Chapter 16 Cybersecurity

Shambhavi Roy

Clinton Daniel
*University of South Florida*, cedanie2@usf.edu

Manish Agrawal
*University of South Florida*, magrawal@usf.edu

Follow this and additional works at: [https://digitalcommons.usf.edu/dit_tb_eng](https://digitalcommons.usf.edu/dit_tb_eng)

Scholar Commons Citation

This Book Chapter is brought to you for free and open access by the The Modernization of Digital Information Technology at Digital Commons @ University of South Florida. It has been accepted for inclusion in *FUNDAMENTALS OF INFORMATION TECHNOLOGY: Textbook – English* by an authorized administrator of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.
If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders.

— Dan Farmer, computer security researcher and programmer

Overview—What is Cybersecurity?

The National Institute of Standards and Technology (NIST), founded in 1901, is part of the U.S. Department of Commerce and supports the U.S. mission to promote today's innovations and industrial competitiveness. This mission is accomplished by advancing measurements and standards in science and technologies that enhance economic security and quality of life. NIST, defines cybersecurity as:

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. 248

At the core of cybersecurity is the motivation to protect information and the systems that manage it. In fact, the U.S. law, 44 USC 3552, defines information security as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—integrity…, confidentiality…, and availability…. 249

In cybersecurity practice, this is commonly known as the CIA triad where C stands for confidentiality, I for integrity, and A for availability. What’s notable here is that cybersecurity is all about information and the systems that support its management. Our information and systems are increasingly under attack from powerful adversaries who would like to steal our information for profit. Therefore, having an understanding of cybersecurity is important to protecting the future of people, resources, and societies. Our journey to this understanding starts with exploring the past so we know how we have arrived to the present. Then, it demands we turn our attention toward studying where we are going in the future.

Before we begin to understand how we got to today’s climate of cybersecurity, let’s first establish some context with the CIA triad. This will help us understand what motivates the actors of cybersecurity in the past, present, and future.

Confidentiality

According to 44 USC 3552(b)(3)(B):

Confidentiality…means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

The law recognizes the right of individuals to privacy, and such right extends to information that, if made public, could cause harm to the person. It is the responsibility of the custodians of the information to
provide that privacy to the individuals whose information they have in their possession. For instance, people rely on banks to protect the privacy of their credit card information. The expectation is that banks (the custodian of the information) should not allow their customer account information to be exposed to those who do not require its access.

Modern cybersecurity services have been put in place by banks to protect the privacy of their customers’ information. Such practices include services such as fraud alerts to customers when credit cards are used in unusual ways. These services provide an opportunity for customers to freeze their credit card so that it cannot be used by someone who has violated their confidential information. This response is typically followed up with changing the compromised credit card information so that the stolen information is no longer useful, and disputing all unwanted charges to the credit card.

**Integrity**

The law under 44 USC 3552(b)(3)(A) defines integrity as:

> Integrity...means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

When you pull information from an information system, for example, your grades from school, or the monthly statement from your bank account, you trust that the information provided is reliable and actionable. For example, when the bank reports the balance in your checking account, you do not think it necessary to calculate the totals of credits, debits, and interest income yourself to verify the amount. Rather, you trust that the bank has made the right calculations. Imagine how complex life would be if the information you received from IT systems could not be trusted to be accurate. Integrity is the aspect of information security that prevents that from happening.

Consider the following example: you have worked really hard throughout the semester to keep up with the grades in all of your classes. Now it’s time for report cards and you expect to see straight A’s in all of your classes. You open your report card, and it shows that you have failed all of your classes. This could be devastating and perhaps ruin your chances of getting into the college of your choice. This is the impact of integrity. Your expectation is that the system that manages your grades in school should maintain its integrity so that you can be rewarded for your hard work. Now that you realize the information has somehow been modified, you will need to dispute the grades and the school will need to investigate how the integrity of its grade information has been violated. An information system without integrity is not useful for any serious work.

**Availability**

Availability as defined by 44 USC 3552(b)(3)(C):

> Availability...means ensuring timely and reliable access to and use of information.

When you log into an online class, you expect it to be online. That in essence is availability. The relevance of availability to information security is self-explanatory. An information system that is unavailable is an information system that is not useful. Most viruses impact availability—they typically delete important files, causing a loss of availability. Even if the files can ultimately be recovered from backup systems or other sources, the time lost in recovering those files represents time not spent doing useful work, i.e., lack of availability.
A famous example of lack of availability occurred on October 4, 2021. Facebook, Instagram, WhatsApp, and Oculus were unavailable globally for a period of time (Figure 248). This availability problem caused a global disruption of information services, which affected many different people and businesses who relied on the Facebook infrastructure for business.

