Instructor Materials Chapter 1: A World of Wizard, Heroes, and Criminals

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1:
A World of Wizard, Heroes, and Criminals

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1 - Sections & Objectives

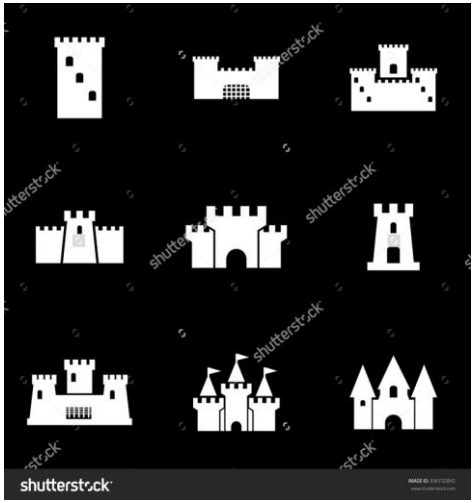
- 1.1 Characteristics of Cybersecurity World
  - Describe the common characteristics comprising the cybersecurity world
- 1.2 Criminals and Cybersecurity Professionals
  - Differentiate the characteristics of cyber criminals and heroes
- 1.3 Comparing Cybersecurity Threats
  - Compare how cybersecurity threats affect individuals, businesses, and organizations
- 1.4 Cybercrime Growth Factors
  - Analyze the organizations and efforts committed to expanding the cybersecurity workforce

1.1 The Cybersecurity World

Cisco | Networking Academy®
Mind Wide Open™

Overview of the Kingdoms

- Websites and Power of Data
  - Great businesses have been created by collecting and harnessing the power of data and data analytics
  - These businesses have the responsibility to protect this data from misuse and unauthorized access
  - The growth of data has created great opportunities for cybersecurity specialists
- Kingdoms
  - Business large and small have recognized the power of big data and data analytics
  - Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
  - The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm



Overview of the Kingdoms (Cont.)

- Cyber wizards now have the technology to track worldwide weather trends, monitor the oceans, and track the movement and behavior of people, animals and objects in real time.
- New technologies, such as Geospatial Information Systems (GIS) and the Internet of Everything (IoE), have emerged. Each depends on collecting and analyzing tremendous amounts of data.
- This growing collection of data can help people save energy, improve efficiencies, and reduce safety risks.

1.2 Cyber Criminals versus Cyber Professionals

Cisco | Networking Academy®
Mind Wide Open™

Cybersecurity Criminals

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.

  White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.

  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.

  Black hat attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists -** Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers -** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

Cybersecurity Specialists

Thwarting the cyber criminals is a difficult task, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database**: The Nation Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all know vulnerabilities. http://www.cvedetails.com/
- **Early Warning Systems**: The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualization of attacks. https://www.honeynet.org/node/960
- **Share Cyber Intelligence**: InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the and the private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks. https://www.infragard.org/

Cybersecurity Specialist (Cont.)

- **ISM Standards**: The ISO 27000 standards are an example of Information Security Management Standards. The standards provide a framework for implementing cybersecurity measures within an organization. http://www.27000.org/
- **New Laws**: The ISACA group track law enacted related to cyber security. These laws can address individual privacy to protection of intellectual property. Examples of these laws include: Cybersecurity Act, Federal Exchange Data Breach Notification Act and the Data Accountability and Trust Act. http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Tools for Thwarting Cybercrime

1.3 Threats to the Kingdom

Cisco | Networking Academy®
Mind Wide Open™

Threat Arenas

- The term cyber wizards refers to the innovators and visionaries that build the cyber kingdom
- Cyber wizards possess the insight to recognize the influence of data and harness that power to build great organizations, provide services and protect people from cyberattacks
- Cyber wizards recognize the threat that data poses if used against people
- A cybersecurity threat is the possibility that a harmful event, such as an attack, will occur
- Cyber vulnerability is a weakness that makes a target susceptible to an attack
- Cyber threats are particularly dangerous to certain industries and the type of information they collect and protect

Threat Arenas (Cont.)

The following examples are just a few sources of data that can come from established organizations:

- **Personal Information**
- **Medical Records**
- **Education Records**
- **Employment and Financial Records**

Threat Arenas (Cont.)

