DIGITAL NOTES
ON
CYBER SECURITY
(R18A0521)

B.TECH III YEAR – II SEM (R18)

(2020-2021)

DEPARTMENT OF INFORMATION TECHNOLOGY

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

(Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post Via. Hakimpet), Secunderabad – 500100, Telangana State, India

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

III Year B.Tech II Sem

L	T/P/D	C
3	-/-/-	3

(RA18A0521) CYBER SECURITY

(Professional Elective 2)

Course objectives:

- To understand various types of cyber-attacks and cyber-crimes
- To learn threats and risks within context of the cyber security
- To have an overview of the cyber laws & concepts of cyber forensics
- To study the defensive techniques against these attacks

UNIT -I

Introduction to Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT - II

Cyberspace and the Law & Cyber Forensics: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy.

Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics

UNIT - III

Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops.

UNIT- IV

Cyber Security: Organizational Implications: Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.

UNIT - V

Privacy Issues: Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Datalinking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc

Cybercrime: Examples and Mini-Cases

Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. **Mini-Cases:** The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.

TEXT BOOKS:

1. Nina Godbole and SunitBelpure, Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Perspectives,Wiley

2. B.B.Gupta,D.P.Agrawal,HaoxiangWang,ComputerandCyberSecurity:Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018.

REFERENCES:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress.

2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&FGroup.

Course Outcomes:

The students will be able to:

1. Analyze cyber-attacks, types of cybercrimes, cyber laws and also how to protect them self and ultimately the entire Internet community from such attacks.
2. Interpret and forensically investigate security incidents
3. Apply policies and procedures to manage Privacy issues
4. Design and develop secure software modules

UNIT-I

Introduction to Cyber Security

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?
Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

  Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.

  But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals – Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:

1) **Web-based attacks**
2) **System-based attacks**

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

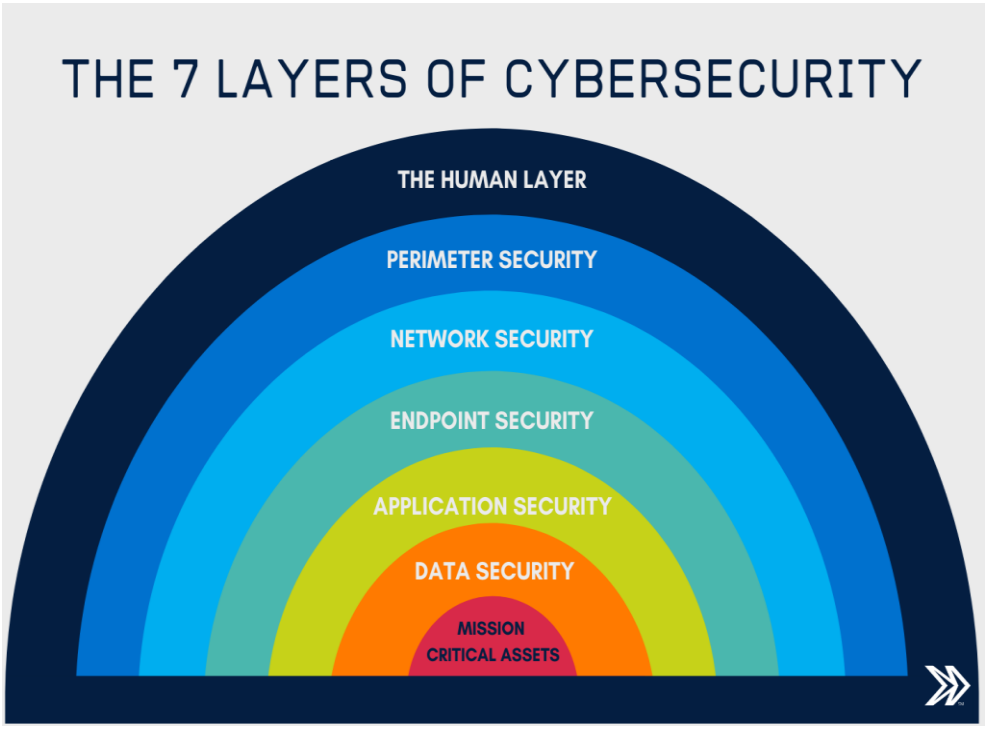
It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.



The 7 layers of cyber security should centre on the mission critical assets you are seeking to protect.

1: Mission Critical Assets – This is the data you need to protect
2: Data Security – Data security controls protect the storage and transfer of data.
3: Application Security – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.
5: Network Security – Network security controls protect an organization's network and prevent unauthorized access of the network.
6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Vulnerability, threat, Harmful acts

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible.
Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.
Examples of common types of security threats include **phishing attacks** that result in the installation of **malware** that infects your data, failure of a staff member to follow data protection protocols that cause a **data breach**, or even a tornado that takes down your company's data headquarters, disrupting access.

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a non-encrypted plain text format.
When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

SECURITY VULNERABILITIES, THREATS AND ATTACKS –

Categories of vulnerabilities

- Corrupted (Loss of integrity)
- Leaky (Loss of confidentiality)
- Unavailable or very slow (Loss of availability)

– Threats represent potential security harm to an asset when vulnerabilities are exploited

- Attacks are threats that have been carried out

- Passive – Make use of information from the system without affecting system resources
- Active – Alter system resources or affect operation
- Insider – Initiated by an entity inside the organization
- Outsider – Initiated from outside the perimeter

Computer criminals

Computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, the purpose of computer security is to prevent these criminals from doing damage.

We say **computer crime** is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously.

One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring.

CIA Triad

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

CIA triad broken down:

Confidentiality

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

Integrity

Data integrity is what the "I" in CIA Triad stands for.

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability

This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Understanding the CIA triad

The CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors.

For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

Assets and Threat

What is an Asset: An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.

For example: An employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets. An organization's most common assets are information assets. These are things such as databases and physical files – i.e. the sensitive data that you store

What is a threat:_A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party.

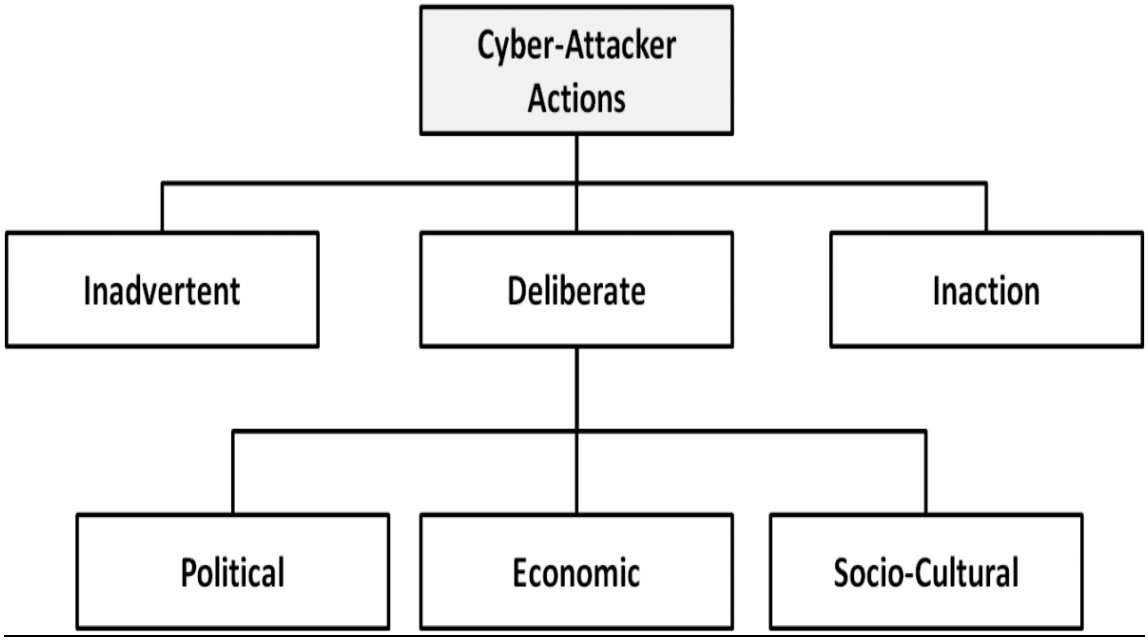
Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

Motive of Attackers

The categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure, operational cyber security risks arise from three types of actions: i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent; ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern here are deliberate actions, of which there are three categories of motivation.

1. ***Political motivations****:* examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.
2. ***Economic motivations****:* examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.
3. ***Socio-cultural motivations****:* examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.



Types of cyber-attacker actions and their motivations when deliberate

Active attacks: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

Types of Active attacks:

Masquerade: in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

Session replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

Message modification: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

In a **denial of service (DoS)** attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

Passive Attacks:*Passive attacks* are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

Types of Passive attacks:

Eavesdropping (tapping): the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

***Traffic analysis*:** the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

Software Attacks: Malicious code (sometimes called *malware*) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging. Common malware examples are listed in the following table:

Attack	Characteristics
Virus	A *virus* is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus: • Requires a host to replicate and usually attaches itself to a host file or a hard drive sector. • Replicates each time the host is used. • Often focuses on destruction or corruption of data. • Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions. • Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book. • Examples: Stoned, Michelangelo, Melissa, I Love You.
Worm	A *worm* is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process of replicating itself. A worm: • Can install a backdoor in the infected computer. • Is usually introduced into the system through a vulnerability. • Infects one system and spreads to other systems on the network. • Example: Code Red.
Trojan horse	A *Trojan horse* is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment. A Trojan horse: • Cannot replicate itself. • Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network. • Often is hidden in useful software such as screen savers or games. • Example: Back Orifice, Net Bus, Whack-a-Mole.
Logic Bomb	A *Logic Bomb* is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack. • A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity. • Logic bombs do not self-replicate.

Hardware Attacks:

Common hardware attacks include:

- Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
- Eavesdropping by gaining access to protected memory without opening other hardware
- Inducing faults, causing the interruption of normal behaviour
- Hardware modification tampering with invasive operations
- Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems
- Counterfeiting product assets that can produce extraordinary operations and those made to gain malicious access to systems.

Cyber Threats-Cyber Warfare: Cyber warfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles.

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyber Crime:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Cyber Terrorism:

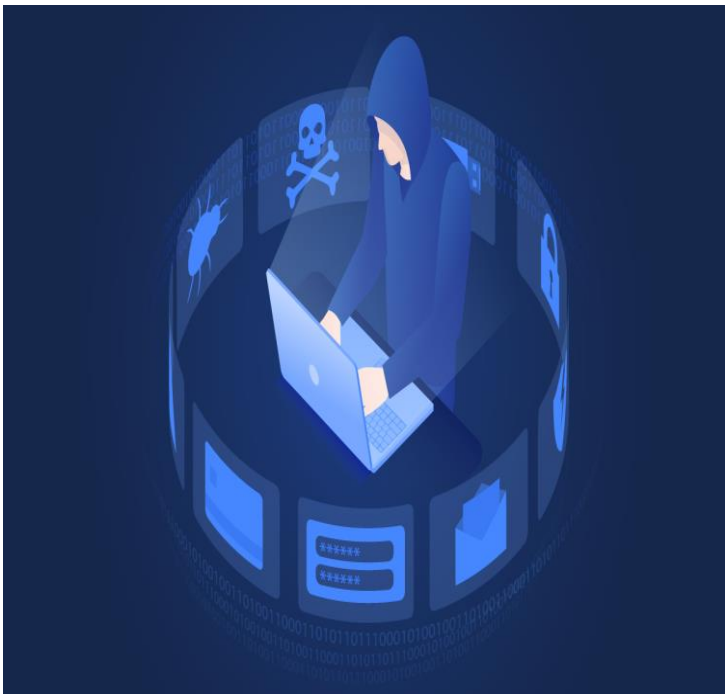
Cyber terrorism is the convergence of cyberspace and **terrorism**. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.

Cyber Espionage:

Cyber spying, or **cyber espionage**, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from

individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet.



Security Policies:

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment.

Need of Security policies-

1) It increases efficiency.

2) It upholds discipline and accountability

3) It can make or break a business deal

4) It helps to educate employees on security literacy

There are some important cyber security policies recommendations describe below-

Virus and Spyware Protection policy:

- It helps to detect threads in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

Firewall Policy:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Application and Device Control:

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

Unit II
CYBERSPACE AND THE LAW & CYBER FORENSICS

CYBERSPACE

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

REGULATIONS

There are five predominant laws to cover when it comes to cybersecurity:

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000.

The primary relevant section of the IPC covers cyber frauds:

Forgery (Section 464)

Forgery pre-planned for cheating (Section 468)

False documentation (Section 465)

Presenting a forged document as genuine (Section 471)

Reputation damage (Section 469)

Companies Act of 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cybersecurity obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body.

NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activities and critical operations - to focus on securing them Demonstrates the trust-worthiness of organizations who secure critical assets Helps to prioritize investments to maximize the cybersecurity ROI Addresses regulatory and contractual obligations Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier

throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

ROLE OF INTERNATIONAL LAWS

In various countries, areas of the computing and communication industries are regulated by governmental bodies λ There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming λ There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes λ There are laws governing trade on the Internet, taxation, consumer protection, and advertising λ There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies λ Some states limit access to the Internet, by law as well as by technical means.

INTERNATIONAL LAW FOR CYBER CRIME

Cybercrime is "international" that there are ‘no cyber-borders between countries’ λ The complexity in types and forms of cybercrime increases the difficulty to fight back \ fighting cybercrime calls for international cooperation λ Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale

THE INDIAN CYBERSPACE

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India’s computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet

access through mobile phones and tablets. Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

NATIONAL CYBER SECURITY POLICY

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

VISION

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

OBJECTIVE

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

INTRODUCTION: CYBER FORENSICS

CYBER FORENSICS:

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence.

Forensic examiners typically analyze data from personal computers, laptops, personal digital assistants, cell phones, servers, tapes, and any other type of media. This process can involve anything from breaking encryption, to executing search warrants with a law enforcement team, to recovering and analyzing files from hard drives that will be critical evidence in the most serious civil and criminal cases.

The forensic examination of computers, and data storage media, is a complicated and highly specialized process. The results of forensic examinations are compiled and included in reports. In many cases, examiners testify to their findings, where their skills and abilities are put to ultimate scrutiny.

DIGITAL FORENSICS:

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

THE NEED FOR COMPUTER FORENSICS

Computer forensics is also important because it can save your organization money. ... From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

CYBER FORENSICS AND DIGITAL EVIDENCE:

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims.

In an effort to fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

FORENSICS ANALYSIS OF EMAIL:

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Various approaches that are used for e-mail forensic are:

- **Header Analysis** – Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis.

