Unit 2: Cyberattacks, Cybersecurity, and Cyber Law

Contents:

2.1 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.
- Business managers, IT professionals, and IT users all face a number of complex trade-offs when making decisions regarding IT security, such as the following:
  i) How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)
  ii) 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?
  iii) 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 against individuals, organizations, and governments continues to grow, and the destructive impact of these crimes is also increasing.
- The brands, reputation, and earnings of many organizations around the world have been negatively impacted by such crimes. As a result, organizations are putting in place a range of countermeasures to combat cybercrime.

For instance, the worldwide financial services industry spent $27.4 billion on IT security and fraud prevention in 2015. And a recent survey of more than 10,000 IT professionals around the world revealed the following:

- 58 percent of global companies have an overall security strategy
- 54 percent have a chief information security officer (CISO) in charge of security
- 53 percent have employee security awareness and training programs
- 52 percent have security standards for third parties
- 49 percent conduct threat assessments
- 48 percent actively monitor and analyze security intelligence

In spite of all these countermeasures, however, the number of computer security incidents surged from 2014 to 2015 in the following industries: public sector organizations; entertainment, media, and

communications; technology and telecommunications companies; pharmaceuticals and life sciences; and power and utilities organizations.

Why Computer Incidents Are So Widespread?

Increasing computing complexity, expanding and changing systems, an increase in the popularity of bring your own device (BYOD) policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.

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. This environment continues to increase in complexity every day. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.

Expanding and Changing Systems Introduce New Risks: Business has moved from an era of stand-alone computers, in which critical data were stored on an isolated mainframe computer in a locked room, to an era in which 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 inter-organizational information systems. Information technology has become ubiquitous and is a necessary tool for organizations to achieve their goals.

However, it is increasingly difficult for IT 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.

Increasing Popularity of BYOD Policies: Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access company computing resources and applications, including email, corporate databases, the corporate intranet, and the Internet.

Supporters of BYOD say it improves employee's productivity by allowing workers to use devices with which they are already familiar—while also helping to create an image of a company as a flexible and progressive employer.

Most companies have found they cannot entirely prevent employees from using their own devices to perform work functions. However, this practice raises many potential security issues as it is highly likely that such devices are also used for non-work activity (browsing websites, shopping, visiting social networks, blogging, etc.) that exposes them to malware much more frequently than a device used strictly for business purposes. That malware may then be spread throughout the company. In addition, many users do not password protect their laptops, tablets, and smartphones or set the timeout to automatically lock the device after a few minutes of not being used. All these create an environment ripe for potential security problems.

Growing Reliance on Commercial Software with Known Vulnerabilities: In computing, 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 need to install a fix to prevent a hacker from taking advantage of a known system vulnerability can create a time-management dilemma for system support personnel trying to balance a busy work schedule. Should they install a patch that, if left uninstalled, could lead to a security breach, or should they complete assigned project work so that the anticipated project savings and benefits from the project can begin to accrue on schedule?

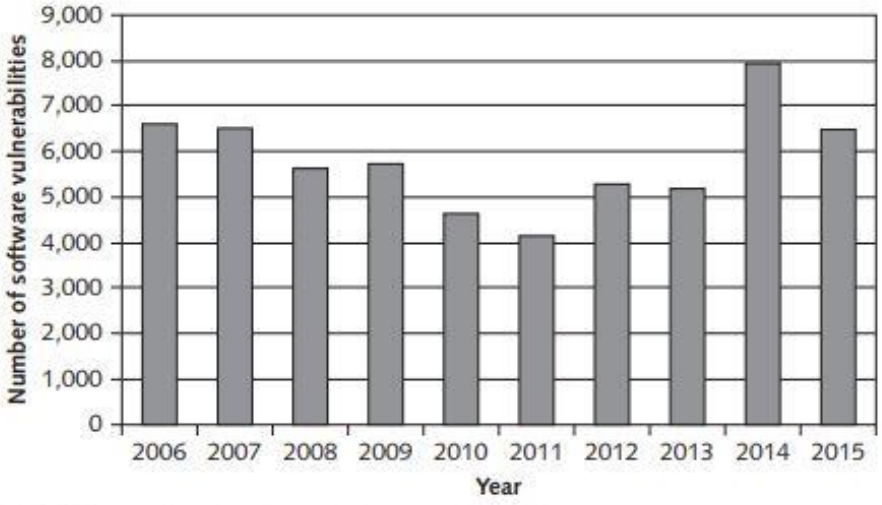


FIGURE 3-1 Total number of software vulnerabilities
Source: National Vulnerability Database

According to the National Vulnerability Database (the U.S. government repository of standards-based vulnerability management data), the number of new software vulnerabilities identified in 2015 dropped 18 percent from the previous year to 6,480.

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.

Increasing Sophistication of Those Who Would Do Harm: Previously, the stereotype of a computer troublemaker was that of an introverted "geek" working on his or her own and motivated by the desire to gain some degree of notoriety. This individual was armed with specialized, but limited, knowledge of computers and networks and use basic tools, perhaps downloaded from the Internet, to execute his or her exploits. While such individuals still exist, it is not this stereotyped individual who is the biggest threat to IT security.

Today's computer threat is much better organized and may be part of an organized group such as:

- Anonymous
- Chaos Computer Club (Europe's largest association of hackers with 7700 registered members)

- Lizard Squad (black hat hacking group, mainly known for their claims of distributed denial-of-service attacks primarily to disrupt gaming-related services)
- TeslaTeam (TeslaTeam is currently the only virtual army in Serbia to openly launch cyber-attacks.)
- Hacker teams sponsored by national governments

These organized groups has an agenda and targets specific organizations and websites.

Some of these groups have ample resources, including fund 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.

Some of the perpetrators of computer crime are:

1. **Black Hat Hacker**: Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems).
2. **Cracker**: An individual who causes problems, steals data, and corrupts systems.
3. **Malicious Insider**: An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations.
4. **Industrial spy**: An individual who captures trade secrets and attempts to gain an unfair competitive advantage.
5. **Cybercriminal**: Someone who attacks a computer system or network for financial gain.
6. **Hacktivist**: An individual who hacks computers or websites in an attempt to promote a political ideology.
7. **Cyberterrorist**: Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units.

Types of Exploits

There are numerous types of computer attacks, with new varieties being invented all the time.

Some of the more common attacks include:

1. Ransomware,
2. viruses,
3. worms,
4. Trojan horses,
5. blended threats,
6. spam,
7. distributed denial-of-service (DDoS) attacks,
8. rootkits,
9. advanced persistent threats,
10. phishing and spear phishing,
11. smishing and vishing,
12. cyberespionage, and
13. cyberterrorism

While we usually think of such exploits being aimed at computers. However, smartphones and other devices are also targeted.

Smartphones continue to become more computer capable. Increasingly, smartphone users store an array of personal identity information on their devices, including credit card numbers and bank account numbers. Smartphones are used to surf the web and transact business electronically. The more people use their smartphones for these purposes, the more attractive these devices become as targets for cyberthieves. One form of smartphone malware runs up charges on users' accounts by automatically sending messages to numbers that charge fees upon receipt of a message.

Ransomware: It is malware that stops you from using your computer/system or accessing your 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 Messenger.

In early February 2016, Hollywood Presbyterian Medical Center was forced to shut down its computer network after hackers encrypted some of its data and demanded a ransom be paid before the data would be unlocked. Initially, the hospital refused to pay the ransom, and hospital employees were forced to resort to paper, pencil, phones, and fax machines to carry out many of their tasks, including accessing patient data. The hospital sought help from the FBI, the Los Angeles Police Department, and cybersecurity consultants, but it was unable to access the data. After a week, the hospital paid the ransom of $12,000. By February 15, access to the data was fully restored, and according to a hospital spokesperson, there was no evidence that any patient or employee data had been accessed.

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 a computer user shares an infected file or sends an email with a virus-infected attachment. In other words, viruses are spread by the action of the "infected" computer user.

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 "WM97/Resume.A" virus is a Word macro virus spread via an email message with the subject line "Resume - Janet Simons." If the email recipient clicks on the attachment, the virus deletes all data in the user's computer or mobile device.

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 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, and 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 each of the Code Red, SirCam, and Melissa worms was estimated to exceed $1 billion, with that of the Conficker, Storm, and ILOVEYOU worms totaling well over $5 billion.

Trojan Horses: A Trojan horse is a seemingly harmless program in which malicious code is hidden. A victim on the receiving end of a Trojan horse is usually tricked into opening it because it appears to be useful software from a legitimate source, such as an update for software the user currently has installed on his or her computer. The program's harmful payload might be designed to enable the hacker to 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" on a computer that enables an attacker to gain future access to the system and compromise confidential or private information. 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, such as a DVD or USB memory stick. Once an unsuspecting user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well—with no significant signs. Common host programs include screen savers, greeting card systems, and games.

