Cyber Security

Student Training Manual

BI Leadership Development Ministries

Douglas A Kossel, Ph.D.

TABLE OF CONTENTS

Module One: Getting Started 7

Workshop Objectives 7

Module Two: Cybersecurity Fundamentals 8

What is Cyberspace? 8

What is Cybersecurity? 9

Why is Cybersecurity Important? 9

What is a Hacker? 9

Case Study 10

Module Two: Review Questions 11

Module Two: Review Questions 12

Module Three: Types of Malware 13

Worms 13

Viruses 14

Spyware 14

Trojans 15

Case Study 15

Module Three: Review Questions 16

Module Three: Review Questions 17

Module Four: Cyber Security Breaches 18

Phishing 18

Identity Theft 19

Harassment 19

Cyber Stalking 20

Case Study *20*

Module Four: Review Questions *21*

Module Four: Review Questions *22*

Module Five: Types of Cyber Attacks **23**

Password Attacks *23*

Denial of Service Attacks *24*

Passive Attack *24*

Penetration Testing *25*

Case Study *25*

Module Five: Review Questions *26*

Module Five: Review Questions *27*

Module Six: Prevention Tips **28**

Craft a Strong Password *28*

Two-Step Verification *29*

Download Attachments with Care *29*

Question Legitimacy of Websites *30*

Case Study *30*

Module Six: Review Questions *31*

Module Six: Review Questions *32*

Module Seven: Mobile Protection **33**

No Credit Card Numbers *33*

Place Lock on Phone *34*

Don't Save Passwords *34*

No Personalized Contacts Listed *35*

Case Study *35*

Module Seven: Review Questions *36*

Module Seven: Review Questions *37*

Module Eight: Social Network Security **38**

Don't Reveal Location *38*

Keep Birthdate Hidden *38*

Have Private Profile *39*

Don't Link Accounts *39*

Case Study *40*

Module Eight: Review Questions *41*

Module Eight: Review Questions *42*

Module Nine: Prevention Software **43**

Firewalls *43*

Virtual Private Networks *44*

Anti-Virus & Anti-Spyware *44*

Routine Updates *45*

Case Study *45*

Module Nine: Review Questions *46*

Module Nine: Review Questions *47*

Module Ten: Critical Cyber Threats **48**

Critical Cyber Threats *48*

Cyber Terrorism *49*

Cyber Warfare *50*

Cyber Espionage *50*

Case Study *51*

Module Ten: Review Questions *52*

Module Ten: Review Questions *53*

Module Eleven: Defense Against Hackers **54**

Cryptography *54*

Digital Forensics *55*

Intrusion Detection *56*

Legal Recourse *56*

Case Study *57*

Module Eleven: Review Questions *58*

Module Eleven: Review Questions *59*

Module Twelve: Wrapping Up **60**

Words from the Wise *60*

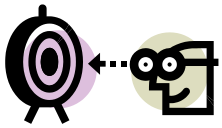
At the end of the day, the goals are simple: safety and security.

Jodi Rell

Module One: Getting Started

Every organization is responsible for ensuring cybersecurity. The ability to protect its information systems from impairment or even theft is essential to success. Implementing effective security measures will not only offer liability protection; it will also increase efficiency and productivity.

Workshop Objectives



Research has consistently demonstrated that when clear goals are associated with learning, it occurs more easily and rapidly. With that in mind, let's review our goals for today.

At the end of this workshop, participants should be able to:

- Understand different types of malware and security breaches
- Know the types of cyberattacks to look out for
- Develop effective prevention methods

U.S. computer networks and databases are under daily cyber-attack by nation states, international crime organizations, subnational groups, and individual hackers.

John O. Brennan

Module Two: Cybersecurity Fundamentals

Before developing and implementing security measures to prevent cyberattacks, you must understand basic concepts associated with cybersecurity and what cyberattacks are. The method(s) of cybersecurity that a company uses should be tailored to fit the needs of the organization.

What is Cyberspace?

Cyberspace is the environment where computer transactions take place. This specifically refers to computer-to-computer activity. Although there is no "physical" space that makes up cyberspace, with the stroke of a few keys on a keyboard, one can connect with others around the world.

Examples of items included in cyberspace are:

- Networks
- Devices
- Software
- Processes
- Information storage
- Applications

What is Cybersecurity?

