Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability, known as the CIA triad (Figure 1), is a guideline for information security for an organization. Confidentiality ensures the privacy of data by restricting access through authentication encryption. Integrity assures that the information is accurate and trustworthy. Availability ensures that the information is accessible to authorized people.

**Confidentiality**

Another term for confidentiality would be privacy. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data. The data may be compartmentalized according to the security or sensitivity level of the information. For example, a Java program developer should not have to access to the personal information of all employees. Furthermore, employees should receive training to understand the best practices in safeguarding sensitive information to protect themselves and the company from attacks. Methods to ensure confidentiality include data encryption, username ID and password, two factor authentication, and minimizing exposure of sensitive information.

**Integrity**

Integrity is accuracy, consistency, and trustworthiness of the data during its entire life cycle. Data must be unaltered during transit and not changed by unauthorized entities. File permissions and user access control can prevent unauthorized access. Version control can be used to prevent accidental changes by authorized users. Backups must be available to restore any corrupted data, and checksum hashing can be used to verify integrity of the data during transfer.

A checksum is used to verify the integrity of files, or strings of characters, after they have been transferred from one device to another across your local network or the Internet. Checksums are calculated with hash functions. Some of the common checksums are MD5, SHA-1, SHA-256, and SHA-512. A hash function uses a mathematical algorithm to transform the data into fixed-length value that represents the data, as shown in Figure 2. The hashed value is simply there for comparison. From the hashed value, the original data cannot be retrieved directly. For example, if you forgot your password, your password cannot be recovered from the hashed value. The password must be reset.

After a file is downloaded, you can verify its integrity by verifying the hash values from the source with the one you generated using any hash calculator. By comparing the hash values, you can ensure that the file has not been tampered with or corrupted during the transfer.

**Availability**

Maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups ensure the availability of the network and data to the authorized users. Plans should be in place to recover quickly from natural or man-made disasters. Security equipment or software, such as firewalls, guard against downtime due to attacks such as denial of service (DoS). Denial of service occurs when an attacker attempts to overwhelm resources so the services are not available to the users.

f1ac4e42c21dad8d6676d00bf2452ef8

875dba9eb6ce4b706f22ce99d6950d1e

cbaaf1f62a9dd90ad4d9b3d0451736b9

# The Consequences of a Security Breach

To protect an organization from every possible cyberattack is not feasible, for a few reasons. The expertise necessary to set up and maintain the secure network can be expensive. Attackers will always continue to find new ways to target networks. Eventually, an advanced and targeted cyberattack will succeed. The priority will then be how quickly your security team can respond to the attack to minimize the loss of data, downtime, and revenue.

By now you know that anything posted online can live online forever, even if you were able to erase all the copies in your possession. If your servers were hacked, the confidential personnel information could be made public. A hacker (or hacking group) may vandalize the company website by posting untrue information and ruin the company’s reputation that took years to build. The hackers can also take down the company website causing the company to lose revenue. If the website is down for longer periods of time, the company may appear unreliable and possibly lose credibility. If the company website or network has been breached, this could lead to leaked confidential documents, revealed trade secrets, and stolen intellectual property. The loss of all this information may impede company growth and expansion.

The monetary cost of a breach is much higher than just replacing any lost or stolen devices, investing in existing security and strengthening the building’s physical security. The company may be responsible for contacting all the affected customers about the breach and may have to be prepared for litigation. With all this turmoil, employees may choose to leave the company. The company may need to focus less on growing and more on repairing its reputation.

# Security Breach Example 1

The online password manager, LastPass, detected unusual activity on its network in July 2015. It turned out that hackers had stolen user email addresses, password reminders, and authentication hashes. Fortunately for the users, the hackers were unable to obtain anyone’s encrypted password vaults.

Even though there was a security breach, LastPass could still safeguard the users’ account information. LastPass requires email verification or multi-factor authentication whenever there is a new login from an unknown device or IP address. The hackers would also need the master password to access the account.

LastPass users also have some responsibility in safeguarding their own accounts. The users should always use complex master passwords and change the master passwords periodically. The users should always beware of Phishing attacks. An example of a Phishing attack would be if an attacker sent fake emails claiming to be from LastPass. The emails ask the users to click an embedded link and change the password. The link in the email goes to a fraudulent version of the website used to steal the master password. The users should never click the embedded links in an email. The users should also be careful with their password reminder. The password reminder should not give away your passwords. Most importantly, the users should enable multi-factor authentication when available for any website that offers it.