Department of Homeland Security (DHS) officials say they have evidence that harmful Trojan horse malware has been planted in the software that runs much of the U.S. critical infrastructure, including oil and gas pipelines, power transmission grids, water distribution and filtration systems, and even nuclear power generation plants. DHS believes that the malware was planted by the Russians as early as 2011 as a deterrent to a U.S. cyberattack on Russia. The Trojan horse would allow unauthorized users to control or shut down key components of U.S. infrastructure remotely from their computer or mobile device.

Another 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.

Malware attacks employing logic bombs compromised some 32,000 Windows, Unix, and Linux systems at half a dozen South Korean organizations, including three major television broadcasters and two large banks. A component of the attack was "wiper" malware triggered by a logic bomb set to begin overwriting a computer's master boot record at a preset time and day.

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, using multiple modes to transport itself, including email, Internet Relay Chat (IRC), and file-sharing networks.

Compiled by: Ridip Khanal

Rather than launching a narrowly focused attack on specific EXE files, a blended threat might attack multiple EXE files, HTML files, and registry keys simultaneously.

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. However, spam is also used to deliver harmful worms and other malware.

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, a cost that can add up if they pay for Internet connection charges on an hourly basis. It also costs money for Internet service providers (ISPs) and online services to transmit spam, which is reflected in the rates charged to all subscribers.

In early 2015, Symantec, a provider of security, storage, and systems management solutions, began noticing multiple instances of short-duration, high-volume spam attacks targeting millions of users. The messages instructed recipients to click on a link to a URL, which, if done, resulted in the Trojan Infostealer.Dyranges(Dyre)" being downloaded to their computer. This Trojan is known to steal financial information.

The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act in US states that it is legal to spam, provided the messages meet a few basic requirements—spammers cannot disguise their identity by using a false return address, the email must include a label specifying that it is an ad or a solicitation, and the email must include a way for recipients to indicate that they do not want future mass mailings.

Many companies—including Google, Microsoft, and Yahoo!—offer free email services. Spammers often seek to use email accounts from such major, free, and reputable web-based email service providers, as their spam can be sent at no charge and is less likely to be blocked. Spammers can defeat the registration process of the free email services by launching a coordinated bot attack that can sign up for thousands of email accounts. These accounts are then used by the spammers to send thousands of untraceable email messages for free. A partial solution to this problem is the 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 and all but the most sophisticated computer programs cannot. For example, humans can read the distorted text but simple computer programs cannot.

DDoS Attacks: A distributed denial-of-service (DDoS) attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks. A DDoS attack does not involve penetration 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 Internet equivalent of dialing a telephone number repeatedly so that all other callers hear a busy signal. The targeted machine essentially holds the line open while waiting for a reply that never comes; eventually, the requests exhaust all resources of the target.

A DoS attack is a malicious attack caused by one computer and one Internet connection as opposed to a distributed denial-of-service **(DDoS**) attack, which involves many devices and multiple Internet connections

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 secretly from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world.

The term botnet is used to describe a large group of such computers, 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. Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second. The target computers become so overwhelmed by requests for service that legitimate users are unable to get through to the target computer.

Dyn is an Internet performance management company that provides network services including Domain Name System (DNS) services for its many clients. DNS is a large distributed database that translates the domain name you enter into your browser (for example, google.com) into the IP address of the device hosting the website for that domain name. Without DNS, your website is "invisible" to users who only know it by its domain name. Starting October 21, 2016, Dyn was hit with a series of massive DDoS attacks. Millions of users on the East coast were unable to reach the websites of Dyn's clients, including Airbnb, Amazon, Comcast, Etsy, GoFundMe, New York Times, PayPal, Shopify, and Twitter. The attack had a severe impact on the website owners, who were unable to provide customer services or generate e-commerce revenue.

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 and can be activated by clicking on a link to a malicious website in an email or opening an infected PDF file. The dropper launches the loader program and then deletes itself. The loader loads the rootkit into memory; at that point, the computer has been compromised.

Rootkits are designed so cleverly that it is difficult even to discover if they are installed on a computer. The fundamental problem with trying to detect a rootkit is that the operating system cannot be trusted to provide valid test results.

Some of the symptoms of rootkit infections are:

- 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.

This can take hours, and the user may be left with a basic working machine, but all locally held data and settings may be lost.

The "2012 rootkit virus" is a malware that deletes information from a computer and makes it impossible to run some applications, such as Microsoft Word.

The longer the rootkit is present, the more damage it causes. The virus asks users to install what appears to be a legitimate update to their antivirus software or some other application. By the time the user sees the prompt to install the software, it is too late; the computer has already been infected by the rootkit.

Advanced Persistent Threat (APT): An 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.

An APT attack advances through the following five phases:

1. Reconnaissance (Inspection)—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 (attack)—The attacker next launches incursions to gain access to the network at a low level to avoid setting off any alarms or suspicion. Some forms of spear phishing may be employed in this phase. 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.

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. The group performs a reconnaissance phase to gather data about system administrators and then uses this information to navigate through various bank systems, including ATMs, financial accounts, and money processing services. Once access to these systems is gained, the hackers steal money by transferring funds to accounts in China and the United States. They have even programmed ATMs to dispense money at specific times for collection.

Compiled by: Ridip Khanal

Phishing: It is the act of illegally using email to try to get the recipient to reveal personal data. In a phishing scam, scam artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward. The requested action may involve clicking on a link to a website or opening an email attachment. These emails, lead consumers to fake websites designed to trick them into disclosing personal data or to download malware onto their computers.

The volume of global phishing attacks is alarming. It is estimated that about 156 million phishing emails are sent each day, with 16 million of those successfully evading email filters. Of those, roughly 50 percent (or 8 million) are opened, and 800,000 recipients per day click on malicious URL links contained in the emails.

Knowledgeable users often become suspicious and refuse to enter data into the fake websites; however, sometimes just accessing the website can trigger an automatic and unnoticeable download of malicious software to a computer.

Indeed, the percentage of malicious URLs in unsolicited emails surged to an average of 10 percent in 2014. As one might guess, financial institutions such as Bank of America, Citibank, Chase, MasterCard, Visa, and Wells Fargo are among the websites that phishers spoof most frequently.

Spear phishing is a variation of phishing in which the phisher sends fraudulent emails 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 phony emails are designed to look like they came from high-level executives within the organization. Employees are directed to a fake website and then asked to enter personal information, such as name, Social Security number, and network passwords.

In early 2016, more than three dozen large and small organizations were victimized by spear phishing attacks that were designed to obtain data from employee tax records. Many of these attacks spoofed the email address of the CEO, CFO, or someone else of authority within the organization, prompting many employees to comply with the request.

Smishing and Vishing: 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. However, the phone number or website is phony and is used to trick unsuspecting victims into providing personal information such as a bank account number, personal identification number, or credit card number, which can then be used to steal money from victims' bank accounts, charge purchases on their credit cards, or open new accounts. In some cases, if victims log on to a website, malicious software is downloaded onto their smartphones, providing criminals with access to information stored on the phones. The number of smishing scams typically increases around the holidays as more people use their smartphones to make online purchases.

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. One recent vishing campaign captured the payment card information of an estimated 250 Americans per day. In the attack, users were sent a message that their ATM card had been deactivated. The users were prompted to call a phone number to reactivate the card by entering their card number and their personal identification number (PIN)—data that were recorded and then used by the criminals to withdraw money from the accounts.

Financial institutions, credit card companies, and other organizations whose customers may be targeted by criminals in this manner should be on the alert for phishing, smishing, and vishing scams. They must be prepared to act quickly and decisively, without alarming their customers if such a scam is detected. Recommended action steps for institutions and organizations include the following:

• Companies should educate their customers about the dangers of phishing, smishing, and vishing through letters, recorded messages for those calling into the company's call center, and articles on the company's website.

• Call center service employees should be trained to detect customer complaints that indicate a scam is being executed. They should attempt to capture key pieces of information, such as the callback number the customer was directed to use, details of the phone message or text message, and the type of information requested.

• Customers should be notified immediately if a scam occurs. This can be done via a recorded message for customers phoning the call center, working with local media to place a news article in papers serving the area of the attack, placing a banner on the institution's web page, and even displaying posters in bank drive-through and lobby areas.

• If it is determined that the calls are originating from within the United States, companies should report the scam to the FBI or the local security personnel's.

• Institutions can also try to notify the telecommunications carrier for the particular numbers to request that they shut down the phone number's victims are requested to call.

Cyber espionage: It 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 committer. These data are typically not public knowledge and may even be protected via patent, copyright, or trade secret.

