Overview of Security Issues in IT

Security in Practice

Most people think of security as a protective measure that's physical, like a home security alarm to prevent theft, or a door with a lock and key to prevent unauthorized entry. While it's true that security is physical, we'll be looking at security from an information technology (IT) perspective. Moreover, we'll focus on the IT view; security is a safeguard. Security is something that we need online—to protect personally identifiable information (PII) and to protect our computers from cyber criminal attack.

Security in practice applies to all types of information. However, in this module we will discuss protecting a specific type of information—PII. We will cover the following aspects of security:

Compromise and Risk

We begin by explaining the concepts of compromise and risk. Compromise is a breach in security, while risk is the threat or likelihood that the compromise would occur. By looking at different facets or dimensions of risk we come to understand what leads to compromise of PII.

Confidentiality, Integrity, and Availability

The best way to illustrate the confidentiality, integrity, and availability (CIA) concept is to give an example. Let's say a piece of PII is exposed on the internet; that is, the PII is public and anyone can see it if they know where to look. That PII is at risk of compromise in one or more of three dimensions: CIA. (Keep in mind that CIA refers to the PII itself.) If someone looks at the PII, it's not secret—the confidentiality is compromised. If someone changes the PII, its integrity is compromised. If someone captures the PII, then its availability is compromised. CIA are the main components or dimensions of risk.

Cyber Criminal Tactics

Cyber criminals use specific methods to confiscate PII and ruin computers. Specialized software called "malware" or malicious software is the cyber criminal's primary method. Malware includes computer viruses, worms, trojan horses, and spyware. A constant barrage of unsolicited e-mails called "spam" is another tactic used by cyber criminals. Sometimes, spam is unwanted advertisements. Either way it's a nuisance.

Protection from Cyber Criminal Attacks

Fortunately, we can take many steps to protect ourselves from cyber criminals. Installing antivirus and firewall software helps protect your computer and files from malware. Using a strong password, following good password guidelines, developing good security habits, and encrypting important information are effective ways to protect yourself from cyber criminal attacks.

Symptoms of a Compromised Computer

How do you know if your computer has already been attacked by a cyber criminal? In this section, we'll review the signs of an infected computer, and let you know what to do about it.

Understanding Compromise and Risk

Many people assume that protecting their information is strictly about safeguarding PII by using strong passwords, making sure to log out of online accounts, using a password to lock your computer and keeping your computer physically secured. These habits are very important, but blindly using these methods ignores other components of your responsibility and capability to protect your information and resources. Two of the most important aspects are

- having a clear understanding of just what is at risk—how extensive and sensitive are the information and resources that you are protecting and how accessible are they?
- recognizing the role that your personal behaviors and decisions play in increasing or mitigating the risk to your information and resources.

When we talk about risk, in most cases we're considering the threat of compromising the resource. In the context of information security, compromise may have a slightly different meaning than you are used to:

Compromise

> (definition)
> In the field of information security, a compromise is a breach in the security of a specific resource—potentially a computer, an account, a file or another resource. A resource can be compromised in many ways, including actions by a malicious attacker hacking into a system, but also by a well-intentioned user forgetting to log out of a machine.

Confidentiality, Integrity, and Availability

We have already talked about compromise and risk, but let's quickly summarize the concepts. A compromise is a specific breach in security. Risk is a threat that the potential security compromise may actually occur.

So what comes first: a compromise or a risk?

If there's a risk to security, does that mean it might happen, or that it already happened? Of course, a risk means that something might happen. Taking a risk or chance comes before acting on that risk. For example, since I left the computer unprotected (taking a risk), a virus infected the computer.

On the other hand, if there's a security compromise, does it mean that it might happen, or that it already happened? Yes, it already happened. A compromise or security breach is a completed action. It's a done deal; it already happened. For example, since someone took

advantage of the unprotected computer to install and activate a virus, the computer is compromised.

Since risk is a chance that something might happen, and compromise is a completed action, then risk comes before compromise.