Although the unavailability of Facebook and its services was not confirmed to be a cybersecurity attack, it demonstrated the impact of how the availability of Internet resources can quickly cause disruption in global information dependent societies. Figure 249 is a screenshot taken by this author on October 4, 2021, which demonstrates how quickly information availability cyber events such as this can become disruptive and cause fear and panic among people.
Update About the October 4, 2021, Outage by Meta

What happened

The October 4 outage occurred due to a command issued by an engineer during routine maintenance that unintentionally took down all the connections in our backbone network, effectively disconnecting Facebook data centers from the Internet globally. Our Facebook Engineering blog provides a more detailed explanation about what caused this outage and why it took time to restore our services. Ads did not deliver during the time our systems were offline, and advertisers were not and will not be billed for ads during the outage. However, we've heard from customers that their campaigns experienced volatility as our services came back online.

Separately, on October 8, a configuration change caused some people and businesses to have trouble accessing some of our apps and products for a shorter period of time. Following discovery of the issue, our teams were able to quickly resolve it and restore access to our services.

Brief History of Cybersecurity Events

To better understand how the domain of cybersecurity functions in today's businesses, it is useful to know about specific incidents that have happened in the past and how they have significantly influenced our business environment. The list of incidents that follow is not intended to be comprehensive. But they do serve as excellent examples of information security concerns at the time of their occurrences. These incidents also played a significant role in establishing some of the important laws and organizations related to cybersecurity. As you read through these various events in history, you will notice how new cybersecurity or technology terms and concepts are gradually introduced into our daily lexicon.

1981—Development of the core Internet technologies (TCP and IP): The core technologies of the Internet were finalized in 1981. There was no mention of security in these technologies, indicating that at that time the technology world was not concerned about cybersecurity. Since TCP and IP were available for free, they became the preferred networking technology for UNIX systems, widely used at universities and various intensive organizations such as hospitals and banks. Without TCP/IP, there would probably be no networking, and without networking, there would probably be little cybersecurity risk.

1982–1983—Gang of 414’s: Computer intrusions began soon after TCP and IP were integrated into industrial equipment. The most highly publicized incident of this time was the gang of 414’s, a group of six teenagers from Milwaukee, who got their name from the telephone area code for Milwaukee. These teenagers found it exciting to get into systems that were supposed to be out of their reach.

Using home computers, phone lines, and default passwords, this group was able to break into approximately 60 high-profile computer systems, including those at the Los Alamos Laboratories and the Memorial Sloan-Kettering Cancer Center in New York. The incident received wide coverage, including a Newsweek cover story titled “Beware: Hackers at play.” This is believed to be the first use of the term “hacker” in the mainstream media in the context of computer security. While the teenagers themselves did no harm, it was easy for the industry to see that the simple techniques used by the kids could easily be replicated by others. As a result, the US Congress held hearings on computer security. After more such incidents, Congress passed the Computer Fraud and Abuse Act of 1986, which made it a crime to break into federal or commercial computer systems.

1988—*Morris worm*: Robert Morris, then a graduate student at Cornell, and now a Professor of Computer Science and Artificial Intelligence at MIT, released a 99-line self-replicating program on November 2, 1988, to measure the size of the then nascent Internet. As a result of a design feature of the program, it brought down many systems it infected, and achieved several landmarks in the process. It is considered the first Internet *worm*. In percentage terms, it is estimated to have brought down the largest fraction of the Internet ever (10%). It also resulted in the first conviction under the 1986 Computer Fraud and Abuse Act. Robert Morris was sentenced to probation, community service, and a fine. The Morris worm prompted the US government to establish the CERT/CC (CERT coordination center) at Carnegie Mellon University as a single point to coordinate industry–government response to Internet emergencies. Prof. Morris was also a co-founder of Viaweb, an e-commerce firm bought by Yahoo and renamed “Yahoo! Store.”

**Father and Son**

As an interesting anecdote, Robert Morris’ father, Bob Morris, designed the password encryption system for the UNIX operating system that is still used today. Even more interestingly, at the time of this incident, the senior Bob Morris was the chief scientist for the National Computer Security Center (NCSC) of the National Security Agency (NSA), the federal agency responsible for designing secure computers.

1995–1998—*Windows 95/98*: Microsoft released Windows 95 on August 24, 1995. The operating system had a graphical interface and was designed to run on relatively inexpensive computers. The release was supported with a heavy marketing push, and within a very short time, it became the most successful operating system ever produced. Windows 95 was designed primarily as a stand-alone single user desktop operating system and, therefore, had almost no security precautions. Most users ran Windows 95 without passwords and most applications ran on Windows 95 with administrative privileges for convenience. However, Windows 95 supported TCP/IP, thereby bringing TCP/IP into mainstream businesses. This combination of a security-agnostic networking technology (TCP/IP)

---

251 While CERT typically stands for Computer Emergency Response Team, CMU has registered the name as a service mark with the US Patents and Trademark Office.


combined with an equally security-agnostic business
desktop created a fertile environment for information
security compromises to flourish. In talks, security
experts sometimes refer to this TCP/IP–Windows 95
environment as the birthplace of the information
security profession.254

1996—Health Insurance Portability and Accountability
Act (HIPAA): This act, which primarily focused on
protecting health insurance for US workers when they
change or lose jobs, also had important information
security implications. Many government leaders
believed at the time that electronic health records
(EHR) were an important instrument to lower rising
health care costs in America. The act, therefore, also
pushed for electronic health records. Since information
security was getting recognized as an important
concern, the law had provisions to make organizations
responsible for maintaining the confidentiality of
patient records in the health-care industry. The health-
care industry has now moved over completely to EHR,
creating significant demand for information security
within the healthcare industry.

