Chapter 2

Cyberattacks, Cybersecurity, and Cyber Law

The Threat Landscape

- The security of data and information systems used in business is of utmost importance
- Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption
- Although the need for security is obvious, it must often be balanced against other business needs; A number of complex trade-offs for making decisions regarding IT security are:
  - How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)

The Threat Landscape

  - What should be done if recommended computer security safeguards make conducting business more difficult for customers and employees, resulting in lost sales and increased costs?
  - If a firm is a victim of a cybercrime, should it pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform affected customers, or take some other action?
- The number of cybercrimes being committed continues to grow and the destructive impact of these crimes is also intensifying on brands, reputation, and earnings; As a result, organizations are putting in place a range of countermeasures to combat cybercrime

The Threat Landscape

- **Why Computer Incidents Are So Prevalent?**
  - A number of factors that have caused a dramatic increase in the number, variety, and severity of security incidents are given below:
  - **Increasing Complexity Increases Vulnerability:**
    - Computing environments have become enormously complex; Cloud computing, networks, computers, mobile devices, virtualization, operating systems, applications, websites, switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code and are becoming complex every day
    - The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches

The Threat Landscape

- **Expanding and Changing Systems Introduce New Risks:**
  - Personal computers and mobile devices connect to networks with millions of other computers, all capable of sharing information
  - Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and interorganizational information systems
  - Information technology has become ubiquitous and necessary tool for organizations to achieve their goals; However, it is increasingly difficult for organizations to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them

The Threat Landscape

– **Increasing Prevalence of BYOD Policies:**

- Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet
- This practice may raises many potential security issues when they use such devices for browsing websites, shopping, visiting social networks, and blogging that exposes them to malware that may then be spread throughout the company
- In addition, many users do not use password or set the timeout to automatically lock the device; All these activities may create security problems

The Threat Landscape

- **Growing Reliance on Commercial Software with Known Vulnerabilities:**
  - An exploit is an attack on an information system that takes advantage of a particular system vulnerability; Often this attack is due to poor system design or implementation
  - Once the vulnerability is discovered, software developers create and issue a “fix,” or patch, to eliminate the problem; Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the web; Any delay in installing a patch exposes the user to a potential security breach

The Threat Landscape

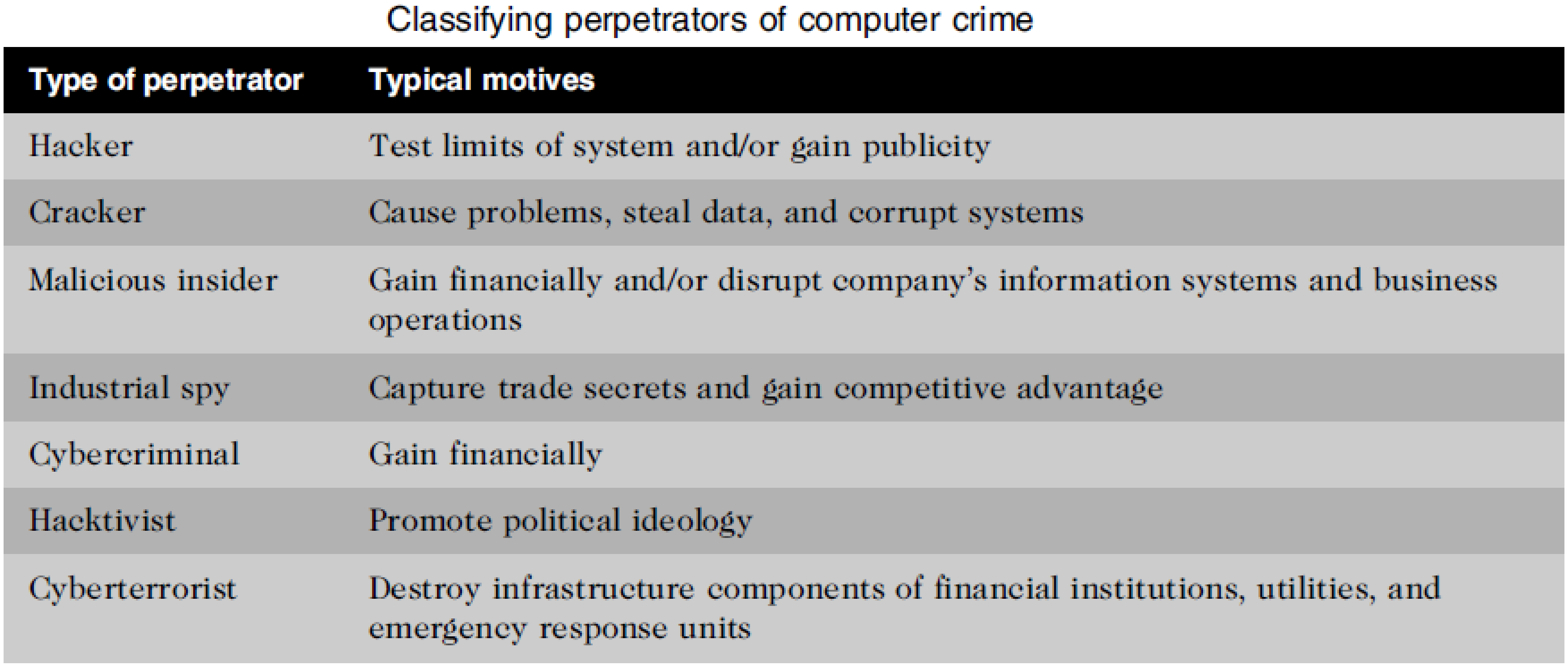
- Clearly, it can be difficult to keep up with all the required patches to fix these vulnerabilities, and U.S. companies increasingly rely on commercial software with known vulnerabilities
- Even when vulnerabilities are exposed, many corporate IT organizations prefer to use already installed software as is rather than implement security fixes that will either make the software harder to use or eliminate “nice-to-have” features that will help sell the software to end users