If the users and service providers both utilize the proper tools and procedures to safeguard the users’ information, the users’ data could still be protected, even in the event of security breach.

# Security Breach Example 2

The high tech toy maker for children, Vtech, suffered a security breach to its database in November 2015. This breach could affect millions of customers around the world, including children. The data breach exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.

A toy tablet had become a new target for hackers. The customers had shared photos and used the chat features through the toy tablets. The information was not secured properly, and the company website did not support secure SSL communication. Even though the breach did not expose any credit card information and personal identification data, the company was suspended on the stock exchange because the concern over the hack was so great.

Vtech did not safeguard the customers’ information properly and it was exposed during the breach. Even though the company informed its customers that their passwords had been hashed, it was still possible for the hackers to decipher them. The passwords in the database were scrambled using MD5 hash function, but the security questions and answers were stored in plaintext. Unfortunately, MD5 hash function has known vulnerabilities. The hackers can determine the original passwords by comparing millions of pre-calculated hash values.

With the information exposed in this data breach, cybercriminals could use it to create email accounts, apply for credits, and commit crimes before the children were old enough to go to school. For the parents of these children, the cybercriminals could take over the online accounts because many people reuse their passwords on different websites and accounts.

The security breach not only impacted the privacy of the customers, it ruined the company’s reputation, as indicated by the company when its presence on the stock exchange was suspended.

For parents, it is a wake-up call to be more vigilant about their children’s privacy online and demand better security for children’s products. For the manufacturers of network-connected products, they need to be more aggressive in the protection of customer data and privacy now and in the future, as the cyberattack landscape evolves.

# Security Breach Example 3

Equifax Inc. is one of the nationwide consumer credit reporting agencies in the United States. This company collects information on millions of individual customers and businesses worldwide. Based on the collected information, credit scores and credit reports are created about the customers. This information could affect the customers when they apply for loans and when they are looking for employment.

In September 2017, Equifax publicly announced a data breach event. The attackers exploited a vulnerability in the Apache Struts web application software. The company believes that millions of U.S. consumers' sensitive personal data were accessed by the cyber criminals between May and July of 2017. The personal data includes the customers' full names, Social Security numbers, birth dates, addresses and other personally identifiable information. There is evidence that the breach may have affected customers in United Kingdom and Canada.

Equifax established a dedicated web site that allows the consumers to determine if their information was compromised, and to sign up for credit monitoring and identity theft protection. Using a new domain name, instead of using a subdomain of equifax.com, this allowed nefarious parties to create unauthorized websites with similar names. These websites can be used as part of a phishing scheme to trick you into providing personal information. Furthermore, an employee from Equifax provided an incorrect web link in social media for worried customers. Fortunately, this web site was taken down within 24 hours. It was created by an individual who use it as an educational opportunity to expose the vulnerabilities that exists in Equifax's response page.

As a concerned consumer, you may want to quickly verify if your information was compromised, so you can minimize the impact. In a time of crisis, you may be tricked into using unauthorized websites. You should be cautious about providing personal information so you do not become a victim again. Furthermore, companies are responsible for keeping our information safe from unauthorized access. Companies need to regularly patch and update their software to mitigate exploitation of known vulnerabilities. Their employees should be educated and informed about the procedures to safeguard the information and what to do in the event of a breach.

Unfortunately, the real victims of this breach are the individuals whose data may have been compromised. In this case, Equifax has the burden of protecting the collected consumer data while conducting credit checks because the customers did not choose to use the services provided by Equifax. The consumer has to trust the company to safeguard the collected information. Furthermore, the attackers can use this data to assume your identity, and it is very difficult to prove otherwise because both the attacker and the victim know the same information. In these situations, the most you can do is be vigilant when you are providing personally identifiable information over the Internet. Check your credit reports regularly (once per month or once per quarter). Immediately report any false information, such as applications for credit that you did not initiate, or purchases on your credit cards that you did not make.

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. Attackers are interested in everything, from credit cards to product designs and anything with value.

**Amateurs** – These people are sometimes called Script Kiddies. They are usually attackers with little or no skill, often using existing tools or instructions found on the Internet to launch attacks. Some of them are just curious, while others are trying to demonstrate their skills and cause harm. They may be using basic tools, but the results can still be devastating.