High-value data include the following:
• Sales, marketing, and new product development plans, schedules, and budgets
• Details about product designs and innovative processes
• Employee personal information
• Customer and client data
• Sensitive information about partners and partner agreements

Tensions have long simmered between the China and the United States over alleged cyberattacks. The U.S. experts claim cyber espionage has helped China to accelerate the research and development process and cut years off the time for that country to acquire new technology in a variety of industries. Alleged targets have included aluminum and steel producers, a company that designs nuclear power plants, a solar panel manufacturer, and an aircraft manufacturer. Meanwhile, China's Foreign Ministry portrays the United States as a hypocrite that engages in cyber espionage by conducting cyber theft, wiretapping, and surveillance activities against Chinese governmental departments, companies, and universities. After years of discussion and behind-the-scenes efforts, President Obama and Chinese President Xi announced in 2015 that the two nations had agreed to initial norms of cyber activities with the two nations pledging each will avoid conducting cyber theft of intellectual property for commercial gain. United States and Chinese officials met again in May 2016 to discuss cybersecurity issues. While no details of the meeting were revealed, the United States State Department stated that "international norms of state behavior and other crucial issues for international security in cyberspace" were addressed. While a statement from China's foreign ministry reported that there was a "positive, deep and constructive discussion" between the two countries, it remains to be seen how much of an impact this agreement will have.

Cyberterrorism: It is the extortion 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.

Indeed, in a statement released by the White House in early 2015, President Obama said, "Cyber threats pose one of the gravest national security dangers that the United States faces."

The Department of Homeland Security (DHS) is a large federal agency with more than 240,000 employees and a budget of almost $65 billion whose goal is to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats." The agency was formed in 2002 when 22 different federal departments and agencies were combined into a unified, integrated cabinet agency. The agency's Office of Cybersecurity and Communications resides within the National Protection and Programs Directorate and is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure. It works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. The DHS website (www.dhs.gov) provides a link that enables users to report cyber incidents. Incident reports go to the US-CERT Incident Reporting System, which assists analysts at the U.S. Computer Emergency Readiness Team (US-CERT) (a partnership between the DHS and the public and private sectors) in providing timely handling of security incidents as well as in conducting improved analysis of such incidents. Established in 2003 to protect the nation's Internet infrastructure against cyberattacks, US-CERT serves as a clearinghouse for information on new viruses, worms, and other computer security topics.

Cyberterrorists try on a daily basis to gain unauthorized access to a number of important and sensitive sites, such as the computers at the British, French, Israeli, and U.S. foreign intelligence agencies; North American Aerospace Defense Command (NORAD); and numerous government ministries and private companies around the world.

Summary: Why are computer incidents so prevalent, and what are their effects?

- Increasing computing complexity, expanding and changing systems, an increase in the prevalence of BYOD policies, a growing reliance on software with known vulnerabilities, and the increasing sophistication of those who would do harm have caused a dramatic increase in the number, variety, and severity of security incidents.
- 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.
- Many different types of people launch computer attacks, including the black hat hacker, cracker, malicious insider, industrial spy, cybercriminal, hacktivist, and cyberterrorist. Each type has a different motivation.
- A white hat hacker is someone who has been hired by an organization to test the security of its information systems allowing the organizations to improve its defenses.
- Ransomware, viruses, worms, Trojan horses, logic bombs, blended threats, spam, DDoS attacks, rootkits, advanced persistent threats, phishing, spear phishing, smishing, vishing, cyberespionage, and cyberterrorism are among the most common computer exploits.
- The DHS has the responsibility to provide for a "safer, more secure America, which is resilient against terrorism and other potential threats." The agency's Office of Cybersecurity and Communications is responsible for enhancing the security, resilience, and reliability of U.S. cyber and communications infrastructure.
- The US-CERT is a partnership between DHS and the public and private sectors that was established to protect the nation's Internet infrastructure against cyberattacks by serving as a clearinghouse for information on new viruses, worms, and other computer security topics.
- Over the years, several laws have been enacted to prosecute those responsible for computer-related crime, including the Computer Fraud and Abuse Act, the Fraud and Related Activity in Connection with Access Devices Statute, the Stored Wire and Electronic Communications and Transactional Records Access Statutes, and the USA Patriot Act.

2.2 CIA Security Triad – Confidentiality, Integrity, Availability

The IT security practices of organizations worldwide are focused on ensuring:

1) Confidentiality,
2) Maintaining integrity, and
3) Guaranteeing the availability of systems and data.

Confidentiality ensures that only those individuals with the proper authority can access sensitive data such as employee personal data, customer and product sales data, and new product and advertising plans.

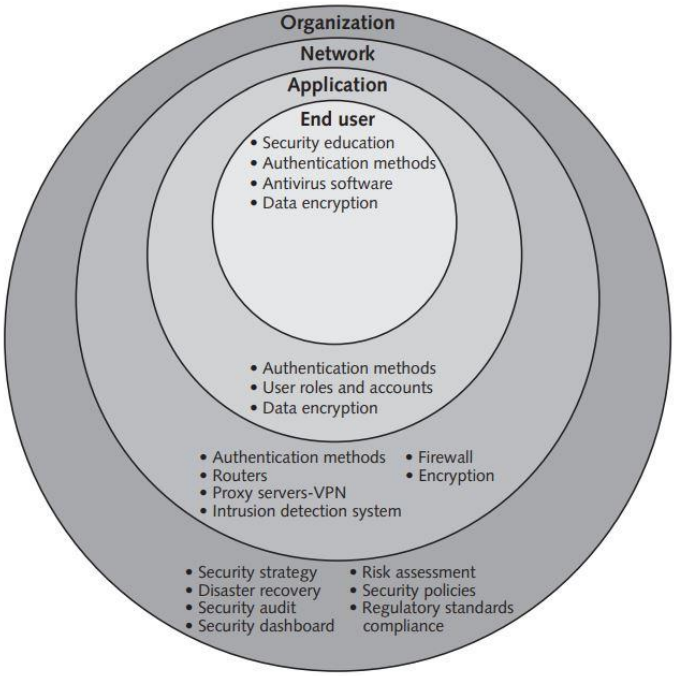
Integrity ensures that data can only be changed by authorized individuals so that the accuracy, consistency, and trustworthiness of data are guaranteed.

Availability ensures that the data can be accessed when and where needed, including during times of both normal and disaster recovery operations. A widely held but difficult-to-achieve standard of

availability for a system or product is known as “five 9s” or 99.999 percent availability. For an operation that runs 365 days per year, 24 hours per day this translates to less than one hour of unavailability per year.

Confidentiality, integrity, and availability are referred to as the CIA security triad.

No organization can ever be completely secured from an attack. 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.



Implementing CIA at the Organization 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.

Completion of these tasks at the organizational level will set a sound foundation and clear direction for future CIA-related actions.

Security Strategy

Implementing CIA security at the organization level requires a risk-based security strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack.

Creating such a strategy typically begins with

i. Performing a risk assessment to identify and prioritize the threats that the organization faces.
ii. The security strategy must define a disaster recovery plan that ensures the availability of key data and information technology assets.
iii. Security policies are needed to guide employees to follow recommended processes and practices to avoid security-related problems.
iv. Periodic security audits are needed to ensure that individuals are following established policies and to assess if the policies are still adequate even under changing conditions.
v. In addition to complying with its internal policies, an organization may also need to comply with standards defined by external parties, including regulatory agencies.
vi. Many organizations employ a security dashboard to help track the key performance indicators of their security strategy.

Risk Assessment:

Risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats. Such threats can prevent an organization from meeting its key business objectives.

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. In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives. A loss event is any occurrence that has a negative impact on an asset, such as a computer contracting a virus or a website undergoing a DDoS attack.

The steps in a general security risk assessment process are as follows:

Step 1 - Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.

Step 2 - Identify the loss events or the risks or threats that could occur, such as a DDoS attack or insider fraud.

Step 3 - Assess the frequency of events or the likelihood of each potential threat; some threats, such as insider fraud, are more likely to occur than others.

Step 4 - Determine the impact of each threat occurring. Would the threat have a minor impact on the organization, or could it keep the organization from carrying out its mission for a lengthy period of time?

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. Due to time and resource limitations, most organizations choose to focus on just those threats that have a high (relative to all other threats) probability of occurrence and a high (relative to all other threats) impact. In other words, first address those threats that are likely to occur and that would have a high negative impact on the organization.

Step 6 - Assess the feasibility of implementing the mitigation options.

Step 7 - Perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a

security breach with the cost of preventing one. The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.

Step 8 - Make the decision on whether or not to implement a particular countermeasure. If you decide against implementing a particular countermeasure, you need to reassess if the threat is truly serious and, if so, identify a less costly countermeasure.

The general security risk assessment process—and the results of that process—will vary by organization. A completed risk assessment identifies the most dangerous threats to a company and helps focus security efforts on the areas of highest payoff.

Disaster Recovery:

Data availability requires implementing products, services, policies, and procedures that ensure that data are accessible even during disaster recovery operations. To accomplish this goal, 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.

A disaster recovery plan focuses on technology recovery and 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.

Disasters can be natural (for example, earthquake, fire, and flood) or manmade (for example, accident, civil unrest, and terrorism).

When developing a disaster recovery plan, organizations should think in terms of not being able to gain access to their normal place of business for an extended period of time, possibly up to several months. 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.

The recovery time for an information system resource should match the recovery time objective for the most critical business processes that depend on that resource. Some business processes are more pivotal to continued operations and goal attainment than others. These processes are called mission-critical processes. Quickly recovering data and operations for these mission-critical processes can make the difference between failure and survival for an organization.

