The Cybersecurity Landscape

Cybersecurity risks and threats are ever-present in our world today. The infrastructure of networks and the Internet are increasingly vulnerable to a wide variety of both physical and cyber attacks. Sophisticated cyber criminals, as well as nations, exploit these vulnerabilities to steal information and money.

Our networks are particularly difficult to secure for a number of reasons:

* Networks are increasingly integrated and complex.
* Networks are connected to physical devices.
* Cyber criminals can access networks from anywhere in the world.

In today’s workforce, there is a shortage of people trained in the field of cybersecurity. Here are just a few of the specialties you might consider for your career:

* Cybersecurity Specialist
* Cybersecurity Forensic Expert
* Information Security Expert
* Ethical Hacker

All of these roles can be part of your work in the exciting, ever-changing, high-demand field of cybersecurity. Students who complete the Cybersecurity Essentials course are prepared to continue their education in more advanced security courses.

Course Overview

By the end of this course, you will be able to:

* Describe the characteristics of criminals and heroes in the cybersecurity realm.
* Describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
* Describe the tactics, techniques and procedures used by cyber criminals.
* Describe how technologies, products, and procedures are used to protect confidentiality.
* Describe how technologies, products, and procedures are used to ensure integrity.
* Describe how technologies, products, and procedures provide high availability.
* Explain how cybersecurity professionals use technologies, processes, and procedures to defend all components of the network.
* Explain the purpose of laws related to cybersecurity.

Who Are the Cyber Criminals?

In the early years of the cybersecurity world, the typical cyber criminals were teenagers or hobbyists operating from a home PC, with attacks mostly limited to pranks and vandalism. Today, the world of the cyber criminals has become more dangerous. Attackers are individuals or groups who attempt to exploit vulnerabilities for personal or financial gain. Cyber criminals are interested in everything from credit cards to product designs, and anything with value.

**Amateurs**

Amateurs, or script kiddies, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks. Some are just curious, while others try to demonstrate their skills and cause harm. They may be using basic tools, but the results can still be devastating.

**Hackers**

This group of criminals breaks into computers or networks to gain access for various reasons. The intent of the break-in determines the classification of these attackers as white, gray, or black hats. White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems. The owners of the system give permission to perform the break-in, and they receive the results of the test. On the other hand, black hat attackers take advantage of any vulnerability for illegal personal, financial or political gain. Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda. Some gray hat hackers publish the facts about the vulnerability on the Internet, so that other attackers can exploit it.

The figure gives details about the terms white hat hacker, black hat hacker, and gray hat hacker.

**Organized Hackers**

These criminals include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and may even provide cybercrime as a service. Hacktivists make political statements to create awareness to issues that are important to them. Hacktivists publically publish embarrassing information about their victims. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded. Their attacks focus on specific goals that are beneficial to their government. Some state-sponsored attackers are even members of their nations’ armed forces.

Click [here](https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864) to learn more about hacker profiles

Thwarting Cyber Criminals

Thwarting the cyber criminals is a difficult task and there is no such thing as a “silver bullet.” However, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

* Creating comprehensive databases of known system vulnerabilities and attack signatures (a unique arrangement of information used to identify an attacker’s attempt to exploit a known vulnerability). Organizations share these databases worldwide to help prepare for and fend off many common attacks.
* Establishing early warning sensors and alert networks. Due to cost and the impossibility of monitoring every network, organizations monitor high-value targets or create imposters that look like high-value targets. Because these high-value targets are more likely to experience attacks, they warn others of potential attacks.
* Sharing cyber intelligence information. Business, government agencies and countries now collaborate to share critical information about serious attacks to critical targets in order to prevent similar attacks in other places. Many countries have established cyber intelligence agencies to collaborate worldwide in combating major cyberattacks.
* Establishing information security management standards among national and international organizations. The ISO 27000 is a good example of these international efforts.
* Enacting new laws to discourage cyberattacks and data breaches. These laws have severe penalties to punish cyber criminals caught carrying out illegal actions.

The figure displays measures to thwart cyber criminals and a brief description of each.

Threats to Internet Services

There are many essential technical services needed for a network, and ultimately the Internet, to operate. These services include routing, addressing, domain naming, and database management. These services also serve as prime targets for cyber criminals.

Criminals use packet-sniffing tools to capture data streams over a network. This means that all sensitive data, like usernames, passwords and credit card numbers, are at risk. Packet sniffers work by monitoring and recording all information coming across a network. Criminals can also use rogue devices, such as unsecured Wi-Fi access points. If the criminal sets this up near a public place, such as a coffee shop, unsuspecting individuals may sign on and the packet sniffer copies their personal information.

Domain Name Service (DNS) translates a domain name, such as www.facebook.com, into its numerical IP address. If a DNS server does not know the IP address, it will ask another DNS server. With DNS spoofing (or DNS cache poisoning), the criminal introduces false data into a DNS resolver’s cache. These poison attacks exploit a weakness in the DNS software that causes the DNS servers to redirect traffic for a specific domain to the criminal’s computer, instead of the legitimate owner of the domain.