**Hackers** – This group of attackers break into computers or networks to gain access. Depending on the intent of the break-in, these attackers are classified as white, gray, or black hats. The white hat attackers break into networks or computer systems to discover weaknesses so that the security of these systems can be improved. These break-ins are done with prior permission and any results are reported back to the owner. 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 in a system. Gray hat hackers may report the vulnerability 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 hackers 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 they may even provide cybercrime as a service to other criminals. Hacktivists make political statements to create awareness to issues that are important to them. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

Internal and External Threats

**Internal Security Threats**

Attacks can be originated 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 also have the potential to cause greater damage than external threats, because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data, as well as different levels of user or administrative privileges.

**External Security Threats**

External threats from amateurs or skilled attackers can exploit vulnerabilities in network or computing devices, or use social engineering to gain access.

Cyberspace has become another important dimension of warfare, where nations can carry out conflicts without the clashes of traditional troops and machines. This allows countries with minimal military presence to be as strong as other nations in cyberspace. Cyberwarfare is an Internet-based conflict that involves the penetration of computer systems and networks of other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause damage or disrupt services, such as shutting down a power grid.

An example of a state-sponsored attack involved the Stuxnet malware that was designed to damage Iran’s nuclear enrichment plant. Stuxnet malware did not hijack targeted computers to steal information. It was designed to damage physical equipment that was controlled by computers. It used modular coding that was programmed to perform a specific task within the malware. It used stolen digital certificates so the attack appeared legitimate to the system. Click Play to view a video about Stuxnet.

Click [here](https://contenthub.netacad.com/legacy/I2CS/2.1/en/course/files/1.4.1.1%20Video%20-%20Breaking%20Down%20Stuxnet.pdf) to read the transcript of this video.

Click [here](https://vimeo.com/25118844) to view another video to learn more about Stuxnet.

# The Purpose of Cyberwarfare

The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

A nation can continuously invade other nation’s infrastructure, steal defense secrets, and gather information about technology to narrow the gaps in its industries and military. Besides industrial and militaristic espionage, cyberwar can sabotage the infrastructure of other nations and cost lives in the targeted nations. For example, an attack can disrupt the power grid of a major city. Traffic would be disrupted. The exchange of goods and services is halted. Patients cannot get the care needed in emergency situations. Access to the Internet may also be disrupted. By affecting the power grid, the attack can affect the everyday life of ordinary citizens.

Furthermore, compromised sensitive data can give the attackers the ability to blackmail personnel within the government. The information may allow an attacker to pretend to be an authorized user to access sensitive information or equipment.

If the government cannot defend against the cyberattacks, the citizens may lose confidence in the government’s ability to protect them. Cyberwarfare can destabilize a nation, disrupt commerce, and affect the citizens’ faith in their government without ever physically invading the targeted nation.

# Chapter 1: The Need for Cybersecurity

This chapter explained the features and characteristics of cybersecurity. It explained why the demand for cybersecurity professionals will only continue to increase. The content explains why your personal online identity and data is vulnerable to cyber criminals. It gives some tips on how you can protect your personal online identity and data.

This chapter also discussed organizational data: what it is, where it is, and why it must be protected. It explained who the cyber attackers are and what they want. Cybersecurity professionals must have the same skills as the cyber attackers. Cybersecurity professionals must work within the bounds of the local, national and international law. Cybersecurity professionals must also use their skills ethically.

Finally, this chapter briefly explained cyberwarfare and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.

If you would like to further explore the concepts in this chapter, please check out the [Additional Resources and Activities](https://contenthub.netacad.com/legacy/I2CS/2.1/en/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) page in Student Resources.

# Chapter 4: Protecting the Organization

This chapter covers some of the technology and processes used by cybersecurity professionals when protecting an organization’s network, equipment and data. First, it briefly covers the many types of firewalls, security appliances, and software that are currently used, including best practices.

Next, this chapter explains botnets, the kill chain, behavior-based security, and using NetFlow to monitor a network.

The third section discusses Cisco’s approach to cybersecurity, including the CSIRT team and the security playbook. It briefly covers the tools that cybersecurity professionals use to detect and prevent network attacks.