- **Bait Tactics** – In bait tactic investigation an e-mail with http: "<imgsrc>" tag having image source at some computer monitored by the investigators is send to the sender of e-mail under investigation containing real (genuine) e-mail address. When the e-mail is opened, a log entry containing the IP address of the recipient (sender of the e-mail under investigation) is recorded on the http server hosting the image and thus sender is tracked. However, if the recipient (sender of the e-mail under investigation) is using a proxy server then IP address of the proxy server is recorded. The log on proxy server can be used to track the sender of the e-mail under investigation. If the proxy server's log is unavailable due to some reason, then investigators may send the tactic e-mail containing a) Embedded Java Applet that runs on receiver's computer or b) HTML page with Active X Object. Both aiming to extract IP address of the receiver's computer and e-mail it to the investigators.

- **Server Investigation** – In this investigation, copies of delivered e-mails and server logs are investigated to identify source of an e-mail message. E-mails purged from the clients (senders or receivers) whose recovery is impossible may be requested from servers (Proxy or ISP) as most of them store a copy of all e-mails after their deliveries. Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction. However, servers store the copies of e-mail and server logs only for some limited periods and some may not co-operate with the investigators. Further, SMTP servers which store data like credit card number and other data pertaining to owner of a mailbox can be used to identify person behind an e-mail address.

- **Network Device Investigation** – In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate

the source of an e-mail message. This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of co-operation by ISP's or failure to maintain chain of evidence.

- **Software Embedded Identifiers** – Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF). Investigating the e-mail for these details may reveal some vital information about the senders e-mail preferences and options that could help client side evidence gathering. The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message.

- **Sender Mailer Fingerprints** – Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent. These headers describe applications and their versions used at the clients to send e-mail. This information about the client computer of the sender can be used to help investigators devise an effective plan and thus prove to be very useful.

EMAIL FORENSICS TOOLS

Erasing or deleting an email doesn't necessarily mean that it is gone forever. Often emails can be forensically extracted even after deletion. Forensic tracing of e-mail is similar to traditional detective work. It is used for retrieving information from mailbox files.

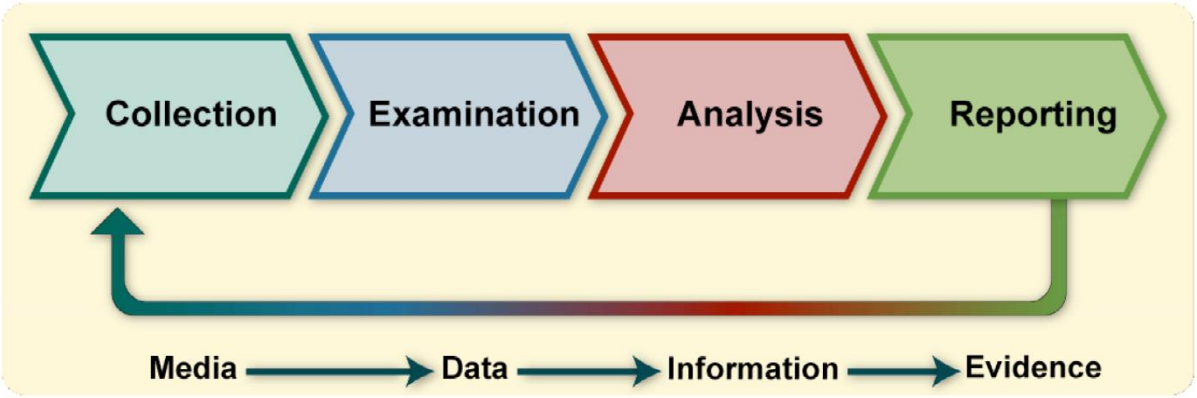
- **MiTec Mail Viewer** – This is a viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases, and single EML files. It displays a list of contained messages with all needed properties, like an ordinary e-mail client. Messages can be viewed in detailed view, including attachments and an HTML preview. It has powerful searching and filtering capability and also allows extracting email addresses from all emails in opened folder to list by one click. Selected messages can be saved to eml files with or without their attachments. Attachments can be extracted from selected messages by one command.

- **OST and PST Viewer** – Nucleus Technologies' OST and PST viewer tools help you view OST and PST files easily without connecting to an MS Exchange server. These tools allow the user to scan OST and PST files and they display the data saved in it including email messages, contacts, calendars, notes, etc., in a proper folder structure.

- **eMailTrackerPro** – eMailTrackerPro analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down. It can trace multiple e-mails at the same time and easily keep track of them. The geographical location of an IP address is key information for determining the threat level or validity of an e-mail message.

- **EmailTracer** – EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies.

DIGITAL FORENSICS LIFECYCLE:



Collection: The first step in the forensic process is to identify potential sources of data and acquire data from them.

Examination: After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.

Analysis: Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

Reporting: The process of preparing and presenting the information resulting from the analysis phase. Many factors affect reporting, including the following:

a. **Alternative Explanations:**When the information regarding an event is incomplete, it may not be possible to arrive at a definitive explanation of what happened. When an event has two or more plausible explanations, each should be given due consideration in the reporting process. Analysts should use a methodical approach to attempt to prove or disprove each possible explanation that is proposed.

b. **Audience Consideration.** Knowing the audience to which the data or information will be shown is important.

c. **Actionable Information.** Reporting also includes identifying actionable information gained from data that may allow an analyst to collect new sources of information

FORENSICS INVESTIGATION:

Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place. This is a general definition, though, since there are a number of different types of forensics.

TYPES OF FORENSICS INVESTIGATION

- Forensic Accounting / Auditing
- Computer or Cyber Forensics
- Crime Scene Forensics
- Forensic Archaeology
- Forensic Dentistry
- Forensic Entomology
- Forensic Graphology
- Forensic Pathology
- Forensic Psychology
- Forensic Science
- Forensic Toxicology

CHALLENGES IN COMPUTER FORENSICS

Digital forensics has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal.But these digital forensics investigation methods face some major challenges at the time of practical implementation. Digital forensic challenges are categorized into three major heads as per Fahdi, Clark, and Furnell are:

- Technical challenges
- Legal challenges
- Resource Challenges

TECHNICAL CHALLENGES

As technology develops crimes and criminals are also developed with it. Digital forensic experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, altering or removing the traces of their crime, in digital forensic this process is called Anti- forensics technique which is considered as a major challenge in digital forensics world.

Anti-forensics techniquesare categorized into the following types:

S. No.	Type	Description
1	Encryption	It is legitimately used for ensuring the privacy of

		information by keeping it hidden from an unauthorized user/person. Unfortunately, it can also be used by criminals to hide their crimes
2	Data hiding in storage space	Criminals usually hide chunks of data inside the storage medium in invisible form by using system commands, and programs.
3	Covert Channel	A covert channel is a communication protocol which allows an attacker to bypass intrusion detection technique and hide data over the network. The attacker used it for hiding the connection between him and the compromised system.

Other Technical challenges are:

- Operating in the cloud
- Time to archive data
- Skill gap
- Steganography

LEGAL CHALLENGES

The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework acquires a soft approach and does not recognize every aspect of cyber forensics, as in *Jagdeo Singh V. The State and Ors* case Hon'ble High Court of Delhi held that *"while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Sec. 65B of the Indian Evidence Act, 1872 the court observed that the secondary electronic evidence without certificate u/s. 65B of Indian Evidence Act, 1872 is not admissible and cannot be looked into by the court for any purpose whatsoever."* This happens in most of the cases as the cyber police lack the necessary qualification and ability to identify a possible source of evidence and prove it. Besides, most of the time electronic evidence is challenged in the court due to its integrity. In the absence of proper guidelines and the nonexistence of proper explanation of the collection, and acquisition of electronic evidence gets dismissed in itself.

Legal Challenges

S.No.	Type	Description
1	Absence of guidelines and standards	In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed.
2	Limitation of the Indian Evidence Act, 1872	The Indian Evidence Act, 1872 have limited approach, it is not able to evolve with the time and address the E-evidence are more susceptible to tampering, alteration, transposition, etc. the Act is silent on the method of collection of e-evidence it only focuses on the presentation of electronic evidence in the court by accompanying a certificate as per subsection 4 of Sec. 65B[12]. This means no

		matter what procedure is followed it must be proved with the help of a certificate.

Other Legal Challenges

- Privacy Issues
- Admissibility in Courts
- Preservation of electronic evidence
- Power for gathering digital evidence
- Analyzing a running computer

Resource Challenges

As the rate of crime increases the number of data increases and the burden to analyze such huge data is also increasing on a digital forensic expert because digital evidence is more sensitive as compared to physical evidence it can easily disappear. For making the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge in itself.

Types of Resource Challenges are:

- Change in technology

Due to rapid change in technology like operating systems, application software and hardware, reading of digital evidence becoming more difficult because new version software's are not supported to an older version and the software developing companies did provide any backward compatible's which also affects legally.

- Volume and replication

The confidentiality, availability, and integrity of electronic documents are easily get manipulated. The combination of wide-area networks and the internet form a big network that allows flowing data beyond the physical boundaries. Such easiness of communication and availability of electronic document increases the volume of data which also create difficulty in the identification of original and relevant data.

Unit 3

CYBERCRIMES: MOBILE AND WIRELESS

INTRODUCTION. Why should *mobile devices* be protected? Every day, *mobile devices* are lost, stolen, and infected. *Mobile devices* can store important business and personal *information*, and are often be used to access University systems, email, banking

Proliferation of mobile and wireless devices:

- people hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.

They might even access corporate networks and pull up a document or two on their mobile gadgets

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

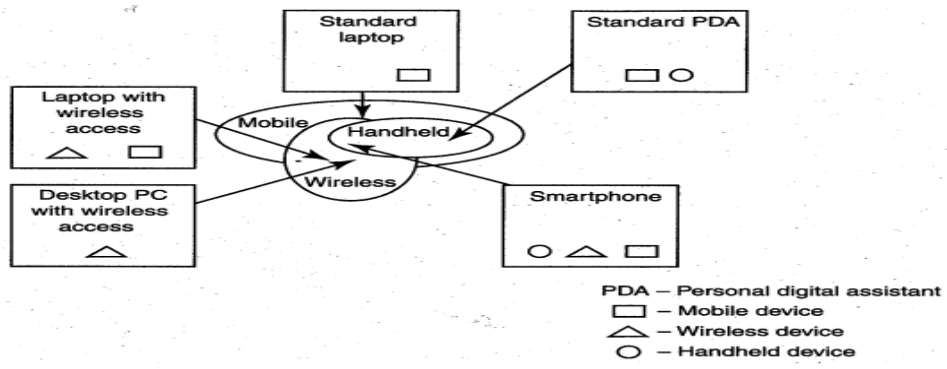


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. Portable computer: It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.

2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. Ultramobile (PC): It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. Smartphone: It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

8. Fly Fusion Pentop computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure below shows the different types of mobility and their implications.

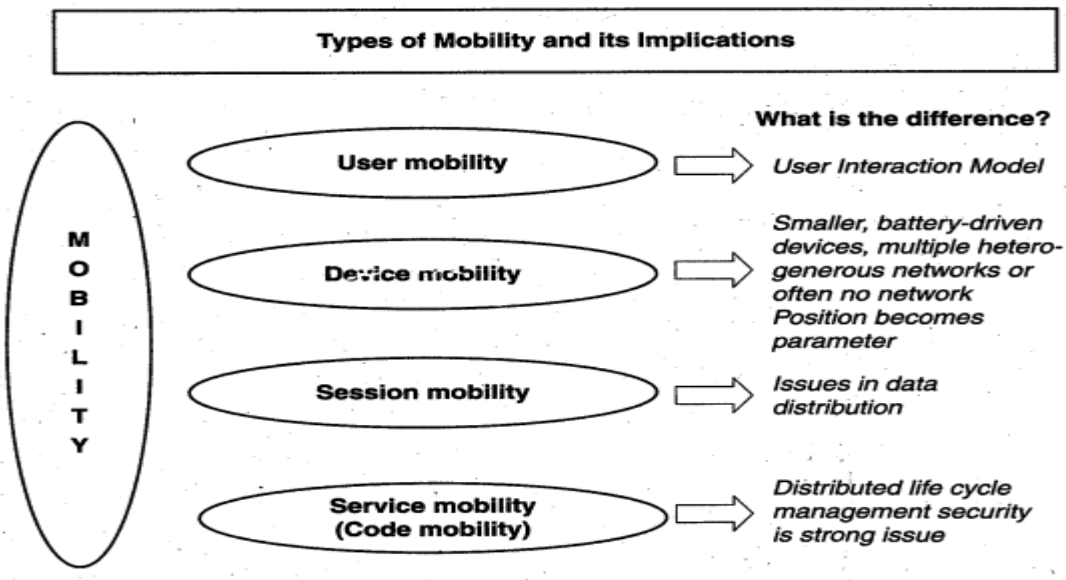


Figure: Mobility types and implications

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks-that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types of attacks against 3G mobile networks are as follows:

1. Malwares, viruses and worms: Although many users are still in the transient process of switching from 2G,2.5G2G,2.5G to 3G,3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- ***Skull Trojan:*** I targets Series 60 phones equipped with the Symbian mobile OS.
- ***Cabir Worm:*** It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- ***Mosquito Trojan:*** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- ***Brador Trojan:*** It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.
- ***Lasco Worm:*** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. Denial-of-service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired Internet service providers (iSPs) is a distributed denial-of-service (DDos) attack .DDoS

attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3. Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. Spoofed policy development process (PDP): These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

5. Signaling-level attacks: The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VolP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Today belongs to "mobile compüting," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment

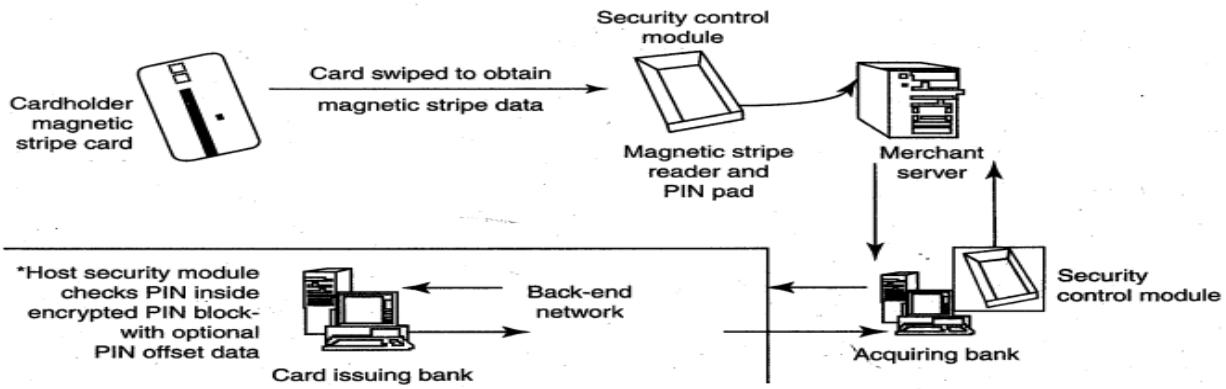


Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)

4. The bank/merchant is notified
5. The credit card transaction is completed.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure.