The Threat Landscape

- **Increasing Sophistication of Those Who Would Do Harm:**
  - Previously, a computer troublemaker was armed with specialized, but limited, knowledge of computers and networks and used rudimentary tools, perhaps downloaded from the Internet, to execute exploits
  - While such individuals still exist, today's computer menace is much better organized and may be part of an organized group that has an agenda and targets specific organizations and websites; Some of these groups have ample resources, including money and sophisticated tools to support their efforts.
  - Today's computer attacker has greater depth of knowledge and expertise in getting around computer and network security safeguards

The Threat Landscape

– The table below summarizes the types of perpetrators of computer mischief, crime, and damage



Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

The Threat Landscape

- **Types of Exploits:**
  - There are numerous types of computer attacks, with new varieties being invented all the time
  - Some of the more common attacks are: ransomware, viruses, worms, Trojan horses, blended threats, spam, distributed denial-of-service (DDoS) attacks, rootkits, advanced persistent threats, phishing and spear phishing, smishing and vishing, cyberespionage, and cyberterrorism
  - Such exploits are more common to smartphones because smartphone users store an array of personal identity information including credit card numbers and bank account numbers and are used to surf the web and transact business electronically

The Threat Landscape

- **Ransomware:**
  - Ransomware is malware that stops you from using your computer or accessing your data (encrypt data) until you meet certain demands, such as paying a ransom or sending photos to the attacker
  - A computer becomes infected with ransomware when a user opens an email attachment containing the malware or is lured to a compromised website by a deceptive email or pop-up window
  - Ransomware can also be spread through removable USB drives or by texting applications such as Yahoo Messenger, with the payload disguised as an image

The Threat Landscape

- **Viruses:**
  - Computer virus has become an umbrella term for many types of malicious code
  - Technically, a virus is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner; For example, a virus may be programmed to display a certain message on an infected computer's display screen, delete or modify a certain document, or reformat the hard drive.
  - Almost all viruses are attached to a file, meaning the virus executes only when the infected file is opened
  - A virus is spread to other machines when an infected file is shared or an email is sent with a virus-infected attachment

The Threat Landscape

- **Macro viruses** have become a common and easily created form of virus; Attackers use an application macro language (such as Visual Basic or VBScript) to create programs that infect documents and templates; After an infected document is opened, the virus is executed and infects the user’s application templates; Macros can insert unwanted words, numbers, or phrases into documents or alter command functions; After a macro virus infects a user’s application, it can embed itself in all future documents created with the application

The Threat Landscape

- **Worms:**
  - Unlike a computer virus, which requires users to spread infected files to other users, a worm is a harmful program that resides in the active memory of the computer and duplicates itself
  - Worms differ from viruses in that they can propagate without human intervention, often sending copies of themselves to other computers by email
  - A worm is capable of replicating itself on your computer so that it can potentially send out thousands of copies of itself to everyone in your email address book, for example

The Threat Landscape

- The negative impact of a worm attack on an organization’s computers can be considerable
  - lost data and programs
  - lost productivity due to workers being unable to use their computers
  - additional lost productivity as workers attempt to recover data and programs
  - lots of effort for IT workers to clean up the mess and restore everything to as close to normal as possible
- The cost to repair the damage done by worms is very high

The Threat Landscape

- **Trojan Horses:**
  - A Trojan horse is a seemingly harmless program in which malicious code is hidden; The receiving end is usually tricked into opening it because it appears to be useful software from a legitimate source, such as an update for software, screen savers, greeting card systems, and games
  - The Trojan house may destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords, or spy on users by recording keystrokes and transmitting them to a server operated by a third party
  - A Trojan horse often creates a “backdoor” that enables an attacker to gain future access to computer system and compromise confidential or private information

The Threat Landscape

- A Trojan horse can be delivered via an email attachment, downloaded to a user’s computer when he or she visits a website, or contracted via a removable media device
- Once an unsuspecting user executes the program that hosts the Trojan horse, the malicious payload is automatically launched
- One type of Trojan horse is a logic bomb, which executes when it is triggered by a specific event; For example, logic bombs can be triggered by a change in a particular file, by typing a specific series of keystrokes, or at a specific time or date

The Threat Landscape

- **Blended Threat:**
  - A blended threat is a sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload
  - A blended threat attack might use server and Internet vulnerabilities to initiate and then transmit and spread an attack on an organization’s computing devices
  - Rather than launching a narrowly focused attack on specific files, a blended threat might attack multiple files with different file types

The Threat Landscape

- **Spam:**
  - Email spam is the use of email systems to send unsolicited email to large numbers of people
  - Most spam is a form of low-cost commercial advertising, sometimes for questionable products such as pornography, phony get-rich-quick schemes, and worthless stock
  - Spam is also an extremely inexpensive marketing tool used by many legitimate organizations; For example, a company might send email to a broad cross section of potential customers to announce the release of a new product in an attempt to increase initial sales
  - Spam is also used to deliver harmful worms and other malware

The Threat Landscape

- Email campaigns are faster and cheaper but give negative reaction to public receiving unsolicited ads
- Spam forces unwanted and often objectionable material into email boxes, detracts from the ability of recipients to communicate effectively due to full mailboxes and relevant emails being hidden among many unsolicited messages, and costs Internet users and service providers millions of dollars annually; It takes user’s time to scan and delete spam email
- There is an even more sinister side to spam – often it is used to entice unsuspecting recipients to take actions that will result in malware being downloaded to their computer