A firewall is a wall or partition that is designed to prevent fire from spreading from one part of a building to another. In computer networking, a firewall is designed to control, or filter, which communications are allowed in and which are allowed out of a device or network, as shown in the figure. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall), or it can be a stand-alone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

Over the years, as computer and network attacks have become more sophisticated, new types of firewalls have been developed which serve different purposes in protecting a network. Here is a list of common firewall types:

* **Network Layer Firewall** – filtering based on source and destination IP addresses
* **Transport Layer Firewall** –filtering based on source and destination data ports, and filtering based on connection states
* **Application Layer Firewall** –filtering based on application, program or service
* **Context Aware Application Firewall** – filtering based on the user, device, role, application type, and threat profile
* **Proxy Server** – filtering of web content requests like URL, domain, media, etc.
* **Reverse Proxy Server** – placed in front of web servers, reverse proxy servers protect, hide, offload, and distribute access to web servers
* **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
* **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

Port-scanning is a process of probing a computer, server or other network host for open ports. In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port-scanning can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

For the purposes of evaluating your own computer network’s firewall and port security, you can use a port-scanning tool like Nmap to find all the open ports on your network. Port-scanning can be seen as a precursor to a network attack and therefore should not be done on public servers on the Internet, or on a company network without permission.

To execute an Nmap port-scan of a computer on your local home network, download and launch a program such as Zenmap, provide the target IP address of the computer you would like to scan, choose a default scanning profile, and press scan. The Nmap scan will report any services that are running (e.g., web services, mail services, etc.) and port numbers. The scanning of a port generally results in one of three responses:

* **Open or Accepted** – The host replied indicating a service is listening on the port.
* **Closed, Denied, or Not Listening** – The host replied indicating that connections will be denied to the port.
* **Filtered, Dropped, or Blocked** – There was no reply from the host.

To execute a port-scan of your network from outside of the network, you will need to initiate the scan from outside of the network. This will involve running an Nmap port-scan against your firewall or router’s public IP address. To discover your public IP address, use a search engine such as Google with the query “what is my ip address”. The search engine will return your public IP address.

To run a port-scan for six common ports against your home router or firewall, go to the Nmap Online Port Scanner at <https://hackertarget.com/nmap-online-port-scanner/> and enter your public IP address in the input box*: IP address to scan…* and press *Quick Nmap Scan*. If the response is *open* for any of the ports: 21, 22, 25, 80, 443, or 3389 then most likely, port forwarding has been enabled on your router or firewall, and you are running servers on your private network, as shown in the figure.

Today there is no single security appliance or piece of technology that will solve all network security needs. Because there is a variety of security appliances and tools that need to be implemented, it is important that they all work together. Security appliances are most effective when they are part of a system.

Security appliances can be stand-alone devices, like a router or firewall, a card that can be installed into a network device, or a module with its own processor and cached memory. Security appliances can also be software tools that are run on a network device. Security appliances fall into these general categories:

**Routers**- Cisco Integrated Services Router (ISR) routers, shown in Figure 1, have many firewall capabilities besides just routing functions, including traffic filtering, the ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities for secure encrypted tunneling.

**Firewalls**- Cisco Next Generation Firewalls have all the capabilities of an ISR router, as well as, advanced network management and analytics. Cisco Adaptive Security Appliance (ASA) with firewall capabilities are shown in Figure 2.

**IPS**- Cisco Next Generation IPS devices, shown in Figure 3, are dedicated to intrusion prevention.

**VPN**- Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client technologies. It is designed for secure encrypted tunneling.

**Malware/Antivirus**- Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.

**Other Security Devices**– This category includes web and email security appliances, decryption devices, client access control servers, and security management systems.

Software is not perfect. When a hacker exploits a flaw in a piece of software before the creator can fix it, it is known as a zero-day attack. Due to the sophistication and enormity of zero-day attacks found today, it is becoming common that network attacks will succeed and that a successful defense is now measured in how quickly a network can respond to an attack. The ability to detect attacks as they happen in real-time, as well as stopping the attacks immediately, or within minutes of occurring, is the ideal goal. Unfortunately, many companies and organizations today are unable to detect attacks until days or even months after they have occurred.