Why in the world do you need to know that risk comes before compromise? To answer that question, let's zero in on risk. Risk is key to how the compromise happened. Risk isn't singular; it has three dimensions—confidentiality, integrity, and availability (often referred to as "CIA").

Let's look at an example of each of the three risk dimensions. Keep in mind that we're looking at one example of each. In reality, each dimension can have lots of examples.

- Confidentiality risk: exposing a secret password and user ID
    - Example: Gabe gives Taylor his user ID and password so that she can finish the report they are co-authoring by the end of the day. Gabe's user ID and password are compromised because they aren't secret once he gives them to Taylor. When the user ID and password are no longer secret, that's a breach of confidentiality.
- Integrity risk: an unauthorized change to shared documents
    - Example: Evelyn accidentally changes the wrong pages on a shared document at work; she changes Robin's pages instead of her own. Robin is furious because she had spent all day making changes to the document, and now she doesn't know whether she can remember all of them.
- Availability risk: improper control of physical access
    - Example: Thomas, a supervisor, finds that he cannot access the data in a personnel file because the permissions for access to that database and the data contained therein have been changed by another supervisor, Martha. The data has not been compromised (there is no security breach), nor has there been a violation of the integrity of the data. But that data is not available to Thomas, and thus there has been a breach of availability.

Each example has a different risk and a single compromise or breach.

TIP... Why do we need to know that risk comes before compromise?
When we know the risk, we can sometimes prevent the compromise.

Now, we have a preview into the dimensions of risk—confidentiality, integrity, and availability. Our next step is to learn more about each dimension so we can apply some techniques and best practices to making good decisions using risk and compromise.

Dimensions of Risk

How Is Risk Assessed?

Assessing risk involves a consideration of how well protected a resource might be, and what the consequences could be if the resource is compromised. Simply asking yourself

whether you are doing something that might “put resources at risk” is probably not a useful approach for most people, though. To some extent, all actions have a degree of risk; your real goal is to assess that risk in a useful way.

That assessment can be a real challenge—security and risk are complicated and multifaceted. Because information protection can seem like a large and all-encompassing issue, security experts break the problem of security into three distinct aspects, considering the confidentiality, integrity, and availability of resources, first as discrete pieces and then collectively.

By focusing on one specific dimension at a time, you’re able to break the process of evaluation down into more manageable parts. And by then considering these parts collectively, you can make decisions that can best reflect your own priorities and responsibilities.

Confidentiality

Confidentiality

(definition)
The confidentiality of a resource refers to who is able to read or access it. Maintaining the confidentiality of a resource does not require that it be completely secret or inaccessible; rather, it is about ensuring that only authorized users—the right people—have access and that unauthorized users—the wrong people—do not. Confidentiality is at risk whenever unauthorized users have access to information, whether explicitly (such as password sharing) or unintentionally (such as mistaken file-sharing permissions or a virus accessing files). “A loss of confidentiality is an unauthorized disclosure of information” (Standards for Security Categorization of Federal Information and Information Systems, n.d.).

Example

A Loss of Confidentiality
Morgan provides computer support for the HiTech organization. She gets a request from Robert, the Human Resources Director, to recover files that were accidentally deleted. After Morgan successfully finishes the file recovery process, she opens a file to make sure its contents are complete. Morgan opens the file and sees the annual salary of each employee in HiTech.

Although Robert authorized Morgan to recover the deleted files, he did not intend to release any information about employees’ salaries—so the confidentiality of the salary information has been compromised or breached.

Integrity

(definition)
Maintaining the integrity of information means ensuring that the data has not been changed inappropriately, whether these changes are accidental and innocent or intentional and malicious. As the name implies,*integrity* addresses the question of how confident you can be about the state of your resources and information. “A loss

of integrity is the unauthorized modification or destruction of information" (Standards for Security Categorization of Federal Information and Information Systems, n.d.)