2000—ILOVEYOU virus: On May 5, 2000, this virus was released by a student in the Philippines. The
virus deleted images on infected computers and automatically sent itself as an email attachment
to all of the Outlook contacts of the infected computers. The virus infected millions of computers
worldwide, and caused billions of dollars in damage. The creators of the virus, Reomel Ramores
and Onel de Guzman, were traced within hours of the release of the virus. However, investigators
realized very quickly that Philippines had no law against writing computer viruses, and had to drop
all charges against the students.255 This incident led to the realization that information security was a
global phenomenon and led to a push from developed countries to encourage developing countries
to revamp their information security laws. However, even today there are significant differences
between countries regarding information security laws. For example, while writing a virus can lead
to fines of up to $250,000 and 10 years of imprisonment in the United States, the punishment in the
Philippines can range from 100,000 Pesos (about $2,500) and up to an amount commensurate to the
damage and up to three years in prison. These international differences are an ongoing challenge to
cybersecurity in technology-intensive societies.

2002—Sarbanes–Oxley Act: During 2000–2002, America witnessed many unpleasant incidents of
corporate fraud involving such legendary companies as Enron, Tyco, and WorldCom. For example, Enron
claimed revenues of over $100 billion in 2000 and declared bankruptcy the next year. MCI-WorldCom
revealed in 2002 that it had overstated its earnings by over $72 billion in the past five quarters. These

254 For example, Dan Geer (chief information security officer for In-Q-Tel, the venture capital arm of
CIA) referred to this in his talk at the ISSA meeting in Tampa, December 2011.
255 Arnold, W. “TECHNOLOGY: Philippines to drop charges on e-mail virus,” New York Times, August
frauds were enabled by fraudulent manipulation of accounting systems, believed to be at the behest of firm leadership. However, during trials the CEOs consistently tried to escape blame by pleading ignorance of accounting procedures and claiming blind trust in their highly paid and well-educated lieutenants. Since the retirements of most Americans are invested in large publicly traded firms, their downfall affects most American families. Compelled to act by these devastating corporate frauds and to ensure correctness in financial reporting, Congress enacted the Sarbanes–Oxley Act in 2002. The act focused on making the key executives personally accountable for the correctness of financial reports filed by publicly traded companies. The act had three major provisions. Section 302 of the act requires the CEO and CFO of firms to sign a declaration of personal knowledge of all the information in annual filings. Section 906 of the act imposes criminal penalties including imprisonment of up to 20 years for incorrect certification. Section 404 of the act required that the certification in Section 302 be based on formal internal controls. Section 404 has had a major impact on the information security profession because it required publicly traded companies to establish formal information security processes in place. This has led to significant investments in internal controls over financial reporting in publicly traded firms, and corresponding growth in the demand for cybersecurity professionals.

2005–2007—Retailer attacks: In December 2006, T.J.Maxx reported that its computer systems, which processed credit card payments, had been breached. On investigation, it was found that the breach had started in July 2005, a year and a half prior to its discovery, and over 45 million credit card and debit card numbers had been stolen. It turned out that the leader of the group involved in the breach was Albert Gonzalez,256 an informer for the US Secret Service and in fact Albert was cooperating with the Secret Service in connection with another case at the time of these attacks. Investigations also revealed that the group had also hacked into the systems at other retailers such as BJ’s Wholesale Club, DSW, Office Max, Boston Market, Barnes & Noble, and Sports Authority. The modus operandi of the group was to drive along US Route 1 in Miami and seek out an insecure store with wireless networks to enter the corporate networks. Later the group improved its methodology and used SQL injection attacks to enter the networks at Hannaford Brothers and Heartland Payment Systems, a credit card payment processing company. Over 125 million credit card numbers were estimated to have been stolen from Heartland, and the company estimated damages at over $12 million. In March 2010, Albert Gonzalez was sentenced to 20 years in prison. He also forfeited over $1.65 million that he had earned from selling fake credit cards based on the stolen information. These incidents highlighted that even large firms had glaring information security weaknesses that could lead to serious embarrassment and losses. The SQL injection attacks, in particular, created an awareness of the need to pay attention to information security during software development, and introduced the term “secure SDLC” to the IT lexicon.

2008—Denial of service attacks in Georgia: Coinciding with the military war between Georgia and Russia in 2008, Georgia was the victim of massive distributed denial of service attacks. The attacks defaced the websites of many media and government organizations, limiting their ability to communicate their viewpoints about the war to their citizens. Many experts believe that the cyber-attacks were caused by Russia as part of a war strategy. If so, these were the first known incidents of cyber-attacks being used as an instrument of warfare.