The Threat Landscape

- The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** states that it is legal to spam, provided the messages meet a few basic requirements – spammers cannot disguise their identity, the email must include a label to specify an ad or a solicitation, and the email must include a way for recipients to indicate that they do not want future mass mailings
- Spammers can sign up thousands of email accounts by launching a coordinated bot attack and use these accounts to send thousands of untraceable email messages for free; We can use of CAPTCHA to ensure that only humans obtain free accounts; CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) software generates and grades tests that humans can pass

The Threat Landscape

- **DDoS Attack:**
  - A **distributed denial-of-service (DDoS) attack** is one in which a malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - **Botnet** is a very large group of such computers (called **zombies**) which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners; The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers
  - A DDoS attack does not involve infiltration of the targeted system; Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in

The Threat Landscape

- The software required to initiate a DDoS is simple to use, and many DDoS tools are readily available at a variety of hacker sites; In a DDoS attack, a tiny program is downloaded secretively from the attacker’s computer to dozens, hundreds, or even thousands of computers all over the world
- The target computers become so overwhelmed by requests for service that legitimate users are unable to get through to the target computer

The Threat Landscape

– **Rootkit:**

- A **rootkit** is a set of programs that enables its user to gain administrator-level access to a computer without the end user’s consent or knowledge
- Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators
- Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer’s configuration
- Rootkits are one part of a type of blended threat that consists of a dropper, a loader, and a rootkit; The dropper code gets the rootkit installation started; The dropper launches the loader program and then deletes itself; The loader loads the rootkit into memory

The Threat Landscape

- Rootkits are designed so cleverly that it is difficult even to discover if they are installed on a computer; The following are some symptoms of rootkit infections:
  - The computer locks up or fails to respond to input from the keyboard or mouse
  - The screen saver changes without any action on the part of the user
  - The taskbar disappears
  - Network activities function extremely slowly
- When it is determined that a computer has been infected with a rootkit, there is little to do but reformat the disk, reinstall the operating system and all applications, and reconfigure the user’s settings, such as mapped drives

The Threat Landscape

- **Advanced Persistent Threat (APT) :**
  - An **advanced persistent threat (APT)** is a network attack in which an intruder gains access to a network and stays there – undetected – with the intention of stealing data over a long period of time (weeks or even months)
  - Attackers in an APT must continuously rewrite code and employ sophisticated evasion techniques to avoid discovery
  - APT attacks target organizations with high-value information, such as banks and financial institutions, government agencies, and insurance companies with the goal of stealing data rather than disrupting services

The Threat Landscape

- An APT attack uses five phases:
  1. **Reconnaissance** – The intruder begins by conducting reconnaissance on the network to gain useful information about the target (security software installed, computing resources connected to the network, number of users)
  2. **Incursion** – The attacker next launches incursions to gain access to the network at a low level; After gaining entrance, the attacker establishes a back door, or a means of accessing a computer program that bypasses security mechanisms
  3. **Discovery –** The intruder now begins a discovery process to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors; These back doors enable the attacker to install bogus utilities for distributing malware that remains hidden in plain sight

The Threat Landscape

4. **Capture –** The attacker is now ready to access unprotected or compromised systems and capture information over a long period of time
5. **Export –** Captured data are then exported back to the attacker’s home base for analysis and/or used to commit fraud and other crimes

- Although APT attacks are difficult to identify, the theft of data can never be completely invisible; Detecting anomalies in outbound data is perhaps the best way for an administrator to discover that the network has been the target of an APT attack
- The hacker group Carbanak is thought to have stolen over $1 billion from banks in China, Russia, the Ukraine, and the United States through APT attack

The Threat Landscape

– **Phishing:**

- **Phishing** is the act of fraudulently using email to try to get the recipient to reveal personal data
- In a phishing scam, people get legitimate-looking emails; The requested action may involve clicking on a link to a website or opening an email attachment; These emails, lead consumers to counterfeit websites designed to trick them into reveal personal data or to download malware onto their computers
- **Spear phishing** is a variation of phishing in which the phisher sends fraudulent emails designed to look like they came from high-level executives within the organization to a certain organization's employees; It is known as spear phishing because the attack is much more precise and narrow, like the tip of a spear

The Threat Landscape

- **Smishing and Vising:**
  - **Smishing** is another variation of phishing that involves the use of texting; In a smishing scam, people receive a legitimate-looking text message telling them to call a specific phone number or log on to a website. This is often done under the guise that there is a problem with the recipient’s bank account or credit card that requires immediate attention
  - **Vishing** is similar to smishing except that the victims receive a voice-mail message telling them to call a phone number or access a website