* **Real Time Scanning from Edge to Endpoint**- Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client/server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.
* **DDoS Attacks and Real Time Response**- DDoS is one of the biggest attack threats requiring real-time response and detection. DDoS attacks are extremely difficult to defend against because the attacks originate from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic, as shown in the figure. For many companies and organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. The ability to detect and respond to DDoS attacks in real-time is crucial.

# Protecting Against Malware

How do you provide defense against the constant presence of zero-day attacks, as well as advanced persistent threats (APT) that steal data over long periods of time? One solution is to use an enterprise-level advanced malware detection solution that offers real-time malware detection.

Network administrators must constantly monitor the network for signs of malware or behaviors that reveal the presence of an APT. Cisco has an Advanced Malware Protection (AMP) Threat Grid that analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts. This provides a global view of malware attacks, campaigns, and their distribution. AMP is client/server software deployed on host endpoints, as a standalone server, or on other network security devices. The figure shows the benefits of the AMP Threat Grid.

Security Best Practices

Many national and professional organizations have published lists of security best practices. The following is a list of some security best practices:

* **Perform Risk Assessment**– Knowing the value of what you are protecting will help in justifying security expenditures.
* **Create a Security Policy**– Create a policy that clearly outlines company rules, job duties, and expectations.
* **Physical Security Measures**– Restrict access to networking closets, server locations, as well as fire suppression.
* **Human Resource Security Measures**– Employees should be properly researched with background checks.
* **Perform and Test Backups**– Perform regular backups and test data recovery from backups.
* **Maintain Security Patches and Updates**– Regularly update server, client, and network device operating systems and programs.
* **Employ Access Controls**– Configure user roles and privilege levels as well as strong user authentication.
* **Regularly Test Incident Response**– Employ an incident response team and test emergency response scenarios.
* **Implement a Network Monitoring, Analytics and Management Tool**- Choose a security monitoring solution that integrates with other technologies.
* **Implement Network Security Devices**– Use next generation routers, firewalls, and other security appliances.
* **Implement a Comprehensive Endpoint Security Solution**– Use enterprise level antimalware and antivirus software.
* **Educate Users**– Educate users and employees in secure procedures.
* **Encrypt data**– Encrypt all sensitive company data including email.

Some of the most helpful guidelines are found in organizational repositories such as the National Institute of Standards and Technology (NIST) Computer Security Resource Center, as shown in the figure.

One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Go [here](https://www.sans.org/about/) to learn more about SANS and the types of training and certifications they offer.

# Botnet

A botnet is a group of bots, connected through the Internet, with the ability to be controlled by a malicious individual or group. A bot computer is typically infected by visiting a website, opening an email attachment, or opening an infected media file.

A botnet can have tens of thousands, or even hundreds of thousands of bots. These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute force password attacks. Botnets are typically controlled through a command and control server.

Cyber criminals will often rent out Botnets, for a fee, to third parties for nefarious purposes.

The figure shows how a botnet traffic filter is used to inform the worldwide security community of botnet locations.

# The Kill Chain in Cyberdefense

In cybersecurity, the Kill Chain is the stages of an information systems attack. Developed by Lockheed Martin as a security framework for incident detection and response, the Cyber Kill Chain is comprised of the following stages:

**Stage 1. Reconnaissance**- The attacker gathers information about the target.

**Stage 2. Weaponization** - The attacker creates an exploit and malicious payload to send to the target.

**Stage 3. Delivery** - The attacker sends the exploit and malicious payload to the target by email or other method.

**Stage 4. Exploitation** - The exploit is executed.

**Stage 5 Installation** - Malware and backdoors are installed on the target.

**Stage 6. Command and Control** - Remote control of the target is gained through a command and control channel or server.

**Stage 7. Action** - The attacker performs malicious actions like information theft, or executes additional attacks on other devices from within the network by working through the Kill Chain stages again.

To defend against the Kill Chain, network security defenses are designed around the stages of the Kill Chain. These are some questions about a company’s security defenses, based on the Cyber Kill Chain:

• What are the attack indicators at each stage of the Kill Chain?

• Which security tools are needed to detect the attack indicators at each of the stages?

• Are there gaps in the company’s ability to detect an attack?

According to Lockheed Martin, understanding the stages of Kill Chain allowed them to put up defensive obstacles, slow down the attack, and ultimately prevent the loss of data. The figure shows how each stage of the Kill Chain equates to an increase in the amount of effort and cost to inhibit and remediate attacks.