As previously mentioned, cybersecurity is the implementation of methods to prevent attacks on a company's information systems. This is done to avoid disruption of the company's productivity. Not only does cybersecurity include controlling physical access to the system's hardware, it protects from danger that may come via network access or the injection of code.

Why is Cybersecurity Important?

Cybersecurity is crucial to a business for a myriad of reasons. The two this section will focus on are data security breaches and sabotage. Both can have dire effects on a company and/or its clients.

Data security breaches can compromise secure information such as:

- Names and social security numbers
- Credit card and bank details
- Trade secrets
- Intellectual property

Computer sabotage serves to disable a company's computers or network to impede the company's ability to conduct business.

What is a Hacker?

In simple terms, a hacker is an individual or group of individuals who use their knowledge of technology to break into computer systems and networks, using a variety of tools to gain access to and utilize other people's data for devious reasons.

There are 3 main types of hackers. They are:

Grey hats: These hackers do so "for the fun of it".

Black hats: These hackers have malevolent reasons for doing so, such as stealing and/or selling data for monetary gain.

White hats: These hackers are employed by companies to hack into systems to find where the company is vulnerable, with the intention of ensuring the safety of the data from hackers with ill intentions.

Case Study

Patrick and Willow are in the process of opening a small answering service business. They are discussing the various needs of the company, including the type of security they are going to use for their computer systems. Patrick tells Willow that he doesn't believe it's necessary to implement any type of computer security because their business is small. Willow states even though their business will start out small, they are still vulnerable and there are many hackers out there that can break into their system and disrupt business.

Module Two: Review Questions

Module Two: Review Questions

Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm.

Anna Maria Chavez

Module Three: Types of Malware

"Malware" is the shortened form for malicious software, which is intrusive software, used to perform actions such as interrupting computer operations and obtaining sensitive information. Acquiring access to private computer systems and brandishing unsolicited advertising are also characteristic of Malware.

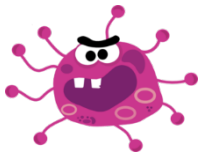
Worms

A computer worm is an independent malware program that reproduces itself to infect other computers. It can spread to other computers without having to attach to an existing program, but still causes some form of damage to the network.

Damage done by worms includes:

- Bandwidth consumption
- Stopping active anti-malware service
- Immobilizing Safe Mode
- Hindering Windows auto update

Viruses



A computer virus is a program that hides within a harmless program that reproduces itself to perform actions such as destroying data. It can infect files and when the file is opened, spread the virus throughout your computer. The virus will further spread if the infected file is shared with others.

Damage done by viruses includes:

- Corrupting files
- Computer slowdown
- Taking over basic functions of the operating system

Spyware

The main purpose of Spyware is to obtain information about an individual or company without their knowledge or consent. The data gathered from this act of "spying" is sometimes sent to another entity. It can also be used to gain control over one's computer without the user realizing it. It is commonly used to track the user's movements and bombard him/her with pop-up ads.

Damage done by spyware includes:

- Collecting personal information
- Installing unsolicited software
- Redirecting web browsers
- Changing computer settings
- Slowing down Internet connection

Trojans

Trojans gain access into computers by misleading users of what it is truly meant to do. They spread in sneaky ways. For example, a user may receive an email attachment that appears to be legitimate, but when he/she opens it, it in fact gives the attacker the opportunity to obtain the user's personal information, such as banking details and passwords.

Damage done by Trojans includes:

- Crashing the computer
- Deleting files
- Corrupting data
- Logging keystrokes

Case Study

Many employees at XYZ Company have noticed that their computers are moving slowly. Harry has complained that somehow the settings he previously had on his computer have changed. Also, when he types in a particular URL for a website, his browser takes him somewhere completely different. Tom notices that files that are supposed to be saved to his computer have been deleted. Harry and Tom go to their supervisor, Jerry, to inquire about what is going on. Jerry turns on his computer and observes similar issues.

Module Three: Review Questions

Module Three: Review Questions

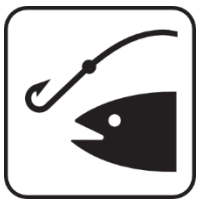
Choosing a hard-to-guess, but easy-to-remember password is important!