The Threat Landscape

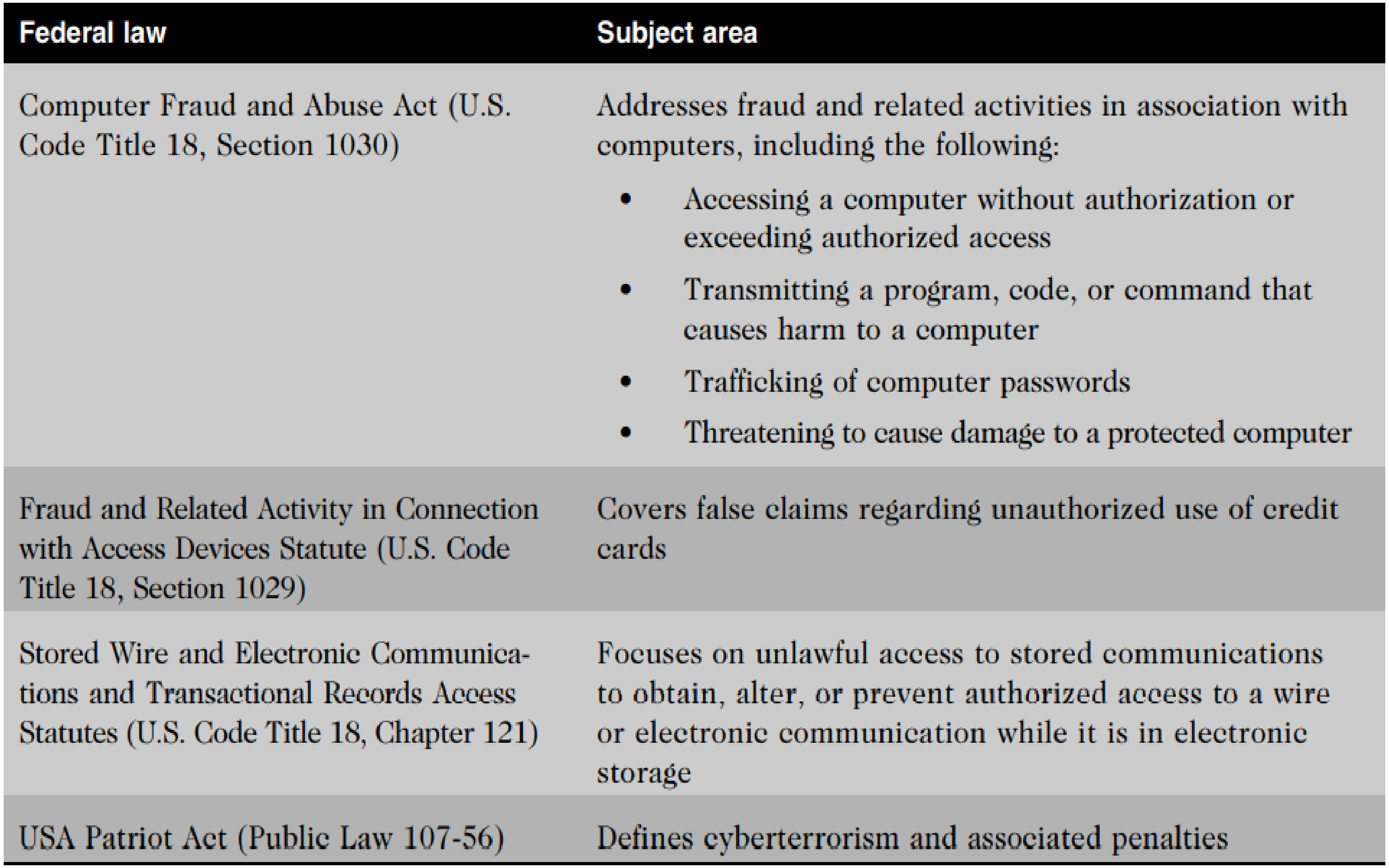
- **Cyberespionage:**
  - Involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms
  - The type of data most frequently targeted includes data that can provide an unfair competitive advantage to the perpetrator that may even be protected via patent, copyright, or trade secret such as
    - Sales, marketing, and new product development plans, schedules, and budgets
    - Details about product designs and innovative processes
    - Employee personal information and customer data
    - Sensitive information about partners and partner agreements

The Threat Landscape

- **Cyberterrorism:**
  - Cyberterrorism is the intimidation of government or civilian population by using information technology to disable critical national infrastructure (for example, energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals
  - It is an increasing concern for countries and organizations around the globe
  - Cyberterrorists try on a daily basis to gain unauthorized access to a number of important and sensitive sites

The Threat Landscape

- **Federal Laws for Prosecuting Computer Attacks:**
  - Over the years, several laws have been enacted to help prosecute those responsible for computer-related crimes



Federal law	Subject area
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Addresses fraud and related activities in association with computers, including the following: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	Covers false claims regarding unauthorized use of credit cards
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Focuses on unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage
USA Patriot Act (Public Law 107-56)	Defines cyberterrorism and associated penalties

The CIA Security Triad

- The IT security practices of organizations worldwide are focused on ensuring **confidentiality**, maintaining **integrity**, and guaranteeing the **availability** of systems and data
- **Confidentiality** ensures that only those individuals with the proper authority can access sensitive data
- **Integrity** ensures that data can only be changed by authorized individuals
- **Availability** ensures that the data can be accessed when and where needed
- Confidentiality, integrity, and availability are referred to as the **CIA security triad**

The CIA Security Triad

- **Layered Security Solution:**
  - The key to prevention of a computer security incident is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up or is detected before much harm is inflicted
  - In a layered solution, if an attacker breaks through one layer of security, another layer must then be overcome
  - Security measures must be planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels to achieve true CIA security