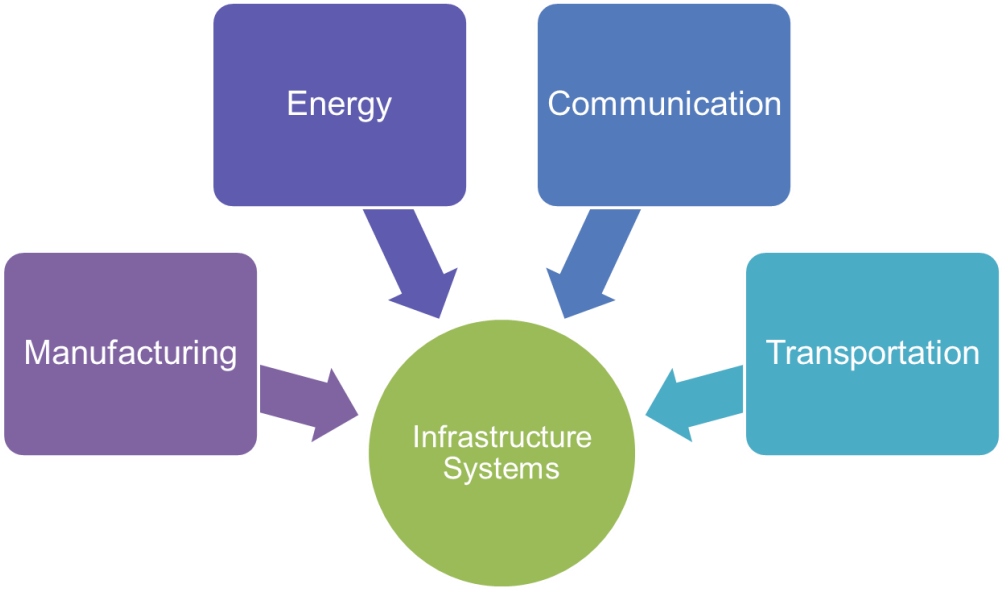
Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

- Criminals use packet-sniffing tools to capture data streams over a network. 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.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.

Threat Arenas (Cont.)

Sectors of the kingdom include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road



Threat Arenas (Cont.)

- On a personal level, everyone needs to safeguard his or her identity, data, and computing devices.
- At the corporate level, it is the employees' responsibility to protect the organization's reputation, data, and customers.
- At the state level, national security and the citizens' safety and well-being are at stake.
- In the U.S., the National Security Agency (NSA) is responsible for intelligence collection and surveillance activities.
- The efforts to protect people's way of life often conflicts with their right to privacy.

1.4 The Dark Forces of Cybersecurity

Cisco | Networking Academy®
Mind Wide Open™

The Spread of the Dark Forces

Attacks can originate from within an organization or from outside of the organization, as shown in the figure.

Internal Security Threats

- An internal user, such as an employee or contract partner, can accidently or intentionally
- 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.

The Spread of the Dark Forces (Cont.)

Vulnerabilities of Mobile Devices - In the past, employees typically used company-issued computers connected to a corporate LAN.

- Today, mobile devices such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or additions to, the traditional PC.
- More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend.
- The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

The Spread of the Dark Forces (Cont.)

- **Emergence Internet-of-Things** - The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet.
- 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.

The Spread of the Dark Forces (Cont.)

Impact of Big Data – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

There are numerous examples of big corporate hacks in the news. As a result, enterprise systems require dramatic changes in security product designs and substantial upgrades to technologies and practices. Additionally, governments and industries are introducing more regulations and mandates that require better data protection and security controls to help guard big data.

The Sophistication of the Dark Forces

Advanced Weapons

- 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.
- 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 are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.
- Intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. Many of the most sophisticated attacks will only launch if the attacker can match the signatures of the targeted victim.

Broader Scope and Cascade Effect

- Federated identity management refers to multiple enterprises that let their users use the same identification credentials gaining access to the networks of all enterprises in the group. The goal of federated identity management is to share identity information automatically across castle boundaries.
- The most common way to protect federated identity is to tie login ability to an authorized device.

The Sophistication of the Dark Forces (Cont.)

Safety Implications

- There are many safety implication associated with the dark forces of cyber security including emergency call centers in the U.S. are vulnerable to cyberattacks that could shut down 911 networks, jeopardizing public safety.
- A telephone denial of service (TDoS) attack uses phone calls against a target telephone network tying up the system and preventing legitimate calls from getting through.
- The next generation 911 call centers are vulnerable because they use Voice-over-IP (VoIP) systems rather than traditional landlines.

Heightened Recognition of Cybersecurity Threats

- The defenses against cyberattacks at the start of the cyber era were low. A smart high school student or script kiddie could gain access to systems.
- Now, countries across the world have become more aware of the threat of cyberattacks. The threat posed by cyberattacks now head the list of greatest threats to national and economic security in most countries.

1.5 Creating More Heroes

Cisco | Networking Academy®
Mind Wide Open™

A Workforce Framework for Cybersecurity

Addressing the Shortage of Cybersecurity Specialists

- In the U.S., the National Institute of Standards and Technologies (NIST) created a framework for companies and organizations in need of cybersecurity professionals. The framework enables companies to identify the major types of responsibilities, job titles, and workforce skills needed.

The Seven Categories of Cybersecurity Wizards

The Workforce Framework categorizes cybersecurity work into seven categories.

- **Operate and Maintain** includes providing the support, administration, and maintenance required to ensure IT system performance and security
- **Protect and Defend** includes the identification, analysis, and mitigation of threats to internal systems and networks
- **Investigate** includes the investigation of cyber events and/or cyber crimes involving IT resources
- **Collect and Operate** includes specialized denial and deception operations and the collection of cybersecurity information

A Workforce Framework for Cybersecurity (Cont.)

- **Analyze** includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence
- **Oversight and Development** provides for leadership, management, and direction to conduct cybersecurity work effectively
- **Securely Provision** includes conceptualizing, designing, and building secure IT systems

Within each category, there are several specialty areas. The specialty areas then define common types of cybersecurity work.

Online Cybersecurity Communities

Professional Organizations

- Cybersecurity specialists must collaborate with professional colleagues frequently. International technology organizations often sponsor workshops and conferences. Visit each site with your class and explore the resources available.

Online Cybersecurity Communities

Cybersecurity Student Organizations and Competitions

- Cybersecurity specialists must have the same skills as hackers, especially black hat hackers, in order to protect against attacks.
- How can an individual build and practice the skills necessary to become a cybersecurity specialist?
- Student skills competitions are a great way to build cybersecurity knowledge skills and abilities.
- There are many national cybersecurity skills competitions available to cybersecurity students.

SkillsUSA®

USCC™
US CYBER CHALLENGE

ncl

Cybersecurity Certifications

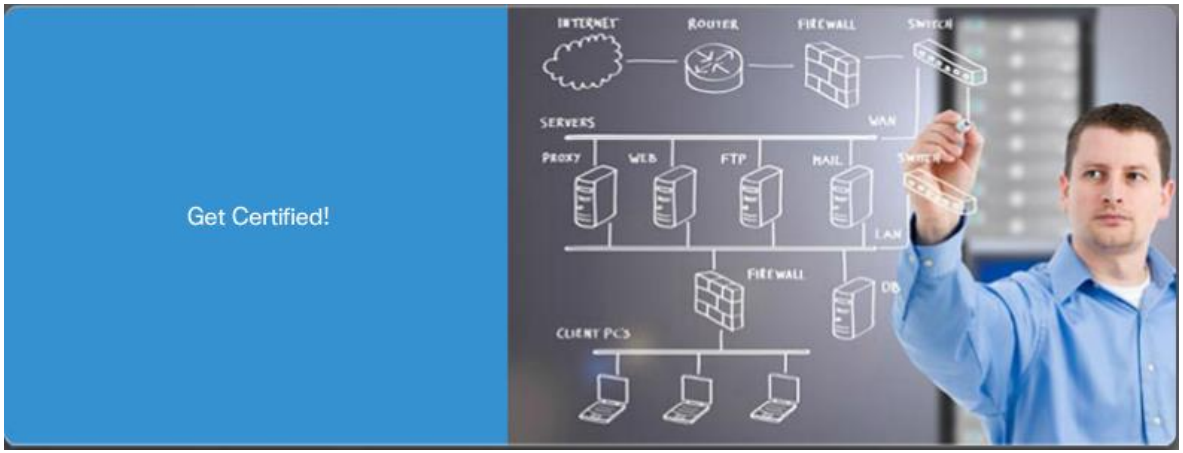
Industry Certifications

In a world of cybersecurity threats, there is a great need for skilled and knowledgeable information security professionals. The IT industry established standards for cybersecurity specialists to obtain professional certifications that provide proof of skills, and knowledge level.

- **CompTIA Security+ -** Security+ is a CompTIA-sponsored testing program that certifies the competency of IT administrators in information assurance.
- **EC-Council Certified Ethical Hacker (CEH) –** CEH is an intermediate-level certification asserts that cybersecurity specialists holding this credential possess the skills and knowledge for various hacking practices.
- **SANS GIAC Security Essentials (GSEC) -** The GSEC certification is a good choice for an entry-level credential for cybersecurity specialists who can demonstrate that they understand security terminology and concepts and have the skills and expertise required for “hands-on” security roles. The SANS GIAC program offers a number of additional certifications in the fields of security administration, forensics, and auditing.

Cybersecurity Certifications (Cont.)

- **(ISC)^2 Certified Information Systems Security Professional (CISSP) -** The CISSP certification is a vendor-neutral certification for those cybersecurity specialists with a great deal of technical and managerial experience. It is also formally approved by the U.S. Department of Defense (DoD) and is a globally recognized industry certification in the security field.
- **ISACA Certified Information Security Manager (CISM) -** Cyber heroes responsible for managing, developing and overseeing information security systems at the enterprise level or for those developing best security practices can qualify for CISM.



Cybersecurity Certifications (Cont.)

Company Sponsored Certifications - Another important credential for cybersecurity specialists are company-sponsored certifications. These certifications measure knowledge and competency in installing, configuring, and maintaining vendor products. Cisco and Microsoft are examples of companies with certifications that test knowledge of their products. Click here to explore the matrix of the Cisco certifications shown in the figure.

Cisco Certified Network Associate Security (CCNA Security) - The CCNA Security certification validates that a cybersecurity specialist has the knowledge and skills required to secure Cisco networks.

Cisco Certifications

	Entry	Associate	Professional	Expert
Architect				CCAr Architect
Cloud		CCNA Cloud	CCNP Cloud	
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center
Design	CCENT	CCDA	CCDP	CCDE
Industrial / IoT		CCNA Industrial		
Routing & Switching	CCENT	CCNA Routing & Switching	CCNP Routing & Switching	CCIE Routing & Switching
Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Service Provider		CCNA SP	CCNP SP	CCIE SP
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Other Certifications	Certified Technician			
Specialist	Business	Data Center	Internet of Things	Network Programmability
	Security	Operating System Software	Service Provider	Collaboration

Cybersecurity Certifications (Cont.)

How to Become a Cyber Hero

Heroes must be able to respond to threats as soon as they occur. This means that the working hours can be somewhat unconventional. Cyber heroes also analyze policy, trends, and intelligence to understand how cyber criminals think. Many times, this may involve a large amount of detective work. Here is good advice for becoming a cybersecurity hero:

- **Study**: Learn the basics by completing courses in IT. Be a life-long learner. Cybersecurity is an ever-changing field, and cybersecurity specialists must keep up.
- **Pursue Certifications**: Industry and company sponsored certifications from organizations such as Microsoft and Cisco prove that one possesses the knowledge needed to seek employment as a cybersecurity specialist.
- **Pursue Internships**: Seeking out a security internship as a student can lead to opportunities down the road.
- **Join Professional Organizations**: Join computer security organizations, attend meetings and conferences, and join forums and blogs to gain knowledge from the experts.

1.6 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- This chapter explained the structure of the cybersecurity world and the reason it continues to grow with data and information as the prized currency.
- It explored the motivation of cyber criminals.
- It explored the spread of the dark forces due to the ever-expanding technical transformations taking place throughout the world.
- It provided details on how to become a cyber hero to help defeat the cyber criminals that empower the dark forces.
- It surveyed the resources available to help create more heroes.
- It explained that cyber professionals must have the same skills as the cyber criminals.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.