June 2009—Establishment of the US Cyber Command: In April 2009, the Wall Street Journal reported that intruders had broken into the computer networks of defense contractors developing the Joint Strike Fighter, also called the F-35 Lightning II. The $300 billion project was the Defense Department’s costliest weapons program ever, and used 7.5 million lines of computer code. Intruders had stolen terabytes of data related to the aircraft’s design and electronics. It was believed that the theft would help enemies plan their defenses against the fighter. The contractors involved in the project include Lockheed Martin, Northrop Grumman, and BAE Systems. Also, in April the Wall Street Journal reported that the US electricity grid had been penetrated by spies from China, Russia, and other countries. The spies also inserted computer software into the grid, which could be used to cause damage by remote control.257 Soon thereafter, on June 23, 2009, the US Cyber Command was created to defend US military computer networks against attacks from adversaries. The US Cyber Command is also responsible for responding in cyberspace as necessary.

2010—Operation Aurora and Google-China: On January 12, 2010, a blog post by Google’s Chief Legal Officer reported that Google had detected an attempt, originating from China, to steal its intellectual property. The attacks were also aimed at accessing the emails of Chinese human-rights activists. The US government soon escalated the incident with Congress announcing its intention to investigate the allegations. The Secretary of State compared the Chinese censorship of the Internet to an information-age Berlin Wall. Further investigations traced the attacks to two educational institutions in China—Shanghai Jiao Tong University and the Lanxiang Vocational School. Jiaotong is home to one of China’s elite computer science programs, and Lanxiang is involved in training computer scientists for the Chinese military.258 China has, however, denied formal government involvement and called the attacks simply an attempt by students to refine their computer skills. This was one of the earliest suspected state-sponsored cybersecurity incidents.

April 17, 2011—Sony PlayStation Network (PSN): Just before summer break of 2011, Sony announced that an external intrusion had compromised its PlayStation Network and Qriocity service, and that hackers had obtained personal information on the 70 million subscribers of the network. In response, the company took the network offline while it tried to ensure that all traces of the offending software had been removed from the network. During that time, millions of kids all over the world who had planned their summer breaks around catching up with online gaming on PSN had to find alternate ways to pass their time. While the intrusion affected a relatively innocuous network, the impact on families around the world was huge and almost every family with kids followed the daily developments around the attacks. Imagine losing out on an entire summer break because of a cybersecurity incident. This actually happened in the summer of 2011.

February 1, 2013—Mandiant APT 1 report: Cybersecurity firm Mandiant released a report alleging that a suspected Chinese military unit, 61398, was engaged in a novel form of state-sponsored cybersecurity attack—advanced persistent threat. An advanced persistent threat is a sophisticated and well-resourced adversary that uses multiple attack methods over an extended period to execute its objectives. Mandiant called this adversary APT1. The report attracted considerable attention among business and government leaders who realized that cyber-attacks were no longer limited to individuals for private gain. The stakes were raised when organizations realized that states could invest military-scale resources to compromise cybersecurity.

2014—Cyber-attack on Yahoo: 500 million accounts were stolen by what was believed to be a state-sponsored actor. Email addresses, passwords, telephone numbers, dates of birth, and names were stolen by cybercriminals hired by Russian agents who targeted Yahoo employees via a phishing campaign. Phishing is a form of social engineering. In this case, a Yahoo employee with network access clicked on a malicious link in an email. This allowed hackers to gain continuous access to the network to obtain confidential data such as security questions and answers that were stored unencrypted by Yahoo. Social engineering attacks have been getting progressively sophisticated since the early 2000s. This cyber-attack on Yahoo is one of the most significant attacks recorded to date. Today, the US Cybersecurity & Infrastructure Security Agency (CISA) publishes security tips on how to avoid social engineering and phishing attacks.

2021—RockYou2021: In 2021, a hacker whose identity has not been disclosed harvested billions of user passwords. To date, this is the largest collection of passwords ever leaked online. The anonymous hacker uploaded a 100GB TXT (text) file to a popular hacker forum that contained approximately 8.4 billion entries of passwords. Some would argue that this number of passwords exposed could cover the entire global online population several times over. Today, the rockyou.txt file is commonly used by cybersecurity researchers and professionals as a wordlist to study or recreate brute force attacks on user passwords. A brute force attack is a programming scripts designed to repeatedly execute its code while attempting to log into a system with a user account. These types of wordlists are managed within software packages found in today's open-source distributions of Linux, such as Kali Linux, which are designed for cybersecurity professionals to assess the security of their systems.

This brief chronology highlights how information security attacks have evolved from technical proofs-of-concept to commercially driven attacks to steal credit card information. Of late even governments are being suspected of pursuing their agendas through cybercrime. In Europe, a remote Romanian
town, Râmnicu Vâlcea, has emerged as the focal point in global cyber money laundering. In the middle of nowhere, this town has car dealerships selling Mercedes-Benz and other expensive cars. Social response has evolved as well, from judges merely warning intruders and laws making specific exceptions for juveniles, in spite of their known involvement in cyber-attacks (414’s), to governments establishing entire military commands to deal with cybersecurity.