The CIA Security Triad

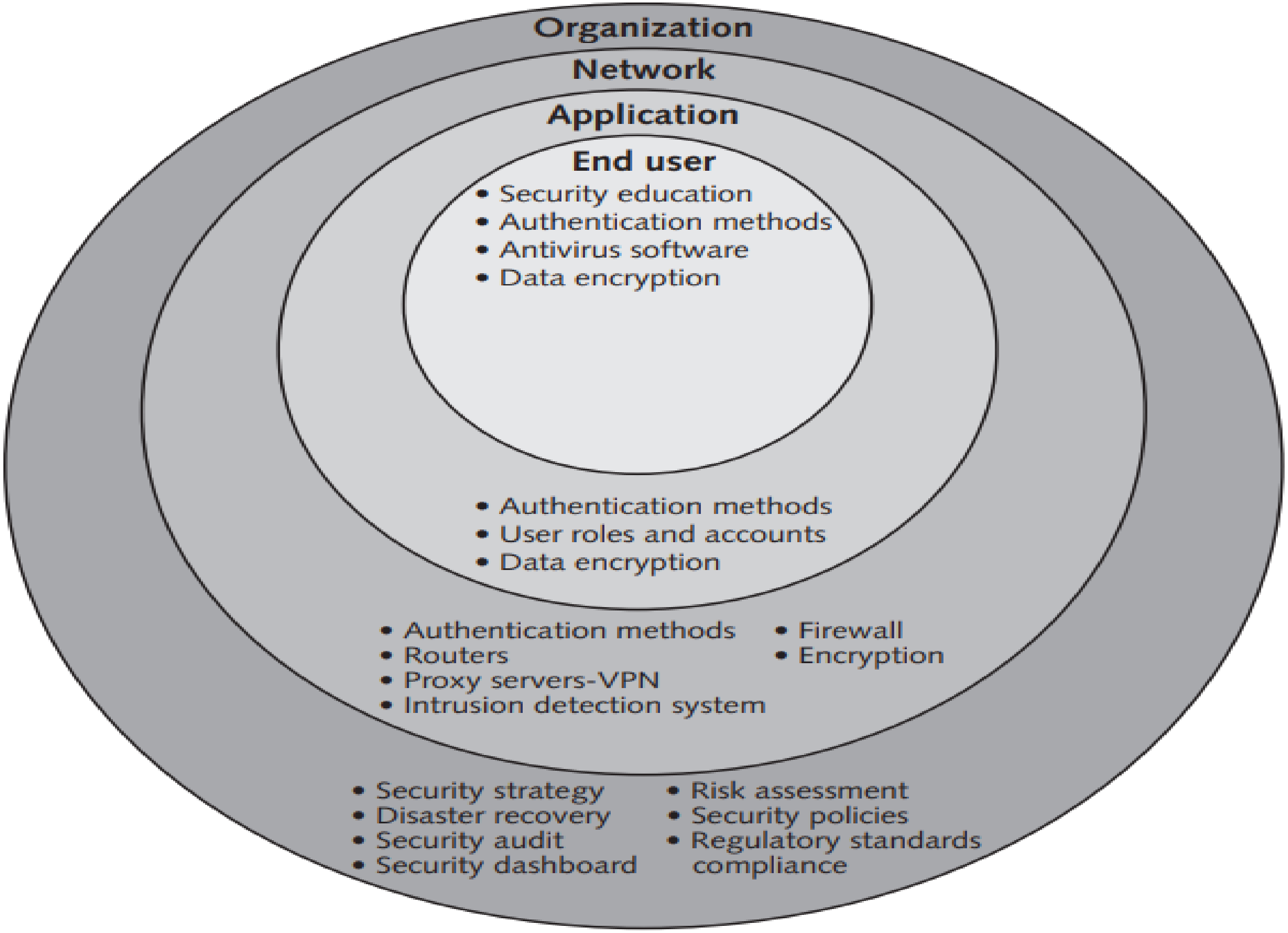


Fig: Implementing CIA security at the organization, network, application, and end-user levels

The CIA Security Triad

- **Implementing CIA at the Organizational Level:**
  - Implementing CIA begins at the organization level with the definition of an overall security strategy, performance of a risk assessment, laying out plans for disaster recovery, setting security policies, conducting security audits, ensuring regulatory standards compliance, and creating a security dashboard
  - **Security Strategy:**
    - Security strategy is the overall strategy of the organization to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack; It includes risk assessment, disaster recovery plan, security policies, security audits, regulatory standards, and security dashboard

The CIA Security Triad

- **Risk Assessment:**
  - Risk assessment is the process of assessing security-related risks to an organization’s assets like computers, networks, softwares, information systems, and databases from both internal and external threats
  - The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats
  - A loss event is any occurrence that has a negative impact on an asset
  - The steps in a general security risk assessment process are as follows:
    1. Step 1 – Identify the set of IT assets about which the organization is most concerned

The CIA Security Triad

2. Step 2 – Identify the loss events or the risks or threats that could occur
3. Step 3 – Assess the frequency of events or the likelihood of each potential threat
4. Step 4 – Determine the impact of each threat occurring
5. Step 5 – Determine how each threat can be mitigated so that it becomes much less likely to occur or, if it does occur, has less of an impact on the organization
6. Step 6 – Assess the feasibility of implementing the mitigation options
7. Step 7 – Perform a cost-benefit analysis to ensure that your efforts will be cost-effective
8. Step 8 – Make the decision on whether or not to implement a particular countermeasure

The CIA Security Triad

- **Disaster Recovery:**
  - Disasters can be natural (for example, earthquake, fire, and flood) or manmade (for example, accident, civil unrest, and terrorism)
  - Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after disaster
  - Organizations typically implement a **disaster recovery plan**, which is a documented process for recovering an organization’s business information system assets – including hardware, software, data, networks, and facilities – in the event of a disaster

The CIA Security Triad

- A disaster recovery plan identifies the people or the teams responsible to take action in the event of a disaster, what exactly these people will do when a disaster strikes, and the information system resources required to support critical business processes
- As part of defining a **business continuity plan**, an organization should conduct a business impact analysis to identify critical business processes and the resources that support them.
- If your organization is hit by a disaster, information systems that are running in the **cloud** are likely to be operational and accessible by workers from anywhere they can access the Internet

The CIA Security Triad

- If the cloud service provider is hit by a disaster, it may cause a serious business disruption; Thus, part of the evaluation of a cloud service provider must include analysis of the provider’s disaster recovery plans
- Files and databases can be protected by making a copy of all files and databases changed during the last few days or the last week, a technique called incremental backup
- Organizations can also hire outside companies to help them perform disaster planning and recovery

