Instructor Materials
Chapter 8: Becoming a Cybersecurity Specialist

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 8: Becoming a Cybersecurity Specialist

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 8 - Sections & Objectives

8.1 Cybersecurity Domains

Describe resources available to students interested in pursuing a career in cybersecurity.

8.2 Understanding the Ethics of Working in Cybersecurity

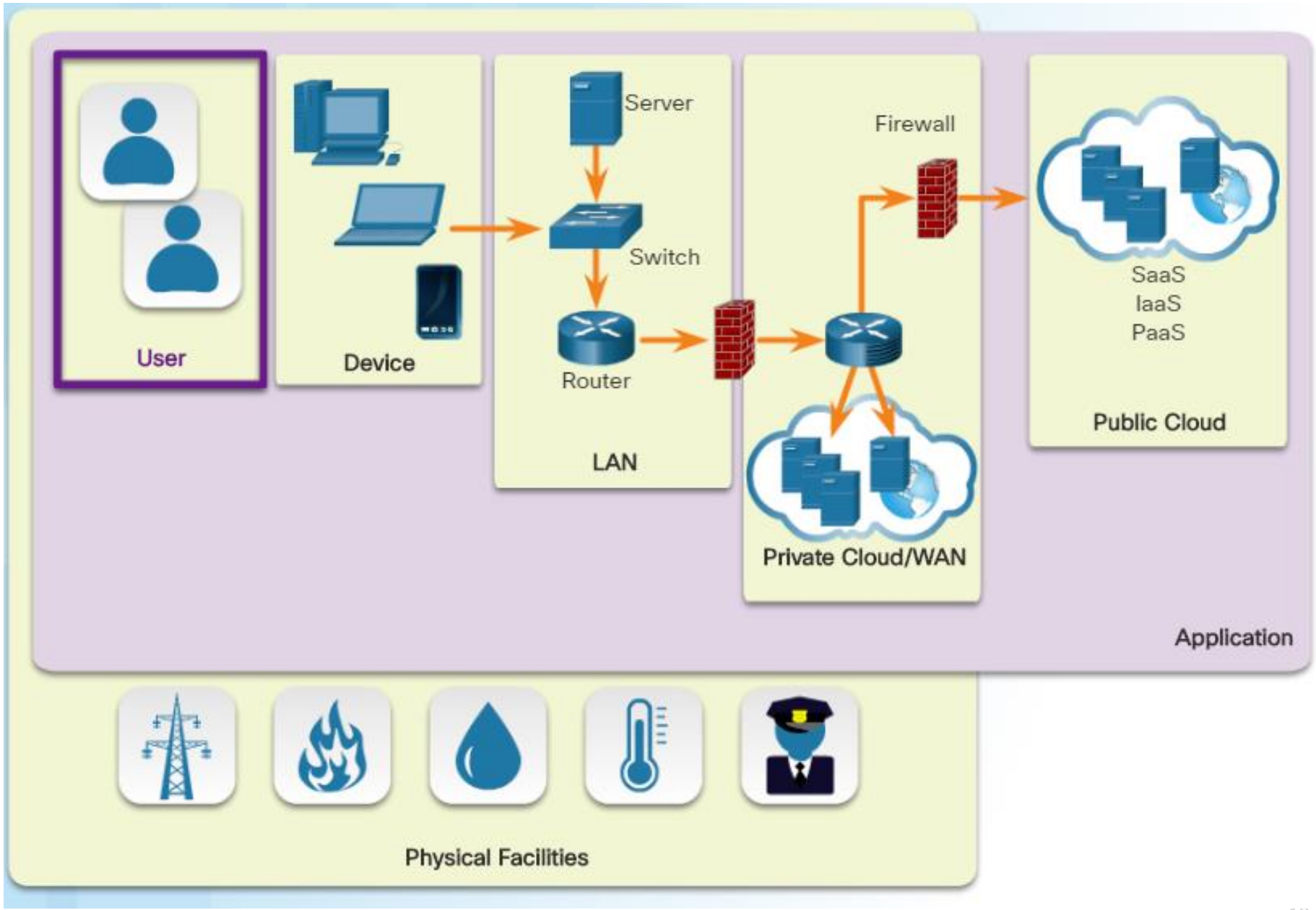
Explain how ethics provide guidance.