As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro-challenges."

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), security etc.

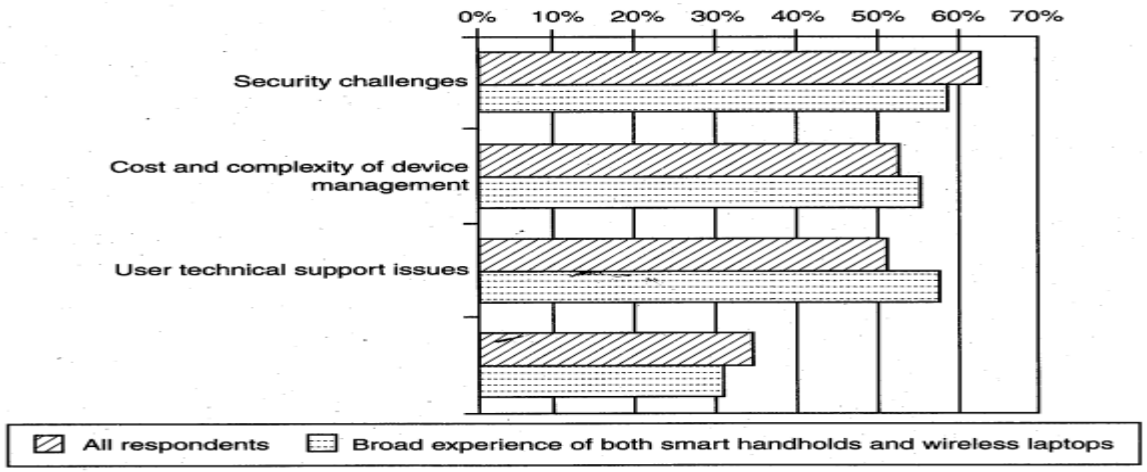


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft Activesync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.

In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be

connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.
Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.
Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

- **Mobile Phone Theft:**

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.
The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- **Mobile - Viruses**
- **Concept of Mishing**
- **Concept of Vishing**
- **Concept of Smishing**
- **Hacking - Bluetooth**

Organizational security Policies and Measures in Mobile Computing Era:
Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their-hand-held devices.One should think about not to keep credit card and bank

account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized
7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one.In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time the the they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20%% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs .

Concept of Laptops:

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop. thieves. are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive..

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.

5. Other measures for protecting laptops are as follows:

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible

- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop
- Making a copy of the purchase receipt, laptop serial number and the description of the laptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly
- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/ access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handing of removable drives/storage mediums /unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls / intrusion detection system (IDSs).
10. Encrypting critical file systems.

Introduction to Cybersecurity

The introductory course for those who want to explore the world of cybersecurity.

Table of Contents

Welcome

When you were a child, did you ever imagine yourself as a Masterful Defender of the Universe — recognizing a threat, protecting the innocent, seeking out the evildoers, and bringing them to justice?

Did you know you can make a career out of that?

- Cybersecurity Guru
- 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.

The Student Support page includes a link to the NetAcad Facebook page and our LinkedIn page. It also contains Additional Resources and Activities for each chapter.

Course Overview

As the course title states, the focus of this course is to explore the field of cybersecurity. In this course, you will do the following:

- Learn the basics of being safe online.
- Learn about different types of malware and attacks, and how organizations are protecting themselves against these attacks.
- Explore the career options in cybersecurity.

By the end of this course, you will be more aware of the importance of being safe online, the potential consequences of cyberattacks, and possible career options in cybersecurity.

Chapter 1: The Need for Cybersecurity

This chapter explains what cybersecurity is and why the demand for cybersecurity professionals is growing. It explains what your online identity and data is, where it is, and why it is of interest to cyber criminals.

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

Also included in this chapter is content that briefly explains cyber warfare and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.

Personal Data

What is Cybersecurity?

The connected electronic information network has become an integral part of our daily lives. All types of organizations, such as medical, financial, and education institutions, use this network to operate effectively. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, you need to safeguard your identity, your data, and your computing devices. At the corporate level, it is everyone's responsibility to protect the organization's reputation, data, and customers. At the state level, national security, and the safety and well-being of the citizens are at stake.

Your Online and Offline Identity

As more time is spent online, your identity, both online and offline, can affect your life. Your offline identity is the person who your friends and family interact with on a daily basis at home, at school, or work. They know your personal information, such as your name, age, or where you live. Your online identity is who you are in cyberspace. Your online identity is how you present yourself to others online. This online identity should only reveal a limited amount of information about you.

You should take care when choosing a username or alias for your online identity. The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

Your Data

Any information about you can be considered to be your data. This personal information can uniquely identify you as an individual. This data includes the pictures and messages that you exchange with your family and friends online. Other information, such as name, social security number, date and place of birth, or mother's maiden name, is known by you and used to identify you. Information such as medical, educational, financial, and employment information, can also be used to identify you online.

Medical Records

Every time you go to the doctor's office, more information is added to your electronic health records (EHRs). The prescription from your family doctor becomes part of your EHR. Your EHR includes your physical health, mental health, and other personal information that may not be medically-related. For example, if you had counseling as a child when there were major changes in the family, this will be somewhere in your medical records. Besides your medical history and personal information, the EHR may also include information about your family.

Medical devices, such as fitness bands, use the cloud platform to enable wireless transfer, storage and display of clinical data like heart rates, blood pressures and blood sugars. These devices can generate an enormous amount of clinical data that could become part of your medical records.

Education Records

As you progress through your education, information about your grades and test scores, your attendance, courses taken, awards and degrees rewarded, and any disciplinary reports may be in your education record. This record may also include contact information, health and immunization records, and special education records including individualized education programs (IEPs).

Employment and Financial Records

Your financial record may include information about your income and expenditures. Tax records could include paycheck stubs, credit card statements, your credit rating and other banking information. Your employment information can include your past employment and your performance.

Where is Your Data?

All of this information is about you. There are different laws that protect your privacy and data in your country. But do you know where your data is?

When you are at the doctor's office, the conversation you have with the doctor is recorded in your medical chart. For billing purposes, this information may be shared with the insurance company to ensure appropriate billing and quality. Now, a part of your medical record for the visit is also at the insurance company.

The store loyalty cards maybe a convenient way to save money for your purchases. However, the store is compiling a profile of your purchases and using that information for its own use. The profile shows a buyer purchases a certain brand and flavor of toothpaste regularly. The store uses this information to target the buyer with special offers from the marketing partner. By using the loyalty card, the store and the marketing partner have a profile for the purchasing behavior of a customer.

When you share your pictures online with your friends, do you know who may have a copy of the pictures? Copies of the pictures are on your own devices. Your friends may have copies of those pictures downloaded onto their devices. If the pictures are shared publicly, strangers may have copies of them, too. They could download those pictures or take screenshots of those pictures. Because the pictures were posted online, they are also saved on servers located in different parts of the world. Now the pictures are no longer only found on your computing devices.

Our Computing Devices

Your computing devices do not just store your data. Now these devices have become the portal to your data and generate information about you.

Unless you have chosen to receive paper statements for all of your accounts, you use your computing devices to access the data. If you want a digital copy of the most recent credit card statement, you use your computing devices to access the website of the credit card issuer. If you want to pay your credit card bill online, you access the website of your bank to transfer the funds using your computing devices. Besides allowing you to access your information, the computing devices can also generate information about you.

With all this information about you available online, your personal data has become profitable to hackers.

They Want Your Money

If you have anything of value, the criminals want it.

Your online credentials are valuable. These credentials give the thieves access to your accounts. You may think the frequent flyer miles you have earned are not valuable to cybercriminals. Think again. After approximately 10,000 American Airlines and United accounts were hacked, cybercriminals booked free flights and upgrades using these stolen credentials. Even though the frequent flyer miles were returned to the customers by the airlines, this demonstrates the value of login credentials. A criminal could also take advantage of your relationships. They could access your online accounts and your reputation to trick you into wiring money to your friends or family. The criminal can send messages stating that your family or friends need you to wire them money so they can get home from abroad after losing their wallets.

The criminals are very imaginative when they are trying to trick you into giving them money. They do not just steal your money; they could also steal your identity and ruin your life.

They Want Your Identity

Besides stealing your money for a short-term monetary gain, the criminals want long-term profits by stealing your identity.

As medical costs rise, medical identity theft is also on the rise. The identity thieves can steal your medical insurance and use your medical benefits for themselves, and these medical procedures are now in your medical records.

The annual tax filing procedures may vary from country to country; however, cybercriminals see this time as an opportunity. For example, the people of the United States need to file their taxes by April 15 of each year. The Internal Revenue Service (IRS) does not check the tax return against the information from the employer until July. An identity thief can file a fake tax return and collect the refund. The legitimate filers will notice when their returns are rejected by IRS. With the stolen identity, they can also open credit card accounts and run up debts in your name. This will cause damage to your credit rating and make it more difficult for you to obtain loans.

Personal credentials can also lead to corporate data and government data access.

Organizational Data

Types of Organizational Data

Traditional Data

Corporate data includes personnel information, intellectual properties, and financial data. The 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. This intellectual property can be considered a trade secret; losing this information can be disastrous for the future of the company. The financial data, such as income statements, balance sheets, and cash flow statements of a company gives insight into the health of the company.

Internet of Things and Big Data

With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure. IoT is a large network of physical objects, such as sensors and equipment that extend beyond the traditional computer network. All these connections, plus the fact that we have expanded storage capacity and storage services through the cloud and virtualization, lead to the exponential growth of data. This data has created a new area of interest in technology and business called “Big Data". With the velocity, volume, and variety of data generated by the IoT and the daily operations of business, the confidentiality, integrity and availability of this data is vital to the survival of the organization.

Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability, known as the CIA triad, 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.

CIA TRIAD

Confidentiality

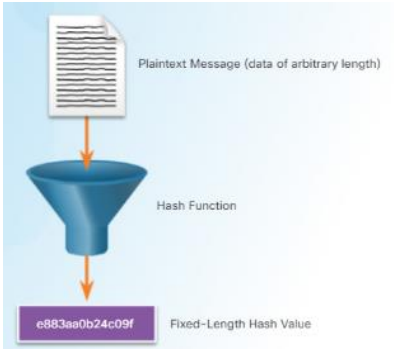
Another term for confidentiality would be privacy. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data. The data may be compartmentalized according to the security or sensitivity level of the information. 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. 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.



CREATING A HASH

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.

1.2.1.3 Lab – Compare Data with a Hash

In this lab, you will generate a hash for a file and use the hash value to compare the integrity of a file.
Follow instructions on Lab document.

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.

1.2.2.5 Lab – What Was Taken?

In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.
Follow instructions on Lab document.

Attackers and Cybersecurity Professionals

Types of Attackers

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.

> **White Hat Hacker** – These are ethical hackers who use their programming skills for good, ethical and legal purposes. White-Hat hackers may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be threatened. Some organizations award prizes or bounties to white hat hackers when they inform them of a vulnerability.
>
> **Grey Hat Hacker** – These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage.an example would be someone who compromises a network without permission and then discloses the vulnerability publicly. A grey hat hacker may disclose a vulnerability to the affected organization after having compromised their network. This allows the organization to fix the problem.
>
> **Black Hat Hacker** – These are unethical criminals who violate computer and network security for personal gain, or for malicious reasons such as attacking networks. Black-hat hackers exploit vulnerabilities to compromise computer and network systems.

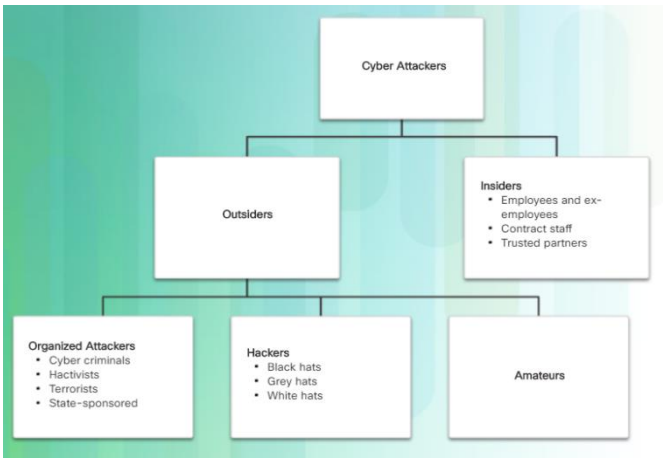
Organized Hackers – These hackers include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and they may even 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

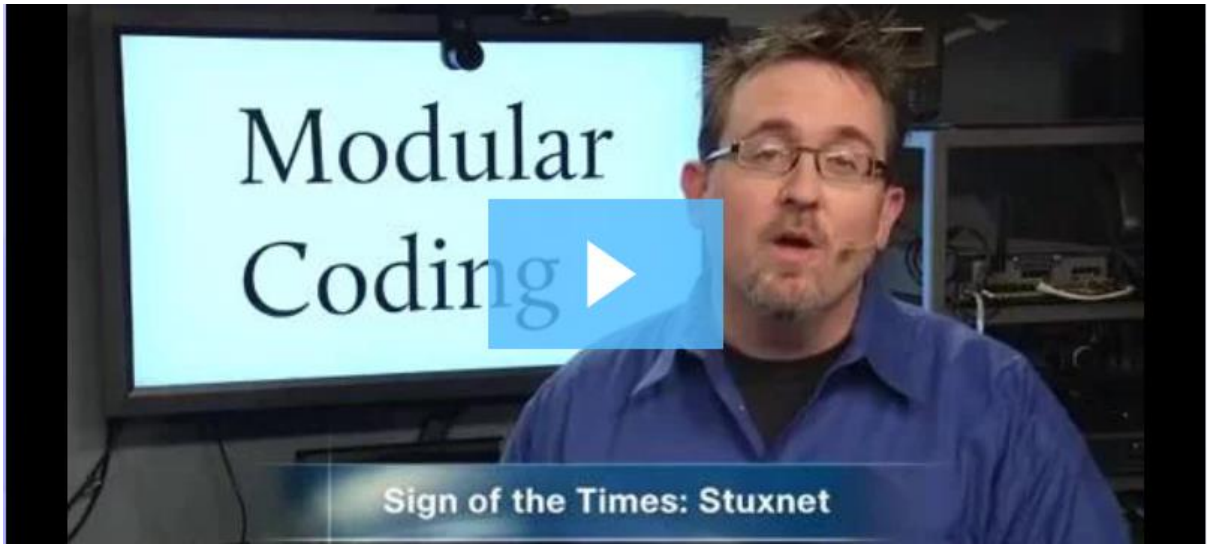
External threats from amateurs or skilled attackers can exploit vulnerabilities in network or computing devices, or use social engineering to gain access.

