER AWARENESS FOR CYBERSECURITY

While using a computer connected to the Internet through cable or wireless network, computer is a primary target for cyber criminals. Hackers are mostly looking for credit card numbers, bank account information and any other information they can use for their own gain. It is not just money-related information they are after; once they invade a computer, intruders can use the hard disk, processor and Internet connection to attack other computers.

Many personal computers are especially vulnerable because in general the average computer user does not realize the risks of being on a network and the protections that are available to guard against these threats. All users need to educate or train themselves and understand the threats in order to more effectively protect their personal information and computer systems.

According to reliable sources, approximately 1.9 billion people are now connected to the internet. Most of these individuals are conducting business, sending emails, researching and staying in touch with other people. But there are also those with evil intentions.

Cybersecurity is similar to home security. Because possible security risks can occur at a variety of levels, it is needed to set up measures that provide multiple layers of defense against these threats. Therefore, your best defense is a thoughtful and proactive offense. By using a layered approach which ensures that an attacker who penetrates one layer of defense, will be stopped by another following layer. (DAMICO, 2009)

Following measures can be adopted to protect computer from external threats:

7.1 Update Software

Just like clothing can get weak, especially the garments we wear the most – software can also develop vulnerabilities. The software we use the most (our operating systems, internet browsers and word-processing programs, for example) become vulnerable because hackers are aware these are the applications most commonly used by computer users. Therefore, a hacker gets the most advantage by finding and exploiting vulnerabilities in software.

Application developers will send out updates for their applications. But it is not enough for the updates to be sent; computer users should download and install these updates.

7.2 Installation of Security Software to Computers

Computer viruses are applications intentionally designed to interfere with the condition of computer. Just like human viruses vary in severity from the flu to the Ebola virus, computer viruses range from the mildly infuriating to the absolute destructive, and come in new and different forms.

While the term spyware implies software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware applications can collect personal information, as well as intervene with the proper functioning of your computer.

By using endpoint security software such as antivirus and anti-spyware and keeping them updated with security patches provide one more necessary and important layer of defense for end user’s computer.

7.3 Use Strong Password

Passwords are an important feature of computer security. They are the leading edge of protection for user accounts. A strong password that is kept private is a critical layer of cybersecurity. The computer and data are only as safe as the password is used to access them. If someone authenticates as you, they are then authorized to do anything you could do on your computer or account.

The number of computers and data illegally accessed are growing every year because of weak passwords. For convenience, most users choose passwords that are easy to remember. Unfortunately, the easier the password is, the easier it is for a hacker to crack it. One of the first things a hacker will do against a system is run an application that will attempt to guess the correct password of the target machine. These applications contain entire dictionaries from several different languages. Besides words found in dictionaries, these applications often contain names, words from popular culture such as movies, songs, application default passwords and novels, list of the most common passwords used (i.e. password1, password2) and common character sequences such as

"123456" or "abcdef". This is why it is so important to use strong passwords, and not share them.

7.4 Limited Use of Privileged Accounts

Many computer users login to their computers as administrator for all their assignments and work related activities. Unfortunately, many email and Web-based attacks take advantage of this by hijacking the security context of the logged-in user which let malicious code in to be executed when the user clicks on something they should not do. This is why logging in and running computer as an administrator makes computer vulnerable to security risks and exploits, such as Trojan horses and other forms of malicious activities.

Common tasks such as checking emails, web browsing, and instant messaging do not require administrative rights. To get more secure, users should log on with a Limited User Account (LUA), and use important privileges only for specific tasks that require them such as downloading or upgrading software.

7.5 Make Backups of Important Files and Folders

Mostly people divide their personal belongings into two broad categories: those items they can replace and those they can't. For the items they can't replace, they have probably stored them in a safe place, either somewhere in their living space or in a lockbox at a bank. In either case, they have probably bought insurance that provides the funds they would need to buy replacements.