Behavior-Based Security

Behavior-based security is a form of threat detection that does not rely on known malicious signatures, but instead uses informational context to detect anomalies in the network. Behavior-based detection involves capturing and analyzing the flow of communication between a user on the local network and a local, or remote destination. These communications, when captured and analyzed, reveal context and patterns of behavior which can be used to detect anomalies. Behavior-based detection can discover the presence of an attack by a change from normal behavior.

* **Honeypots** - A Honeypot is a behavior-based detection tool that first lures the attacker in by appealing to the attacker’s predicted pattern of malicious behavior, and then, when inside the honeypot, the network administrator can capture, log, and analyze the attacker’s behavior. This allows an administrator to gain more knowledge and build a better defense.
* **Cisco’s Cyber Threat Defense Solution Architecture** - This is a security architecture that uses behavior-based detection and indicators, to provide greater visibility, context, and control. The goal is to know who, what, where, when, and how an attack is taking place. This security architecture uses many security technologies to achieve this goal.

# NetFlow

NetFlow technology is used to gather information about data flowing through a network. NetFlow information can be likened to a phone bill for your network traffic. It shows you who and what devices are in your network, as well as when and how users and devices accessed your network. NetFlow is an important component in behavior-based detection and analysis. Switches, routers, and firewalls equipped with NetFlow can report information about data entering, leaving, and travelling through the network. Information is sent to NetFlow Collectors that collect, store, and analyze NetFlow records.

NetFlow is able to collect information on usage through many different characteristics of how data is moved through the network, as shown in the figure. By collecting information about network data flows, NetFlow is able to establish baseline behaviors on more than 90 different attributes.

# CSIRT

Many large organizations have a Computer Security Incident Response Team (CSIRT) to receive, review, and respond to computer security incident reports, as shown in Figure 1. The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents. To prevent security incidents, Cisco CSIRT provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review, as shown in Figure 2.

Cisco’s CSIRT collaborates with Forum of Incident Response and Security Teams (FIRST), the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE), and the DNS Operations Analysis and Research Center (DNS-OARC).

There are national and public CSIRT organizations like the CERT Division of the Software Engineering Institute at Carnegie Mellon University, that are available to help organizations, and national CSIRTs, develop, operate, and improve their incident management capabilities.

Security Playbook

Technology is constantly changing. That means cyberattacks are evolving too. New vulnerabilities and attack methods are discovered continuously. Security is becoming a significant business concern because of the resulting reputation and financial impact from security breaches. Attacks are targeting critical networks and sensitive data. Organizations should have plans to prepare for, deal with, and recover from a breach.

One of the best way to prepare for a security breach is to prevent one. There should be guidance on identifying the cybersecurity risk to systems, assets, data, and capabilities, protecting the system by the implementation of safeguards and personnel training, and detecting cybersecurity event as soon as possible. When a security breach is detected, appropriate actions should be taken to minimize its impact and damage. The response plan should be flexible with multiple action options during the breach. After the breach is contained and the compromised systems and services are restored, security measures and processes should be updated to include the lessons learned during the breach.

All this information should be compiled into a security playbook. A security playbook is a collection of repeatable queries (reports) against security event data sources that lead to incident detection and response. Ideally the security playbook must accomplish the following actions:

* Detect malware infected machines.
* Detect suspicious network activity.
* Detect irregular authentication attempts.
* Describe and understand inbound and outbound traffic.
* Provide summary information including trends, statistics, and counts.
* Provide usable and quick access to statistics and metrics.
* Correlate events across all relevant data sources.

Tools for Incident Prevention and Detection

These are some of the tools used to detect and prevent security incidents:

* **SIEM**– A Security Information and Event Management (SIEM) system is software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network.
* **DLP**– Data Loss Prevention Software (DLP) is a software or hardware system designed to stop sensitive data from being stolen from or escaping a network. A DLP system may focus on file access authorization, data exchange, data copying, user activity monitoring, and more. DLP systems are designed to monitor and protect data in three different states: data in-use, data in-motion and data at-rest. Data in-use is focused on the client, data in-motion refers to data as it travels through the network, and data at-rest refers to data storage.
* **Cisco ISE and TrustSec** – Cisco Identity Services Engine (Cisco ISE) and Cisco TrustSec enforce access to network resources by creating role-based access control policies that segment access to the network (guests, mobile users, employees) without added complexity. Traffic classification is based on user or device identity. Click play in the figure to learn more about ISE.
* Click [here](https://contenthub.netacad.com/legacy/I2CS/2.1/en/course/files/4.3.3.1%20Video%20-%20Fundamentals%20of%20ISE.pdf) to read the transcript of this video.