If your billing system doesn't work and you can't send out invoices, your company is at the risk of going out of business due to cash flow issues. Cloud computing has added another dimension to disaster recovery planning. 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.

Files and databases can be protected by making a copy of all files and databases (i.e. backup). Failover is another approach to backup. When a server, network, or database fails or is no longer functioning, failover automatically switches applications and other programs to a redundant or replicated server, network, or database to prevent an interruption of service.

It is instructed that a disaster plan be practiced and improvements be made to the plan based on the results of the test. Unfortunately, a recent survey of IT managers revealed that as many as one in eight have either never tested their organization's disaster recovery solution or have no idea exactly when it

was last tested. One reasonable approach to testing is to simulate a disaster for a single critical portion (for example, order processing or customer billing) of your business during a time of low business activity. The next disaster plan test should then target a different area of the business.

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 defines 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. The details of how to accomplish the goals of the policy are typically provided in separate documents and procedure guidelines.

The security policy typically includes:

- acceptable use policy,
- email policy,
- password protection policy,
- remote access policy, and
- software installation policy.

Experienced IT managers understand that users will often attempt to avoid security policies or simply ignore them altogether. Because of that, automated system rules should mirror an organization's written policies whenever possible. Automated system rules can often be put into practice using the configuration options in a software program.

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 alert about changing the default usernames and passwords for specific devices when they are added to an organization's network. Cybercriminals and others looking to access the networks of various organizations can easily find information online regarding the default username and password combinations for many vendors' products.

A growing area of concern for security experts is the use of wireless devices to access corporate email, store confidential data, and run critical applications, such as inventory management and sales force automation. Mobile devices such as smart phones can be susceptible to viruses and worms. However, the primary security threat for mobile devices continues to be loss or theft of the device. Cautious companies have begun to include special security requirements for mobile devices as part of their security policies.

In some cases, users of laptops and mobile devices must use a virtual private network (VPN) to gain access to their corporate network.

Security Audits:

Another important prevention tool is a security audit that evaluates whether an organization has a well-considered security policy in place and if it is being followed.

For example, if a policy says that all users must change their passwords every 30 days, the audit must check how well that policy is being implemented.

The audit should also review who has access to particular systems and data and what level of authority each user has. It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

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. A thorough security audit should also test system safeguards to ensure that they are operating as intended.

Such tests might include trying the default system passwords that are active when software is first received from the vendor. The goal of such a test is to ensure that all such known passwords have been changed. Some organizations will also perform a penetration test of their defenses. This entails assigning individuals to try to break through the measures and identify vulnerabilities that still need to be addressed. The individuals used for this test are knowledgeable and are likely to take unique approaches in testing the security measures.

Regulatory Standards Compliance:

In addition to the requirement to comply with your own security program, the organization may also be required to comply with one or more standards defined by external parties. In that case, the organization's security program must include a definition of what those standards are and how the organization will comply.

It includes the standards developed by the government authorities and industry regulators.

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.

#	Key performance measure	Goal	Actual	Status
1	Number of segregation-of-duty violations	0	2	Red
2	Number of users with weak, noncompliant passwords	<5	4	Green
3	Percentage of critical IT assets that passed penetration tests	>96%	93%	Yellow
4	Backlog of software security patches and updates	<3	3	Green
5	Number of days since last internal security audit	<90	94	Yellow
6	Percentage of employees and contractors who passed security exam	>95%	87%	Red
7	Score on last disaster-recovery test	>90%	93%	Green

Red - Immediate action required
Yellow -Caution, should be monitored
Green - OK, goal has been met

Implementing CIA at the Network Level

The Internet provides a wide-open pathway for anyone in the world to reach your organization's network. As a result, organizations are continuing to move more of their business processes to the Internet to better serve customers, suppliers, employees, investors, and business partners.

However, unauthorized network access by a hacker or offended employee can result in compromised sensitive data and severely degrade services, with a resulting negative impact on productivity and operational capability. This, in turn, can create a severe strain on relationships with customers, suppliers, employees, investors, and business partners, who may question the capability of the organization to protect its confidential information and offer reliable services.

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.

CIA can be implemented in network level by using tools/techniques like:

i. Authentication methods
ii. Firewall
iii. Routers
iv. Encryption
v. Proxy servers and virtual private networks
vi. Intrusion detection system

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;
- insert a smart card and enter the associated PIN;
- provide a fingerprint, voice pattern sample, or retina scan.

The policy makers in security system at present recommends a **two-factor authorization**. This approach adds another identity check along with the password system.

A number of multifactor authentication schemes can be used, such as biometrics, one-time passwords, or hardware tokens that plug into a USB port on the computer and generate a password that matches the one used by a bank's security system.

The use of biometric technology has been slow to develop due to cost and privacy concerns. However, MasterCard recently announced it will begin rolling out its new MasterCard Identity Check service that allows users to take an initial ID photo that will be used to create a digital map of their face, which will be stored on MasterCard's servers. When the user wants to make a payment using a smartphone, the MasterCard app will capture his or her image, which, along with a user-entered password, will be authenticated against the stored image before the transaction is approved. MasterCard's system also offers a fingerprint sensor that can be used to verify purchases.

Apple's new Apple Pay system makes use of the fingerprint sensors on newer iPhones. Consumers paying with Apple Pay, which is tied to a credit or debit card, just hold their iPhone close to the contactless reader with their finger on the Touch ID button.

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 network access based on the organization's access policy.

Any Internet traffic that is not explicitly permitted into the internal network is denied entry through a firewall. Similarly, 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. Software vendors Agnitum, Check Point, Comodo, Kaspersky, and Total Defense provide some of the top-rated firewall software used to protect personal computers. Their software provide antivirus, firewall, antispam, parental control, and phishing protection capabilities and sell for $30 to $80 per single user license.

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.

Encryption:

Encryption is the process of scrambling messages or data in such a way that only authorized parties can read it.

It is used to protect billions of online transactions each day, enabling consumers to order more than $300 billion in merchandise online and banks to route some $40 trillion in financial transactions each year.

It enables organizations to share sensitive sales data, promotion plans, new product designs, and project status data among employees, suppliers, contractors, and others with a need to know.

Encryption enables physicians and patients to share sensitive healthcare data with labs, hospitals, and other health treatment facilities as well as insurance carriers.

To complete such transactions, sensitive data—including names, physical addresses, email addresses, phone numbers, account numbers, health data, financial data, passwords, and PINs—must be sent and received.

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.

Symmetric algorithms use the same key for both encryption and decryption. Asymmetric algorithms use one key for encryption and a different key for 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.

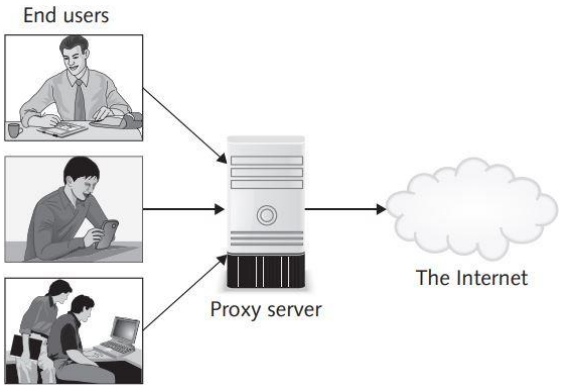
Some of the common encryption methods used are:

1. Advanced Encryption Standard (AES) – 128, 192, 256 bits - Symmetric encryption
2. Rivest-Shamir-Adleman (RSA) – Asymmetric encryption
3. Triple Data Encryption Standard (TripleDES) – Symmetric encryption – advanced form of DES
4. Twofish - 128 bits – Symmetric encryption – successor of Blowfish
5. Elliptic Curve Cryptography (ECC) – Asymmetric encryption

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. Transport Layer Security (TLS) is a communications protocol or system of rules that 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 so that even if somebody does listen in, they won't be able to determine what is being communicated.

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 on the Internet for you.



When you enter the URL for a website, the request is forwarded to the proxy server, which relays the request to the server where the website is hosted. The homepage of 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.

When you access a website directly, the server hosting the website can see your IP address and store cookies on your computer, but a proxy server can hide your IP address and block cookies from being sent to your device. A proxy server relays those packets for you and strips the originating address so instead of your IP address, the website only sees the address of the proxy server.

Remote users working at home, from a client's office, or in a branch office often have a need to access sensitive data on a company's private servers; however, doing so from an unsecured public network, such as a coffee shop wireless hotspot, could expose that data to unauthorized users with ill intentions.

A VPN enables remote users to securely access an organization's collection of computing and storage devices and share data remotely. 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.