For example, the files containing financial records, that assignment you've been writing for the past few months, and pictures you took last summer with your digital camera. What happens if your computer malfunctions or is destroyed by an intruder? Are these files gone forever? Do you have a way to continue working on important computer files when you have a malfunction or an intruder attack?

Most users know that intruders try to break into their home computer to gain access to files and computer's resources. Another way to gain access to the same information is by stealing backups. It is more difficult, since a thief must physically be where backups are, whereas an intruder can access home computer from any network connection in the world. The key is to know where the media is that contains your backed up files.

Just like important papers stored in a safe place at your house, you also need to be careful about your backups being destroyed if your living space is destroyed or damaged.

7.6 Secure Physical Environment

Every high-tech security tip can be followed, but if the physical environment is insecure, information is insecure. Being attentive of surroundings and implementing preventative measures against threats and attacks in place are part of everyday life.

The amount of laptops is increasing for both business and personal use. The portability of laptops makes them more convenient. However, users must also be aware of the security risks from the loss or theft of laptops, and take proper measures. The potential loss is dual; the loss of the laptop itself and any personal or sensitive data that it may contain.

Attach the laptop with a security cable to something fixed or to a heavy piece of furniture when it is unattended. User should secure laptop with a strong password, but don't keep the password in the laptop case or on a piece of paper stick to the laptop.

7.7 Always Use Secure Wireless

Wireless networks commonly known as WiFi, allow user to connect to the internet without relying on cables. If a home, office, airport, or even coffee shop has a wireless connection, it can be accessed from anywhere that is within that wireless area.

Wireless networks rely on radio waves rather than cables to connect computers to the internet. A transmitter, known as a wireless access point, is wired into an internet connection. This provides a "hotspot" that transmits the connectivity over radio waves.

Since wireless networks do not require a cable between a computer and the internet connection, it is possible for attackers who are within range to hijack or intercept vulnerable connection.

A practice known as wardriving involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is usually posted online. Some individuals who participate in wardriving have malicious

intention and can use this information to hijack home wireless network or intercept the connection between your computer and a particular hotspot.

By changing default passwords makes it harder for hijackers to take control of the device. Only allow authorized users to access the network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses.

It is a good security practice to install a firewall on network. It can also be installed directly on wireless devices (a host-based firewall). Attackers who can directly tap into wireless network may be able to dodge network firewall.

7.8 Understanding Peer to Peer Technology and Social Networking

Peer-to-Peer (or P2P) file-sharing is a technology that allows user to share files online through an informal network. P2P gives access to a large amount of information, but due to other computers on the network being able to search for files on one's own computer, exposure to viruses, spyware and malicious code is potential.

Social Networking websites such as Facebook, Twitter, and LinkedIn became popular on the internet, but can also be places that identity thieves use to capture personal information they can use against users. Phishers, account thieves, and malware pushers frequently try to access your account through gaming application scams, malicious script scams, and click-jacking. Their goal is to get access to user personal information so they can exploit it. So think before you click, because you are the first line of defense.

7.9 Secure Messaging

Instant messaging and email are new phenomena which have made communication easy and instantaneous and a soft target for hackers and identity thieves. Spam and phishing attempts hit a mailbox possibly hundreds of times a day. So how can one know that the attachment just received in email is free of malware?

A user can protect his account by implementing following measures:

- Never respond to emails that request personal financial information
- Visit banks' websites by typing the URL into the address bar

- Keep a regular check on your accounts
- Check the website you are visiting is secure
- Be cautious with emails and personal data
- Always report suspicious activity

8. CONCLUSION AND DISCUSSION

The purpose of thesis is to find out the cybersecurity threats caused by cyber criminals and elaborate them with quality research methods. Cyberspace has evolved into a highly interdependent and technologically dynamic environment. The vulnerability of networks around the world presents challenges to securing the organizations, schools and government agencies from cyber attacks.

The only hope for securing classified and highly sensitive information, and the safety of the public and the country, is through public and private sector partnerships. The complexity of maintaining secure networks, systems, and offices, makes it virtually impossible for one sector to achieve success without the support of the others. By working together, the government and the private sector can influence the fundamental skills, expertise, and assets that each provides to reduce cyber risk.