8.3 Next Step

Explain how to take the next step to become a cybersecurity professional.

8.1 Cybersecurity Domains

Cisco | Networking Academy®
Mind Wide Open™



User Domain

Common User Threats and Vulnerabilities

- The User Domain includes the users who access the organization's information system.
- Users can be employees, customers, business contractors and other individuals that need access to data.
- Users are often the weakest link in the information security systems and pose a significant threat to the confidentiality, integrity, and availability of the organization's data.

Managing User Threats

- Conduct security awareness training and user education.
- Enable and automate content filtering and antivirus scanning.
- Disable internal CD drives and USB ports.
- Minimize permissions, restrict access, track and monitor users and enable intrusion detection.

Device Domain

Common Threats to Devices

- Unattended workstations, user downloads, unpatched software
- Malware, use of unauthorized media, and violations of the acceptable use policy.

Device Domain Threats	Countermeasure to Manage Threat
Unattended workstations	Establish user account policies for passwords and threshold lockouts
User downloads	Establish access control policies, standards, procedures, and guidelines
Unpatched software	Update and apply security patches according to defined policies, standards, procedures, and guidelines
Malware	Enable an automated antivirus solution to scan systems and update antivirus software
Unauthorized media	Disable internal CD drives and USB ports
Acceptable Use Policy Violation	▪ Use content filtering ▪ Use antivirus scanning for downloaded files ▪ Disable internal CD drives and USB port

Local Area Network Domain

Common Threats to the LAN

- Unauthorized LAN access, unauthorized access to systems, applications, wireless networks and data
- Network operating system software vulnerabilities, misconfigurations and failure to perform updates
- Unauthorized network probing and port scanning

LAN Domain Threats	Countermeasure to Manage Threat
Unauthorized LAN access	• Secure wiring closets, data centers, computer rooms • Define strict access control policies, procedures, and guidelines
Unauthorized access to systems, applications, and data	• Define strict access control policies, procedures, and guidelines • Restrict access privileges for folders and files based on need
Network operating system software vulnerablitities	• Implement policy to patch and update operating systems
Network operating system unpatched	• Implement policy to patch and update operating systems
Unauthorized access by rogue users	• Require passphrases or authentication for wireless networks
Exploits of data in-transit	• Implement encryption between devices and wireless networks
LAN servers with different hardware or operating systems	• Implement LAN server configuration standards
Unauthorized network probing and port scanning	• Conduct post-configuration penetration tests
Firewall misconfiguration	• Conduct post-configuration penetration tests

Private Cloud (WAN) Domain

Common Threats to the Private Cloud:

- Unauthorized network probing, port scanning and access to resources.
- Router, firewall, or network device operating system software vulnerability and misconfiguration.
- Remote users accessing the organization's infrastructure and downloading sensitive data.

Private Cloud Domain Threats	Countermeasure to Manage Threat
Unauthorized network probing and port scanning	• Disable ping, probing, and port scanning
Unauthorized access to resources	• Implement intrusion detection and prevention systems
Router, firewall, or network device operating system software vulnerability	• Update devices with security fixes and patches
Router, firewall, or network device configuration error	• Conduct penetration tests post configuration • Test inbound and outbound traffic
Remote users download sensitive data	• Implement data classification standard • Implement file transfer monitoring and scanning

Cybersecurity Domains

Public Cloud Domain

Common Threats to the Public Cloud:

- Data breaches, loss or theft of intellectual property and compromised credentials.
- Federated identity repositories are a high-value target.
- Account hijacking, social engineering attacks and lack of understanding on the part of the organization.