Cyberwarfare

What is Cyberwarfare?

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.



Breaking Down Stuxnet (Video Transcript)

You know when it comes to security news, It's always puzzling what gets reported. As viewers of this show, you know there's a very regular rhythm of security issues that are always bubbling just below the surface and it takes something truly profound to grab the public's attention. Well one new threat making the rounds did have the right mix of ingredients last summer. Stuxnet. I mean it makes sense, right? Computer attacks, nuclear power. Foreign governments, sabotage. Spy versus spy, but how much of it is real? Enough to say it's a sign of the times. Now as all good threats, the details will continue to evolve, but I do think that there are five items worth paying attention to here. the first one, non-trivial distribution. Primarily spread via USB sticks. Think non-internet connected systems that then propagate by escalating privilege levels through zero day exploits, notable for the fact that true zeros are special and they're only valuable for a short period of time. Very expensive, very hard to come by. The next one, sophistication. This is an intelligent worm. Initially targeting Windows computers, where it even installs its own drivers using a stolen but legitimate certificate. The offending certificate gets revoked of course, but then another one gets added within 24 hours. Our third point, modular coding. This thing can get new tires while still on the road. Multiple control servers. First in Malaysia, then Denmark, now more, including peer-to-peer. In fact, when two run into each other, they compare versions and make sure that they're both updated. Fourth point, unique targeting. Windows is just the intermediary, the friend of the friend. Stuxnet is looking for a particular model of PLC. That's programmable logic controller, which is technically not SCADA as it's often reported. These are small imbedded condustrial control systems that run all sorts of automated processes, from factories to oil refineries to nuclear power plants. Stuxnet will leverage the vulnerability in the controller software to reach in and change very specific bits of data. Shut things off. Don't grease a bearing for 10 minutes. Don't sound an alarm. This is really unique knowledge. Respectable coding skills that imply a higher level of patience of good funding resources. Our final point, motive. Stuxnet does not perform... Excuse me. It does not threaten. It performs sabotage. Really has no criminal focus. Does not spread indiscriminately or steal credit card information or login credentials. It does not recruit systems into a botnet. It targets infrastructure, our most essential necessities like power, water, safety and much, much more. You know these are older systems. Very established. Generally run with the mentality of hey, if it ain't broke, don't fix it. These things don't get watched over and patched by technical handlers who understand these kind of things. Not yet anyway. So stay tuned. This one is not done. We all have a lot to learn and somebody is working hard to teach us.

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.

Summary: 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 page in Student Resources.

Chapter 2: Attacks, Concepts and Techniques

This chapter covers the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware are discussed. The different ways that attackers can infiltrate a system is covered, as well as denial of service attacks.

Most modern cyberattacks are considered to be blended attacks. Blended attacks use multiple techniques to infiltrate and attack a system. When an attack cannot be prevented, it is the job of a cybersecurity professional to reduce the impact of that attack.

Analyzing a Cyberattack

Finding Security Vulnerabilities

Security vulnerabilities are any kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it. An *exploit* is the term used to describe a program written to take advantage of a known vulnerability. The act of using an exploit against a vulnerability is referred to as an attack. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

Software vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code, despite all the effort companies put into finding and patching software vulnerabilities, it is common for new vulnerabilities to surface. Microsoft, Apple, and other operating system producers release patches and updates almost every day. Application updates are also common. Applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

In 2015, a major vulnerability, called SYNful Knock, was discovered in Cisco IOS. This vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco 1841, 2811, and 3825 routers. The attackers could then monitor all network communication and had the ability to infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed in the routers. To avoid this, always verify the integrity of the downloaded IOS image and limit the physical access of the equipment to authorized personnel only.

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. While some companies have penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited, third party security researchers also specialize in finding vulnerabilities in software.

Google's Project Zero is a great example of such practice. After discovering a number of vulnerabilities in various software used by end-users, Google formed a permanent team dedicated to finding software vulnerabilities.

Hardware vulnerabilities

Hardware vulnerabilities are often introduced by hardware design flaws. RAM memory for example, is essentially capacitors installed very close to one another. It was discovered that, due to proximity, constant changes applied to one of these capacitors could influence neighbor capacitors. Based on that design flaw, an exploit called Rowhammer was created. By repeatedly rewriting memory in the same addresses, the Rowhammer exploit allows data to be retrieved from nearby address memory cells, even if the cells are protected.

Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and a physical security are sufficient protection for the everyday user.

Categorizing Security Vulnerabilities

Most software security vulnerabilities fall into one of the following categories:

Buffer overflow – This vulnerability occurs when data is written beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Non-validated input – Programs often work with data input. This data coming into the program could have malicious content, designed to force the program to behave in an unintended way. Consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

Race conditions – This vulnerability is when the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or proper timing.

Weaknesses in security practices – Systems and sensitive data can be protected through techniques such as authentication, authorization, and encryption. Developers should not attempt to create their own security algorithms because it will likely introduce vulnerabilities. It is strongly advised that developers use security libraries that have already created, tested, and verified.

Access-control problems – Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

Nearly all access controls and security practices can be overcome if the attacker has physical access to target equipment. For example, no matter what you set a file's permissions to, the operating system cannot prevent someone from bypassing the operating system and reading the data directly off the disk. To protect the machine and the data it contains, physical access must be restricted and encryption techniques must be used to protect data from being stolen or corrupted.

Types of Malware

Short for Malicious Software, malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system. Below are a few common types of malware:

Spyware – This malware is design to track and spy on the user. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses.

Adware – Advertising supported software is designed to automatically deliver advertisements. Adware is often installed with some versions of software. Some adware is designed to only deliver advertisements but it is also common for adware to come with spyware.

Bot – From the word robot, a bot is malware designed to automatically perform action, usually online. While most bots are harmless, one increasing use of malicious bots are botnets. Several computers are infected with bots which are programmed to quietly wait for commands provided by the attacker.

Ransomware – This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting data in the computer with a key unknown to the user. Some other versions of ransomware can take advantage of specific system vulnerabilities to lock down the system. Ransomware is spread by a downloaded file or some software vulnerability.

Scareware – This is a type of malware designed to persuade the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation. In reality, no problems were assessed or detected and if the user agrees and clears the mentioned program to execute, his or her system will be infected with malware.

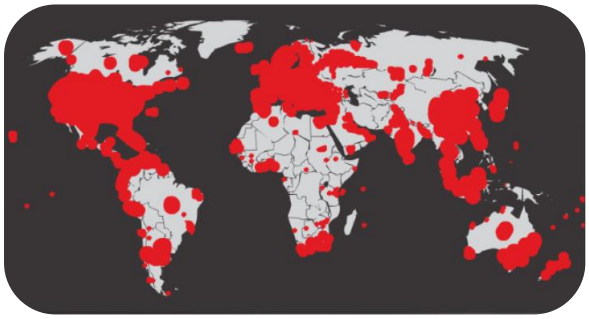
Rootkit – This malware is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect. Often, a computer infected by a rootkit must be wiped and reinstalled.

Virus - A virus is malicious executable code that is attached to other executable files, often legitimate programs. Most viruses require end-user activation and can activate at a specific time or date. Viruses can be harmless and simply display a picture or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate to avoid detection. Most viruses are now spread by USB drives, optical disks, network shares, or email.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. Often, Trojans are found in image files, audio files or games. A Trojan horse differs from a virus because it binds itself to non-executable files.

Worms – Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network. Worms share similar patterns. They all have an enabling vulnerability, a way to propagate themselves, and they all contain a payload.

Worms are responsible for some of the most devastating attacks on the Internet. As shown in Figure 1, in 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers as shown in Figure 2.



Man-In-The-Middle (MitM) – MitM allows the attacker to take control over a device without the user's knowledge. With that level of access, the attacker can intercept and capture user information before relaying it to its intended destination. MitM attacks are widely used to steal financial information. Many malware and techniques exist to provide attackers with MitM capabilities.

Man-In-The-Mobile (MitMo) – A variation of man-in-middle, MitMo is a type of attack used to take control over a mobile device. When infected, the mobile device can be instructed to exfiltrate user-sensitive information and send it to the attackers. ZeuS, an example of an exploit with MitMo capabilities, allows attackers quietly to capture 2-step verification SMS messages sent to users.

Symptoms of Malware

Regardless of the type of malware a system has been infected with, these are common malware symptoms:

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.

Social Engineering

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. For example, an attacker could call an authorized employee with an urgent problem that requires immediate network access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

These are some types of social engineering attacks:

- **Pretexting** - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
- **Tailgating** - This is when an attacker quickly follows an authorized person into a secure location.
- **Something for Something (Quid pro quo)** - This is when an attacker requests personal information from a party in exchange for something, like a free gift.

Wi-Fi Password Cracking

Wi-Fi password cracking is the process of discovering the password used to protect a wireless network. These are some techniques used in password cracking:

Social engineering – The attacker manipulates a person who knows the password into providing it.

Brute-force attacks – The attacker tries several possible passwords in an attempt to guess the password. If the password is a 4-digit number, for example, the attacker would have to try every one of the 10000 combinations. Brute-force attacks usually involve a word-list file. This is a text file containing a list of words taken from a dictionary. A program then tries each word and common combinations. Because brute-force attacks take time, complex passwords take much longer to guess. A few password brute-force tools include Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

Network sniffing – By listening and capturing packets sent on the network, an attacker may be able to discover the password if the password is being sent unencrypted (in plain text). If the password is encrypted, the attacker may still be able to reveal it by using a password cracking tool.

Phishing

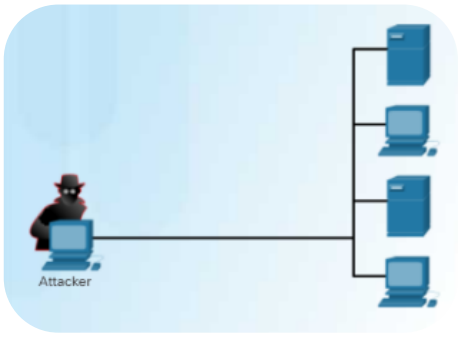
Phishing is when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information. An example of phishing is an email forged to look like it was sent by a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing emails are customized to a specific person. The attacker researches the target's interests before sending the email. For example, an attacker learns the target is interested in cars, and has been looking

to buy a specific model of car. The attacker joins the same car discussion forum where the target is a member, forges a car sale offering and sends email to the target. The email contains a link for pictures of the car. When the target clicks on the link, malware is installed on the target's computer.

Vulnerability Exploitation

Exploiting vulnerabilities is another common method of infiltration. Attackers will scan computers to gain information about them. Below is a common method for exploiting vulnerabilities:



Step 1. Gather information about the target system. This could be done in many different ways such as a port scanner or social engineering. The goal is to learn as much as possible about the target computer.

Step 2.One of the pieces of relevant information learned in step 1 might be the operating system, its version, and a list of services running on it.

Step 3. When the target's operating system and version is known, the attacker looks for any known vulnerabilities specific to that version of OS or other OS services.

Step 4. When a vulnerability is found, the attacker looks for a previously written exploit to use. If no exploits have been written, the attacker may consider writing an exploit.

Figure 1 portrays an attacker using **whois**, a public Internet database containing information about domain names and their registrants. Figure 2 portrays an attacker using the **nmap** tool, a popular port scanner. With a port scanner, an attacker can probe ports of a target computer to learn about which services are running on that computer.

Advanced Persistent Threats

One way in which infiltration is achieved is through advanced persistent threats (APTs). They consist of a multi-phase, long term, stealthy and advanced operation against a specific target. Due to its complexity and skill level required, an APT is usually well funded. An APT targets organizations or nations for business or political reasons.

Usually related to network-based espionage, APT's purpose is to deploy customized malware on one or multiple of the target's systems and remain undetected. With multiple phases of operation and several customized types of malware that affect different devices and perform specific functions, an individual attacker often lacks the skill-set, resources or persistence to carry out APTs.

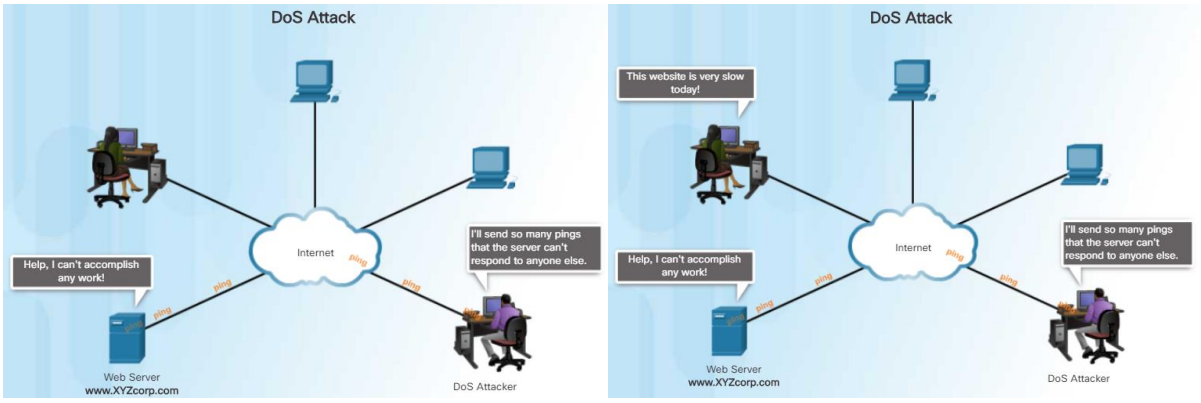
DoS

Denial-of-Service (DoS) attacks are a type of network attack. A DoS attack results in some sort of interruption of network service to users, devices, or applications. There are two major types of DoS attacks:

Overwhelming Quantity of Traffic - This is when a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or a crash of a device or service.

Maliciously Formatted Packets - This is when a maliciously formatted packet is sent to a host or application and the receiver is unable to handle it. For example, an attacker forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets. This causes the receiving device to run very slowly or crash.

DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

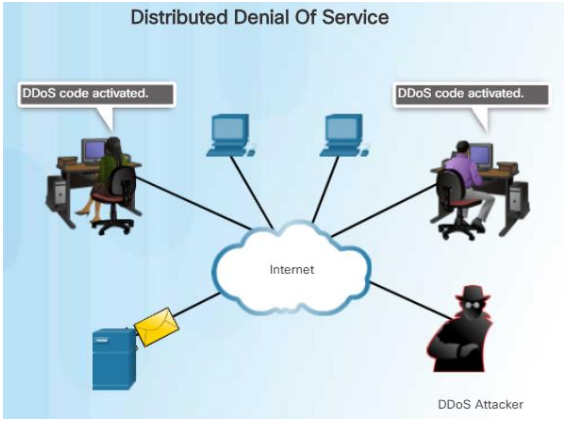


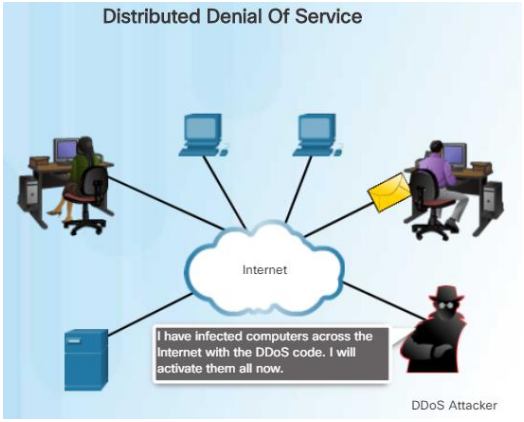
DDoS

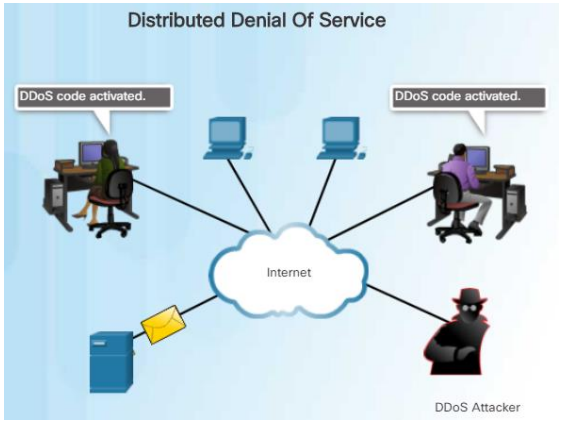
A Distributed DoS Attack (DDoS) is similar to a DoS attack but originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:

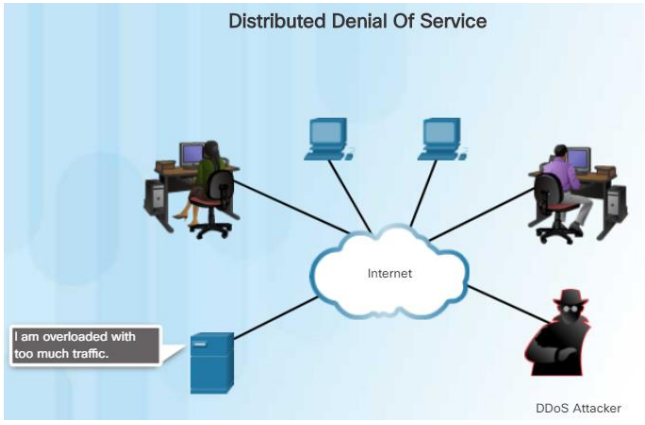
An attacker builds a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems.

The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs handler systems to make the botnet of zombies carry out a DDoS attack.









SEO Poisoning

Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, a malicious user could use SEO to make a malicious website appear higher in search results. This technique is called SEO poisoning.

The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or perform social engineering. To force a malicious site to rank higher in search results, attackers take advantage of popular search terms.

The Cybersecurity Landscape

What is a Blended Attack?

Blended attacks are attacks that use multiple techniques to compromise a target. By using several different attack techniques at once, attackers have malware that are a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes. This trend of blended attacks is revealing more complex malware and placing user data at great risk.

The most common type of blended attack uses spam email messages, instant messages or legitimate websites to distribute links where malware or spyware is secretly downloaded to the computer. Another common blended attack uses DDoS combined with phishing emails. First, DDoS is used to take down a popular bank website and send emails to the bank's customers, apologizing for the inconvenience. The email also directs the users to a forged emergency site where their real login information can be stolen.

Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and Slammer are better categorized as blended attacks, as shown below:

- Some Nimbda variants used email attachments; file downloads from a compromised web server; and Microsoft file sharing (e.g., anonymous shares) as propagation methods.
- Other Nimbda variants were able to modify the system's guest accounts to provide the attacker or malicious code with administrative privileges.

The recent Conficker and ZeuS/LICAT worms were also blended attacks. Conficker used all the traditional distribution methods.

What is Impact Reduction?

While the majority of successful companies today are aware of common security issues and put considerable effort towards preventing them, no set of security practices is 100% efficient. Because a breach is likely to happen if the prize is big, companies and organizations must also be prepared to contain the damage.

It is important to understand that the impact of a breach is not only related to the technical aspect of it, stolen data, damaged databases, or damage to intellectual property, the damage also extends to the company's reputation. Responding to a data breach is a very dynamic process.

Below are some important measures a company should take when a security breach is identified, according to many security experts:

- Communicate the issue. Internally employees should be informed of the problem and called to action. Externally, clients should be informed through direct communication and official announcements. Communication creates transparency, which is crucial in this type of situation.
- Be sincere and accountable in case the company is at fault.

- Provide details. Explain why the situation took place and what was compromised. It is also expected that the company take care of the costs of identity theft protection services for affected customers.
- Understand what caused and facilitated the breach. If necessary, hire forensics experts to research and learn the details.
- Apply what was learned from the forensics investigation to ensure similar breaches do not happen in the future.
- Ensure all systems are clean, no backdoors were installed, and nothing else has been compromised. Attackers will often attempt to leave a backdoor to facilitate future breaches. Make sure this does not happen.
- Educate employees, partners, and customers on how to prevent future breaches.

Summary: Attacks, Concepts and Techniques

This chapter covered the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware explained. Some of the malware that was discussed included viruses, worms, Trojan horses, spyware, adware, and others.

The different ways that attackers can infiltrate a system was covered, including social engineering, Wi-Fi Password Cracking, Phishing, and vulnerability exploitation. The different types of denial of service attacks were also explained.

Blended attacks use multiple techniques to infiltrate and attack a system. Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and slammer are better categorized as blended attacks. When an attack cannot be prevented, it is the job of a cybersecurity professional is to reduce the impact of that attack.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 3: Protecting Your Data and Privacy

This chapter focuses on your personal devices and your personal data. It includes tips for protecting your devices, creating strong passwords and safely using wireless networks. It also discusses maintaining your data securely.

Your online data is worth something to cyber criminals. This chapter briefly covers authentication techniques to help you maintain your data securely. It also covers ways to enhance the security of your online data with tips about what to do and what not to do online.

Protecting your Data

Protect Your Computing Devices

Your computing devices store your data and are the portal to your online life. Below is a short list of steps you can take to protect your computing devices from intrusion:

- **Keep the Firewall On** – Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data. Turn on your firewall:

  Windows 7 or 8.1: http://windows.microsoft.com/en-us/windows/turn-windows-firewall-on-off
  Windows 10: http://windows.microsoft.com/en-us/windows-10/turn-windows-firewall-on-or-off
  Mac OS X: https://support.apple.com/en-us/HT201642

- **Use Antivirus and Antispyware** – Malicious software, such as viruses, Trojan horses, worms, ransomware and spyware, are installed on your computing devices without your permission, in order to gain access to your computer and your data. Viruses can destroy your data, slow down your computer, or take over your computer. One way viruses can take over your computer is by allowing spammers to broadcast emails using your account. Spyware can monitor your online activities, collect your personal information, or produce unwanted pop-up ads on your web browser while you are online. A good rule is to only download software from trusted websites to avoid getting spyware in the first place. Antivirus software is designed to scan your computer and incoming email for viruses and delete them. Sometimes antivirus software also includes antispyware. Keep your software up to date to protect your computer from the newest malicious software.

- **Manage Your Operating System and Browser** – Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. To protect your computer and your data, set the security settings on your computer and browser at medium or higher. Update your computer's operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors.

- **Protect All Your Devices** – Your computing devices, whether they are PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access. The stored information should be encrypted, especially for sensitive or confidential data. For mobile devices, only store necessary information, in case these devices are stolen or lost when you are away from your home. If any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage service provider, such as iCloud or Google drive.

IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. If vulnerabilities are found in the firmware, the IoT device is likely to stay vulnerable. To make the problem worse, IoT devices are often designed to call home and require Internet access. To reach the Internet, most IoT devices manufacturers rely on the customer's local network. The result is that IoT devices are very likely to be comprised and when they are, they allow access to the customer's local network and data. The best way to protect yourself from this scenario is to have IoT devices using an isolated network, sharing it only with other IoT devices.

Visit Shodan at https://www.shodan.io/, a web-based IoT device scanner.

Use Wireless Networks Safely

Wireless networks allow Wi-Fi enabled devices, such as laptops and tablets, to connect to the network by way of the network identifier, known as the Service Set Identifier (SSID). To prevent intruders from entering your home wireless network, the pre-set SSID and default password for the browser-based administrative interface should be changed. Hackers will be aware of this kind of default access information. Optionally, the wireless router can also be configured to not broadcast the SSID, which adds an additional barrier to discovering the

network. However, this should not be considered adequate security for a wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on the wireless router. Even with WPA2 encryption enabled, the wireless network can still be vulnerable.

In October 2017, a security flaw in the WPA2 protocol was discovered. This flaw allows an intruder to break the encryption between the wireless router and the wireless client, and allow the intruder to access and manipulate the network traffic. This vulnerability can be exploited using **K**ey **R**einstallation **A**tta**ck**s (KRACK). It affects all modern, protected Wi-Fi networks. To mitigate an attacker, a user should update all affected products: wireless routers and any wireless capable devices, such as laptops and mobile devices, as soon as security updates become available. For laptops or other devices with wired NIC, a wired connection could mitigate this vulnerability. Furthermore, you can also use a trusted VPN service to prevent the unauthorized access to your data while you are using the wireless network.

Visit https://www.krackattacks.com/, to learn more about KRACK.

When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. However, it is best to not access or send any sensitive personal information over a public wireless network. Verify whether your computer is configured with file and media sharing and that it requires user authentication with encryption. To prevent someone from intercepting your information (known as "eavesdropping") while using a public wireless network, use encrypted VPN tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

Visit https://www.fcc.gov/consumers/guides/protecting-your-wireless-network, to learn more about protecting yourself when using wireless networks.

Many mobile devices, such as smartphones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off when you are not using it.

Use Unique Passwords for Each Online Account

You probably have more than one online account, and each account should have a unique password. That is a lot of passwords to remember. However, the consequence of not using strong and unique passwords leaves you and your data vulnerable to cyber criminals. Using the same password for all your online accounts is like using the same key for all your locked doors, if an attacker was to get your key, he would have the ability to access everything you own. If criminals get your password through phishing for example, they will try to get into your other online accounts. If you only use one password for all accounts, they can get into all your accounts, steal or erase all your data, or decide to impersonate you.

We use so many online accounts that need passwords that is becomes too much to remember. One solution to avoid reusing passwords or using weak passwords is to use a password manager. A password manager stores and encrypts all of your different and complex passwords. The manager can then help you to log into your online accounts automatically. You only need to remember your master password to access the password manager and manage all of your accounts and passwords.

Tips for choosing a good password:

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

- Do not use dictionary words or names in any languages
- Do not use common misspellings of dictionary words
- Do not use computer names or account names
- If possible use special characters, such as: ! @ # $ % ^ & * ( )
- Use a password with ten or more characters

Use Passphrase Rather Than a Password

To prevent unauthorized physical access to your computing devices, use passphrases, rather than passwords. It is easier to create a long passphrase than a password, because it is generally in the form of a sentence rather than a word. The longer length makes passphrases less vulnerable to dictionary or brute force attacks. Furthermore, a passphrase maybe easier to remember, especially if you are required to change your password frequently. Here are some tips in choosing good passwords or passphrases:

Tips in choosing a good passphrase:

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

- Choose a meaningful statement to you
- Add special characters, such as ! @ # $ % ^ & * ( )
- The longer the better
- Avoid common or famous statements, for example, lyrics from a popular song

Recently, United States National Institute for Standards and Technology (NIST) published improved password requirements. NIST standards are intended for government application but can also serve as a standard for others as well. The new guidelines aim to provide better user experience and put the burden of user verification on the providers.

Summary of the new guidelines:

- 8 characters minimum in length, but no more than 64 characters
- No common, easily guessed passwords, such as password, abc123
- No composition rules, such as having to include lowercase and uppercase letters and numbers
- Improve typing accuracy by allowing the user to see the password while typing
- All printing characters and spaces are allowed
- No password hints
- No periodical or arbitrary password expiration
- No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history

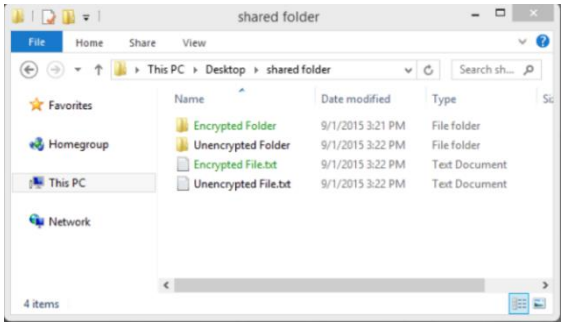
Visit https://pages.nist.gov/800-63-3/, to learn more about the improved NIST password requirement.

Even with access to your computers and network devices secured, it is also important to protect and preserve your data.

3.1.1.5 Lab – Create and Store Strong Passwords

In this lab, you will explore the concepts to create strong passwords and how to store it securely.
Follow instructions on Lab document

Encrypt Your Data



Your data should always be encrypted. You may think you have no secrets and nothing to hide so why use encryption? Maybe you think that nobody wants your data. Most likely, this is probably not true.

Are you ready to show all of your photos and documents to strangers? Are you ready to share financial information stored on your computer to your friends? Do you want to give out your emails and account passwords to the general public?

This can be even more troublesome if a malicious application infects your computer or mobile device and steals potentially valuable information, such as account numbers and passwords, and other official documents. That kind of information can lead to identity theft, fraud, or ransom. Criminals may decide to simply encrypt your data and make it unusable until you pay the ransom.

What is encryption? Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form. The encryption itself does not prevent someone from intercepting the data. Encryption can only prevent an unauthorized person from viewing or accessing the content.