While cyber attacks will continue to increase, government organizations can achieve tighter security by working with experienced communications and network providers to prevent cyber crime before it happens and defend against cyber attacks when they occur.

As a result, computer and information security continue to grow in importance. The gap between attackers' capabilities and ability to defend against them is widening. Neglecting security is the worst thing we can do. Always weigh costs versus benefits when considering security measures. It must be noted that law is always seven steps behind the technology. This is so because we have a tendency to make laws when the problem reaches at its zenith. The enforcement of rights requires a "qualitative effort" and not a "quantitative effort".

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. The history of this society is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible measure is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more strict to check crime.

9. REFERENCES:

Anonymous. (1998). *Maximum Security.* Indianapolis: SAMS.

B., M. (2012). *Chrysallid Enterprise Technology Solutions*. Retrieved December 12, 2012, from http://www.linkedin.com/groups/Chrysallid-Enterprise-Technology-Solutions-Cybersecurity-4738988/about

c5franey. (2011). *Disaster Recovery Plan*. Retrieved March 21, 2012, from Study Mode: http://www.studymode.com/essays/Disaster-Recovery-Plan-809693.html

DAMICO, T. M. (2009). *Cyber Attack Prevention for the Home User: How to Prevent a Cyber Attack*. Retrieved May 07, 2013, from Student Plus: http://www.studentpulse.com/articles/47/cyber-attack-prevention-for-the-home-user-how-to-prevent-a-cyber-attack

Douligeris, C., & Serpanos, D. (2007). *Network Security, Current Status and Future Directions.* Canada: John Wiley & Sons Inc.

Goodman, D. (2004). *Spam Wars.* New York: SelectBooks.

ll, O. C. (2011). *Mobile Apps: New Frontier for Cybercrime*. Retrieved December 9, 2012, from Trend Micro: http://about-threats.trendmicro.com/RelatedThreats.aspx?language=en&name=Mobile+Apps%3A+New+Frontier+for+Cybercrime

Rouse, M. (2012). *botnet (zombie army).* Retrieved February 09, 2013, from SearchSecurity: http://searchsecurity.techtarget.com/definition/botnet

Stilgherrian. (2013). *WordPress attack highlights 30 million targets*. Retrieved May 02, 2013, from ZDNet: http://www.zdnet.com/wordpress-attack-highlights-30-million-targets-7000014256/

Sukumar, S. (2011). *How to Prevent Email Bombing*. Retrieved June 21, 2012, from Buzzle: http://www.buzzle.com/articles/how-to-prevent-email-bombing.html

Viega, J. (2009). *the myths of security.* Sebastopol, USA: O'Reilly Media.

Whitman, D. M., & Mattord, H. J. (2009). *Principles of Information Security*. Massachusetts, USA: Course Technology.

10. APPENDIX-I

Questions

1. How many computers do you have in your school network?
2. Which server technology are you using inside the office?
3. Which operating systems are in use in the school?
4. How do you define cybersecurity?
5. Does the Cybersecurity really help to protect the network or is it just a myth?
6. How do you protect school's network?
7. What kind of devices you use for the cybersecurity?
8. How many times you faced security threats (internally and externally) and how did you manage it?
9. Do you think firewalls really help to protect the network?
10. Do you think anti-virus software can protect from internet threats, if yes than how?
11. Is there any disadvantage of antivirus software?
12. How much money school spends per year for cybersecurity?
13. Do you think it is easy to get rid of spam emails?
14. How can junk emails be blocked?
15. Can we prevent the attack from reoccurring?
16. Are password managers effective and safe?
17. Is it easy to steal or hack someone's password?
18. You received an email promotion stating that you won a new car how can you prove or disprove the legitimacy of this promotion?
19. How big a threat is for cybersecurity in schools or universities?
20. What are the biggest mistakes schools do regarding cybersecurity?
21. What strategies should a network manager follow to prevent the threats?
23. Any suggestion for new users?