The CIA Security Triad

- **Security Policies:**
  - A security policy defines an organization’s security requirements, as well as the controls and sanctions needed to meet those requirements
  - A good security policy delineates responsibilities and the behavior expected of members of the organization
  - A security policy outlines what needs to be done but not how to do it; How to do are provided in separate documents and procedure guidelines
  - The SANS Institute offers a number of security-related policy templates (www.sans.org/security-resources/policies) that can help an organization to quickly develop effective security policies

The CIA Security Triad

- Automated system rules should mirror written policies whenever possible; For example, if a written policy states that passwords must be changed every 30 days, then all systems should be configured to enforce this policy automatically
- System administrators must also be vigilant about changing the default usernames and passwords for specific devices (such as Wi-Fi routers) when they are added to an organization’s network
- Mobile devices should be used with special security requirements to access corporate email, store confidential data, and run critical applications; Laptops and mobile devices must use a VPN to gain access to their corporate network

The CIA Security Triad

- **Security Audits:**
  - Security audit evaluates whether an organization has a well-considered security policy in place and if it is being followed
  - The audit should also review who has access to particular systems and data and what level of authority each user has
  - One result of a good audit is a list of items that needs to be addressed in order to ensure that the security policy is being met
  - Security audit should also test system safeguards to ensure that they are operating as intended
  - Some organizations will also perform a penetration test to check for exploitable vulnerability

The CIA Security Triad

- **Regulatory Standards Compliance:**
  - Organization are required to comply with one or more standards defined by external parties
  - Organization’s security program must include a definition of what those standards are and how the organization will comply
  - For example, Health Insurance Portability and Accountability Act (Public Law 104–191), Sarbanes-Oxley Act (Public Law 107–204 116 Stat. 745)

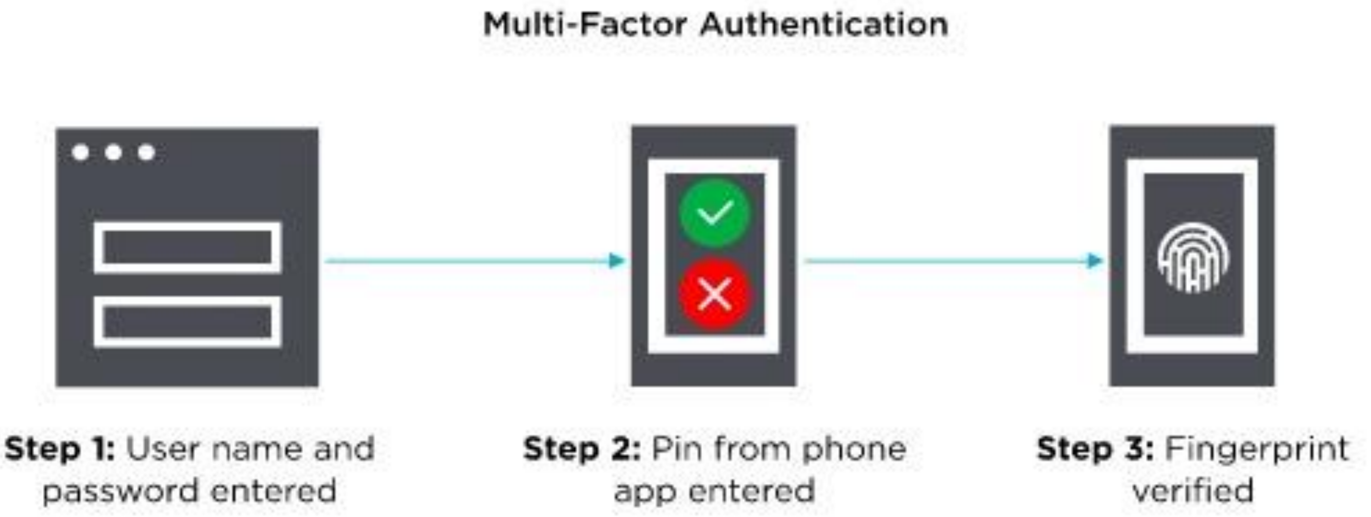
The CIA Security Triad

- **Security Dashboard:**
  - Many organizations use security dashboard software to provide a comprehensive display of all key performance indicators related to an organization's security defenses, including threats, exposures, policy compliance, and incident alerts
  - The purpose of a security dashboard is to reduce the effort required to monitor and identify threats in time to take action
  - Data that appear in a security dashboard can come from a variety of sources, including security audits, firewalls, applications, servers, and other hardware and software devices

The CIA Security Triad

- **Implementing CIA at the Network Level:**
  - Organizations must carefully manage the security of their networks and implement strong measures to ensure that sensitive data are not accessible to anyone who is not authorized to see it
  - **Authentication Methods:**
    - To maintain a secure network, an organization must authenticate users attempting to access the network by requiring them to enter a username and password; inserting a smart card and entering the associated PIN; or providing a fingerprint, voice pattern sample, or retina scan
    - A number of multifactor authentication schemes can also be used

The CIA Security Triad


Multi-Factor Authentication
Step 1: User name and password entered
Step 2: Pin from phone app entered
Step 3: Fingerprint verified

- **Firewall:**
  - Installation of a corporate firewall is the most common security precaution taken by businesses
  - A firewall is a system of software, hardware, or a combination of both that stands guard between an organization’s internal network and the Internet and limits internal network access based on the organization’s access policy from outside

The CIA Security Triad

- Most firewalls can be configured so that internal network users can be blocked from gaining access to websites deemed inappropriate for employees
- Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities
- A **next-generation firewall (NGFW)** is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by filtering network traffic dependent on the packet contents; Compared to first- and second-generation firewalls, a NGFW goes deeper to inspect the content of packets and match sequences of bytes for harmful activities, such as known vulnerabilities, exploit attacks, viruses, and malware