Example

A Loss of Integrity

Nicholas, a technical writer on the systems development team, is writing the new user guide for the Masters Plumbing Supplies inventory system. He sends the version 1 draft of the user guide to the development team for review, received all of their editorial changes two weeks ago, and incorporated them into a new version 2 of the user guide. He sent version 2 of the guide to team members for review last week and has already incorporated some of their changes into the next version of the user guide.

Just as Nicholas finishes incorporating Jim's comments into the new version 3 user guide, Jim calls Nicholas and tells him that he incorporated his comments into the wrong version. Jim incorporated his version 3 comments into version 1 instead of version 2. Now Nicholas doesn't know the new information from the original information in the user guide. Since the information in the user guide is mixed up between versions 2 and 3, the information in the user guide has lost its integrity. Nicholas can't be sure which version of the user guide is correct; the integrity of the user guide is compromised because of Jim's error in using the wrong version for his editorial changes.

Availability

Availability

(definition)
The availability of a resource refers to how timely and reliable access to that resource is. Maintaining the availability of a resource means that authorized users are able to reliably get to the specific machine or information when needed; availability can be threatened by technical malfunctions (such as a networking problem that prevents access) or by human factors, such as a changed password. "A loss of availability is the disruption of access to or use of information or an information system" (Bement, 2008).

Example

A Loss of Availability
Xing had set up a workstation for new employees to use until their permanent computers are assigned, but he hasn't been especially diligent about keeping it up to date. This carelessness comes back to haunt him when someone maliciously attacks the computer by exploiting a software vulnerability to access his machine and change the passwords on it. Now Xing can't log in to the computer to perform the updates.

Because he has physical access to the machine, Xing will eventually be able to get the work done. The process won't be fast, and during that time he won't be able to perform the updates; the availability of this resource has been compromised.

As you can see, considering how you protect your information and resources using these three dimensions can allow for more focus in evaluating your risks. It can also help you more clearly identify the possible consequences if your resources are compromised.

Confidentiality, Integrity, and Availability in Practice

So far, we've learned about the three dimensions of risk—confidentiality, integrity, and availability—one at a time. The reality is that most threats and compromises can involve multiple dimensions. Sharing your password, for example, can compromise both the availability and the confidentiality of your information if someone changes your password and looks at what the password is protecting. It can also compromise the integrity of your information if someone changes it without your permission. In practice, this means you should consider possible dangers and threats in the context of all three of the dimensions that you've learned.

What's at Stake?

Although some of the examples that are included above may seem extreme or unlikely, it's important to understand just what is at stake if your user ID and password are compromised. If you worked at Monumental Corporation with Michael and Sammy, what type of data can be exposed if your user ID and password are used without your permission? Is there really a danger of someone changing your files or information?

Recognize that your user ID and password are the key to an exceptional amount of corporate and personal information. With regard to confidentiality, for example, someone with your credentials may be able to see:

- your e-mail
- your work schedule
- your salary and other human resource–related information
- your work records, including your active and inactive files.

In addition to being able to review information that most people would consider confidential, your user ID and password allow you (and anyone who has your access) to change information, including:

- altering your work schedule for meetings
- sending and changing any e-mails
- changing or deleting your work files.

Finally, using your user ID and password, someone can place severe limits on the availability of some of your resources by:

- changing your password
- deleting your files
- cancelling or changing access to some programs or files.

It's important for you to understand that these are not just theoretical possibilities; all of the bullet points above represent actual resource compromises that have affected actual people. Sometimes these compromises have been the result of malicious actions. Sometimes they've occurred by mistake or been intended as pranks. However, they are situations that real people have had to face.