# IDS and IPS

An Intrusion Detection System (IDS), shown in the figure, is either a dedicated network device, or one of several tools in a server or firewall that scans data against a database of rules or attack signatures, looking for malicious traffic. If a match is detected, the IDS will log the detection, and create an alert for a network administrator. The Intrusion Detection System does not take action when a match is detected so it does not prevent attacks from happening. The job of the IDS is merely to detect, log and report.

The scanning performed by the IDS slows down the network (known as latency). To prevent against network delay, an IDS is usually placed offline, separate from regular network traffic. Data is copied or mirrored by a switch and then forwarded to the IDS for offline detection. There are also IDS tools that can be installed on top of a host computer operating system, like Linux or Windows.

An Intrusion Prevention System (IPS) has the ability to block or deny traffic based on a positive rule or signature match. One of the most well-known IPS/IDS systems is Snort. The commercial version of Snort is Cisco’s Sourcefire. Sourcefire has the ability to perform real-time traffic and port analysis, logging, content searching and matching, and can detect probes, attacks, and port scans. It also integrates with other third party tools for reporting, performance and log analysis.

# Chapter 4: Protecting the Organization

This chapter began by discussing some of the technology and processes used by cybersecurity professionals when protecting an organization’s network, equipment and data. This included types of firewalls, security appliances, and software.

Botnets, the kill chain, behavior-based security, and using NetFlow to monitor a network were covered.

Finally, Cisco’s approach to cybersecurity, including the CSIRT team and the security playbook were explained. It briefly covers the tools that cybersecurity professionals use to detect and prevent network attacks, including SIEM, DLP, Cisco ISE and TrustSec, as well as IDS and IPS systems.

If you would like to further explore the concepts in this chapter, please check out the [Additional Resources and Activities](https://contenthub.netacad.com/legacy/I2CS/2.1/en/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) page in Student Resources.

# Chapter 5: Will Your Future Be in Cybersecurity

This chapter covers the legal and ethical issues that arise when working in cybersecurity. It also discusses educational and career paths for cybersecurity. There are educational paths towards certifications that you may wish to pursue with the Cisco Networking Academy. Some of these certifications are prerequisites to Specialization Certificates in many areas of networking, including cybersecurity.

The Networking Academy Talent Bridge page (netacad.com under Resources) provides good information to help you write a great résumé and prepare for a job interview. It also contains listings for Cisco and Cisco Partner jobs. Three external Internet job search engines are presented for you to explore.

# Legal Issues in Cybersecurity

Cybersecurity professionals must have the same skills as hackers, especially black hat hackers, in order to protect against attacks. One difference between a hacker and a cybersecurity professional is that the cybersecurity professional must work within legal boundaries.

**Personal Legal Issues**

You do not even have to be an employee to be subject to cybersecurity laws. In your private life, you may have the opportunity and skills to hack another person’s computer or network. There is an old saying, “Just because you can does not mean you should.” Keep this in mind. Most hackers leave tracks, whether they know it or not, and these tracks can be followed back to the hacker.

Cybersecurity professionals develop many skills which can be used for good or evil. Those who use their skills within the legal system, to protect infrastructure, networks, and privacy are always in high demand.

**Corporate Legal Issues**

Most countries have some cybersecurity laws in place. They may have to do with critical infrastructure, networks, and corporate and individual privacy. Businesses are required to abide by these laws.

In some cases, if you break cybersecurity laws while doing your job, it is the company that may be punished and you could lose your job. In other cases, you could be prosecuted, fined, and possibly sentenced.

In general, if you are confused about whether an action or behavior might be illegal, assume that it is illegal and do not do it. Your company may have a legal department or someone in the human resources department who can answer your questions before you do something illegal.

**International Law and Cybersecurity**

The area of cybersecurity law is much newer than cybersecurity itself. As mentioned before, most countries have some laws in place, and there will be more laws to come.

Ethical Issues in Cybersecurity

In addition to working within the confines of the law, cybersecurity professionals must also demonstrate ethical behavior.