Public Cloud Domain Threats	Countermeasure to Manage Threat
Data breaches	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Loss or theft of intellectual property	• Due diligence • Use of encryption • Data backup
Compromised credentials	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Use of federated identity repositories	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Account hijacking	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Lack of understanding on the part of organization	• Due diligence on agreement responsibilities
Social engoneering attacks that lure the victim	• Security awareness programs
Compliance violations	• Due diligence • Policies

Physical Facilities Domain

Common Threats to Physical Facilities:

- Natural threats including weather problems, geological hazards, and power interruptions
- Unauthorized access to the facilities, open lobbies, theft, unlocked data center, lack of surveillance
- Social engineering, breach of electronic perimeter defenses

Physical Facilities Domain Threats	Countermeasure to Manage Threat
Natural threats including weather and geological problems	• Develop a disaster recovery plan • Develop a business continuity plan
Unauthorized access to facilities	• Implement badge encryption for entry access
Power interruptions	• Develop a disaster recovery plan
Social engineering	• Implement badge encryption for entry access • Conduct security awareness training regularly
Breach of electronic perimeter defenses	• Test building security using both cyber and physical means to covertly gain access
Theft	• Implement an asset tagging system • Establish policies and procedures for visitors
An open lobby	• Implement badge encryption for entry access
Lack of surveillance	• Implement CCTV coverage of all entrances • Test building security using both cyber and physical means to covertly gain access
An unlocked data center	• Implement badge encryption for entry access

Application Domain

Common Threats to Applications:

- Unauthorized access to data centers, computer rooms, and wiring closets
- Server downtime for maintenance, IT systems down for extended periods
- Network operating system software vulnerability
- Unauthorized access to systems
- Data loss

Application Domain Threats	Countermeasure to Manage Threat
Unauthorized access to data centers, computer rooms, and wiring closets	• Policies, standards, and procedures for staff and visitors
Server downtime for maintenance	• Disaster recovery plan • Business continuity plan
Network operating system software vulnerability	• Patches and updates completed regularly
Unauthorized access to systems	• Multi-factor authentication • Monitor log files
Data loss	• Data classification standards • Backup procedures
Downtime of IT systems for an extended period	• Disaster recovery plan • Business continuity plan
Software development vulnerabilities	• Conduct software testing prior to launch

8.2 Understanding the Ethics of Working in Cybersecurity

Cisco | Networking Academy®
Mind Wide Open™

Ethics and Guiding Principles

Ethics of a Cybersecurity Specialist

Ethics is the little voice in the background guiding a cybersecurity specialist as to what he should or should not do, regardless of whether it is legal. The organization entrusts the cybersecurity specialist with the most sensitive data and resources. The cybersecurity specialist needs to understand how the law and the organization's interests help to guide ethical decisions.

Computer Ethics Institute

The Computer Ethics Institute is a resource for identifying, assessing, and responding to ethical issues throughout the information technology industry. CEI was one of the first organizations to recognize the ethical and public policy issues arising from the rapid growth of the information technology field.

Cyber Laws and Liability

Cybercrime

Laws prohibit undesired behaviors. Unfortunately, the advancements in information system technologies are much faster than the legal system can accommodate. A number of laws and regulations affect cyberspace.

Cybercrime

A computer may be involved in a cybercrime in a couple of different ways. There is computer-assisted crime, computer-targeted crime, and computer-incidental crime. Child pornography is an example of computer-incidental crime; the computer is a storage device and is not the actual tool used to commit the crime.

Organizations Created to Fight Cybercrime

There are a number of agencies and organizations out there to aid the fight against cybercrime.

Cyber Laws and Liability (Cont.)

Civil, Criminal, and Regulatory Cyber Laws

In the United States, there are three primary sources of laws and regulations: statutory law, administrative law, and common law. All three sources involve computer security. The U.S. Congress established federal administrative agencies and a regulatory framework that includes both civil and criminal penalties for failing to follow the rules.