The CIA Security Triad

- **Routers:**
  - A router is a networking device that connects multiple networks together and forwards data packets from one network to another; An ISP installs router to connect the ISP’s network to home network
  - Routers enable you to create a secure network by assigning it a passphrase so that only individuals who have the passphrase can connect to your network
  - As an additional layer of security, the router also provides you the capability to specify the unique media access control (MAC) address of each legitimate device connected to the network and restrict access to any other device that attempts to connect to the network
  - Most routers also have an option to restrict access to specific websites, thus blocking access to websites that are known to infect user devices with malware

The CIA Security Triad

- **Encryption:**
  - **Encryption** is the process of scrambling messages or data in such a way that only authorized parties can read it
  - It enables organizations to share and keep sensitive data secure
  - An **encryption key** is a value that is applied (using an algorithm) to a set of unencrypted text (plaintext) to produce encrypted text that appears as a series of seemingly random characters (ciphertext) that is unreadable by those without the encryption key needed to decipher it
  - There are two types of encryption algorithms: **symmetric** and **asymmetric**.

The CIA Security Triad

- **Symmetric algorithms** use the same key for both encryption and decryption; **Advanced Encryption Standard (AES)** is the most widely used symmetric algorithm; Wireless Protected Access 2 (WPA2), which is the most commonly used security protocol for wireless networks today, employs the AES encryption algorithm
- **Asymmetric algorithms** use one key for encryption and a different key for decryption; **RSA** algorithm invented by Rivest, Shamir and Adleman is the most widely used asymmetric algorithm
- The ability to keep encrypted data secret is not determined by the encryption algorithm, which is widely known, but rather on the encryption key; In general, the longer the key, the stronger the encryption

The CIA Security Triad

- Many online shoppers fear the theft of their credit card numbers and banking information; To help prevent this type of theft, the **Transport Layer Security (TLS)** communications protocol is used to secure sensitive data; TLS ensures privacy between communicating applications and their users on the Internet; TLS enables a client (such as a web browser) to initiate a temporary, private conversation with a server (such as an online shopping site or bank); Before the client and server start communicating, they perform an automated process called a “handshake” during which they exchange information about who they are and which secret codes and algorithms they will use to encode their messages to each other; Then, for the duration of the conversation, all the data that pass between the client and server is encrypted

The CIA Security Triad

– **Proxy Servers and Virtual Private Networks:**

  - A proxy server serves as an intermediary between a web browser and another server on the Internet that makes requests to websites, servers, and services
  - The request of the website from you is forwarded to the proxy server, which relays the request to the server; The website is returned to the proxy server, which then passes it on to you; Thus the website sees the proxy server as the actual visitor and not you
  - By forcing employees to access the Internet through a proxy server, companies can prevent employees from accessing certain websites
  - A proxy server can also capture detailed records of all the websites each employee has visited, when, and for how long

The CIA Security Triad

- A proxy server thus can hide your IP address and block cookies from being sent to your device
- A VPN enables remote users to securely access an organization’s collection of computing and storage devices and share data remotely through Internet
- To connect to a VPN, you launch a VPN client on your computer and perform some form of authentication using your credentials
- Your computer then exchanges keys to be used for the encryption process with the VPN server
- Once both computers have verified each other as authentic, all of your Internet communications are encrypted and secured from eavesdropping

The CIA Security Triad

- **Intrusion Detection System:**
  - An intrusion detection system (IDS) is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment
  - Such activities usually signal an attempt to breach the integrity of the system or to limit the availability of network resources
  - **Knowledge-based approaches** and **behavior-based approaches** are two fundamentally different approaches to intrusion detection

The CIA Security Triad

- **Knowledge-based IDS** contains information about specific attacks and system vulnerabilities and watch for attempts to exploit these vulnerabilities, such as repeated failed login attempts or recurring attempts to download a program to a server; When such an attempt is detected, an alarm is triggered
- A **behavior-based IDS** models normal behavior of a system and its users from reference information collected by various means; The IDS compares current activity to this model and generates an alarm if it finds a deviation; For example, unusual traffic at odd hours

The CIA Security Triad

- **Implementing CIA at the Application Level:**
  - *Authentication methods*, *user roles and accounts*, and *data encryption* are key elements of the application security layer
  - These elements must be in place to ensure that only authorized users have access (with their defined roles and responsibilities) to the organization’s applications and data
  - **Authentication Methods:**
    - For many applications, users are required to enter username and password as a form of single-factor authentication
    - Two-factor authentication requires the user to provide two types of credential

The CIA Security Triad

– **User Roles and Accounts:**

  - Another important safeguard at the application level is the creation of roles and user accounts
  - Once users are authenticated, they have the authority to perform their responsibilities and nothing more
  - Even within one department, not all members should be given the same capabilities
  - An effective system administrator will identify the similarities among users and create profiles associated with these groups

– **Data Encryption:**

  - Data encryption should be used within applications to ensure that the sensitive data are protected from unauthorized access

The CIA Security Triad

- **Implementing CIA at the End User Level:**
  - *Security education*, *authentication methods*, *antivirus software*, and *data encryption* must all be in place to protect the individual end-user
  - **Security Education:**
    - Creating and enhancing user awareness of security policies is an ongoing security priority for companies
    - Users must be educated about the importance of security so that they will be motivated to understand and follow security policies
    - Users must help protect an organization's information systems and data by doing the following:
      - ➢ Guarding their passwords to protect against unauthorized access to their accounts