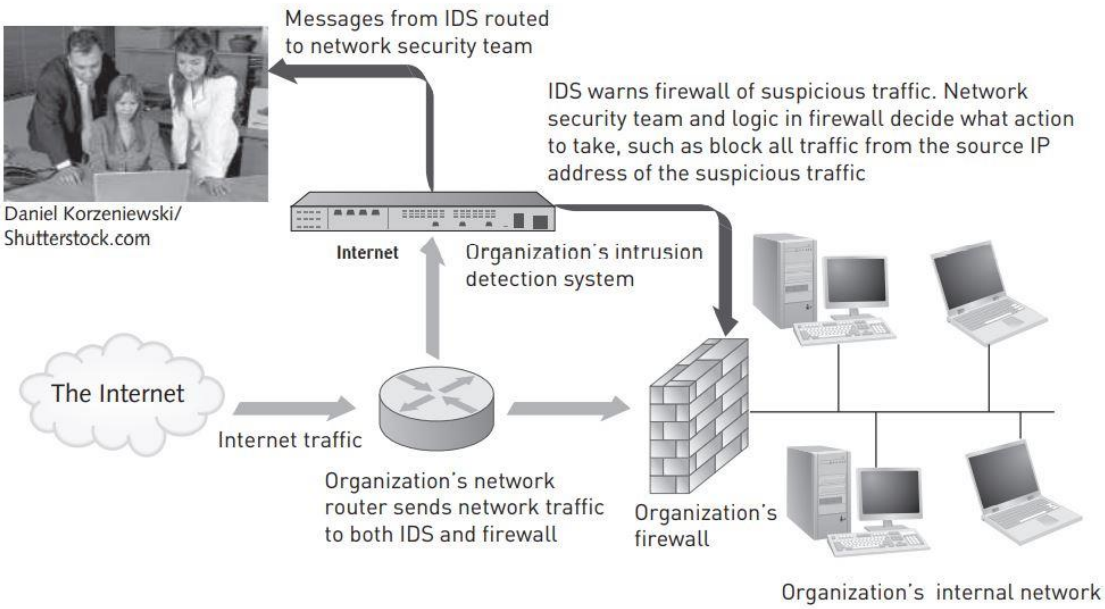
Intrusion Detection System:

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.

Intrusion detection has two approaches: Knowledge-based approaches and behavior-based approaches

Knowledge-based IDSs contain 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. Examples include unusual traffic at odd hours or a user in the human resources department who accesses an accounting program that he or she has never before used.



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 to the organization's applications and data and that their access is limited to actions that are consistent with their defined roles and responsibilities.

Authentication Methods

For many applications, users are required to enter a username and password to gain access. This is a form of single-factor authentication as the user needs to provide just one credential, a password to gain access.

Two-factor authentication requires the user to provide two types of credential before being able to access an account; the two credentials can be any of the following:

- Something you know, such as a PIN or password
- Something you have, such as some form of security card or token
- Something you are, such as a biometric (for example, a fingerprint or retina scan)

Two-factor authentication is required to withdraw money from a cash machine. You must present your bank card (something that you have) and a PIN (something that you know) to obtain cash from the machine.

User Roles and Accounts

Another important safeguard at the application level is the creation of roles and user accounts so that once users are authenticated, they have the authority to perform their responsibilities and nothing more.

For example, members of the finance department should have different authorizations from members of the human resources department. An accountant should not be able to review the pay and attendance records of an employee, and a member of the human resources department should not know how much was spent to modernize a piece of equipment. Even within one department, not all members should be given the same capabilities. Within the accounting department, for example, some users may be able to approve invoices for payment, but others may only be able to enter them.

An effective system administrator will identify the similarities among users and create profiles associated with these groups.

Data Encryption

Major enterprise systems such as enterprise resource planning (ERP), customer relationship management (CRM), and product lifecycle management (PLM) access sensitive data residing on data storage devices located in data centers, in the cloud, or at third-party locations. Data encryption should be used within such applications to ensure that these sensitive data are protected from unauthorized access.

Implementing CIA at the End-User Level

Security education, authentication methods, antivirus software, and data encryption must all be in place to protect what is often the weakest link in the organization's security perimeter—the individual end-user.

Security Education:

Creating and enhancing user awareness of security policies is an ongoing security priority for companies. Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow security policies. This can often be accomplished by discussing recent security incidents that affected the organization.

Users must understand that they are a key part of the security system and that they have certain responsibilities.

For example, 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
- 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)

Security assessment question
Do you have the most current version of your computer's operating system installed?
Do you have the most current version of firewall, antivirus, and malware software installed?
Do you install updates to all your software when you receive notice that a new update is available?
Do you use different, strong passwords for each of your accounts and applications—a minimum of 10 characters, with a mix of capital and lowercase letters, numbers, and special characters?
Are you familiar with and do you follow your organization's policies in regard to accessing corporate websites and applications from your home or remote locations (for example, access via a VPN)?
Have you set the encryption method to WPA2 and changed the default name and password on your home wireless router?
When using a free, public wireless network, do you avoid checking your email or accessing websites requiring a username and password?
Do you refrain from clicking on a URL in an email from someone you do not know?
Do you back up critical files to a separate device at least once a week?
Are you familiar with and do you follow your organization's policies regarding the storage of personal or confidential data on your device?
Does your device have a security passcode that must be entered before it accepts further input?
Have you installed Locate My Device or similar software in case your device is lost or stolen?
Do you make sure not to leave your device unattended in a public place where it can be easily stolen?
Have you reviewed and do you understand the privacy settings that control who can see or read what you do on Facebook and other social media sites?

Authentication Methods:

End users should be required to implement a security passcode that must be entered before their computing/communications device accepts further input. If your device supports Touch ID, you can use your fingerprint instead of your passcode. Again, a number of multifactor authentication schemes can be used.

Antivirus Software:

Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.

Antivirus software scans for a specific sequence of bytes, known as a virus signature that indicates the presence of a specific virus. If it finds a virus, the antivirus software informs the user, and it may clean, delete, or quarantine any files, directories, or disks affected by the malicious code. Good antivirus software 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, checks programs when they are downloaded, and scans email attachments before they are opened.

Some of the widely used antivirus software products are Norton AntiVirus from Symantec, Personal Firewall from McAfee, and Internet Security from Kaspersky.

It is crucial that antivirus software be continually updated with the latest virus signatures. In most corporations, the network administrator is responsible for monitoring network security websites frequently and downloading updated antivirus software as needed. Many antivirus vendors recommend—and provide for—automatic and frequent updates. Unfortunately, antivirus software is not able to identify and block all viruses.

Data Encryption:

While you should already have a login password for your mobile computing device or workstation, those measures won't protect your data if someone steals your device—the thief can simply remove your storage device or hard drive and plug it into another computing device and access the data. 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.

Summary: What can be done to implement a strong security program to prevent cyberattacks?

- The IT security practices of organizations worldwide must be focused on ensuring confidentiality, maintaining integrity, and guaranteeing the availability of their systems and data. Confidentiality, integrity, and availability are referred to as the CIA security triad.
- An organization's security strategy must include security measures that are planned for, designed, implemented, tested, and maintained at the organization, network, application, and end-user levels.
- Every organization needs a risk-based strategy with an active governance process to minimize the potential impact of any security incident and to ensure business continuity in the event of a cyberattack. Key elements of such a strategy include a risk assessment to identify and prioritize the threats that the organization faces, a well-defined disaster recovery plan that ensures the availability of key data and information technology assets, definition of security policies needed to guide employees to follow recommended processes and practices to avoid security-related

problems, periodic security audits to ensure that individuals are following established policies and to assess if the policies are still adequate even under changing conditions, compliance standards defined by external parties, and use of a security dashboard to help track the key performance indicators of their security strategy.

- The concept of reasonable assurance in connection with IT security recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved.
- Authentication methods, a firewall, routers, encryption, proxy servers, VPN, and an IDS are key elements of the network security layer.
- Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer.
- Security education, authentication methods, antivirus software, and data encryption are key elements of the end-user security layer.

2.3 Response to Cyberattack

An organization should be prepared for the worst—a successful 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. Sometimes system administrators take the discovery of an intruder as a personal challenge and lose valuable time that should be used to restore data and information systems to normal.

Some of the activities performed in case of cyberattack are:

- Incident notification
- Protection of evidence and activity logs
- Incident containment
- Eradication
- Incident follow-up
- Using an MSSP (managed security service provider)
- Computer Forensics

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.

Questions to cover include the following:

- 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 security personnel's be contacted?
- Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, an online discussion groups.

All parties working on the problem must be kept informed and up to-date without using systems connected to the compromised system. The intruder may be monitoring these systems and emails to learn what is known about the security breach.

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. Because such inaction is perceived by many to be unethical and harmful, a number of state and federal laws have been passed to force organizations to reveal when customer data have been breached.

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

Incident Containment:

Often, it is necessary to act quickly to contain an 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 to warrant shutting down or disconnecting critical systems from the network.

How such decisions are made, how fast they are made, and who makes them are all elements of an effective response plan.

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/malware eradication, a new backup must be created. Throughout this process, a log should be kept of all actions taken. This will prove helpful during the incident follow-up phase and ensure that the problem does not recur. It is imperative to back up critical applications and data regularly. Many organizations, however, have implemented inadequate backup processes and found that they could not fully restore original data after a security incident. All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original, and this process must be tested to confirm that it works.