The Basic Information Security Model

Information security is a very broad subject area because most information security incidents exploit some new weakness in an organization. Maintaining information security, therefore, requires attention to almost every aspect of the organization. To provide structure to these efforts, it is useful to organize all the activities associated with maintaining information security into a unified model. A model is used to represent a concept that exists in the real world. This will make it easy for you to understand what motivates cybersecurity events. Let's start with examining the model diagrammed in Figure 250.

Figure 250 represents a framework for understanding information security. The core components of this model illustrate the relationship between assets, vulnerabilities, threats, and controls. These four components are extremely important to understand any cybersecurity event or case where information is the target.

---

Assets

At the center of Figure 250 are assets. In the context of information security, an asset is defined as a resource or information that is to be protected. All security scenarios, whether related to information security or simply related to securing one’s own property, start with an asset that is considered valuable enough for you to put forth special efforts on protecting it from harm. Information security is no different. If some information or related resource is valuable to the organization, the organization needs to put forth a special effort to secure it.

There are, however, two important differences between conventional assets and information assets—invisibility and duplicability. In most security scenarios that you are likely to be familiar with, the items to be protected can be seen and felt. For example, you lock your cars to prevent theft. You install home alarm systems to prevent home break-ins. In both cases, the assets are visible to the naked eye. The damage is also visible. If someone breaks into your car or home, the damage is immediately visible. If there are closed-circuit cameras in the vicinity, they will capture the act of vandalism.

But information security is different. The assets in information security are not tangible artifacts that can be seen and felt. Instead, they are data and information stored as 0s and 1s on computers, tapes, phones, and other devices. While the hard drives and other devices are themselves visible, the valuable data stored on these devices is invisible. If the data is stolen over the network, the transfer of data is not visible to cameras or other conventional security devices. The thieves may even operate from another country, thousands of miles away, safe from the scrutiny of conventional security agencies.

The second important difference between conventional assets and information assets is duplicability. Continuing with the car example, if your car is stolen, you will notice the missing car in the morning. This is because the car can only exist in one place at any given time. However, information can be duplicated. If your data is stolen, you will not notice the theft until it is brought to your attention. For example, if someone finds your laptop unattended, emails a copy of your assignment to himself and submits the copied assignment as his own work, you will have no idea of the act of plagiarism unless the instructor brings it to your attention.

These two differences between conventional assets and information assets—invisibility and duplicability—make information security a considerably different challenge than conventional security. Conventional security methods such as locks and guards are not very effective at maintaining information security. For example, conventional locks will do little to prevent the theft of data over the network. A stolen conventional asset such as gold can be recovered and restored to its owner. But stolen data may be copied to a hundred locations and even if a few of these copies are destroyed, it is almost impossible to deny the thief the benefit of having access to the data. Information security controls, therefore, must try to prevent theft in the first place and detect and block thefts as they occur through constant monitoring.
IT Assets

In the most common scenario you will encounter, the information assets are stored in an IT system. Paper-based systems simply cannot provide the density of information storage required by modern organizations. An IT system is defined as an assembly of computer hardware, software, and firmware, configured for the purpose of processing, storing, or forwarding information. In a small family-owned business, this IT system may be as simple as an Excel spreadsheet.

Threats

A threat is defined as the capabilities, intentions, and attack methods of adversaries to exploit or cause harm to assets. In the Excel example, a worker may want to exploit the lack of password protection on the file and modify their hourly rate. These threats are shown in the framework of Figure 250 as arrows.

Today, it is common practice among cybersecurity professionals to use a framework created by Mitre called “MITRE ATT&CK.” Mitre is a non-profit federally funded research and development organization. This framework from Mitre includes real-world observations through a globally accessible knowledge inventory of tactics and techniques used by cybercriminals to exploit vulnerabilities in IT systems. The MITRE ATT&CK knowledge inventory is a tremendous source for what is called threat intelligence. NIST (National Institute of Standards and Technology) defines threat intelligence as:

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Basically, there are public and private threat intelligence resources available to cybersecurity professionals that provide a collection of information necessary to understand the global threats actively seeking to exploit the vulnerability of IT system assets. For instance, Figure 251 illustrates a threat intelligence report published by the MITRE ATT&CK knowledge base that warns of three threats (Axiom, GOLD SOUTHFIELD, and Hikit), which have been used to execute phishing campaigns to gain access to victim IT systems.

FIGURE 251 — Threat intelligence resources make referencing and identifying malicious attacks easier for professionals.

As illustrated in Figure 251, Axiom is a suspected Chinese cyber espionage group while GOLD SOUTHFIELD is a group motivated for financial gain. Both groups are considered global threats to cybersecurity. The third name mentioned in Figure 251, Hikit, is classified as malware that can be used to remotely connect to an IT system for the purpose of creating a persistent threat. Persistent threats are used to cause damage to an IT system at any time a malicious actor chooses.

The most popular types of threats observed in cybersecurity include viruses, worms, phishing, and malware. Viruses and worms are computer programs that adversely affect computers and propagate through the network without the user's consent. The difference between a virus and a worm is that a virus uses other programs (e.g., the user's email client) to spread, whereas the worm can propagate all by itself. Since the authors of worms and viruses know that most users use antivirus software, modern-day worms and viruses are designed to cause all possible damage within minutes of release.

Phishing is an attempt to compromise a user by masquerading as a trustworthy entity in electronic communication. Early phishing attacks attempted to acquire information such as usernames, passwords, and credit card details. Most people receive at least one or two of these emails every week. The emails appear to originate from banks and lead users to visit a website that looks like the bank's website. At the website, users are asked to provide their username and password in order to make some correction at the bank. While the emails and target website appear to be legitimate, they really aren't. A careful look at the URL will show that the website has been hosted at a compromised server.

Users can easily fall victim to a phishing attack.
Malware (malicious software) is a general term used to describe software or code specifically designed to exploit a computer, or the data it contains, without the user’s consent. A very common way for malware to reach computers is via free downloads where the malware author creates a computer software that appears to be very useful and distributes it for free. When unsuspecting users download and install this apparently useful software, the malware is installed along with it. This is called the Trojan horse technique.

Vulnerabilities

Information security becomes important because all systems have vulnerabilities. A vulnerability is a weakness in an information system that gives a threat the opportunity to compromise an asset. The vulnerability of an asset enables threats. In the case of the Excel-based IT system discussed above, such vulnerabilities include unauthorized access that may cause loss of confidentiality or integrity and hard drive failures that may cause loss of availability. If we reached some state of utopia where no vulnerabilities existed in IT systems, we would not have to study information security and would not need a cadre of professionals dedicated to information security. However, modern software products are large. For example, Microsoft Windows took millions of lines of code to create. It is difficult to anticipate and eliminate all possible vulnerabilities in such large products.

To deal with vulnerabilities, the software industry in collaboration with the federal government has invested considerable resources to create an inventory of known software vulnerabilities. This is the Common Vulnerabilities and Exposures (CVE) list. The CVE list aims to provide common names and identifiers for all publicly known software vulnerabilities. The list is also maintained by Mitre.

Vulnerabilities can be classified into specialized categories such as software vulnerabilities. A software vulnerability is an error in the specification, development, or configuration of software such that its execution can violate the security policy. For example, a software developer may create a website that requires user input within a textbox prior to submitting a form. However, if the developer does not write code to validate the input of the user on the web form it is possible for a malicious hacker to inject Structure Query Language (SQL) into the textbox when the form is submitted. This is also called a SQL Injection attack.

Figure 252 illustrates a SQL Injection attempt on ChatGPT. ChatGPT is a free Artificial Intelligence (AI) website by OpenAI that allows a user to enter text in a textbox. ChatGPT then analyzes the text and attempts to respond to the text using AI, similar to the way a human may answer a verbal query. Here, as seen in Figure 252, the user attempts to inject malicious SQL and ChatGPT does not allow the code to execute. This illustrates how the ChatGPT developers have written code that validates the user input to prevent any software vulnerabilities of the IT system.

---

Controls

All IT systems will be vulnerable for the foreseeable future. Also, in this timeframe there will be dedicated attackers threatening to exploit these vulnerabilities for personal gain or other motives. What does a system administrator do to defend the computers they are in charge of?

The role of information security is to minimize the impact of threats. This is done by deploying security controls around the vulnerable IT system. Security controls are safeguards used to minimize the impact of threats. Within the framework illustrated in Figure 250, these controls are shown as the ring around the IT system. The width of the arrows in Figure 250 indicates the relative frequencies of the different categories of threats seen by a typical organization. Most threats are blocked by the controls commonly adopted by organizations. For example, most operating systems now come with a firewall configured with some default settings and encourage users to use a strong password to secure the administrative user account on their computers. Commercially, even the smallest businesses backup their important files on external storage appliances or other Internet services and keep their computers locked to prevent unauthorized access.

Even rudimentary controls such as firewalls and passwords can successfully block a large majority of the threats facing organizations. However, as shown in Figure 250, even the best security controls have holes. For example, users often prefer memorable passwords over secure passwords. They are also often irregular in backing up their data even if they have spent hundreds or thousands of dollars to purchase backup systems. Threats exploit these weaknesses in security controls to reach the vulnerable IT systems. These threats are shown by the arrow on the right, which has breached the controls and reached the IT system. Fortunately, many of these threats may yet do no harm, as shown by the inability of the arrow on the right of Figure 250 to reach the IT system.