**Personal Ethical Issues**

A person may act unethically and not be subject to prosecution, fines or imprisonment. This is because the action may not have been technically illegal. But that does not mean that the behavior is acceptable. Ethical behavior is fairly easy to ascertain. It is impossible to list all of the various unethical behaviors that can be exhibited by someone with cybersecurity skills. Below are just two. Ask yourself:

* Would I want to discover that someone has hacked into my computer and altered images in my social network sites?
* Would I want to discover that an IT technician whom I trusted to fix my network, told colleagues personal information about me that was gained while working on my network?

If your answer to any of these questions was ‘no’, then do not do such things to others.

**Corporate Ethical Issues**

Ethics are codes of behavior that are sometimes enforced by laws. There are many areas in cybersecurity that are not covered by laws. This means that doing something that is technically legal still may not be the ethical thing to do. Because so many areas of cybersecurity are not (or not yet) covered by laws, many IT professional organizations have created codes of ethics for persons in the industry. Below is a list of three organizations with Codes of Ethics:

* The CyberSecurity Institute (CSI)
* The Information Systems Security Association (ISSA)
* The Association of Information Technology Professionals (AITP)

Cisco has a team devoted exclusively to ethical business conduct. Go [here](http://csr.cisco.com/pages/governance-and-ethics) to read more about it. This [site](http://investor.cisco.com/investor-relations/governance/code-of-conduct/default.aspx) contains an eBook about Cisco’s Code of Business Conduct, and a pdf file. In both files is an “Ethics Decision Tree”, as shown in the figure. Even if you do not work for Cisco, the questions and answers found in this decision tree can easily be applied to your place of work. As with legal questions, in general, if you are confused about whether an action or behavior might be unethical, assume that it is unethical and do not do it. There may be someone in your company’s human resources or legal department who can clarify your situation before you do something that would be considered unethical.

Search online to find other IT-related organizations with codes of ethics. Try to find what they all have in common.

Cybersecurity Jobs

Many other businesses and industries are hiring cybersecurity professionals. There are several online search engines to help you find the right job in cybersecurity:

* [ITJobMatch](https://itjobmatch.com/) – The ITJobMatch search engine specializes in IT jobs of every kind, all over the globe.
* [Monster](http://jobs.monster.com/search/?q=cybersecurity) – Monster is a search engine for all types of jobs. The link provided goes directly to cybersecurity jobs.
* [CareerBuilder](http://www.careerbuilder.com/jobs/keyword/cyber-security) – CareerBuilder is also a search engine for all types of jobs. The link provided goes directly to cybersecurity jobs.

These are just three of many different online job search sites. Even if you are just starting your education in IT and cybersecurity, looking at job search engines is a good way to see what kinds of jobs are available, all over the world.

Depending on your interest in cybersecurity, different types of jobs can be available to you, and they can require specialized skills certifications. For example, a penetration tester, also known as an ethical hacker, searches and exploits security vulnerabilities in applications, networks and systems. To become a penetration tester, you will need to gain experience in other IT jobs, such as security administrator, network administrator, and system administrator. Each one of these jobs requires its own set of skills that will help you become a valuable asset to an organization.

Our hope is that this course has peaked your interest in pursuing an education in IT and cybersecurity and then continuing on to an exciting career! The Cisco Networking Academy provides many courses for you to continue your education in Cybersecurity. We encourage you to enroll in the next course, Cybersecurity Essentials, to continue to build strong foundational knowledge in Cybersecurity. Check out the Cisco Networking Academy and see a list of [courses](https://www.netacad.com/courses/) that are available. Furthermore, you can also access [career resources](http://www.netacad.com/careers) available in Cisco Networking Academy.

Just for fun, click [here](http://newsroom.cisco.com/supersmartsecurity) to read a graphic novel about a cybersecurity superhero!

# Chapter 5: Will Your Future Be in Cybersecurity?

This chapter began by discussing the legal and ethical issues that professionals in cybersecurity commonly face. It also presented educational and career paths for those who wish to become cybersecurity professionals. Three external Internet job search engines are presented for you to explore.

If you would like to further explore the concepts in this chapter, please check out the [Additional Resources and Activities](https://contenthub.netacad.com/legacy/I2CS/2.1/en/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) page in Student Resources.