Kevin Mitnick

Module Four: Cyber Security Breaches

Cyber security breaches are the result of secure information being released to a treacherous environment. Whether the data is released intentionally or unintentionally, the consequences can have long-lasting effects, from harassment to identity theft.

Phishing



Cybercriminals who use phishing scams aim to obtain personal information by appearing to be a legitimate source. Many times, they masquerade as a major company, such as a bank, appealing to your desire to keep your information safe.

For example, they may send an email that says, “We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

Clicking the link or responding to the email can take you to a website that looks authentic, but is in fact a spoof site that serves to steal your information and use it for malicious purposes, such as commit crimes using your name or using your bank information for personal gain.

Identity Theft

Identity theft can be considered one of the worst case scenarios when it comes to cyber security breaches. Whether hacking into a company's computer system to assume the identity of the company or doing so to steal the identities of the company's customers / clients, the end result can be disastrous.

Those who seek to steal another's identity typically do so and move on quickly, making it difficult to track and prosecute the perpetrator. This is why "an ounce of prevention is worth a pound of cure".

There are many ways to help prevent identity theft. Some examples are:

- Be mindful of phishing websites
- Utilize an Anti-virus / Anti-malware program
- Don't respond to unsolicited requests for secure information

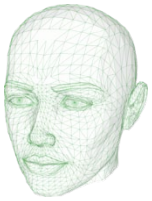
Harassment

Cyberbullying is not just limited to individuals. Cyberbullies can use their vices to ruin the reputation of a company as well. Many companies have social media accounts that allow the general public to post comments, complaints, and suggestions. Some use this opportunity to post cruel and negative comments, or even threats.

What are some ways to handle cyberbullies?

- **Do not immediately respond.** When one feels attacked, the immediate tendency is to respond out of emotion. Doing so could escalate the issue, so take some time to process the information and compose yourself before dealing with the issue.
- **Tell the cyberbully to stop.** Granted, this may not always work, but sometimes being told that the behavior is not acceptable is all one needs in order to cease.
- **Get the authorities involved.** Contact the police. The police many times have the necessary tools to track down the culprit and help put a stop to the behavior.

Cyber Stalking



Cyberstalking a company can include acts such as false accusations and defamation, which can affect the standing of the company in the community. The cyber stalkers' intention is typically to intimidate or in some way influence the victim. Cyberstalking is a criminal offense that is punishable under the anti-stalking laws.

Being found guilty of cyberstalking could lead to penalties from a restraining order against the assailant to the assailant serving jail time.

Anti-Stalking Tips:

- Be sure you always have physical access control over your computer, to prevent the stalker from gaining that control without your knowledge.
- Always log out of programs before stepping away from your desk. Utilize a screensaver and password.
- Protect your passwords. Do not share them. Change them often.
- Keep your security software updated.

Case Study

Paula works for and also banks with 123 Bank. She received what appears to be an email from the bank that stated, "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity." As she got ready to click the link, something told her to consult with her co-worker, Emily, to confirm this is something that their bank does. Emily told Paula that their company doesn't send out such emails. In fact, most companies do not.

Module Four: Review Questions

Module Four: Review Questions

Module Five: Types of Cyber Attacks

Cyber attacks are orchestrated by individuals or groups to destroy the information systems, networks, etc. of others. From installing Spyware on a computer to obliterating a company's entire infrastructure, cyber-attacks can have devastating effects on many.

Password Attacks

Passwords are intended to prevent unauthorized access to your accounts, so it's important to use passwords that are strong in order to prevent threats against the privacy and security of the data associated with your company and customers.

Why is it important to use a strong password?

There is software available to hackers that will allow them to try various passwords in an attempt crack the code of and infiltrate your system.

How to protect your business:

- Create a password that is easy for you to remember but difficult for someone else to figure out
- Include upper and lower case letters, numbers, and symbols
- Craft a password that is long
- Regularly update your password

Denial of Service Attacks

Denial of service attacks are just as its name states. Its goal is to make a network unavailable to its intended users. This type of attack can be used against individuals where they consecutively enter the wrong password enough times that they are locked out of their account. It can also manifest as a network being so overloaded that no one can get in.