Packets transport data across a network or the Internet. Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication. Packet forgery allows a criminal to disrupt or intercept packets. This process enables the criminal to hijack an authorized connection or denies an individual’s ability to use certain network services. Cyber professionals call this a man-in-the-middle attack.

The examples given only scratch the surface of the types of threats criminals can launch against Internet and network services.

Internal and External Threats

**Internal Security Threats**

Attacks can originate from within an organization or from outside of the organization, as shown in the figure. An internal user, such as an employee or contract partner, can accidently or intentionally:

* Mishandle confidential data
* Threaten the operations of internal servers or network infrastructure devices
* Facilitate outside attacks by connecting infected USB media into the corporate computer system
* Accidentally invite malware onto the network through malicious email or websites

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal attackers typically have knowledge of the corporate network, its resources, and its confidential data. They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

**External Security Threats**

External threats from amateurs or skilled attackers can exploit vulnerabilities in networked devices, or can use social engineering, such as trickery, to gain access. External attacks exploit weaknesses or vulnerabilities to gain access to internal resources.

**Traditional Data**

Corporate data includes personnel information, intellectual property, and financial data. Personnel information includes application materials, payroll, offer letters, employee agreements, and any information used in making employment decisions. Intellectual property, such as patents, trademarks and new product plans, allows a business to gain economic advantage over its competitors. Consider this intellectual property as a trade secret; losing this information can be disastrous for the future of the company. Financial data, such as income statements, balance sheets, and cash flow statements, gives insight into the health of the company.

The Emergence of the Internet of Things

The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet. The technological evolution associated with the advent of the IoT is changing commercial and consumer environments. IoT technologies enable people to connect billions of devices to the Internet. These devices include appliances, locks, motors, and entertainment devices, to name just a few. This technology affects the amount of data that needs protection. Users access these devices remotely, which increases the number of networks requiring protection.

With the emergence of IoT, there is much more data to be managed and secured. All of these connections, plus the expanded storage capacity and storage services offered through the Cloud and virtualization, has led to the exponential growth of data. This data expansion created a new area of interest in technology and business called “Big Data".

Using Advanced Weapons

Software vulnerabilities today rely on programming mistakes, protocol vulnerabilities, or system misconfigurations. The cyber criminal merely has to exploit one of these. For example, a common attack involved constructing an input to a program in order to sabotage the program, making it malfunction. This malfunction provided a doorway into the program or caused it to leak information.

There is a growing sophistication seen in cyberattacks today. An advanced persistent threat (APT) is a continuous computer hack that occurs under the radar against a specific object. Criminals usually choose an APT for business or political motives. An APT occurs over a long period with a high degree of secrecy using sophisticated malware.

Algorithm attacks can track system self-reporting data, like how much energy a computer is using, and use that information to select targets or trigger false alerts. Algorithmic attacks can also disable a computer by forcing it to use memory or by overworking its central processing unit. Algorithmic attacks are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.

Finally, the new generation of attacks involves intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. However, with greater attention to detection and isolation of cyberattacks, cyber criminals must be more careful. They cannot risk early detection or the cybersecurity specialists will close the gates of the castle. As a result, many of the more sophisticated attacks will only launch if the attacker can match the object signature targeted.

Cloud-based Technology Safeguards

Cloud-based technologies shift the technology component from the organization to the cloud provider. The three main cloud computing services include:

* **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider’s servers.
* **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
* **Platform as a Service (PaaS)** provides access to the development tools and services used to deliver the applications.

Cloud service providers have extended these options to include IT as a Service (ITaaS), which provides IT support for IaaS, PaaS, and SaaS service models. In the ITaaS model, an organization contracts with the Cloud provider for individual or bundled services.

Cloud service providers use virtual security appliances that run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.

Policies

A security policy is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.

A comprehensive security policy accomplishes several tasks:

* It demonstrates an organization’s commitment to security.
* It sets the rules for expected behavior.
* It ensures consistency in system operations, software and hardware acquisition and use, and maintenance.
* It defines the legal consequences of violations.
* It gives security staff the backing of management.

Security policies inform users, staff, and managers of an organization’s requirements for protecting technology and information assets. A security policy also specifies the mechanisms needed to meet security requirements.

As shown in the figure, a security policy typically includes:

* **Identification and authentication policies -** Specifies authorized persons that can have access to network resources and outlines verification procedures.
* **Password policies -** Ensures passwords meet minimum requirements and are changed regularly.
* **Acceptable use policies -** Identifies network resources and usage that are acceptable to the organization. It may also identify ramifications for policy violations.
* **Remote access policies -** Identifies how remote users can access a network and what is remotely accessible.
* **Network maintenance policies -** Specifies network device operating systems and end user application update procedures.
* **Incident handling policies -** Describes how security incidents are handled.

One of the most common security policy components is an acceptable use policy (AUP). This component defines what users can and cannot do on the various system components. The AUP should be as explicit as possible to avoid misunderstanding. For example, an AUP lists specific websites, newsgroups, or bandwidth intensive applications that users cannot access using company computers or the company network.