Industry Specific Laws

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Import/Export Encryption Restrictions

Security Breach Notification Laws

- Electronic Communications Privacy Act (ECPA)
- Computer Fraud and Abuse Act (1986)

Cyber Laws and Liability (Cont.)

Protecting Privacy

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- U.S. Children's Internet Protection Act (CIPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- California Senate Bill 1386 (SB 1386)

International Laws

- Convention on Cybercrime
- Electronic Privacy Information Center (EPIC)

Cybersecurity Information Websites

National Vulnerability Database (NVD) - is a U.S. government repository of standards-based vulnerability management data that uses the Security Content Automation Protocol (SCAP).

CERT - The Software Engineering Institute (SEI) at Carnegie Mellon University helps government and industry organizations to develop, operate, and maintain software systems that are innovative, affordable, and trustworthy. It is a Federally Funded Research and Development Center sponsored by the U.S. Department of Defense.

Internet Storm Center - provides a free analysis and warning service to Internet users and organizations. It also works with Internet Service Providers to combat malicious cyber criminals. The Internet Storm Center gathers millions of log entries from intrusion detection systems every day using sensors covering 500,000 IP addresses in over 50 countries.

The Advanced Cyber Security Center (ACSC) - is a non-profit organization that brings together industry, academia, and government to address advanced cyber threats. The organization shares information on cyber threats, engages in cybersecurity research and development, and creates education programs to promote the cybersecurity profession.

Cybersecurity Weapons

Vulnerability Scanners - assess computers, computer systems, networks, or applications for weaknesses. Vulnerability scanners help to automate security auditing by scanning the network for security risks and producing a prioritized list to address weaknesses.

Penetrating Testing (or pen testing) - is a method of testing the areas of weaknesses in systems by using various malicious techniques. Pen testing is not the same as vulnerability testing. Vulnerability testing just identifies potential problems. Pen testing involves a cybersecurity specialist who hacks a website, network, or server with the organization's permission to try to gain access to resources without the knowledge of usernames, passwords, or other normal means.

Packet Analyzers (or packet sniffers) - intercept and log network traffic. The packet analyzer captures each packet, shows the values of various fields in the packet, and analyzes its content. A sniffer can capture network traffic on both wired and wireless networks.

Security Tools - There is no one size fits all when it comes to the best security tools. Much depends on the situation, circumstance, and personal preference. A cybersecurity specialist must know where to go to get sound information.

8.3 Next Step

Cisco | Networking Academy®
Mind Wide Open™

Exploring the Cybersecurity Profession

Defining the Roles of Cybersecurity Professionals

The ISO standard defines the role of cybersecurity professionals. The ISO 27000 framework requires:

- A senior manager responsible for IT and ISM (often the audit sponsor)
- Information security professionals and security administrators
- Site/physical security manager and facilities contacts
- HR contact for HR matters such as disciplinary action and training
- Systems and network managers, security architects and other IT professionals

Job Search Tools

A variety of websites and mobile applications advertise information technology jobs. Each site targets varying job applicants and provides different tools for candidates researching their ideal job position:

- Indeed.com
- CareerBuilder.com
- USAJobs.gov

8.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- This chapter categorizes the information technology infrastructure created by the advancement of technology into seven domains.
- The chapter discussed the laws that affect technology and cybersecurity requirements.
- Laws such as FISMA, GLBA, and FERPA focus on protecting confidentiality.
- Laws that focus on the protection of integrity include FISMA, SOX, and FERPA, and laws that concern availability include FISMA, GLBA, SOX, and CIPA.
- In addition to the laws in force, the cybersecurity specialist needs to understand how the use of computers and technology affect both individuals and society.
- The chapter also explored the opportunity to become a cybersecurity specialist.
- Finally, this chapter discussed several tools available to cybersecurity specialists.