Damage caused by denial of service attacks:

- Network performs slowly
- A specific website is inaccessible
- No websites are accessible
- Receiving a large amount of spam emails

Passive Attack

A passive attack is conducted to simply find the vulnerabilities of system, but not change any data at that time. Think of it in terms of a conversation that two people are having and the passive attacker is eavesdropping in on the conversation. Although it may seem like a harmless act at the time, if the intruder is able to obtain the “right” information, he/she can use that in the future to cause irreparable damage.

A passive attack is different from an active attack, which aims to change data of the system at the time of the attack.

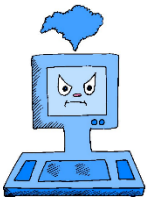
Penetration Testing

Penetration testing can be a positive tool for an organization. It is done to unearth the vulnerabilities of a computer system, then take advantage of those vulnerabilities to get an idea of the impact an actual attack will have on the system.

There are many reasons why a company would utilize penetration testing. Some of these include:

- Establish the likelihood of a specific attack occurring
- Detect high risk vulnerabilities that can result from a grouping of low risk vulnerabilities that take place in a particular pattern
- Determine the bearing an attack will have on a company
- Assess the company's network risk management capabilities

Case Study



Kurt and Jeff are new hires with Bob's Electronics. They are at their desks, setting up their computer passwords. Kurt tells Jeff he should create a password that is long and includes letter, numbers, and symbols, so it will be difficult for others to figure out. Jeff said he doesn't trust his memory to such a password and will probably create one that just has letters. Three months later, Jeff notices he has started receiving a lot of spam in his inbox. A week after, he tries to login to his system by inputting his password, but it locks him out after several failed attempts, and he has to call technical support for assistance.

Module Five: Review Questions

Module Five: Review Questions

Module Six: Prevention Tips

Although it may not be possible to completely avoid falling victim to cybercrime, having a tool kit of prevention methods could help your organization minimize the risk of such crimes damaging the reputation of your company or faith of your clients/customers.

Craft a Strong Password

One of the easiest steps to keeping your data safe is to craft solid login credentials. If possible, remember the password so that it doesn't have to be written down. If you must have the password written down on hard copy somewhere, be sure to store it in a secure location, with few people who have access to it.

What are some tips for creating a strong password?

1. Use a unique password for each of your accounts. Do not use one password for all of them.
2. Ensure your password consists of letters, numbers, and symbols. This would make it harder for others to figure out.
3. Avoid using common words or consecutive characters to make up your password (e.g. Do not use "password" as your password. Do not use a password such as Office111).

Two-Step Verification

Two-Step Verification is a way of authenticating and individual's identity using two components, before he/she gains access.

The idea behind this process is that although an imposter has one piece of the victim's identifying information, they most likely don't have two.

Examples of information that may be used for authentication purposes:

- Token
- Key
- Password
- Pin
- Fingerprint
- Voice recognition

Download Attachments with Care

It's important to always download email attachments with care, even if the email appears to be from a credible source. Although the attachment seems to have a well-known extension (e.g. .PDF, .doc, etc.), it could in fact be a Trojan.

Protect yourself by considering these steps:

- Regularly update software patches.
- "Go with your gut". If something doesn't seem right, it probably isn't.
- Save and scan the true source of the attachment before opening it.

Question Legitimacy of Websites

There are many websites that at first glance, look like legitimate sites. But, upon further examination, you realize it is a spoof. Opening such a site could lead to damage such as slowing down the speed of your computer or even worse, the loss of files or stolen identity. It is important to take precautionary measures when visiting websites, even if it is a site you have visited in the past.

- Type the complete URL in the browser
- When doing a Google/Bing search, do not open websites with names that just don't look right
- Question the intentions of the sender when you receive an unsolicited email to visit a particular website
- Make sure your Anti-Spyware/Anti-Virus program is up-to-date so it can warn you of a website that looks suspicious

Case Study

The new employee trainer, Ann at Investment Management Company is discussing with the trainees tips to keep in mind as they are creating the passwords for the different work systems they will have to log into, so that the passwords are strong and not easy to figure out. She also talks about the company's two-step verification process to ensure that only the authorized person can access the account. Lastly, she goes over determining whether or not a website is legitimate before opening it. Carl, one of the trainees states that he is curious about the company's policy on opening attachments from co-workers and outside sources.

Module Six: Review Questions

Module Six: Review Questions

The beginnings of the hacker culture as we know it today can be conveniently dated to 1961, the year MIT acquired the first PDP-1.

Eric S. Raymond

Module Seven: Mobile Protection

It is just as important to protect your Smartphone as it is your computer. With phones having many of the same capabilities as computers, they are open to many of the same vulnerabilities that computers face. This module will discuss several small but effective steps to take to ensure mobile protection.

No Credit Card Numbers

Many times, it seems convenient to store credit card numbers on your phone so you have them at your fingertips and you don't necessarily have to rely on your memory. But, just as it is easy for you to access these numbers, it is easy for someone who means harm to access them.

If for some reason it is absolutely necessary for you to store this information on your phone, it is important for you to take extreme measures to make sure the data is safeguarded, such as tokenization and/or encryption.

Place Lock on Phone

Enabling a lock on your phone when not in use, and a pin or password to unlock the phone could help prevent unauthorized use of the phone. Just as we talked about in a previous module, if you set a password on your phone, it is important to create a strong password.

As a reminder, keep these tips in mind when creating your password:

- Use a unique password for each of your accounts. Do not use one password for all of them.
- Ensure your password consists of letters, numbers, and symbols. This would make it harder for others to figure out.
- Avoid using common words or consecutive characters to make up your password (e.g. Do not use "password" as your password. Do not use a password such as Office111).

Don't Save Passwords

When it comes to passwords, the ideal situation would be to remember them so there is no trail of what they are, which could make it easy for an unauthorized user to utilize them. But the fact is, most people have unique passwords for each account they have. Because of this, it may be necessary to use a back-up method in case they are forgotten. If this is the case, write them down and securely store them. Do not save them on your phone.

- Write them down and treat them as you would any other important documents by locking them in a safe or drawer that requires a key.
- Invest in a password manager service.

No Personalized Contacts Listed

You've created a lock on your phone and regularly lock it when it's not in use. You quickly step away from your desk with your phone on it, and forget to lock it. Someone who doesn't have permission to touch your phone decides to go through your contact list. John sees the name Bob Jones with "ABC Company Manager" in parentheses. John writes down Bob's name and number and decides to use it to solicit Bob's business.

This is one scenario of what can happen when your phone includes a personalized contact list. In this example, the result, while uncomfortable, is not an extreme situation. Just think what could have happened!

Case Study

Delores and Earl have recently been given cell phones by their company to be able to conduct business while they are away from the office. Their manager encourages them to lock their phones each time they are not in use and make sure they memorize the password to unlock it. Delores tells Earl that she's happy they have the phones because she can save her customers' credit card information on it so she doesn't always have to refer to her paper file when she needs to conduct a transaction for them. Earl states that it is best not to do that because if her phone gets hacked, the customers' financial data may be compromised.

Module Seven: Review Questions

Module Seven: Review Questions

The hacker mindset doesn't actually see what happens on the other side, to the victim.

Kevin Mitnick

Module Eight: Social Network Security

Many people forget that with social networking, although they are not meeting with people face-to-face, revealing too much information about oneself could still lead to dangerous situations, such as social engineering attacks. This module will discuss some of the ways to protect yourself from being lulled into a false sense of security.

Don't Reveal Location

This seems like an issue of common sense, but many need to be reminded that revealing your location to strangers is never a good idea. Some social media sites require that you input your location, and if that's the case, you can use your creativity to make a fake location or input one a city/state different from where you are actually located. In some instances, the website will allow you to continue without entering anything in the location field.

The Internet is a public source and with disclosing your actual location to strangers, you could open yourself to crimes such as burglary, harassment, or stalking .

Keep Birthdate Hidden

Giving away your birthdate seems like a harmless act, but when a criminal has your birthday, they have one of the several pieces of information needed to steal your identity. If you absolutely must list your birthdate, do not include the year.

Have Private Profile

Just because you post something, doesn't mean it's for everybody to see. Although social media is a useful way of networking professionally and promoting your business, failing to properly manage your profile and privacy settings could have consequences that you cannot undo.

Each social media platform has its own instructions for updating the settings of your profile so that information is distributed according to your wishes. Be sure to thoroughly read through these guidelines.

Some of the most common social media websites:

- Facebook
- Instagram
- Twitter
- Google+
- LinkedIn
- Pinterest

Don't Link Accounts

Although linking social media accounts may be a convenience to you, it is making it easier for thieves to find you. It is especially important that you don't link your personal accounts with your business accounts. Some content on one of your social media sites may not be appropriate for content on another site. For example content you post on Facebook, which is a relatively informal site, may not be appropriate for your LinkedIn account, which is a more formal setting.

What are some other reasons why you shouldn't link your social media accounts?

- Automated posting
- Same messages across different platforms
- Increased risk of identity theft
- More of a chance of receiving spam in inbox (which can be malware and/or viruses)

Case Study

Reagan and Isabel have opened a candy shop. Reagan has been charged with setting up and managing the company's social media account. She enjoys using her personal social media in her spare time and believes this is the perfect opportunity to sharpen her skills. Since she already has a lot of followers on her own social media accounts, she feels it makes sense to just link the business account to hers. This way she doesn't have to work quite as hard to drive traffic to the business. She discusses her plan with Isabel. Isabel questions the idea because Reagan's accounts have a lot of visible personal information that she doesn't think their customers need to know.

Module Eight: Review Questions

Module Eight: Review Questions

As the United States attorney in Manhattan, I have come to worry about few things as much as the gathering cyber threat.

Preet Bharara

Module Nine: Prevention Software

Now we've gotten to the good stuff! We've thoroughly covered the many dangers lurking, with the hopes of taking over your computer systems and even steal your identity. It's now time to talk about the proactive steps you can take to protect yourself and your business. While you may not be able to completely avoid these risks, there are many ways to lessen your exposure to threats, vulnerabilities, and attacks.

Some well-known countermeasures are listed below.

Firewalls

Firewalls use pre-set security rules to keep track of and regulate the incoming and outgoing traffic of your network system.

Think of a fire wall as a blockade between the internal network, which is a trusted source, and external networks which are presumed to not be safe.

The two types of firewalls are network firewalls and host-based firewalls. Network firewalls specifically filter the flow of traffic concerning at least two networks, while host-based firewalls deal with one host that manages the traffic in and out of that particular machine.

Virtual Private Networks

Virtual private networks (VPNs) are private networks that spread across a public network (the Internet). VPNs enable users to send and receive information across the public network as if they are connected to the private networks.

An example of this would be a company that gives its employees access to its Intranet while not inside of the office. This would be called Remote Access VPN.

Another type of VPN is Site-to-Site VPN. This is where one company has offices in different geographical locations. Users are able to connect the network of one office site to the network of another office site.

The above VPN types are based on a variety of VPN security protocols, which come with different qualities and degree of security.

Protocols:

- Internet Protocol Security
- Layer 2 Tunneling Protocol
- Point-to-Point Tunneling Protocol
- Secure Sockets Layer and Transport Layer Security
- OpenVPN
- Secure Shell

Anti-Virus & Anti-Spyware

Anti-Virus Software

Anti-Virus Software protects users from many different threats. Some of these include viruses, browser hijackers, rootkits, Trojans, worms, and Ransomware.

Anti-Spyware Software

Anti-Spyware Software aims to detect and dispose of spyware programs that the user doesn't intend to have on his system. These Spyware programs are installed on the computer without the user's knowledge or consent and collects information about them. Spyware can cause damage such as posing a security risk and reducing system performance.

Examples of companies that offer Anti-Virus/ Anti-Spyware programs:

- McAfee
- Kaspersky
- Bitdefender
- Norton

To ensure you Anti-Virus/ Anti-Spyware programs are working properly, it is crucial that you regularly update your settings and run scheduled scans to check for anything suspicious.

Routine Updates

Operating systems regularly release updates to address security issues and improve computer performance. The three categories that these fall into are high priority, suggested, and drivers.

High priority updates are just as their name states. They are very important and should be non-negotiable. Examples of such updates include security patches and bug fixes.

Suggested updates can help improve the performance of your computer, but not typically do not allow for major problems, if not installed.

Drivers can be a bit more complicated if you're not versed in what they are and how to install them. If you are positive that you need the update for that driver, install it. Otherwise, it could be more of a headache than it is worth.