Incident Follow-Up:

Of course, an essential part of follow-up is to determine how the organization's security was compromised so that it does not happen again. Often the fix is as simple as getting a software patch from a product vendor. However, it is important to look deeper than the immediate fix to discover why the incident occurred. If a simple software fix could have prevented the incident, then why wasn't the fix installed before the incident occurred?

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 that includes a detailed chronology of events and the impact of the incident. This report should identify any mistakes so that they are not repeated in the future. The experience from this incident should be used to update and revise the security incident response plan.

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
- 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

Using an MSSP (Managed Security Service Provider):

Keeping up with computer criminals—and with new laws and regulations—can be scary for organizations. Criminal or hackers are constantly poking and pushing, trying to breach the security defenses of organizations. Also, law require businesses to prove that they are securing their data. For most small and midsized organizations, the level of in-house network security expertise needed to protect their business operations is too costly to acquire and maintain.

As a result, many organizations outsource their network security operations to a managed security service provider (MSSP), which is a company that monitors, manages, and maintains computer and network security for other organizations. MSSPs include such companies as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon.

MSSPs provide a valuable service for IT departments drowning in amounts of alerts and false alarms coming from VPNs; antivirus, firewall, and IDSs; and other security-monitoring systems. In addition, some MSSPs provide vulnerability scanning and web blocking and filtering capabilities.

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.

A computer forensics investigation may be opened in response to a criminal investigation or civil litigation. It may also be launched for a variety of other reasons, for example,

- to retrace steps taken when data have been lost,
- to assess damage following a computer incident,
- to investigate the unauthorized disclosure of personal or corporate confidential data, or
- to confirm or evaluate the impact of industrial espionage.

Computer forensics investigators work as a team to investigate an incident and conduct forensic analysis by using various methodologies and tools to ensure the computer network system is secure in an organization.

For example, accounting, tax, and advisory company Grant Thornton International has a number of IT labs around the world that employ forensic experts who examine digital evidence for use in legal cases. To support its investigators, Grant Thornton has deployed forensic software called Summation (a web based legal document, electronic data, and transcript review platform that supports litigation teams) and Forensic Toolkit (used to scan a hard drive to find a variety of information, including deleted emails and text strings, to crack encryption). These two applications provide Grant Thornton a combination of mobile forensics, computer forensics, and functions for encoding and reviewing multilingual documents.

Proper handling of a computer forensics investigation is the key to fighting computer crime successfully in court. In addition, extensive training and certification increases the stature of a computer forensics investigator in a court of law.

Numerous certifications relate to computer forensics, including the

- CCE (Certified Computer Examiner),
- CISSP (Certified Information Systems Security Professional),
- CSFA (CyberSecurity Forensic Analyst), and
- GCFA (Global Information Assurance Certification Certified Forensics Analyst).

The EnCE Certified Examiner program certifies professionals who have mastered computer investigation methods as well as the use of Guidance Software's EnCase computer forensic software.

Numerous universities (both online and traditional) 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.

Summary: What actions must be taken in the event of a successful security intrusion?

- No security system is perfect, so systems and procedures must be monitored to detect a possible intrusion. 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. The response plan should address notification, evidence protection, activity log maintenance, containment, eradication, and follow-up.

Compiled by: Ridip Khanal

- Organizations must implement fixes against well-known vulnerabilities and conduct periodic IT security audits.
- Many organizations outsource their network security operations to a MSSP, which is a company that monitors, manages, and maintains computer and network security for other organizations.
- Organizations must be knowledgeable of and have access to trained experts in computer forensics 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.

2.4 Cyber Law

Cyber law, also known as cybercrime law, is legislation focused on the acceptable behavioral use of technology including computer hardware and software, the internet, and networks.

Cyber law helps protect users from harm by enabling the investigation and prosecution of online criminal activity. It applies to the actions of individuals, groups, the public, government, and private organizations.

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law is referred to as the Law of the Internet.

In business, cyber law protects companies from unlawful access and theft of their intellectual property.

Importance of Cyber Law

Like any law, a Cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a Cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.

The importance of Cyber law are:

- It dictates all actions and reactions in Cyberspace.
- All online transactions are ensured to be safe and protected
- All online activities are under watch by the Cyber law officials.
- Security for all data and property of individuals, organizations, and Government
- Helps curb illegal cyber activities with due diligence
- All actions and reactions implemented on any cyberspace has some legal angle associated with it
- Keeps track of all electronic records
- Helps to establish electronic governance

Punishments?

The increase in Internet traffic has led to a higher proportion of legal issues worldwide. Because Cyber laws vary by jurisdiction and country, enforcement is challenging, and restitution ranges from fines to imprisonment.

There are different forms of punishment depending on the type of cyber law you broke, who you offended, where you broke the law, and where you live. In many situations, breaking the rules on a website result in your account becoming suspended or banned and your IP addressed blocked. To determine the consequences of your action for minor offenses, we recommend reviewing the company's terms of service or rules.

If you've committed a more serious offense such as hacking, attacking another person or website, or causing another person or company distress, additional action may be taken against you.

Types of Cyber Law

In most of the countries, different types of Cyber Law includes:

Copyright: These days' copyright violations come under Cyber law. It protects the rights of companies and individuals to get profit from their creative work. In earlier days, online copyright violation was easier. But due to the introduction of Cyber law, it has become difficult to violate copyright.

Defamation: Generally, people use the internet to speak out their minds. But in the case of fake public statements on the internet that are bound to hamper someone's business and reputation that is when defamation law comes into the picture. Defamation Laws are a kind of civil law.

Fraud: Consumers these days depend on Cyber Law to prevent online fraud. IT law prevents credit card theft, identity theft, and other money-related crimes that are bound to happen online. People who commit online fraud, face state criminal charges. They may also witness a civil action by the victim.

Harassment and Stalking: Some statements made by people can violate criminal law that refuses stalking and harassment online. When somebody posts threatening statements repeatedly about somebody else, this violates both criminal and civil laws.

Freedom of Speech: The internet is used as a medium of free speech. But there are laws to avoid free speech that may cause immorality online. Cyber lawyers should advise their clients about the amount of free speech allowed online. Sometimes the Cyber lawyers fight cases for their clients where they debate whether their client's actions are within the permissible limit of free speech.

Trade Secrets: Businesses depend on Cyber laws to preserve their trade secrets. For example, some organizations might steal online algorithms or features designed by another firm. In this case, Cyber laws empower the victim organization to take legal action to protect its secrets.

Contracts and Employment Laws: You might have agreed upon many terms and conditions while opening a website or downloading some software. This is where the Cyber law is used. These Terms & Conditions are designed for online privacy concerns.

Categories of Cyber crime

Individual- Cybercrimes against individuals involve crimes like online harassment, distribution and trafficking of child pornography, manipulation of personal information, use of offensive data, and identity theft for personal benefit.

Property- Usage, and transmission of harmful programs, theft of information and data from financial institutions, intruding cyberspace, computer vandalism, and unauthorized possession of information digitally are some of the crimes under the property.

Government- The crimes that come under this are cyber terrorism, manipulation, threats, and misuse of power against the Government and citizens. Groups or Individuals terrorizing Government websites is when this form of cyber terrorism occurs.

Cyber Law as per countries

While cybercrime impacts the global community, the adoption of cybercrime legislation varies among countries. 72% percent of countries have cyber laws, 9% have draft legislation, and 19% have no cyber laws, according to 2019 data from the United Nations. Many states develop new cyber laws as additions to their current codes. Some countries amend their existing national codes with legislative language on cybercrime.

The first cyber law was the Computer Fraud and Abuse Act, enacted in 1986 in US. Known as CFAA, this law prohibits unauthorized access to computers and includes detail about the levels of punishment for breaking that law.

US

The US does not have a unified set of cyber regulations, but rather a combination of federal and state rules that govern private-sector cybersecurity. This has complicated compliance, as companies have to navigate different – as well as constantly evolving – federal and state laws.

“In 2018 at least 35 states, D.C. and Puerto Rico introduced or considered more than 265 bills or resolutions related to cybersecurity,” according to the National Conference of State Legislatures. CIO Online recently reported that this year alone, 30 bills had been introduced in the House of Representatives and another seven in the Senate “that directly deal with cybersecurity issues.”

As a result, if an enterprise experiences a data breach, the varying legal requirements of notifying authorities and the persons affected can be quite complex. Each state may also levy fines and penalties, which are compounded by any sector-specific federal regulations and potential enforcement actions.

India

The Cyber Law named IT Act 2000 came into consideration on 17th October 2000 to deal with e-commerce and Cybercrime in India. This law is recently amended on 2021 including rules to regulate social media and OTT (over-the-top) platform.
Apart from the IT Act 2000, there are other laws that entail Cyber security are:

- Company Rules 2014 under the Companies Act 2013, makes it mandatory for all companies to ensure that all digital records and security systems are tight and sealed to avoid tampering and illegal access.

- The Indian Penal Code Act 1860 punishes any crime committed in cyberspace (such as cheating, harassment, hacking, breach of privacy, etc)
- Sector-specific regulations are also established, such as: The department of telecommunication, The Reserve Bank of India, and the Insurance Regulatory.

Nepal

The Electronic Transactions Act, 2063 (2008): This is Nepal's first cyber law. Cyber crimes were dealt with under the Country's criminal code before this law came into force. Since the cases of Cyber crime increased, it became necessary to enact a separate law. Chapter 9 of the Act deals with offences relating to computers, the main highlights of which are as follows:

- Pirating or destroying any computer system intentionally without authority carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Accessing any computer system without authority results in imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Intentional damage to or deleting data from a computer system carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- Publication of illegal material in electronic form carries imprisonment for 5 years, or a fine of one hundred thousand rupees, or both.
- Commission of a computer fraud carries imprisonment for two years, or a fine of one hundred thousand rupees, or both.

The Children's Act, 2048 (1992): The aim of this Act is to protect and uphold the rights of children. It also prohibits child pornography. Section 16(2) of the Act prohibits individuals from capturing any immoral picture of a child. Section 16(3) of the Act prohibits publication and distribution of any such photographs of children.

The Copyright Act, 2059 (2002): This act protects the copyright of ideas, including a computer program. It prohibits people from copying and modifying the original work of others, and using it for their own advantage or economic benefits.

The Individual Privacy Act, 2018: This act is the first legislation in Nepal to protect the right to privacy of its people, and define personal information. It protects the privacy of body, family life, residence, property, and communication. It puts the responsibility on public entities to protect the personal data of individuals. They cannot transfer such data to anyone without the consent of the owner. The Act prescribes a general punishment for violation of privacy as three years of imprisonment, or a fine of NPR 30,000, or both.

Banking Offences and Punishment Act 2064 (2008): This act codifies a number of relevant offenses, such as: unauthorized withdrawals or payment, unauthorized payments via electronic means, alterations to account/ledger, forgery or fraud.

National Penal Code Act (2017): This act includes prohibition of abetment, forgery, breaching privacy through electronic means, writing letters with dishonest intention of causing annoyance, punishment for libel.

Constitution of Nepal 2072

The constitution of Nepal provides some fundamental rights and duties, such as:

- Right to Freedom
- Right to equality
- Right to communication
- Right to justice
- Right against torture
- Right against preventive detention
- Right to information
- Right to privacy

National Cybersecurity Policy 2078 (Draft)

2.6 Provision of Electronic Transaction Act of Nepal

The government of Nepal passed "The Electronic Transaction and Digital Signature Act-Ordinance" popularly known as "Cyber Law" on 30th Bhadra 2061 BS (15 September, 2004). But the government of Nepal (House of Representatives) has approved the Electronic Transaction Act-2063 only on 4th December 2006 and the Ministry of environment, science and technology (MoEST) formulated the Regulations. After that Rules regarding cyber-crime is passed on 2064 BS known as ETA 2064.

Before this there were no any cyber laws in Nepal to regulate and control cyber-crimes. And the cyber-crimes were used to be treated as other traditional crimes being based on the national code. In fact the cyber-crimes were not used to be recognized as special crimes.

The Electronic Transaction Act, 2063 (2008)

Preamble:

WHEREAS, it is expedient to make, legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured;

And where as, for controlling the acts of unauthorized use of electronic records or of making alteration in such records through the illegal manner,

Now, therefore, be it enacted by the House of Representatives in the First Year of the issuance of the Proclamation of the House of Representatives, 2063(2007) .

Chapter 1: Preliminary [प्रारम्भिक]

1. Short Title, Extension, and Commencement:
   (1) This Act may be called "The Electronic Transactions act, 2063 (2008)".
   (2) This Act shall be deemed to have been commenced from 24 Bhadra 2063 (sep.2, 2006).
   (3) This Act shall extend throughout Nepal and shall also apply to any person residing anywhere by committing an offence in contravention to this Act.

2. Definitions:

"Computer" means an electro-magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic and memory functions by manipulating electro-magnetic or optical

impulses, and also includes all acts of input, output, processing, storage and computer software or communication facilities which are connected or related to the computer in any computer system or computer network.

"Computer Network" means an interrelationship between two or more than two computers having interconnection with each other or in contact of communication.

"Computer Resource" means a computer, computer system, computer network, data, computer database or software.

Chapter 2: Provisions relating to Electronic Record and Digital Signatures [विद्युतीय अभिलेख तथा डिजिटल हस्ताक्षर सम्बन्धी व्यवस्था]

3. Authenticity of Electronic Record [विद्युतीय अभिलेखको प्रामाणिकता]

(1) Any subscriber may, subject to the provisions of this section, authenticate to any electronic record by his/her personal digital signature. [यस दफाको अधीनमा रही कुनै पनि ग्राहकले आफ्नो डिजिटल हस्ताक्षरद्वारा कुनै विद्युतीय अभिलेखलाई प्रामाणिकता प्रदान गर्न सक्नेछ ।]
(2) While authenticating the electronic record pursuant to Subsection (1), an act of transforming such electronic record to other electronic record shall be effected by the use of asymmetric crypto system and hash function. [उपदफा (१) बमोजिम विद्युतीय अभिलेखलाई प्रामाणिकता प्रदान गर्ने कार्य गर्दा त्यस्तो विद्युतीय अभिलेख अर्को विद्युतीय अभिलेखमा हस्तान्तरण हुने कार्य एसिमेट्रिक क्रिप्टो सिस्टम र ह्यास फङ्शनको प्रयोगबाट भएको हुन आवश्यक हुनेछ ।]
(3) Any person may verify the electronic record by using the public key of the subscriber. [कुनै पनि व्यक्तिले ग्राहकको सार्वजनिक साँचोको प्रयोग गरी विद्युतीय अभिलेखको सम्पुष्टि गर्न सक्नेछ ।]

4. Legal Recognition of Electronic Record [विद्युतीय अभिलेखको कानूनी मान्यता]
5. Legal Recognition of Digital Signature [डिजिटल हस्ताक्षरको कानूनी मान्यता]
6. Electronic Records to be Kept Safely [विद्युतीय अभिलेख सुरक्षित राख्नु पर्ने]
7. Electronic Record May Fulfill the Requirement of Submission of any Original Document [कुनै अभिलेखको सक्कल पेश गर्नु पर्ने आवश्यकता विद्युतीय अभिलेखले पूरा गर्ने]
8. Secured Electronic Records [सुरक्षित विद्युतीय अभिलेख]
9. Secured Digital Signature [सुरक्षित डिजिटल हस्ताक्षर]

Chapter 3: Provision Relating to Dispatch, Receipt and Acknowledgement of Electronic Records [विद्युतीय अभिलेखको सम्प्रेषण, प्राप्ति र स्वीकार सम्बन्धी व्यवस्था]

10. Electronic Record to be attributed to Originator [विद्युतीय अभिलेख उत्पत्तिकर्ताको मानिन]
11. Procedure of Receipt and Acknowledgement of Electronic Record [विद्युतीय अभिलेखको प्राप्ति स्वीकार गर्ने प्रक्रिया]
12. Time and Place of Dispatch and Receipt of Electronic Record [विद्युतीय अभिलेखको सम्प्रेषण र प्राप्तिको समय तथा स्थान]

Chapter 4: Provisions Relating to Controller and Certifying Authority [नियन्त्रक तथा प्रमाणीकरण गर्ने निकाय सम्बन्धी व्यवस्था]

13. Appointment of the Controller and other Employees [नियन्त्रक तथा अन्य कर्मचारीको नियुक्ति]
14. Functions, Duties and Powers of the Controller [नियन्त्रकको काम, कर्तव्य र अधिकार]
15. License to be obtained [इजाजतपत्र प्राप्त गर्नु पर्ने]

16. Application to be submitted for a license [इजाजतपत्र प्राप्त गर्न निवेदन दिनु पर्ने]
17. Other Functions and Duties of the Certifying Authority [प्रमाणीकरण गर्ने निकायको अन्य काम तथा कर्तव्य]
18. Procedure for granting of a license [इजाजतपत्र प्रदान गर्ने कार्यविधि]
19. Renewal of License [इजाजतपत्र नवीकरण गर्नु पर्ने]
20. License may be suspended [इजाजतपत्र निलम्बन गर्न सक्ने]
21. License may be revoked [इजाजतपत्र रद्द गर्न सक्ने]
22. Notice of Suspension or revocation of a License [इजाजतपत्र निलम्बन वा रद्द गरिएको सूचना]
23. Recognition to Foreign Certifying Authority may be given [प्रमाणीकरण गर्ने विदेशी निकायलाई मान्यता दिन सक्ने]
24. The Controller may issue Orders [नियन्त्रकले निर्देशन जारी गर्न सक्ने]
25. The Controller may delegate power [नियन्त्रकले अधिकार प्रत्यायोजन गर्न सक्ने]
26. The Controller may investigate [नियन्त्रकले जाँचबुझ गर्न सक्ने]
27. Performance Audit of Certifying Authority [प्रमाणीकरण गर्ने निकायको कार्य सम्पादन परीक्षण]
28. The Controller to have the Access to Computers and data [नियन्त्रकले कम्प्युटर र तथ्याङ्कमा पहुँच पाउने]
29. Record to be maintained [अभिलेख राख्नु पर्ने]

Chapter 5: Provisions Relating to Digital Signatures and Certificates [डिजिटल हस्ताक्षर तथा प्रमाणपत्र सम्बन्धी व्यवस्था]

30. Certifying Authority may issue a Certificate [प्रमाणीकरण गर्ने निकायले प्रमाणपत्र जारी गर्न सक्ने]
31. Apply to obtain a Certificate [प्रमाणपत्र प्राप्त गर्नको लागि निवेदन निवेदन दिनु पर्ने]
32. Certificate may be suspended [प्रमाणपत्र निलम्बन गर्न सक्ने]
33. Certificate may be revoked [प्रमाणपत्र रद्द गर्न सक्ने]
34. Notice of Suspension or Revocation [निलम्बन वा रद्द गरिएको सूचना]

Chapter 6: Functions, Duties and Rights of Subscriber [ग्राहकको काम, कर्तव्य र अधिकार]

35. To Generate Key Pair [जोडी साँचो सृजना गर्ने]
36. To Accept a Certificate [प्रमाणपत्र स्वीकार गर्ने]
37. To retain the private key in a secured manner [निजी साँचोलाई सुरक्षित साथ राख्नु पर्ने]
38. To deposit the private key to the Controller [निजी साँचो नियन्त्रक समक्ष दाखिला गर्नु पर्ने]

Chapter 7: Electronic Record and Government use of Digital Signatures [विद्युतीय अभिलेख र डिजिटल हस्ताक्षरको सरकारी प्रयोग]

39. Government Document may be published in electronic form [विद्युतीय स्वरुपमा सरकारी कागजपत्रहरु प्रकाशन गर्न सकिने]
40. To Accept the Document in Electronic Form [विद्युतीय स्वरुपमा कागजपत्रहरु स्वीकार गर्ने]
41. Use of Digital Signature in Government Offices [सरकारी कार्यालयहरुमा डिजिटल हस्ताक्षरको प्रयोग]

Chapter 8: Provisions Relating to Network Service [नेटवर्क सेवा सम्बन्धी व्यवस्था]

42. Liability of Network Service Providers [नेटवर्क सेवा प्रदान गर्नेको दायित्व]
43. Network Service Provider not to be liable [नेटवर्क सेवा प्रदान गर्नेले दायित्व व्यहोर्नु नपर्ने]

Chapter 9: Provisions Relating to Offence Relating to Computer [कम्प्युटर सम्बन्धी कसूर]

44. To Pirate, Destroy or Alter computer source code: [कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गर्ने]

When computer source code is required to be kept as it is position for the time being the prevailing law, if any person, knowingly or with malafide intention, pirates, destroys, alters computer sources code to be used for any computer, computer programme, computer system or computer network or cause, other to do so, he/she shall be liable to the punishment with imprisonment not exceeding three years or with a fine not exceeding two hundred thousand Rupees or with both.

45. Unauthorized access of Computer Materials: [कम्प्युटर सामग्रीमा अनधिकृत पहुँच]

If any person with an intention to have access in any programme, information or data of any computer, uses such a computer without authorization of the owner of or the person responsible for such a computer or even in the case of authorization, performs any act with an intention to have access in any programme, information or data contrary to from such authorization, such a person shall be liable to the punishment with the fine not exceeding Two Hundred Thousand Rupees or with imprisonment not exceeding three years or with both depending on the seriousness of the offence.

46. Damage to any Computer and Information System [कम्प्युटर र सूचना प्रणालीमा क्षति पुऱ्याउने]

47. Publication of illegal materials in electronic form [विद्युतीय स्वरुपमा गैरकानूनी कुरा प्रकाशन गर्ने]

(1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both.
(2) If any person commit an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment.

48. Confidentiality to Divulge [गोपनीयता भङ्ग गर्ने]
49. To inform False statement [झुट्टा व्यहोराको सूचना दिने]
50. Submission or Display of False License or Certificates [झुट्टा इजाजतपत्र वा प्रमाणपत्र पेश गर्ने वा देखाउने]
51. Non-submission of Prescribed Statements or Documents [तोकिएका विवरण वा कागजात दाखिला नगर्ने]
52. To commit computer fraud [कम्प्युटर जालसाजी गर्ने]
53. Abetment to commit computer related offence [कम्प्युटर सम्बन्धी कसूर गर्न दुरुत्साहन]
54. Punishment to the Accomplice [मतियारलाई सजाय]
55. Punishment in an offence committed outside Nepal [नेपाल राज्य बाहिरगरेको कसूरमा हुने सजाय]
56. Confiscation [जफत गर्ने]
57. Offences Committed by a corporate body [सङ्गठित संस्थाले गरेको कसूर]
58. Other Punishment [अन्य सजाय]
59. No Hindrance to Punish under the Laws prevailing [प्रचलित कानून बमोजिम सजाय गर्न बाधा नपुग्ने]

Chapter 10: Provisions Relating to Information Technology Tribunal [सूचना प्रविधि न्यायाधिकरण सम्बन्धी व्यवस्था]

60. Constitution of a Tribunal [न्यायाधिकरणको गठन]
61. Qualification of the Member of the Tribunal [न्यायाधिकरणका सदस्यको योग्यता]
62. Terms of office, remuneration and conditions of service of the Member of the Tribunal [न्यायाधिकरणका सदस्यहरुको पदावधि, पारिश्रमिक र सेवाका शर्त]

63. Circumstances under which office shall be fallen vacant and filling up a vacancy [पद रिक्त हुने अवस्था र रिक्त पदको पूर्ति]
64. Staff of the Tribunal [न्यायाधिकरणका कर्मचारी]
65. Procedures to be followed by the Tribunal [न्यायाधिकरणले पालना गर्नु पर्ने कार्यविधि]

Chapter 11: Provisions Relating to Information Technology Appellate Tribunal [सूचना प्रविधि पुनरावेदन न्यायाधिकरण सम्बन्धी व्यवस्था]

66. Establishment and formation of the Appellate Tribunal [पुनरावेदन न्यायाधिकरणको स्थापना र गठन]
67. Qualification of the Member of the Appellate Tribunal [पुनरावेदन न्यायाधिकरणको सदस्यको योग्यता]
68. Terms of office, remuneration and conditions of service of the Member of the Appellate Tribunal [पुनरावेदन न्यायाधिकरणको सदस्यको पदावधि, पारिश्रमिक र सेवाका शर्त]
69. Conditions of vacancy of Office and filling up such vacancy [पद रिक्त हुने अवस्था र रिक्त पदको पूर्ति]
70. Staff of the Appellate Tribunal [पुनरावेदन न्यायाधिकरणका कर्मचारी]
71. Procedures to be followed by the Appellate Tribunal [पुनरावेदन न्यायाधिकरणले अपनाउनु पर्ने कार्यविधि]

Chapter 12: Miscellaneous [विविध]

72. Provisions may be made by an Agreement [सम्झौताद्वारा व्यवस्था गर्न सकिने]
73. Government of Nepal may issue Directives [नेपाल सरकारले निदे नेपाल सरकारले निर्देशन दिन सक्ने]
74. Time limitations to file a Complaint [उजुर गर्ने हदम्याद]
75. Government of Nepal to be a Plaintiff [नेपाल सरकार वादी हुने]
76. Compensation to be recovered [क्षतिपूर्ति भराउ क्षतिपूर्ति भराउनु पर्ने]
77. This Act shall not Apply [यो ऐन लागू नहुने]
78. Power to Frame Rules [नियम बनाउने अधिकार]
79. To Frame and Enforce the Directives [निर्देशिका बनाई लागू गर्ने]
80. Effect of inoperativeness of the Electronic Transactions Ordinance, 2063 (2008) [विद्युतीय (इलेक्ट्रोनिक) कारोबार अध्यादेश, २०६२ निष्क्रिय भएपछि त्यसको परिणाम]

Practice Questions:

1. Briefly describe the difference between a risk assessment and an IT security audit.
2. Identify and briefly discuss a real-world example of a legitimate organization using spam in an effective and nonintrusive manner to promote a product or service.
3. Some IT security personnel believe that their organizations should employ former computer criminals who now claim to be white hat hackers to identify weaknesses in their organizations' security defenses. Do you agree? Why or why not?
4. Hundreds of a bank's customers have called the customer service call center to complain that they are receiving text messages on their phone telling them to access a website and enter personal information to resolve an issue with their account. What action should the bank take?
5. How would you distinguish between a hacktivist and a cyberterrorist? Should the use of hacktivists by a country against enemy organizations be considered an act of war? Why or why not? How about the use of cyberterrorists?
6. What advantages does the use of an MSSP offer a small retailers? Can you think of any potential drawbacks of this approach? Is there a danger in placing too much trust in an MSSP? Explain.
7. What are the provisions to the offense related to the Computer in Electronic Transaction Act 2063?
8. Explain Cyber Law in detail including its necessity considering the Nepalese society.

Compiled by: Ridip Khanal