The History if cybersecurity

welcome to week 2

Welcome back! When it comes to security, there is so much to learn, and I'm thrilled to be part of your career journey.

This is such an exciting time to be learning about security! When I learned about international hacks that impacted both private companies and government organizations, I was inspired to want to work in security because I realized how dynamic and important this field is.

One reason there are so many jobs in the security field today, is because of attacks that happened in the 1980s and 1990s. Decades later, security professionals are still actively working to protect organizations and people from variations of these early computer attacks.

In this section of the course, we'll discuss viruses and malware, and introduce the concept of social engineering. Then, we'll discuss how the digital age ushered in a new era of threat actors. Knowing the evolution of each attack is key to protecting against future attacks. Lastly, we'll provide an overview of eight security domains.

Next up, we'll travel back in time, to explore some of the viruses, data breaches, and malware attacks that have helped shape the industry as we know it today.

Past cybersecurity attacks

The security industry is constantly evolving, but many present-day attacks are not entirely new. Attackers often alter or enhance previous methods. Understanding past attacks can provide direction for how to handle or investigate incidents in your job as a security analyst.

First, let's go over a couple of key terms that will support your understanding of the attacks we'll discuss.

A computer virus is malicious code written to interfere with computer operations and cause damage to data and software. The virus attaches itself to programs or documents on a computer, then spreads and infects one or more computers in a network.

A worm is a type of computer virus that can duplicate and spread on its own without human involvement.

Today, viruses are more commonly referred to as malware, which is software designed to harm devices or networks.

Two examples of early malware attacks that we'll cover are the Brain virus and the Morris worm. They were created by malware developers to accomplish specific tasks. However, the developers underestimated the impact their malware would have and the amount of infected computers there would be. Let's take a closer look at these attacks and discuss how they helped shape security as we know it today.

In 1986, the Alvi brothers created the Brain virus, although the intention of the virus was to track illegal copies of medical software and prevent pirated licenses, what the virus actually did was unexpected. Once a person used a pirated copy of the software, the virus-infected that computer. Then, any disk that was inserted into the computer was also infected. The virus spread to a new computer every time someone used one of the infected disks. Undetected, the virus spread globally within a couple of months. Although the intention was not to destroy data or hardware, the virus slowed down productivity and significantly impacted business operations.

The Brain virus fundamentally altered the computing industry, emphasizing the need for a plan to maintain security and productivity. As a security analyst, you will follow and maintain strategies put in place to ensure your organization has a plan to keep their data and people safe.

Another influential computer attack was the Morris worm. In 1988, Robert Morris developed a program to assess the size of the internet. The program crawled the web and installed itself onto other computers to tally the number of computers that were connected to the internet. Sounds simple, right? The program, however, failed to keep track of the computers and had already compromised and continued to re-install itself until the computers ran out of memory and crashed.

About 6,000 computers were affected, representing 10% of the internet at the time.

This attack cost millions of dollars in damages due to business disruptions and the efforts required to remove the worm.

After the Morris worm, Computer Emergency Response Teams, known as CERTs®, were established to respond to computer security incidents. CERTs still exist today, but their place in the security industry has expanded to include more responsibilities.

Later in this program, you'll learn more about the core functions of these security teams and gain hands-on practice with detection and response tools.

Early attacks played a key role in shaping the current security industry. And coming up, we'll discuss how attacks evolved in the digital age.

Attacks in the digital age

With the expansion of reliable high-speed internet, the number of computers connected to the internet increased dramatically. Because malware could spread through the internet, threat actors no longer needed to use physical disks to spread viruses.

To better understand attacks in the digital age, we'll discuss two notable attacks that relied on the internet: the LoveLetter attack and the Equifax breach.

In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over $10 billion dollars in damages. The LoveLetter attack is the first example of social engineering.

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

After the LoveLetter, attackers understood the power of social engineering. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Many people are now prioritizing convenience over privacy. The trade-off of this evolving shift is that these tools may lead to increased vulnerability, if people do not use them appropriately.

As a security professional, your role is to identify and manage inappropriate use of technology that may place your organization and all the people associated with it at risk. One way to safeguard your organization is to conduct regular internal trainings, which you as a future security analyst may be asked to lead or participate in.

Today, it's common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive. Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Now, let's discuss the Equifax breach. In 2017, attackers successfully infiltrated the credit reporting agency, Equifax. This resulted in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans.

The records included personally identifiable information including social security numbers, birth dates, driver's license numbers, home addresses, and credit card numbers. From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. The company failed to take the actions needed to fix multiple known vulnerabilities in the months leading up to the data breach.

In the end, Equifax settled with the U.S. government and paid over $575 million dollars to resolve customer complaints and cover required fines.

While there have been other data breaches before and after the Equifax breach, the large settlement with the U.S. government alerted companies to the financial impact of a breach and the need to implement preventative measures.

These are just a couple of well-known incidents that have shaped the security industry. Knowing about them will help you in your security career. Understanding different types of malware and social engineering attacks will allow you to communicate about security risks during future job interviews.

As a future security professional, constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job. By noticing similar trends, patterns, and methodologies, you may be able to identify a potential breach and limit future damage.

Finally, understanding how security affects people's lives is a good reminder of why the work you will do is so important!

Common attacks and their effectiveness

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, *and* the evolving tactics and techniques threat actors use, will help you better protect organizations and people.

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

- **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.

- **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.

- **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data.

- **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.

- **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

- **Viruses:** Malicious code written to interfere with computer operations and cause damage to data, software, and hardware. A virus attaches itself to programs or documents, on a computer. It then spreads and infects one or more computers in a network.

- **Worms:** Malware that can duplicate and spread itself across systems on its own.

- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware:** Malware that’s used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It’s the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

- **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.
-

USB baiting: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.

- **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it’s also a risk.

Reasons why social engineering attacks are effective include:

- **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they’re told.
- **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others’ trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.

- **Scarcity:** A tactic used to imply that goods or services are in limited supply.

- **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.

- **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.

- **Urgency:** A threat actor persuades others to respond quickly and without questioning.

Key takeaways

In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it’s so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks.

Sean: Keep your cool during a data breach

Hi, my name is Sean. I'm a Technical Program Manager in Google workspace. I am a 30 year security veteran within the security space across six different industries. During your first data breach, the most important thing that you can do is keep your cool. Everyone around is going to be freaking out. If you are on the security team and you are managing the incident, you have to legitimately be the cool guy in the room. Be that person that has the pause in the conversation. Somebody might be like, do you know what's going on? I absolutely do. I think the biggest breach I've ever had was a phone call. An engineer for another financial, bought a server off eBay. That server fired it up hadn't been wiped. Twenty million credit card records were on it. That triggered a whole review of we had not been controlling for how do third parties because we were now outsourcing data centers. How do third parties wipe the servers that we no longer use? The first thing you're going to do is to contain the breach. If you are still hemorrhaging data, you go through your progressions to stop hemorrhaging data. So if that means shutting down a server, shutting down a data center, shutting down comms, whatever, stopping the data loss is that is your number one priority. Your job as an incident manager or as somebody working a breach is to stop the breach and then investigate the breach. So executing your incident management by plan is the most important thing that an entry level person can keep in mind.
(Required)
en

Introduction to security frameworks and controls

Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start?

As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls.

In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.

There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.

The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.

The last core component of security frameworks is monitoring and communicating results. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.

Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls.
Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk.

Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves.

In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users.