Cybersecurity controls can be classified as physical, procedural, and technical. Physical controls use traditional non-technical methods of preventing harm. Typically, they prevent unauthorized users from being able to enter technical facilities. Examples of such controls include locks, fire extinguishers, background checks, and doors. Procedural controls are prescribed plans of action that govern the use of computer resources. Examples of procedural controls include the procedures for obtaining computer accounts, procedures for escalating privileges, procedures for modifying programs, procedures for hiring, and requirements that users change their passwords periodically. Technical controls are the security measures built into the information system itself. Common examples include passwords, firewalls, intrusion detection systems, system updates, and antivirus software.
Cyber Hygiene

The US Cybersecurity & Infrastructure Security Agency (CISA) defines cyber hygiene as those practices that reduce the risk of a successful cyber-attack. Today, it is important for people to understand how to use good cyber hygiene practices in order to safely use online IT systems and resources. Some intuitive practices of good cyber hygiene include simple measures of updating the security of your technical devices. For instance, if your mobile device has a software update, it will typically notify you by displaying an alert on your screen. A mobile device user can choose to ignore these updates or take the time to download and install them. Keeping your mobile device up to date is an excellent way to maintain good cyber hygiene and prevent cybercriminals from causing harm to your personal information.

Other types of good cyber hygiene practice include the use of end-point protection (formerly called antivirus) software and changing your passwords regularly. Antivirus software, such as McAfee, are designed to protect your identity, privacy, and devices. This protection is accomplished through software products that are designed to monitor your devices for known viruses and other malicious technologies that have the intent of harming the user.

Password management is one of the most effective ways to practice good cyber hygiene. Keeping passwords safe and secure include practices such as:

- avoid using the same password for multiple accounts;
- change passwords on a regular basis;
- passwords should be at least 12 or more characters long;
- passwords should include a mixture of upper and lower-case letters plus symbols and letters;
- avoid obvious passwords such as sequential numbers like 1234 or personal information someone could acquire on your social media accounts such as your pet’s name or your first car;
- avoid sharing passwords with others;
- use a password manager to help generate, store, and manage all your passwords in one security online account, for example: 1Password, https://1password.com/;
- use apps that require multi-factor authentication, for example, many social media accounts require a login username/password and a code sent as a text to your cell phone to complete the login process;
- back up your important files in a secure and protected location, for example, on an external hard drive or cloud storage;
- don’t post private information such as your home address or phone number on social media accounts;

---


• check all your social media privacy settings because each social media account is slightly different and designed to protect its users when settings are appropriately applied;
• keep your devices locked with a password or PIN when not in use;
• do not use websites or apps that disclose private information on a public Wi-Fi;
• only make online transactions on websites that are secure (this requires a URL with https:// rather than just http://);
• change the default name of your home Wi-Fi router—in other words, don’t leave your home router with the same name it has been given by the manufacturer when you took it out of the box;
• setup a guest network on your home Wi-Fi so that guests in your home use this network instead of the one setup for your personal use;
• use firewalls to prevent malicious software from accessing your home network;
• encrypt devices that contain sensitive data, for example, removable USB drives; and
• before selling or disposing of a device, it is a good practice to wipe the hard drive clean.

Overall, people are typically the weakest link to a cybersecurity attack. Many cyber-attacks are designed to exploit the vulnerabilities of people and their poor cyber hygiene. For instance, cyber-attack techniques such as social engineering are used by malicious actors with the intent of getting people to expose specific information they would otherwise be unwilling to share. This specific information, exposed by poor cyber hygiene, can be used against a person to do horrible things such as stealing their identity or emptying their bank accounts. Therefore, as technologies evolve over time it will continue to be a basic necessity for the general population to stay informed on what it takes to practice good cyber hygiene.

Teams in Cybersecurity

Professionals who work in cybersecurity often work in teams to respond to or investigate a cybersecurity event. These teams must be familiar with the tactics, techniques, and procedures (TTP) used by bad actors in a cybersecurity event. Tactics can be described as the basic methods used by the hacker to gain access to a system or information. A technique may include the tools or methods used by the hacker to gain access to the system or information. Finally, the procedure describes how a hacker carries out the techniques step-by-step.

Cybersecurity teams need to be familiar with the TTPs known by the cybersecurity intelligence community in order to understand the behavior of a hacker. This behavioral understanding is what teams need to better protect companies and systems from being attacked. One of the world’s largest open-source repository of TTP knowledge used by cybersecurity teams is the MITRE ATT&CK framework. Cybersecurity teams can use this real-world threat intelligence to help make the world a safer place to live.

Although people may commonly call a bad actor a malicious hacker, not all hackers are bad. Cybersecurity teams have evolved over time to specialize in different areas of behavior commonly engaged by hackers. In fact, the members of these specialized teams could also be called hackers.
Essentially, hackers are classified by the intent of their behavior. Whether the actor has bad or good intentions, cybersecurity teams must understand all classifications of hacker behavior.

The following summarizes the two common types of cybersecurity teams that specialize in the TTPs used by actors involved in a cybersecurity event:

**Red Teams:** These cybersecurity teams consist of operators that use tools and techniques typically used by malicious actors to attack a system or the information it manages. If this were a sport, you could think of Red Teams as the “offense.” Cybersecurity attacks executed by Red Teams are often called campaigns. The intent of a Red Team operator (hacker) is to help companies understand how their security weaknesses (vulnerabilities) can be exploited by a malicious actor. This understanding can help the company put better business and technology practices in place to protect their systems from future attacks.