Software programs are used to encrypt files, folders, and even entire drives.

Encrypting File System (EFS) is a Windows feature that can encrypt data. EFS is directly linked to a specific user account. Only the user that encrypted the data will be able to access it after it has been encrypted using EFS. To encrypt data using EFS in all Windows versions, follow these steps:

Step 1. Select one or more files or folders.

Step 2. Right-click the selected data **>Properties**.

Step 3. Click **Advanced…**

Step 4. Select the **Encrypt contents to secure data** check box.

Step 5. Files and folders that have been encrypted with EFS are displayed in green, as shown in the figure.

Back up Your Data

Your hard drive may fail. Your laptop could be lost. Your smart phone stolen. Maybe you erased the original version of an important document. Having a backup may prevent the loss of irreplaceable data, such as family photos. To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly and automatically.

The additional location for your backed up files can be on your home network, secondary location, or in the cloud. By storing the backup of the data locally, you have total control of the data. You can decide to copy all of your data to a network attached storage device (NAS), a simple external hard drive, or maybe select only a few important folders for backup on thumb drives, CDs/DVDs, or even tapes. In that scenario, you are the owner and you are totally responsible for the cost and maintenance of the storage device equipment. If you subscribe to a cloud storage service, the cost depends on the amount storage space needed. With a cloud storage service like Amazon Web Services (AWS), you have access to your backup data as long as you have access to your account. When you subscribe to online storage services, you may need to be more selective about the

data being backed up due to the cost of the storage and the constant online data transfers. One of the benefits of storing a backup at an alternate location is that it is safe in the event of fire, theft or other catastrophes other than storage device failure.

3.1.2.3 Lab – Back up Data to External Storage

In this lab, you will use an external disk and a remote disk to back up your data.
Follow instruction on the lab document.

Deleting Your Data Permanently

When you move a file to the recycle bin or trash and delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools can still recover the file due to a magnetic trace left on the hard drive.

In order to erase data so that it is no longer recoverable, the data must be overwritten with ones and zeroes multiple times. To prevent the recovery of deleted files, you may need to use tools specifically designed to do just that. The program SDelete from Microsoft (for Vista and higher), claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OSX are some tools that claim to provide a similar service.

The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. It has been the folly of many criminals in thinking their files were impenetrable or irrecoverable.

Besides storing data on your local hard drives, your data may also be stored online in the cloud. Those copies will also need to be deleted. Take a moment to ask yourself, “Where do I save my data? Is it backed up somewhere? Is it encrypted? When you need to delete your data or get rid of a hard drive or computer, ask yourself, “Have I safeguarded the data to keep it from falling into the wrong hands?”

3.1.2.5 Lab – Who Owns Your Data?

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.
Follow instructions on the lab document.

Safeguarding Your Online Privacy

Two Factor Authentication

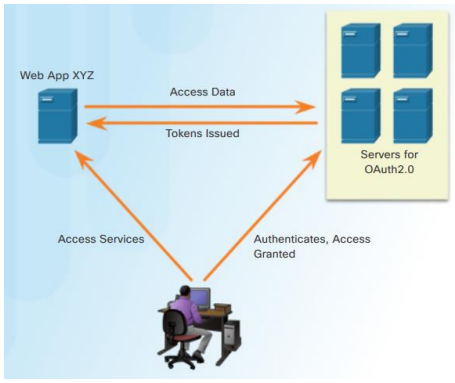
Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication to add an extra layer of security for account logins. Besides the username and password, or personal identification number (PIN) or pattern, two factor authentication requires a second token, such as a:

- **Physical object** - credit card, ATM card, phone, or fob
- **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition

Even with two factor authentication, hackers can still gain access to your online accounts through attacks such as phishing attacks, malware, and social engineering.

Visit https://twofactorauth.org/, to find out if websites you visit use two factor authentication.

OAuth 2.0



Open Authorization (OAuth) is an open standard protocol that allows an end user's credentials to access third party applications without exposing the user's password. OAuth acts as the middle man to decide whether to allow end users access to third party applications. For example, say you want to access web application XYZ, and you do not have a user account for accessing this web application. However, XYZ has the option to allow you to log in using the credentials from a social media website ABC. So you access the website using the social media login.

For this to work, the application 'XYZ' is registered with 'ABC' and is an approved application. When you access XYZ, you use your user credentials for ABC. Then XYZ requests an access token from ABC on your behalf. Now you have access to XYZ. XYZ knows nothing about you and your user credentials, and this interaction is totally seamless for the user. Using secret tokens prevents a malicious application from getting your information and your data.

Do Not Share Too Much on Social Media

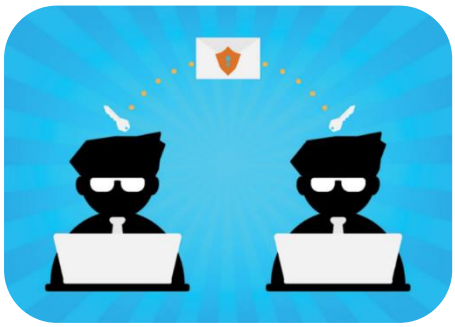
If you want to keep your privacy on social media, share as little information as possible. You should not share information like your birth date, email address, or your phone number on your profile. The people who need to know your personal information probably already know it. Do not fill out your social media profile completely, only provide the minimum required information. Furthermore, check your social media settings to allow only people you know to see your activities or engage in your conversations.

The more personal information you share online, the easier it is for someone to create a profile about you and take advantage of you offline.

Have you ever forgotten the username and password for an online account? Security questions like "What is your mother's maiden name?" or "In what city were you born?" are supposed to help keep your account safe from intruders. However, anyone who wants to access your accounts can search for the answers on the Internet.

You can answer these questions with false information, as long as you can remember the false answers. If you have a problem remembering them, you can use password manager to manage them for you.

Email and Web Browser Privacy



Every day, millions of email messages are used to communicate with friends and conduct business. Email is a convenient way to communicate with each other quickly. When you send an email, it is similar to sending a message using a postcard. The postcard message is transmitted in plain sight of anyone who has access to look, and the email message is transmitted in plain text, and is readable by anyone who has access. These communications are also passed among different servers while in route to the destination. Even when you erase your email messages, the messages can be archived on the mail servers for some time.

Anyone with physical access to your computer, or your router, can view which websites you have visited using web browser history, cache, and possibly log files. This problem can be minimized by enabling the in-private browsing mode on the web browser. Most of the popular web browsers have their own name for private browser mode:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

With private mode enabled, cookies are disabled, and temporary Internet files and browsing history are removed after closing the window or program.

Keeping your Internet browsing history private may prevent others from gathering information about your online activities and enticing you to buy something with targeted ads. Even with private browsing enabled and cookies disabled, companies are developing different ways of fingerprinting users in order to gather information and track user behavior. For example, the intermediary devices, such as routers, can have information about a user's web surfing history.

Ultimately, it is your responsibility to safeguard your data, your identity, and your computing devices. When you send an email, should you include your medical records? The next time you browse the Internet, is your transmission secure? Just a few simple precautions may save you problems later.

This figure shows two businessmen with computer laptop send email data with protection shield and key decryption.

3.2.2.3 Lab – Discover Your Own Risky Online Behavior

In this lab, you will identify risky online behavior and explore some tips on how to become safer online.
Follow instructions on lab document.

Summary: Protecting Your Data and Privacy

This chapter focused on your personal devices, your personal data. It included tips for protecting your devices, creating strong passwords and safely using wireless networks. It covered data backups, data storage and deleting your data permanently.

Authentication techniques were discussed to help you maintain your data securely. It briefly covered how easy it is to share too much information on social media and how to avoid this security risk.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 4: Protecting the Organization

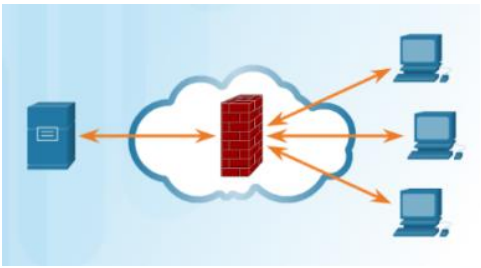
This chapter covers some of the technology and processes used by cybersecurity professionals when protecting an organization's network, equipment and data. First, it briefly covers the many types of firewalls, security appliances, and software that are currently used, including best practices.

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.

Firewalls

Firewall Types

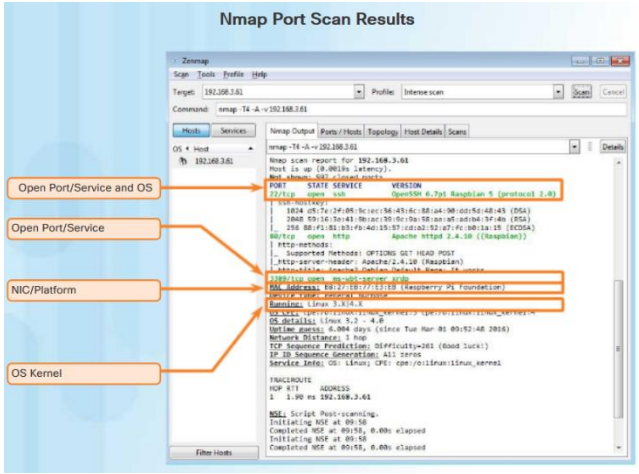


A firewall is a wall or partition that is designed to prevent fire from spreading from one part of a building to another. In computer networking, a firewall is designed to control, or filter, which communications are allowed in and which are allowed out of a device or network, as shown in the figure. 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



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.

Security Appliances

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.

FIGURE 1

FIGURE 2

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.

FIGURE 3

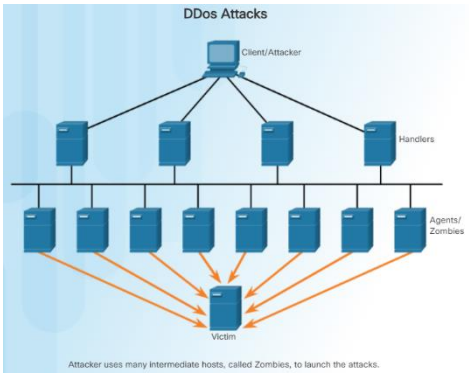
VPN - Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client technologies. It is designed for secure encrypted tunneling.

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.

Detecting Attacks in Real Time

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

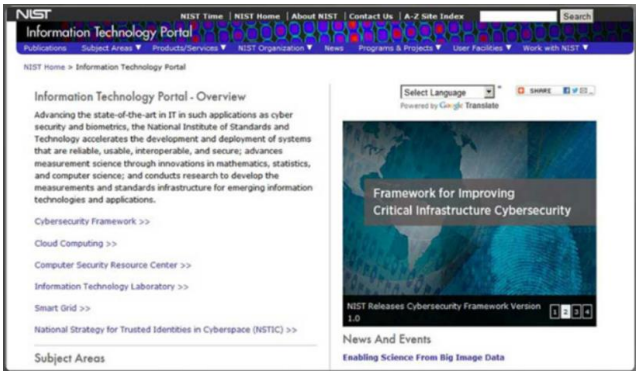
How do you provide defense against the constant presence of zero-day attacks, as well as advanced persistent threats (APT) that steal data over long periods of time? One solution is to use an enterprise-level advanced malware detection solution that offers real-time malware detection.

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.

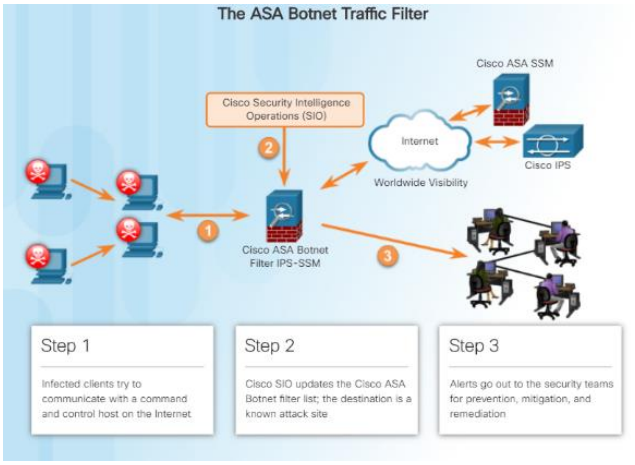
Some of the most helpful guidelines are found in organizational repositories such as the National Institute of Standards and Technology (NIST) Computer Security Resource Center, as shown in the figure.

One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Visit https://www.sans.org/about/, to learn more about SANS and the types of training and certifications they offer.

Behavior Approach to Cybersecurity

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.

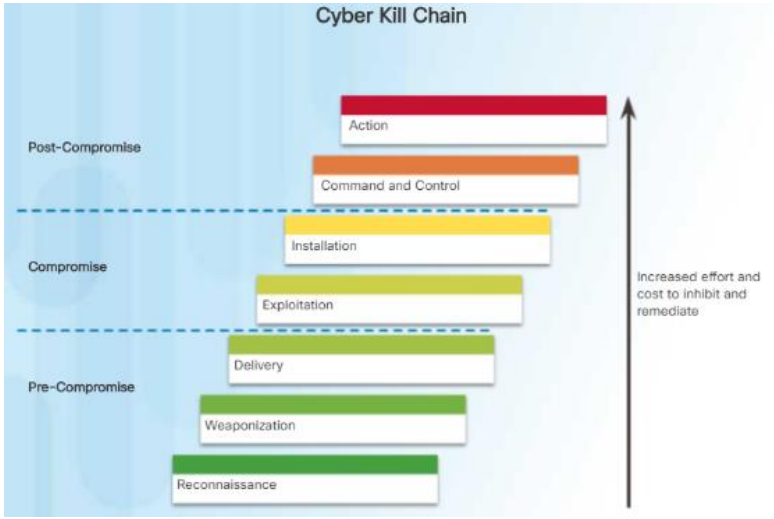


A botnet can have tens of thousands, or even hundreds of thousands of bots. These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute force password attacks. Botnets are typically controlled through a command and control server.

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:

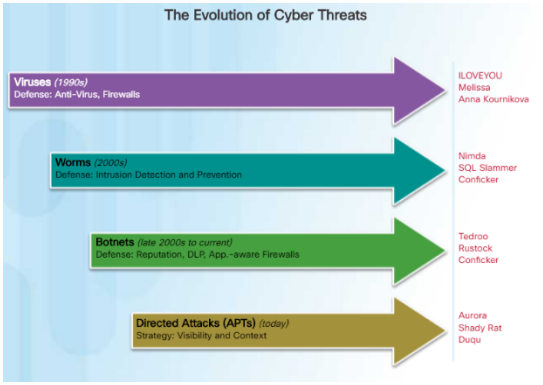
- What are the attack indicators at each stage of the Kill Chain?
- Which security tools are needed to detect the attack indicators at each of the stages?