Case Study

Greg and Richard are in a meeting discussing the recent cyberattack their company underwent. They are bouncing ideas off of each other regarding what methods they want to implement to prevent this from happening again. Greg says at a minimum, they should invest in Anti-Virus/Anti-Spyware software. Richard agrees and says they should also look into firewalls and making sure their operating system is conducting routine updates as it should. Greg questions what security measure they should have in place for when they are working on their business computers away from the office.

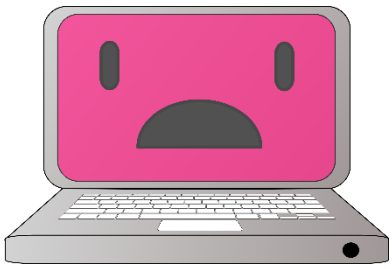
Module Nine: Review Questions

Module Nine: Review Questions

Cyber war takes place largely in secret, unknown to the general public on both sides.

-Noah Feldman

Module Ten: Critical Cyber Threats



Critical cyber threats are those that if carried out, could have a debilitating effect on an organization or even a country. In the case of a country, it could negatively impact aspects such as security, national economic security, and national public health.

Critical Cyber Threats

Source: www.grist.org

As mentioned above, these cyber threats are not designed to temporarily disable an organization, but completely destroy it. To give you an idea of the magnitude of such an attack, again using a country as an example, according to the Department of Homeland Security, some of the critical infrastructures of a country that can be demolished as a result include:

- Energy
- Defense
- Transportation
- Food and agriculture
- Emergency services
- Communications
- Water and wastewater
- Manufacturing
- Chemical
- Commercial facilities
- Dams
- Finance
- Healthcare
- Government facilities
- Nuclear facilities

Cyber Terrorism

Cyber terrorism is cyber threats/attacks on a large scale. These acts are designed to terrorize the Internet as a whole or entire computer networks. This is done by tools such as spreading viruses to computers.

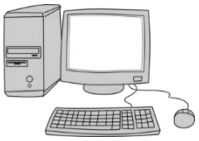
Examples of Cyber terrorism include:

- In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

- In 1998, Spanish protesters bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the Web site for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

Source: https://en.wikipedia.org/wiki/Cyberterrorism

Cyber Warfare



Cyber warfare is a means of war against another state or country to damage that other state/country's information networks. Many times this is carried out via computer viruses or denial of service attacks.

Examples of Cyber warfare include:

- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

Source: http://searchsecurity.techtarget.com/definition/cyberwarfare

Cyber Espionage

The purpose of cyber espionage is to obtain the secrets of another, without their permission. The perpetrator of the espionage is typically trying to acquire sensitive, proprietary, or classified information. This can be committed against anyone from an individual to a company to a country. The information will be used as an advantage against the one from whom the information was stolen. It can be accomplished through means such as cracking, Trojans, and the installation of Spyware.

Examples of cyber espionage include:

- The Wall Street Journal reported that unnamed government officials told the Wall Street Journal that cyberspies from China and Russia had broken into computer systems used by companies maintaining the three North American electrical grids.
- Canadian researchers revealed in late March that a cyber-spy network based in China had broken into diplomatic computer systems involving 103 different countries. Beijing denied any official involvement, but the investigation had begun when the Dalai Lama, Tibet's leader-in-exile, noticed that sensitive documents from his own PCs had turned up in Chinese hands.
- Just after Barack Obama's election victory in November, Newsweek revealed that both the Illinois senator's campaign and that of his rival, Sen. John McCain, had been spied upon by a foreign power that had placed spyware on staffers' computers.

Source: http://www.foxnews.com/story/2009/04/22/five-serious-cases-cyberespionage.html

Published in 2009

Case Study

In the past few weeks, Lucky's Cleaners has been receiving harassing emails from a local competitor that says they are going to ruin Lucky's reputation and run them out of business. Martha, the owner is concerned that they may bad mouth them to prospective clients and may even do something to their computer system that will negatively impact business without them knowing it. Martha sits down with Robert, the cleaner's manager, to discuss what is going on and what they can do to fix the problem.

Module Ten: Review Questions

Module Ten: Review Questions

Cyber-attacks are not what makes the cool war 'cool.' As a strategic matter, they do not differ fundamentally from older tools of espionage and sabotage.

Noah Feldman

Module Eleven: Defense Against Hackers

”The best defense is a good offense”. Rather than reacting to attacks once they’ve occurred, a wise strategy is to prepare proactive measures, so that if the time comes, you can completely bypass the attack or lessen the blow of it.

Cryptography

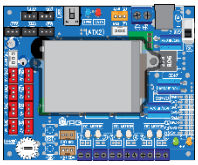
Cryptography is basically defined as a secret method of writing. This is done so that only authorized parties are able to interpret the message.

It is used in various industries, such as banking and health to protect the privacy and security of companies and customers’/patients’ information.

Examples of encryption methods include:

- International Data Encryption Method (IDEA)
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Digital Forensics



By many, computer systems have become a tool for committing various crimes. Because of this, law enforcement officials have decided to use this very tool to counteract the criminals' use of computers to commit online and offline crimes. In essence, they have decided to "Fight fire with fire".

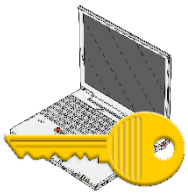
In digital forensics, law enforcement collects and analyzes the data in such a way that it can be used in court against the perpetrator.

Examples of cases where digital forensics was used:

- BTK Killer: Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.
- Joseph E. Duncan III: A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty.
- Sharon Lopatka: Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass.

Source: https://en.wikipedia.org/wiki/Computer_forensics

Intrusion Detection



Intrusion detection is a vital asset to a computer system. Intrusion detection systems (IDSs) inform the administrator or a security information and event management system of unauthorized programs or people on the network. There are a variety of IDSs to choose from.

When looking to invest in an IDS, there are several questions to ask yourself.

- What does our business need in an IDS?
- Will our network support the IDS system?
- Can we afford an IDS?
- What do we do if something goes wrong with the IDS?
- As our business grows, we can still use this IDS?

Some manufacturers of IDSs include:

- Dakota Alert, Inc.
- Juniper Networks
- Linear, LLC
- PureTech Systems, Inc.
- Telguard

Legal Recourse

The majority of computer hacking crimes are punishable under the Computer Fraud and Abuse Act (18 U.S.C. §1030). There may be additional penalties under state law.

Under this act, there are penalties for committing the following offenses involving computer:

- Obtaining National Security Information
- Accessing a Computer and Obtaining Information
- Trespassing in a Government Computer
- Accessing a Computer to Defraud & Obtain Value
- Intentionally Damaging by Knowing Transmission
- Recklessly Damaging by Intentional Access
- Negligently Causing Damage & Loss by Intentional Access
- Trafficking in Passwords
- Extortion Involving Computers

Penalties may include monetary and/or prison sentences. For example, an individual who is found guilty of a first offense of illegally obtaining national security information can serve up to 10 years in prison.

Case Study

Frank and Joel are talking about the importance of doing their best to prevent hackers from getting to their system, and if by chance, they are able to break in, what can be done to bring them to justice. Frank says since their bank holds a lot of private information of their customers, they need to consider some type of encryption method so only their employees can interpret data. Joel says an intrusion detection system would also be a good idea so they can be notified of suspicious activity before it causes too much damage. They both agree researching how digital forensics works and legal recourse that can be taken against cybercriminals will be worth their while.

Module Eleven: Review Questions

Module Eleven: Review Questions

People ask me all the time, 'What keeps you up at night?' And I say, 'Spicy Mexican food, weapons of mass destruction, and cyber-attacks.

Dutch Ruppersberger

Module Twelve: Wrapping Up

Although this workshop is coming to a close, we hope that your journey to Cyber Security is just beginning. Please take a moment to review and update your action plan. This will be a key tool to guide your progress in the days, weeks, months, and years to come. We wish you the best of luck on the rest of your travels!

Words from the Wise

- **Janet Reno:** Everybody should want to make sure that we have the cyber tools necessary to investigate cyber-crimes, and to be prepared to defend against them and to bring people to justice who commit it.
- **Kevin Mitnick**: Somebody could send you an office document or a PDF file, and as soon as you open it, it's a booby trap and the hacker has complete control of your computer. Another major problem is password management. People use the same password on multiple sites, so when the hacker compromises one site, they have your password for everywhere else.
- **Frank Abagnale:** The police can't protect consumers. People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will