The CIA Security Triad

    - Prohibiting others from using their passwords
    - Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
    - Reporting all unusual activity to the organization’s IT security group
    - Taking care to ensure that portable computing and data storage devices are protected (hundreds of thousands of laptops are lost or stolen per year)

- **Authentication Methods:**
  - End users should be required to implement a security passcode that must be entered before their computing/communications device accepts further input
  - Again, a number of multifactor authentication schemes can be used

The CIA Security Triad

- **Antivirus Software:**
  - Good antivirus software installed on user’s computer checks vital system files when the system is booted up, monitors the system continuously for virus-like activity, scans disks, scans memory when a program is run, check programs when they are downloaded, and scans email attachments before they are opened
  - If finds a virus, it informs the user, and it may clean, delete, or quarantine any files, directories, or disks affected by the malicious code; Antivirus software must be continually updated with the latest virus signatures
- **Data Encryption:**
  - If you have sensitive information on your computer, you need to employ full-disk encryption, which protects all your data even if your hardware falls into the wrong hands

Response to Cyberattack

- An organization should be prepared for the attack that defeats all or some of a system’s defenses and damages data and information systems
- A response plan should be developed well in advance of any incident and be approved by both the organization’s legal department and senior management; A well-developed response plan helps keep an incident under technical and emotional control
- In a security incident, the primary goal must be to regain control and limit damage, not to attempt to monitor or catch an intruder

Response to Cyberattack

- **Incident Notification:**
  - A key element of any response plan is to define who to notify and who not to notify in the event of a computer security incident such as
    - Within the company, who needs to be notified, and what information does each person need to have?
    - Under what conditions should the company contact major customers and suppliers?
    - How does the company inform them of a disruption in business without unnecessarily alarming them?
    - When should local authorities or the FBI be contacted?
  - Most security experts recommend against giving out specific information about a compromise in public forums

Response to Cyberattack

- A critical ethical decision that must be made is what to tell customers and others whose personal data may have been compromised by a computer incident; Many organizations are tempted to conceal such information for fear of bad publicity and loss of customers; A number of laws have been passed to force organizations to reveal such information

- **Protection of Evidence and Activity Logs:**
  - An organization should document all details of a security incident as it works to resolve the incident
  - Documentation captures valuable evidence for a future prosecution and provides data to help during the incident eradication and follow-up phases

Response to Cyberattack

  - It needs to capture all system events, the specific actions taken (what, when, and who), and all external conversations (what, when, and who) in a logbook; An organization should establish a set of document-handling procedures using the legal department as a resource because this may become court evidence

- **Incident Containment:**
  - It is necessary to act quickly to control the attack and to keep a bad situation from becoming even worse
  - The incident response plan should clearly define the process for deciding if an attack is dangerous enough; How such decisions are made, how fast they are made, and who makes them are all elements of an effective response plan

Response to Cyberattack

- **Eradication:**
  - Before the IT security group begins the eradication effort, it must collect and log all possible criminal evidence from the system and then verify that all necessary backups are current, complete, and free of any malware
  - Creating a forensic disk image of each compromised system on write-only media both for later study and as evidence can be very useful
  - After virus eradication, a new backup must be created.
  - Throughout this process, a log should be kept of all actions taken

Response to Cyberattack

- **Incident Follow-Up:**
  - Determine how the organization’s security was compromised so that it does not happen again
  - A review should be conducted after an incident to determine exactly what happened and to evaluate how the organization responded; One approach is to write a formal incident report; The key elements of a formal incident report should include the following:
    - IP address and name of host computer(s) involved
    - The date and time when the incident was discovered
    - How the incident was discovered
    - The method used to gain access to the host computer
    - A detailed discussion of vulnerabilities that were exploited

Response to Cyberattack

    - A determination of whether or not the host was compromised as a result of the attack
    - The nature of the data stored on the computer (customer, employee, financial, etc.)
    - A determination of whether the accessed data are considered personal, private, or confidential
    - The number of hours the system was down
    - The overall impact on the business
    - An estimate of total monetary damage from the incident
    - A detailed chronology of all events associated with the incident
- Develop an estimate of the monetary damage
- Estimate amount of effort that should be put into capturing the perpetrator

Response to Cyberattack

  - The potential for negative publicity must also be considered
  - Organization must consider whether it has an ethical or a legal duty to inform customers or clients of a cyberattack that may have put their personal data or financial resources at risk

- **Using Managed Security Service Provider (MSSP):**
  - For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations is too costly
  - As a result, many organizations outsource their network security operations to a MSSP, which is a company that monitors, manages, and maintains computer and network security for organizations

Response to Cyberattack

- **Computer Forensics:**
  - Computer forensics is a discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law
  - Computer forensics investigators work as a team to investigate an incident and conduct forensic analysis by using various methodologies and tools
  - Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in court

Response to Cyberattack

- Computer forensics investigation requires extensive training and certification and knowledge of laws that apply to gathering of criminal evidence; Numerous certifications relate to computer forensics are CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensics Analyst)
- Numerous universities offer degrees specializing in computer forensics; Such degree programs should include training in accounting, particularly auditing, as this is very useful in the investigation of cases involving fraud

Cyber Law

- The computer-generated world of internet is known as **cyberspace** and the laws prevailing this area are known as **Cyber laws** and all the users of this space come under the ambit of these laws as it carries a kind of worldwide jurisdiction
- Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology; In short, cyber law is the law governing computers and the internet
- Cyber law consists of rules that dictate how people and companies should use the internet and computers

Cyber Law

- Cyber law is important because it touches almost all aspects of transactions and activities involving the internet, World Wide Web and cyberspace
- Cyber law encompasses laws relating to:
  - Cyber crimes
  - Electronic and digital signatures
  - Intellectual property
  - Data protection and privacy