- 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

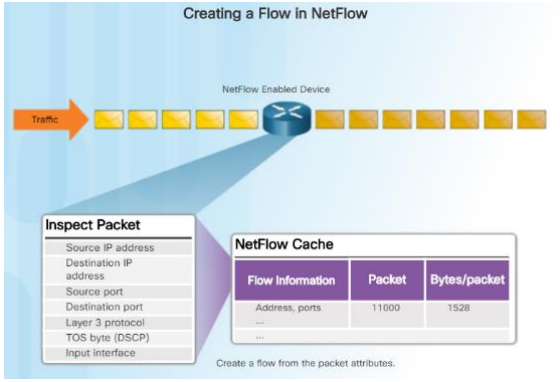
Behavior-based security is a form of threat detection that does not rely on known malicious signatures, but instead uses informational context to detect anomalies in the network. Behavior-based detection involves capturing and analyzing the flow of communication between a user on the local network and 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.

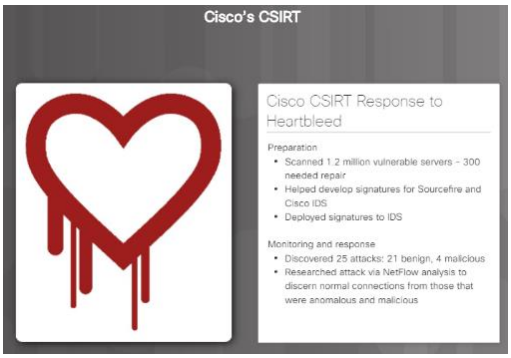
NetFlow is able to collect information on usage through many different characteristics of how data is moved through the network, as shown in the figure. By collecting information about network data flows, NetFlow is able to establish baseline behaviors on more than 90 different attributes.

Cisco's Approach to Cybersecurity

CSIRT

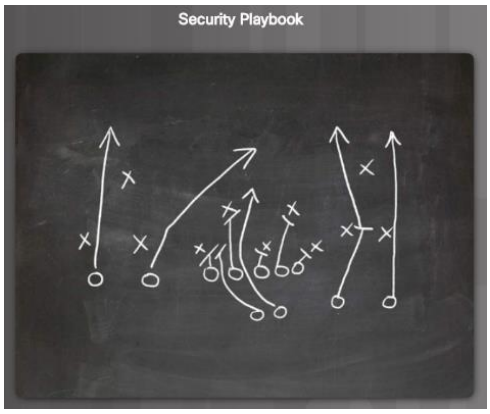
Many large organizations have a Computer Security Incident Response Team (CSIRT) to receive, review, and respond to computer security incident reports, as shown in Figure 1. The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations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

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.

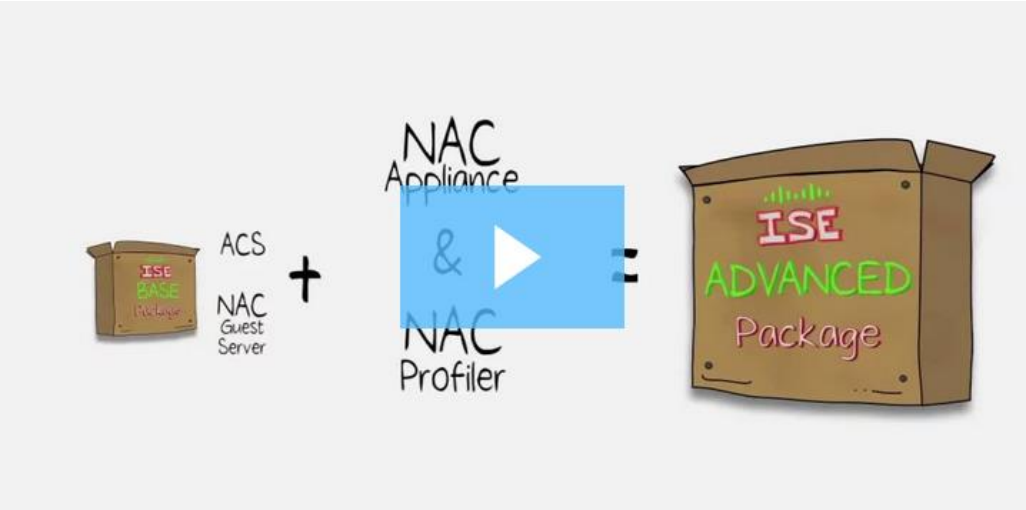
All this information should be compiled into a security playbook. A security playbook is a collection of repeatable queries (reports) against security event data sources that lead to incident detection and response. Ideally the security playbook must accomplish the following actions:

- 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.



Fundamentals of ISE – Video Transcript

I remember my first security policy. So simple. Good stuff on, bad stuff off. Over the years, however, defining good and bad as gotten really difficult. So one policy quickly became two, then 10, then more and forget about just defining these policies, I need to enforce them as well. Now there's compliance and the need to prove I'm secure. On top of all that, everyone's bringing in his or her favorite Wi-Fi device and expecting full network access. Keeping up with this stuff takes time, people, and money, not to mention how I translate policy terms like location, users, devices, and applications into geek speak like IPs, MACs, ACLs, ports, and 802.1x. Enough! An answer for us. The Cisco Identity Servers Engine or ISE is an identity-based policy platform that enables compliance, enhances security, and streamlines operations. Its unique architecture lets you gather real-time contextual information about users and devices to proactively enforce governance policy across the entire network infrastructure. When you think about it, how could all this be attempted otherwise? As the central policy component for Cisco's TrustSec Solution, ISE is the single source for policy definition, control, and reporting. So, you want to be on my network? Let me show you the tool set. Triple A. Authentication, authorization, and accounting. Hey, what's your username and your password? Cool. Now let me give you access to just what you need and by the way, I'm logging this whole session just in case. Posture. Is this device clean? Carrying any suspicious applications or viruses? No? Profiler. You say you're a printer, but now you act like a web camera? I'm going to show you the door. Out! And now, guest management. Just need temporary access? No problem. You get just enough access, but when your time is up, it's up. And automatically. Nice thing for me, I don't even have to set you up as a guest. All that's handled by the person who wanted you to visit Now many of you are saying to yourself right now, self, this sounds just like Cisco NAC and ACS. And you're right. That's where it starts. ISE combines the functionality of both, but with simpler deployment and common management. Moving forward, ISE will extend more deeply into the network, into the data center, and the application stack. The Cisco Identity Services Engine is the single source of truth for end points all across the network. Now, there are really just two packages to understand here. The base package is all about authentication, ID, and guest services like what you find in Cisco ACS and NAC Guest Server. The advanced package adds profiling and posture services into the mix. A deeper more intelligent analysis of anything requesting access. NAC Appliance and Profiler, they'd be your reference points here. And anticipating your next logical question, no, this does not mean end of life for NAC or ACS. Every network is different. ICS is for those of us who want to consolidate policies in an 802.1x framework. If that's not you because say you want a choke point that's in line, or maybe you're just looking to authenticate a network device admins or something. Well, existing NAC or ACS products? They're going to be a better fit. Now speaking of fit, you have three different hardware appliances to choose from, as well as a VMwarebased and virtualized appliance. And because Cisco's shipping on the same hardware used by NAC and ACS today, there's a built-in level of investment protection. Always a good point to make to the bean counters, right? Now unlike other solutions, Cisco ISE has the ability to run specific functions at critical points in the network. For example, a pair of ISE appliances for administration, maintenance, and troubleshooting, and logging, and a high availability configuration. This could be located centrally, but with distributed appliances for making policy decisions as close to the user or device as possible communicating to your Cisco network infrastructure for enforcement. This is a really important design point to call out here. Cisco ISE works with your existing network devices, switches, wireless controllers, VPN concentrators, to balance the workload and keep enforcement as close to the end point as possible. If you have legacy gear in your network, no worries. ISE can make enforcement work with these as well. Now this example was a large network design simply to illustrate the flexibility available. You can still get tremendous value from just two of these things. Redundancy, right? Start small, add capacity through additional appliances or extra licenses whenever needed. All right. Our assault on complexity continues now with a simple interface including things like a centralized dashboard with hotlinks to more Video - Fundamentals of ISE ? Cisco and/or its affiliates. All rights reserved. Cisco Confidential Page 2 of 2 www.netacad.com details, flexible filtering of your

active session, drag and drop re-ordering of rules, reusable objects. ISE uses state of the art widgets to make page-hopping and crazy scrolling a thing of the past. You're just going to love the clarity ISE provides here. Visibility into what just happened, when it happened, who or what was involved and how it was taken care of. We all know that complexity is the enemy of good security. This is why the ISE dashboard and the reporting tools, the live logs, are so robust and valuable. So there you have it. Cisco Identity Services Engine. Single point of truth restoring visbility and control to the edge of your network. Enough already, huh? Why don't you check it out for yourself? For more information, visit cisco.com/go/ise.

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.

Summary: 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 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.

Cybersecurity Legal and Ethical Issues, Education and Careers

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.

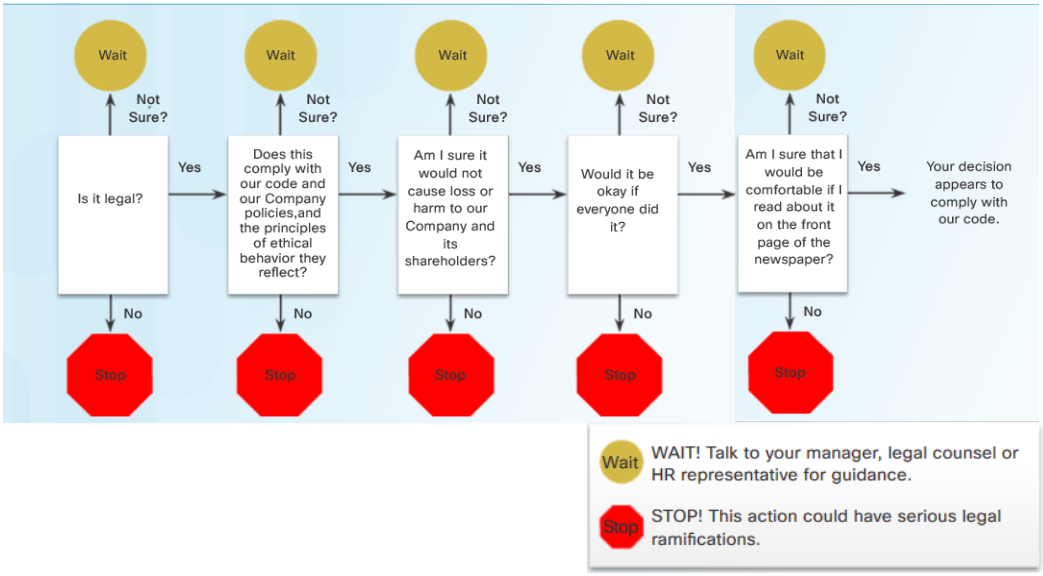
In general, if you are confused about whether an action or behavior might be illegal, assume that it is illegal and do not do it. Your company may have a legal department or someone in the human resources department who can answer your questions before you do something illegal.

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) has published a code of ethics that you can read here http://csisite.net/training/ethicsconduct.htm
- The Information Systems Security Association (ISSA) has a code of ethics found here http://www.issa.org/?page=CodeofEthics
- The Association of Information Technology Professionals (AITP) has both a code of ethics and a standard of conduct found here http://www.aitp.org/?page=EthicsConduct

Cisco has a team devoted exclusively to ethical business conduct. Visit 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

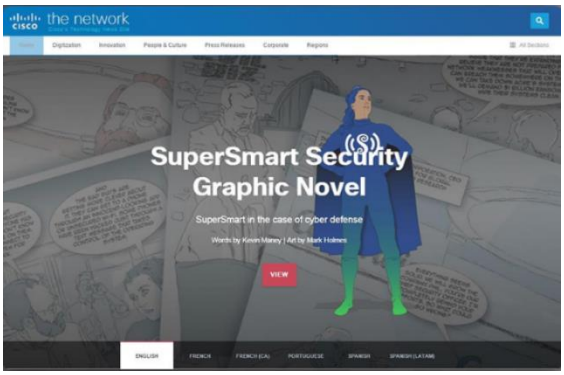
Many other businesses and industries are hiring cybersecurity professionals. There are several online search engines to help you find the right job in cybersecurity:

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

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 that are available. Furthermore, you can also access career resources available in Cisco Networking Academy.



Just for fun, go to http://newsroom.cisco.com/supersmartsecurity to read a graphic novel about a cybersecurity superhero!

Before You Go

Congratulations! You are nearly done with this course. Before you go, have a look at all the ways that NetAcad can support your education and your career!

- **Cisco Cert Exams and Discount Vouchers** – You have worked so hard to complete this course. Now it is time to think about how your new skills and knowledge can help when taking industry-recocognized certification exams, Not only that, netacad.com might also be able to help save you money on the cost of exams!
- **Talent Bridge** – Is It time to find a GREAT job? Talent Bridge can help. Register today at https://www.netacad.com/careers/employment-opportunities/learn-about-talent-bridge, and start your search. Talent Bridge can match your skills and experience with jobs at Cisco and Cisco Partners. They are always looking for NetAcad Alumni!
- **Career Resources** – Is this your first job search? Maybe it's been a long time since you've looked for a job. Click **Careers** at the top of netacad.com. You'll find great information on employment opportunities, webinars, career advice, pathways, certifications and success stories. While you're here, click **Courses** at the top of the page. At the bottom of the drop down menu, click **All Courses** to see what else Netacad has to offer.

Summary: 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 page in Student Resources.

CYBERSECURITY FOR
SMALL BUSINESS

CYBERSECURITY BASICS

Cyber criminals target companies of all sizes.

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT
YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

PROTECT YOUR WIRELESS NETWORK

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take. You can find it at FTC.gov/DataBreach.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

Understanding THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

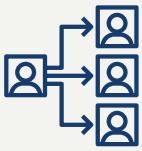
NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

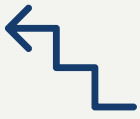
1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:



Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.



Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

3. DETECT

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

Check your network for unauthorized users or connections.

Investigate any unusual activities on your network or by your staff.

4. RESPOND

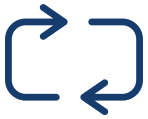
Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER

After an attack:



Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/Programs-Projects/Small-Business-Corner-SBC.

LEARN MORE AT: FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

Store securely

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

Limit physical access

When records or devices contain sensitive data, allow access only to those who need it.