Cyber Criminal Tactics

Example

Since starting his new job in another city, Gustaph finds himself relying on Facebook to stay connected with friends and family back home. Shortly after logging in one afternoon, Gustaph receives a Facebook message with a link to "Funny Party Pictures" from his cousin Vivian. Certain the pictures must be from his family's annual picnic that he missed the previous weekend, Gustaph clicks the link to view the pictures, but they don't appear. Then he tries to move and click the mouse again but the mouse arrow freezes. Frustrated, he presses the power button until computer turns off. When he powers it back on again, the computer boots to a blue screen, rather than the login screen Gustaph expected. He restarts his computer a few more times, only to get the same result. Giving up, Gustaph takes his computer to a computer repair shop in town, where he learns that his computer was infected with malware. A virus had erased his hard drive and all the information he had on it.

Gustaph ends up spending a lot of time finding all the CDs containing the software applications he had loaded on his machine. In some cases, he has to dig up records of legal copies he had downloaded from the software provider. He looks through his emails for links to software purchases. He does his best to give the repair shop all the software to configure his computer back to the way it was before the crash. Some software could not be recovered, because Gustaph had obtained it from a friend without a user license. The cost of restoring his computer is more than $400. Since Gustaph had never backed up his files, all his personal files, resume, photos, music, and movies were lost entirely. All he has left is the information in his emails.

In the previous module on Privacy, you learned how cyber criminals try to lure you into providing access to your computing resources and personal information through social engineering scams, particularly phishing. It's important that you also know about other methods cyber criminals use to force their way into your computer.

Cyber criminals

(definition)

In computing, cyber criminals are people who circumvent security controls in order to gain unauthorized access to computers and networks.

In the past, these individuals were often motivated by the intellectual exercise of defeating security controls. Today, cyber criminals are often motivated by money or political ambitions such as revenge or competitive advantage. Much like in the physical world, where thieves must use a variety of tools and specialized knowledge to bypass locks, alarm systems, guards, and other lines of defense, cyber criminals similarly use a variety of tools and specialized knowledge to bypass computer security controls.

Malware

(definition)
The tools that cyber criminals often use can be generalized as “malware” and may consist of computer viruses, worms, trojan horses, and spyware. These types of specialized software take advantage of vulnerabilities in computer hardware and software. Malware is short for “malicious software.”

Computer Viruses

(definition)
Computer viruses piggyback on other programs or files in order to infect your computer. Viruses can spread to other computers via e-mail, websites, file sharing, USB drives, and other removable media. Cyber criminals rely on social engineering and require user intervention to spread a computer virus, i.e., someone has to open an attachment or file, click on a link, or plug in a USB drive. Viruses may cause a computer's processing function to slow down considerably.

Worms

(definition)
Worms, unlike viruses, spread across networks by exploiting software vulnerabilities to launch copies of themselves on new victims without user intervention. Simply connecting to a network with a computer running outdated software may result in a worm infection.

Trojan horses

(definition)
Trojan horses are malicious programs disguised as legitimate software. Victims are lured into installing them with promises of desired functionality. Viruses and worms may silently install trojan horses to further compromise systems, or they may be buried deep within legitimate software. “Backdoor” trojan horses can even facilitate unauthorized access to computers. Bolder trojan horses may pretend to be security programs, which generate imaginary virus warnings and demand payment to remove viruses that in reality do not exist.

Spyware

(definition)
Spyware is a type of malware that collects information about computers or their users and sends it to third parties without consent. Besides secretly monitoring user actions (e.g., logging keystrokes, e-mails, or instant messages) spyware can collect personally identifiable information (PII), which may lead to identity theft. Spyware may interfere with web browsing; even when using bookmarks or typing in the URL for a website, the browser will redirect to a fraudulent site designed to capture user names and passwords

or inject malicious content. An example of this would be a phony form on a legitimate-looking banking site asking for PII.

Modern malware tends to combine traits from all four categories—computer viruses, worms, trojan horses, spyware—to the point that the terms have become nearly synonymous.

Spam

(definition)
Spam messages are unsolicited messages sent to e-mail accounts or cell phones from advertisers or cyber criminals. Advertisers use spam to attract attention to their products. Advertising spam can be a nuisance, but is often benign to computers. Spam messages can also contain fraudulent information, like check overpayment scams, foreign lotteries, investment schemes, and other cons. Although these kinds of spam can separate someone from their money, they won't harm computers. Other spam messages have malware attached or include links to malicious sites. Opening those attachments or clicking those links may install malware.

Protection from Cyber Criminal Attacks

How do you protect yourself and your computer from the cyber criminal attacks you've learned about?

Install Antivirus Software

Antivirus software scans your computer and files to protect it from known viruses. Since new malware is always being released, you'll need to update your antivirus software regularly and configure it to scan your computer at least once a week.

Install Firewall Software

As related to information technology, a firewall is a protective layer or "wall" between the computer and internet. While antivirus software scans your computer and files, firewall software monitors, blocks, and filters activity between your computer and the internet. Like antivirus software, firewall software needs to be updated regularly to maintain its effectiveness. Antivirus and firewall software may sometimes be purchased in a single package.

There are good, legal, and free software alternatives when considering antivirus and firewall software. Just type "free antivirus software" or "free firewall software" into a search engine. Be sure, however, that the site you choose is a trusted site such as a recognized product review site: PCWorld, CNET, and Comodo are some of the best-known.

Install Software Updates

Operating systems software developers continuously improve their products to add more security and to fix errors in previously released versions. It is important to download and install updates as soon as you are notified that an update is available in order to keep your devices (phones,computers, tablets, etc.) secure.

Use a Strong Password

It's a good practice to change all your passwords every 90 days. If you suspect that any of your passwords have been compromised, change them immediately.

A strong password is reasonably difficult to guess in a short period of time, either through human guessing or through the use of specialized software.

Password Guidelines

The following are general recommendations for creating a strong password. A strong password *should*...

- be at least eight characters in length
- contain both upper and lowercase alphabetic characters (A-Z, a-z)
- include at least one numeric character (0-9)
- use at least one special character (e.g., ~ ! @ # $ % ^ & * ( ) _ - + =).

A strong password *should not*...

- spell a word or series of words that can be found in a standard dictionary
- spell a word with a number added to the beginning and/or the end
- be based on any personal information such as user ID, family name, pet, birthday, etc.

The following are several recommendations for maintaining a strong password:

- **Do not share your password with anyone for any reason.** Passwords should not be shared with anyone, including any managers, coworkers, or friends. If someone needs information that's on your computer, e-mail the file or place the file on a shared network. Passwords should not be shared even for the purpose of computer support or repair.
- **Change your password periodically.** As a general rule, changing your password every 90 days is recommended. If you suspect someone has compromised your account, change your password immediately. If you work in an office, report the incident to computer security personnel.
- **Consider using a passphrase instead of a password.** A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase "My fav2rite N@SCAR dri4er!" is 26 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.
- **Do not write your password down or store it in an insecure manner.** To the extent possible, avoid writing down your passwords. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed.
- **Avoid reusing a password.** When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, with or without your knowledge, reusing a password could allow that user account to become compromised once again. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

- **Avoid using the same password for multiple accounts.** Though using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect, allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your credit card account or your online banking account.
- **Do not use automatic logon functionality.** The option of storing your password so that you can save time by skipping your password entry the next time you log on is called automatic logon functionality. Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.
- **Consider using a strong password generator to create passwords.** There are many such programs available. Type “strong password generator” into any search engine to find programs that are available for use.
- **Consider using a password “base.”** Remembering a great number of different passwords is challenging. Consider using a base portion of a password and then changing some portion to use as separate password. Do not just add numbers to the end of the base portion, however. Scatter the changes into the middle of the password base. For example, if the base is “Utahlowa” then one password might be: Uta4hlo9wa. Then change the numbers in the password to be used with the next site, keeping the Uta-hlo-wa.

Develop Good Security Habits

Throughout this module, you have been introduced to good security practices. Here's a summary of good security habits for your reference.

- Never open unexpected e-mail attachments. If in doubt, verify the authenticity by calling or sending a new e-mail to the sender using a phone number or address from a source other than the suspect e-mail. An attachment could be malware in disguise.
- Beware of links sent to you via e-mail, on social networking sites, or through text messages. Maliciously crafted links could direct you to malware or phishing sites.
- Be sure to use logon passwords. Never leave your computer unattended without locking it, even if you’re stepping away for only a minute.
- Consider locking up laptops in a desk or cabinet drawer when not in use. Unsecured laptops are easy targets for thieves.
- Always lock your doors and never leave your computer unattended in a public location to avoid physical theft.
- If you share your computer with friends, keep an eye on what they might be doing to your computer and with your identity.
- When visiting websites that require logging in, make sure you log out when you're done.
- When you finish using a computer, log out of it.
- Watch out for “shoulder surfing.” Make sure no one is watching you enter your password or other personal information.
- Always backup your data and files, and lock the backups in a safe place.
- Use encryption (see below) for sensitive data storage and transmission.

Encryption

Encryption is the process of transforming information from plain text into an unreadable format to keep it secret. Only authorized entities should be able to reverse the process. Using encryption, information can be stored or transmitted via shared media without risking disclosure.

When encrypting information, applications will typically ask you for a password. The password is the key to locking and unlocking the information. If you lose the password, you won't be able to recover your information. Certain applications like Microsoft Word provide optional encryption functionality. You'll want to know whether the applications you use support encryption. If they don't, you'll want to avoid using them when processing sensitive data including passwords and other PII.

Certain websites, especially ones that allow financial transactions, use encryption between your browser and their server. This can be discerned by looking at the URL. If the URL begins with "http://" then the communication between your browser and the web server is not encrypted. If the URL begins with "https://" then the communication is encrypted. The "s" after "http" stands for "secure." Some browsers may provide additional encryption indicators such as displaying lock icons and changing the color of the address bar.

Encryption provides a way to keep private information private in an increasingly public world.

What Are Some Signs That a Computer Is Compromised?

Symptoms computers may experience when compromised include system crashes (the computer doesn't turn on), unexplained disk activity, frequent error messages, lots of advertising pop-up windows that appear without actual web browsing, and unexplained variations in the computer's performance and behavior.

The following is a list of indicators of a possible computer compromise or infection:

- Pop-up ads increase in frequency.
- Pop-up ads appear even when you're not browsing the web.
- The home page of your web browser changes without your authorization.
- Your computer seems less responsive than it should be.
- Your internet access is persistently slower than usual.
- Programs fail to start because Windows is "low on resources."
- Programs such as the Task Manager or the Control Panel fail to start and report "permission denied" errors, even though you have administrative rights to your machine.
- Your firewall cannot be started.
- Antivirus software cannot be updated or fails to enable.
- Your computer is crashing or "blue-screening" often.

Responding to a Compromise

If you believe that your computer has been compromised, you may be able to run an up-to-date antivirus scan and quarantine some of the infected files. There's a chance that file quarantining followed by removing the quarantined files can permanently fix the problem.

In almost all cases of computer compromise, you'll need to have your computer serviced by a professional to get it working properly.

To Sum Up

Threats on the internet are similar in concept to threats on the road. You are better protected when you follow traffic regulations and take certain precautions. Good safety measures include keeping your car well-maintained, fastening your seatbelt, stopping at stop signs and traffic lights, and avoiding potholes. To avoid theft, you keep your valuables locked away and out of sight. You lock your car when leaving it unattended.

Take the same types of security and safety measures on your computer and on the network. Keep your computer running well by updating your software and backing up your files regularly. Install antivirus software and make sure it updates frequently. Avoid opening the door to untrusted sources by not opening their attachments, not clicking on their links, not installing their software, and not providing them with your sensitive data or password. Protect your personal information from theft by locking it behind strong passwords that you do not share with others. Physically lock up your computing devices when unattended. Remember: Prevention is the best protection!

References

Bement, A. L. (2008). *FIPS PUB 199 standards for security Categorization of federal information and information systems*. Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.