**Blue Teams:** These cybersecurity teams focus on the constant defense of systems and information managed by organizations. It is common for companies to work with Security Operation Centers (SOC), which consist of multiple Blue Teams dedicated to keeping a close watch on all the systems critical to conducting their daily business. Blue Teams are trained to use tools designed to protect, capture, analyze, and respond to a cybersecurity event. For instance, in the event a company’s system is attacked by a malicious actor or malware a Blue Team will work together to investigate what happened. Once they understand what happened, they will work to understand how it happened and recommend a mitigating response to prevent the event from happening again.

Overall, you can consider cybersecurity as a “team sport.” It requires teams of individuals working together to endlessly understand the offensive and defensive TTPs used by hackers across the globe. Ultimately, these “good” hackers are motivated with a passion to prevent the “bad” hackers from harming the security of information and the management of critical systems.
**Asset:** A resource or information that is to be protected

**Brute Force Attack:** A programming script designed to repeatedly execute its code while attempting to log into a system with a user account

**CIA Triad:** The provision of confidentiality, integrity, and availability; by protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

**Control:** Safeguards used to minimize the impact of threats

**Cyber Hygiene:** The practices that reduce the risk of a successful cyber-attack

**Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to make sure its availability, integrity, authentication, confidentiality, and nonrepudiation

**Denial of Service Attack:** The act of more than one networked computer overwhelming a network with fraudulent traffic

**Hacker:** A person who wishes to gain access to an identified target to learn more about the target and exploiting the target for an attack

**Information Security:** Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

**Malicious Actor:** Someone or something that causes harm in the digital domain

**Phishing:** Attempting to compromise a user by masquerading as a trustworthy entity in electronic communication

**Social Engineering:** When deception is used to make a person give up private information or provide unauthorized access to a computer system or network

**Threat:** The capabilities, intentions, and attack methods of adversaries to exploit or cause harm to assets

**Virus:** A computer program that uses other programs to spread and adversely affect computers and propagate through the network without the user’s consent

**Vulnerability:** A weakness in an information system that contributes to a threat with the opportunity to compromise an asset

**Worm:** A computer program that can propagate all by itself and adversely affect computers and propagate through the network without the user’s consent
Chapter Case

The Red Team Operators

NIST defines a “Red Team” as a group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.273 In the figure below, two Red Team operators are attempting to exploit any vulnerabilities by the Widget Inc. Human Resources (HR) department.

Damian Hatter, Red Team Operator 1, walked past the Widget Inc. HR department and looked through several of the windows to observe the general layout of the room prior to entering. He noticed that a single HR clerk was sitting behind a front desk and there were several workstations positioned across the room that were shielded by cubicle walls. Hatter then walked in the HR department and approached the HR clerk behind the front desk. He asked the clerk if he could fill out an application for a job opening. The clerk then directed him to sit down at a workstation and click the shortcut icon located on the PC desktop to begin the application process. Hatter then proceeded as instructed by sitting down at one of the workstations while the clerk remained sitting behind the front desk.

Shortly after Hatter sat down at a workstation, he began to evaluate the PC for vulnerabilities. His primary goal was to implant a backdoor274 and maintain network persistence275 through a remote command and control server (C2).276 To accomplish this, he first started with verifying that he could use one of the open USB ports located on the PC. He reached into his pocket, pulled out his USB flash drive, and inserted it into an open USB port. The Windows Operating System immediately responded with a notification confirming that the USB port access was enabled. Upon confirmation, Hatter proceeded with opening his USB flash drive and executed a malicious program he had installed earlier prior to leaving his office desk. The malicious program running on his USB flash drive then successfully communicated with his C2 instance running on a remote system located offsite.

from Widget Inc. Once he confirmed that his C2 instance could communicate with the malicious program executed from a networked PC located inside of the Widget Inc. network, his goal was complete. Hatter then ejected his USB flash drive, placed it in his pocket, and left the HR room.

As soon as Hatter left the HR room, Wanna Bee, Red Team Operator 2, walked in and went directly to a workstation without confronting the HR desk clerk. As soon as he sat down at the workstation, he immediately used a web browser to navigate to a website that he had previously setup on a remote webserver for the purpose of downloading malicious software. The user account setup on the PC had enough privileges to download and execute applications directly from the Internet. Upon successfully downloading and executing the malicious software, Bee was able to communicate with the remote C2 system.

Hatter and Bee had successfully gained unauthorized persistent access to the Widget Inc. network. This was accomplished through exploiting unsecure physical and technical entry points.
Chapter Case (continued)

Question 1: What vulnerabilities do you think exist in the HR department?

Question 2: Identify as many cybersecurity controls as you can that you think should be added to the HR department based on this case scenario. Be sure to consider physical, procedural, or technical controls.