Send reminders

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

Keep stock

Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR

SMALL BUSINESS

HOW TO PROTECT DATA ON YOUR DEVICES

A burglary, lost laptop, stolen mobile phone, or misplaced flash drive — all can happen due to lapses in physical security. But they're less likely to result in a data breach if information on those devices is protected. Here are a few ways to do that:

Require complex passwords

Require passwords that are long, complex, and unique. And make sure that these passwords are stored securely. Consider using a password manager.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Limit login attempts

Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.

Encrypt

Encrypt portable media, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside of the company, like to an accountant or a shipping service.

TRAIN YOUR EMPLOYEES

Include physical security in your regular employee trainings and communications. Remind employees to:

Shred documents

Always shred documents with sensitive information before throwing them away.

Erase data correctly

Use software to erase data before donating or discarding old computers, mobile devices, digital copiers, and drives. Don't rely on "delete" alone. That does not actually remove the file from the computer.

Promote security practices in all locations

Maintain security practices even if working remotely from home or on business travel.

Know the response plan

All staff should know what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. Use *Data Breach Response: A Guide for Business* for help creating a response plan. You can find it at FTC.gov/DataBreach.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

RANSOMWARE

Someone in your company gets an email.

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That's a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransomware can take a serious toll on your business.

HOW IT HAPPENS

Criminals can start a ransomware attack in a variety of ways.

Scam emails

with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.

Server vulnerabilities

which can be exploited by hackers.

Infected websites

that automatically download malicious software onto your computer.

Online ads

that contain malicious code — even on websites you know and trust.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

Have a plan

How would your business stay up and running after a ransomware attack? Put this plan in writing and share it with everyone who needs to know.

Back up your data

Regularly save important files to a drive or server that's not connected to your network. Make data backup part of your routine business operations.

Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication, and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.

Alert your staff

Teach them how to avoid phishing scams and show them some of the common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

WHAT TO DO IF YOU'RE ATTACKED

Limit the damage

Immediately disconnect the infected computers or devices from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected.

Contact the authorities

Report the attack right away to your local FBI office.

Keep your business running

Now's the time to implement that plan. Having data backed up will help.

Should I pay the ransom?

Law enforcement doesn't recommend that, but it's up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. However, paying the ransom may not guarantee you get your data back.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties – they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. You can find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

PHISHING

You get an email that looks like it's from someone you know.

It seems to be from one of your company's vendors and asks that you click on a link to update your business account. Should you click? Maybe it looks like it's from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

HOW

PHISHING WORKS

You get an email or text

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

It looks real

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

It's urgent

The message pressures you to act now — or something bad will happen.

What happens next

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

WHAT YOU CAN DO

Before you click on a link or share any of your sensitive business information:

Check it out

Look up the website or phone number for the company or person behind the text or email. Make sure that you're getting the real company and not about to download malware or talk to a scammer.

Talk to someone

Talking to a colleague might help you figure out if the request is real or a phishing attempt.

Make a call if you're not sure

Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

Back up your data

Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

Keep your security up to date

Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.

Alert your staff

Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.

Deploy a safety net

Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.

WHAT IF YOU FALL FOR A PHISHING SCHEME

Alert others

Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.

Limit the damage

Immediately change any compromised passwords and disconnect from the network any computer or device that's infected with malware.

Follow your company's procedures

These may include notifying specific people in your organization or contractors that help you with IT.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business* (FTC.gov/DataBreach).

Report it

Forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

BUSINESS EMAIL IMPOSTERS

A scammer sets up an email address that looks like it's from your company.

Then the scammer sends out messages using that email address. This practice is called spoofing, and the scammer is what we call a business email imposter.

Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

HOW TO PROTECT YOUR BUSINESS

Use email authentication

When you set up your business's email, make sure the email provider offers email authentication technology. That way, when you send an email from your company's server, the receiving servers can confirm that the email is really from you. If it's not, the receiving servers may block the email and foil a business email imposter.

Keep your security up to date

Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

Train your staff

Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

WHAT TO DO

IF SOMEONE SPOOFS YOUR COMPANY'S EMAIL

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks. You don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

CYBERSECURITY FOR
SMALL BUSINESS

TECH SUPPORT SCAMS

You get a phone call, pop-up, or email telling you there's a problem with your computer.

Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then:

Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it

Install malware that gives them access to your computer and sensitive data, like user names and passwords

Try to sell you software or repair services that are worthless or available elsewhere for free

Try to enroll you in a worthless computer maintenance or warranty program

Ask for credit card information so they can bill you for phony services or services available elsewhere for free

Direct you to websites and ask you to enter credit card, bank account, and other personal information

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

If a caller says your computer has a problem, hang up. A tech support call you don't expect is a scam — even if the number is local or looks legitimate. These scammers use fake caller ID information to look like local businesses or trusted companies.

If you get a pop-up message to call tech support, ignore it. Some pop-up messages about computer issues are legitimate, but do not call a number or click on a link that appears in a pop-up message warning you of a computer problem.

If you're worried about a virus or other threat, call your security software company directly, using the phone number on its website, the sales receipt, or the product packaging. Or consult a trusted security professional.

Never give someone your password, and don't give remote access to your computer to someone who contacts you unexpectedly.

WHAT TO DO IF YOU'RE SCAMMED

If you shared your password with a scammer, change it on every account that uses this password. Remember to use unique passwords for each account and service. Consider using a password manager.

Get rid of malware. Update or download legitimate security software. Scan your computer, and delete anything the software says is a problem. If you need help, consult a trusted security professional.

If the affected computer is connected to your network, you or a security professional should check the entire network for intrusions.

If you bought bogus services, ask your credit card company to reverse the charges, and check your statement for any charges you didn't approve. Keep checking your credit card statements to make sure the scammer doesn't try to re-charge you every month.

Report the attack right away to the FTC at FTC.gov/Complaint.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

CYBER INSURANCE

Recovering from a cyber attack can be costly.

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?

Make sure your policy includes coverage for:

- ☐ Data breaches (like incidents involving theft of personal information)
- ☐ Cyber attacks (like breaches of your network)
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Cyber attacks that occur anywhere in the world (not only in the United States)
- ☐ Terrorist acts

Also, consider whether your cyber insurance provider will:

- ☐ Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- ☐ Provide coverage in excess of any other applicable insurance you have
- ☐ Offer a breach hotline that's available every day of the year at all times

LEARN MORE AT:
FTC.gov/SmallBusiness

NAIC National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.

CYBERSECURITY FOR
SMALL BUSINESS

WHAT IS FIRST-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- ☐ Legal counsel to determine your notification and regulatory obligations
- ☐ Customer notification and call center services
- ☐ Crisis management and public relations
- ☐ Forensic services to investigate the breach
- ☐ Recovery and replacement of lost or stolen data
- ☐ Lost income due to business interruption
- ☐ Cyber extortion and fraud
- ☐ Fees, fines, and penalties related to the cyber incident

WHAT IS THIRD-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- ☐ Payments to consumers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages, and judgments
- ☐ Accounting costs

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness

LEARN MORE AT: FTC.gov/SmallBusiness

NAIC National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.

CYBERSECURITY FOR
SMALL BUSINESS

EMAIL AUTHENTICATION

Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they're from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

WHAT TO KNOW —

Some web host providers let you set up your company's business email using your domain name (which you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they're from your business. If your business email uses your company's domain name, make sure that your email provider has these three email authentication tools:

Sender Policy Framework (SPF)

tells other servers which servers are allowed to send emails using your business's domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can't find a match, the email can be flagged as suspicious.

Domain Keys Identified Mail (DKIM)

puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization's servers and hasn't been tampered with in transit.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

is the essential third tool for email authentication. SPF and DKIM verify the address the server uses "behind the scenes." DMARC verifies that this address matches the "from" address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have other servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you're notified when this happens.

It takes some expertise to configure these tools so that they work as intended and don't block legitimate email. Make sure that your email hosting provider can set them up if you don't have the technical knowledge. If they can't, or don't include that in their service agreement, consider getting another provider.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION
Homeland Security
NIST National Institute of Standards and Technology U.S. Department of Commerce
SBA U.S. Small Business Administration

CYBERSECURITY FOR
SMALL BUSINESS

WHAT TO DO IF YOUR
EMAIL IS SPOOFED

Email authentication helps keep your business's email from being used in phishing schemes because it notifies you if someone spoofs your company's email. If you get that notification, take these actions:

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov (an address used by the FTC) and to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).

Notify your customers

If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks: you don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. And if your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

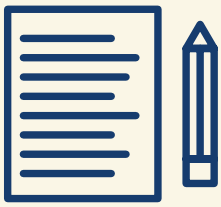
CYBERSECURITY FOR
SMALL BUSINESS

VENDOR SECURITY

Your business vendors may have access to sensitive information.

Make sure those vendors are securing their own computers and networks. For example, what if your accountant, who has all your financial data, loses his laptop? Or a vendor whose network is connected to yours gets hacked? The result: your business data and your customers' personal information may end up in the wrong hands — putting your business and your customers at risk.

HOW TO MONITOR YOUR VENDORS



Put it in writing

Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable.

Verify compliance

Establish processes so you can confirm that vendors follow your rules. Don't just take their word for it.

Make changes as needed

Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR SMALL BUSINESS

HOW TO PROTECT YOUR BUSINESS

Control access

Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job.

Use multi-factor authentication

This makes vendors take additional steps beyond logging in with a password to access your network — like a temporary code on a smartphone or a key that's inserted into a computer.

Secure your network

Require strong passwords: at least 12 characters with a mix of numbers, symbols, and both capital and lowercase letters. Never reuse passwords, don't share them, and limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Safeguard your data

Use properly configured, strong encryption. This protects sensitive information as it's transferred and stored.

WHAT TO DO IF A VENDOR HAS A DATA BREACH

Contact the authorities

Report the attack right away to your local police department. If they're not familiar with investigating information compromises, contact your local FBI office.

Confirm the vendor has a fix

Make sure that the vendor fixes the vulnerabilities and ensures that your information will be safe going forward, if your business decides to continue using the vendor.

Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that at *Data Breach Response: A Guide for Business*. Find it at FTC.gov/DataBreach.

LEARN MORE AT: FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

Homeland Security

CYBERSECURITY FOR
SMALL BUSINESS

HIRING A WEB HOST

You may want a new or upgraded website for your business.

But if you don't have the skills to set up the web presence you want, you may want to hire a web host provider to do it for you. Whether you're upgrading a website or launching a new business, there are many web-hosting options. When comparing services, security should be a top concern.

WHAT TO LOOK FOR

Transport Layer Security (TLS)

The service you choose should include TLS, which will help to protect your customers' privacy. (You may have heard of its predecessor, Secure Sockets Layer, or SSL.) TLS helps make sure that your customers get to your real website when they type your URL into the address bar. When TLS is correctly implemented on your website, your URL will begin with https://.

TLS also helps make sure the information sent to your website is encrypted. That's especially important if you ask customers for sensitive information, like credit card numbers or passwords.

Email authentication

Some web host providers let you set up your company's business email using your domain name (that's part of your URL, and what you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. If you don't have email authentication, scammers can impersonate that domain name and send emails that look like they're from your business.

When your business email is set up using your company's domain name, make sure that your web host can give you these three email authentication tools:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

CYBERSECURITY FOR

SMALL BUSINESS

WHAT TO LOOK FOR

Software updates

Many web host providers offer pre-built websites or software packages designed to make it quick and easy to set up your company's website. As with any software, it is essential that you use the latest versions with up-to-date security patches. Make sure you know how to keep the website's software up to date, or whether the web host provider will do this for you.

Website management

If a web host provider is managing your website, you may have to go through that provider to make any changes — though you may be able to log in and make some changes yourself. Some web host providers may instead offer you the option of managing the website on your own. It's important to clarify from the beginning who will manage the website after it's built.

WHAT TO ASK

When you're hiring a web host provider, ask these questions to make sure you're helping protect your customer information and your business data.

- ☐ Is TLS included in the hosting plan? paid add-on? Will I set it up myself or will you help me set it up?
- ☐ Can my business email use my business website name? If so, can you help me set up SPF, DKIM, and DMARC email authentication technology? (If not, consider looking for a provider that does.)
- ☐ Are the most up-to-date software versions available with your service, and will you keep software updated? If it's my responsibility to keep software updated, is it easy for me to do?
- ☐ After the website is set up, who will be able to make changes to it? Will I have to go through you? Will I be able to log in and make changes on my own? If I can log in to make changes, is multi-factor authentication available?

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration

CYBERSECURITY FOR
SMALL BUSINESS

SECURE REMOTE ACCESS

Employees and vendors may need to connect to your network remotely.

Put your network's security first. Make employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routine.

HOW TO

PROTECT DEVICES

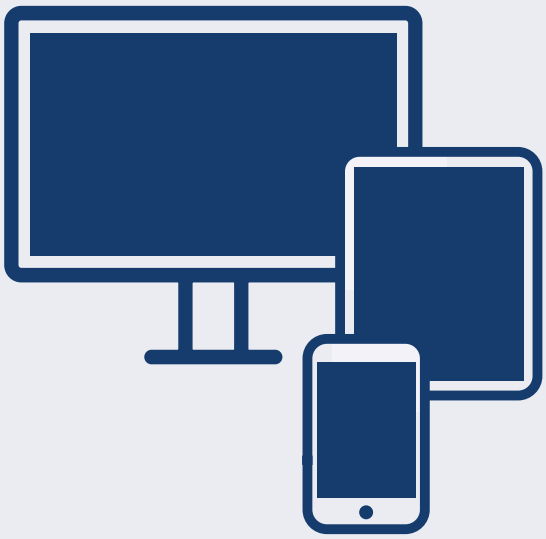
Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and make sure your employees and vendors do as well:

Always change any pre-set router passwords and the default name of your router. And keep the router's software up to date; you may have to visit the router's website often to do so.

Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it's lost or stolen. This is especially important if the device stores any sensitive personal information.

Change smartphone settings to stop automatic connections to public Wi-Fi.

Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.



LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CYBERSECURITY FOR

SMALL BUSINESS

HOW TO CONNECT REMOTELY TO THE NETWORK

Require employees and vendors to use secure connections when connecting remotely to your network. They should:

Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can't read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

WHAT TO DO TO MAINTAIN SECURITY

Train your staff:

Include information on secure remote access in regular trainings and new staff orientations.

Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

Before letting any device — whether at an employee's home or on a vendor's network — connect to your network, make sure it meets your network's security requirements.

Tell your staff about the risks of public Wi-Fi.

Give your staff tools that will help maintain security:

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.
- Consider creating a VPN for employees to use when connecting remotely to the business network.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it's separate from and not connected to your business network.
- Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration