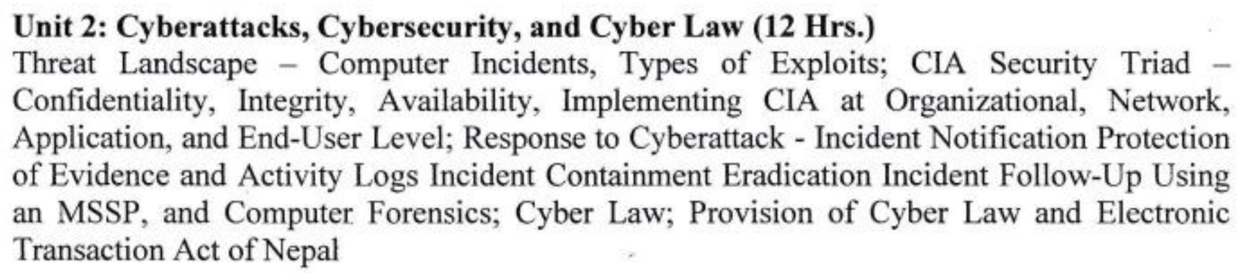
Unit 2: Cyberattack, cybersecurity and Cyber Law

Syllabus:



Unit 2: Cyberattacks, Cybersecurity, and Cyber Law (12 Hrs.)
Threat Landscape – Computer Incidents, Types of Exploits; CIA Security Triad – Confidentiality, Integrity, Availability, Implementing CIA at Organizational, Network, Application, and End-User Level; Response to Cyberattack - Incident Notification Protection of Evidence and Activity Logs Incident Containment Eradication Incident Follow-Up Using an MSSP, and Computer Forensics; Cyber Law; Provision of Cyber Law and Electronic Transaction Act of Nepal

==

Threat Landscape

A threat landscape also called a threat environment is a collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends.

The security of data and information systems used in business are importance. As confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption. Now a days a number of cybercrimes being committed against individuals, organizations, and governments continues to grow, and the destructive impact of these crimes is also intensifying. The brands, reputation, and earnings of many organizations around the world have been negatively impacted by such crimes. 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:

- How much effort and money should be spent to safeguard against computer crime?
- What should be done if recommended computer security safeguards make conducting business more difficult for customers and employees, resulting in lost sales and increased costs?
- If a firm is a victim of a cybercrime, should it pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform affected customers, or take some other action?

In order to safeguard against cybercrime many organizations are putting in place a range of countermeasures against it. For instance, the **worldwide financial services** industry spent billion Doller on IT security and fraud prevention in each and every year. 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 analyse security intelligence

In spite of all these countermeasures, however, the number of computer security incidents has grown in the following industries: public sector organizations; entertainment, media, and communications; technology and telecommunications companies; pharmaceuticals and life sciences; and power and utilities organizations.

Computer Incidents

Increasing computing complexity, expanding and changing systems, an increase in the prevalence 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.

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. Proponents 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 nonwork 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.

It is worth noting that employees also have concerns with BYOD policies, primarily related to privacy. Most people place a high priority on keeping any prying eyes, including those of their employer, from looking at the personal photos, text messages, and email stored on their personal mobile devices

1.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.

2.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 interorganizational 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.

3.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?

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, as shown in Figure 3-1.10

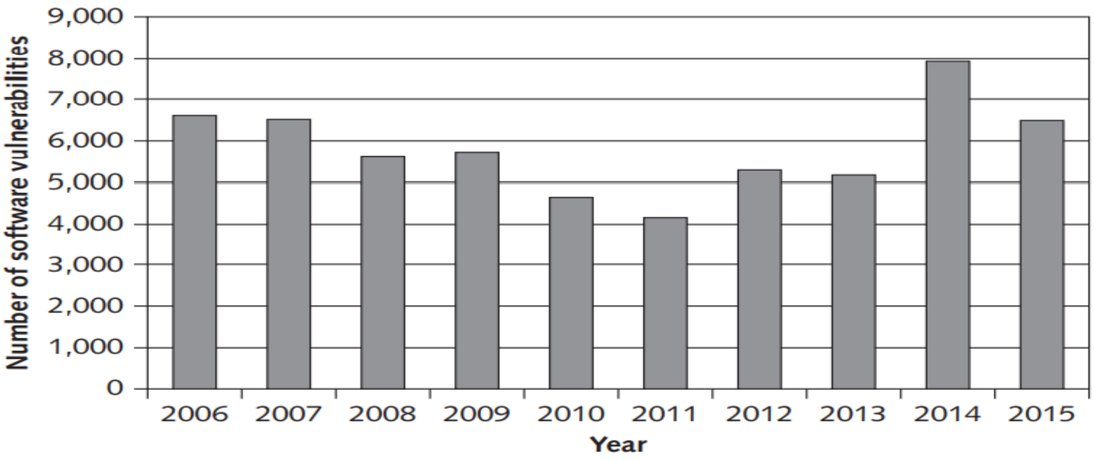


FIGURE 3-1 Total number of software vulnerabilities

Source: National Vulnerability Database

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

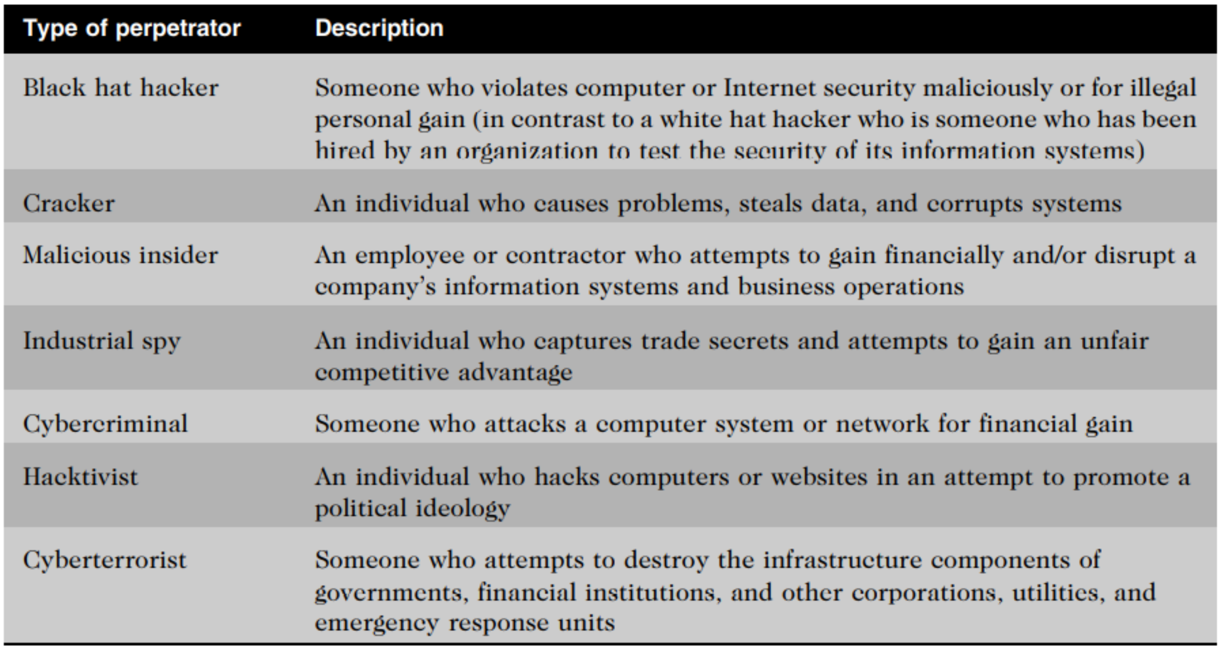
5.Increasing Sophistication of Those Who Would Do Harm

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 used rudimentary 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 menace is much better organized and may be part of an organized group (for example, Anonymous, Chaos Computer Club, Lizard Squad, TeslaTeam, and hacker teams sponsored by national governments) that has an agenda and targets specific organizations and websites. Some of these groups have ample resources, including money and sophisticated tools to support their efforts. Today’s computer attacker has greater depth of knowledge and expertise in getting around computer and network security safeguards.

Table 3-1 summarizes the types of perpetrators of computer mischief, crime, and damage.

TABLE 3-1 Classifying perpetrators of computer crime



Type of perpetrator	Description
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)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company’s information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hacktivist	An individual who hacks computers or websites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

Types of Exploits

While we usually think about exploits being aimed at computers, 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.

There are numerous types of computer attacks including ransomware, viruses, worms, Trojan horses, blended threats, spam, distributed denial-of-service (DDoS) attacks, rootkits, advanced persistent threats, phishing and spear phishing, smishing and vishing, cyberespionage, and cyberterrorism which are explained as follows.

Ransomware

Ransomware is malware that stops you from using your computer 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 Yahoo Messenger, with the payload disguised as an image.

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

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.

Example of virus are Network Virus, Boot Sector Virus etc

Worms

A computer worm is a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems. A computer worm duplicates itself to spread to uninfected computers. It often does this by exploiting parts of an operating system that are automatic and invisible to the user.

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.

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.

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 telltale 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 nonauthorized 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.

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. 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.

The cost of creating an email campaign for a product or service can be several hundreds to a few thousand dollars, compared to tens of thousands of dollars for direct-mail campaigns. In addition, email campaigns might take only a couple of weeks (or less) to develop. However, the benefits of spam to companies may be largely offset by the public's generally negative reaction to receiving unsolicited ads.

Spam forces unwanted and often objectionable material into email boxes, detracts from the ability of recipients to communicate effectively due to full mailboxes and relevant emails being hidden among many unsolicited messages, and costs Internet users and service providers millions of dollars annually. It takes user's time to scan and delete spam email, 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.

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.

DDoS Attacks

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

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 infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in—the 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.

In a DDoS attack, a tiny program is downloaded surreptitiously 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, soccervillage.com) into the IP address of the device hosting the website for that domain name (for example, 206.35.184.101). 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. The following are some symptoms of rootkit infections:

The computer locks up or fails to respond to input from the keyboard or mouse.

- The screen saver changes without any action on the part of the user.
- The taskbar disappears.
- Network activities function extremely slowly

Advanced Persistent Threat

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

An APT attack advances through the following five phases:

1. **Reconnaissance—**The intruder begins by conducting reconnaissance on the network to gain useful information about the target (security software installed, computing resources connected to the network, number of users).
2. **Incursion—**The attacker next launches incursions to gain access to the network at a low level 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 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.

Phishing

Phishing is the act of fraudulently using email to try to get the recipient to reveal personal data. In a phishing scam, con 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 counterfeit websites designed to trick them into divulging personal data or to download malware onto their computers.

Savvy 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.

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 perpetrated. 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.
- 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.

Cyberespionage

Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms. The type of data most frequently targeted includes data that can provide an unfair competitive advantage to the perpetrator. 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

Cyberterrorism

Cyberterrorism is the intimidation of government or civilian population by using information technology to disable critical national infrastructure (for example, energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals. It is an increasing concern for countries and organizations around the globe. 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.

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.

The CIA Security Triad

The CIA Triad is an information security model designed to guide policies for information security within organization. It guides an organization's efforts towards ensuring data security. The three principles—confidentiality, integrity, and availability which is also the full for CIA in cybersecurity, form the cornerstone of a security infrastructure.

Confidentiality

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.

Confidentiality refers to an organization's efforts to keep their data private or secret. In practice, it's about controlling access to data to prevent unauthorized disclosure. Typically, this involves ensuring that only those who are authorized have access to specific assets and that those who are unauthorized are actively prevented from obtaining access.

As an example, only authorized Payroll employees should have access to the employee payroll database. Furthermore, within a group of authorized users, there may be additional, more stringent limitations on precisely which information those authorized users are allowed to access.

Another example: it’s reasonable for ecommerce customers to expect that the personal information they provide to an organization (such as credit card, contact, shipping, or other personal information) will be protected in a way that prevents unauthorized access or exposure.

Countermeasures to protect confidentiality include data classification and labelling; strong access controls and authentication mechanisms; encryption of data in process, in transit, and in storage; steganography; remote wipe capabilities; and adequate education and training for all individuals with access to data etc.

Integrity

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

In InfoSec, integrity is about ensuring that data has not been tampered with and, therefore, can be trusted. It is correct, authentic, and reliable.

For example, ecommerce customers, expect product and pricing information to be accurate, and that quantity, pricing, availability, and other information will not be altered after they place an order.

Similarly, Banking customers need to be able to trust that their banking information and account balances have not been tampered with. Ensuring integrity involves protecting data in use, in transit (such as when sending an email or uploading or downloading a file), and when it is stored, whether on a laptop, a portable storage device, in the data centre, or in the cloud.

Countermeasures that protect data integrity include encryption, hashing, digital signatures, digital certificates, intrusion detection systems, auditing, version control, and strong authentication mechanisms and access controls etc.

Availability

Availability ensures that the data can be accessed when and where needed, including during times of both normal and disaster recovery operations. That is, availability means that networks, systems, and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.

Countermeasures to help ensure availability include redundancy (in servers, networks, applications, and services), hardware fault tolerance (for servers and storage), regular software patching and system upgrades, backups, comprehensive disaster recovery plans, and denial-of-service protection solutions etc.

Implementing CIA at the Organization Level

Implementing CIA begins at the organization level with the definition of following…

- 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 performing a risk assessment to identify and prioritize the threats that the organization faces.

The security strategy must define a disaster recovery plan that ensures the availability of key data and information technology assets. Security policies are needed to guide employees to follow recommended processes and practices to avoid security-related problems. 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.

In addition to complying with its internal policies, an organization may also need to comply with standards defined by external parties, including regulatory agencies. 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:

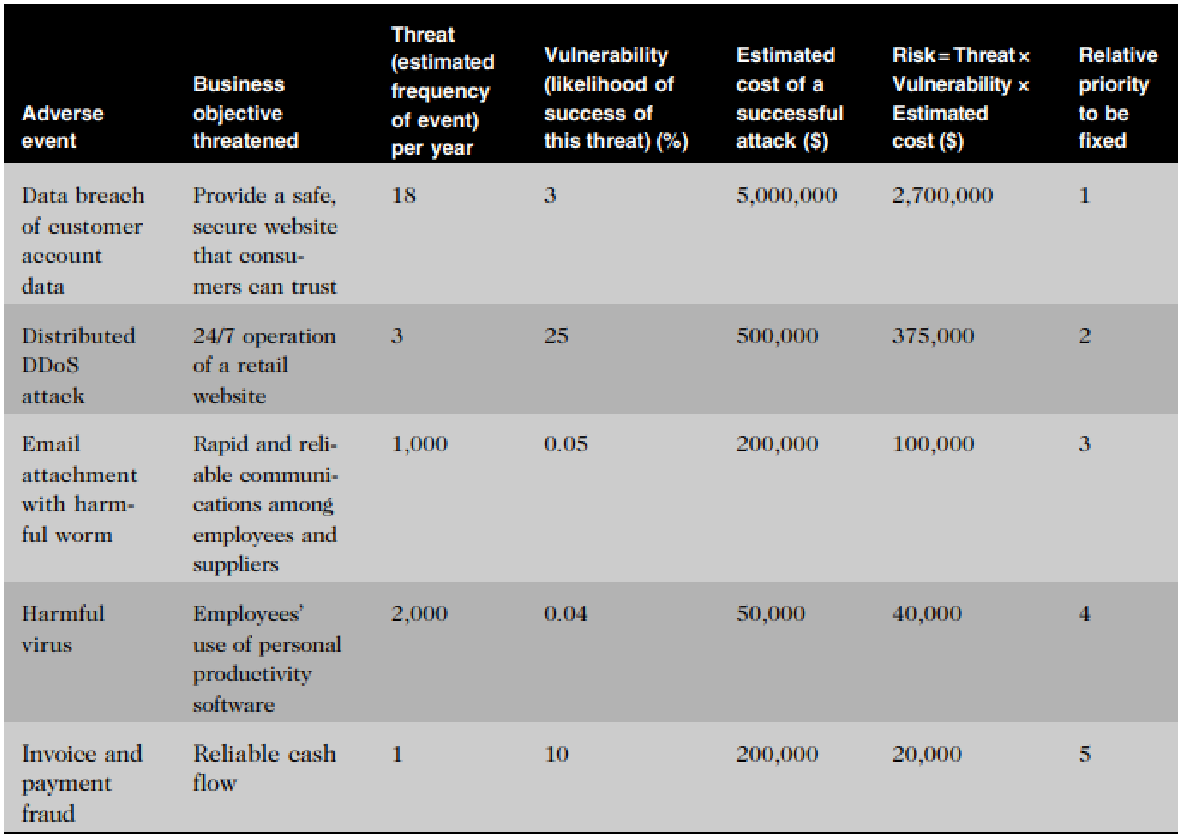
- Step 1—Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.
- Step 2—Identify the loss events or the risks or threats that could occur, such as 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.

Table below illustrates a risk assessment for a hypothetical organization.

TABLE 3-3 Risk assessment for a hypothetical company



Adverse event	Business objective threatened	Threat (estimated frequency of event) per year	Vulnerability (likelihood of success of this threat) (%)	Estimated cost of a successful attack ($)	Risk = Threat × Vulnerability × Estimated cost ($)	Relative priority to be fixed
Data breach of customer account data	Provide a safe, secure website that consumers can trust	18	3	5,000,000	2,700,000	1
Distributed DDoS attack	24/7 operation of a retail website	3	25	500,000	375,000	2
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	1,000	0.05	200,000	100,000	3
Harmful virus	Employees' use of personal productivity software	2,000	0.04	50,000	40,000	4
Invoice and payment fraud	Reliable cash flow	1	10	200,000	20,000	5

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.

Data stored in the cloud may be insulated from the effects of a disaster if it is stored at the site of the service provider, which could be hundreds of miles from the organization. On the other hand, if the cloud service provider is hit by a disaster, it may cause a serious business disruption for your organization even if it is otherwise unaffected by a distant disaster.

Thus, part of the evaluation of a cloud service provider must include analysis of the provider's disaster recovery plans. Files and databases can be protected by making a copy of all files and databases changed during the last few days or the last week, a technique called incremental backup.

This approach to backup uses an image log, which is a separate file that contains only changes to applications or data. Whenever an application is run, an image log is created that contains all changes made to all files. If a problem occurs with a database, an old database with the last full backup of the data, along with the image log, can be used to re-create the current database. Organizations can also hire outside companies to help them perform disaster planning and recovery.

For individuals and some applications, backup copies of important files can be placed on the Internet. 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.

Security Policies

A security policy defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements. A good security policy delineates responsibilities and the behavior expected of members of the organization. A security policy outlines what needs to be done but not how to do it. The details of how to accomplish the goals of the policy are typically provided in separate documents and procedure guidelines.

The SysAdmin, Audit, Network, Security (SANS) Institute's website (www.sans .org) offers a number of security-related policy templates that can help an organization to quickly develop effective security policies.

Experienced IT managers understand that users will often attempt to circumvent 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 vigilant 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 smartphones can be susceptible to viruses and worms. However, the primary security threat for mobile devices continues to be loss or theft of the device. Wary 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) (a method employing encryption to provide secure access to a remote computer over the Internet) 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.

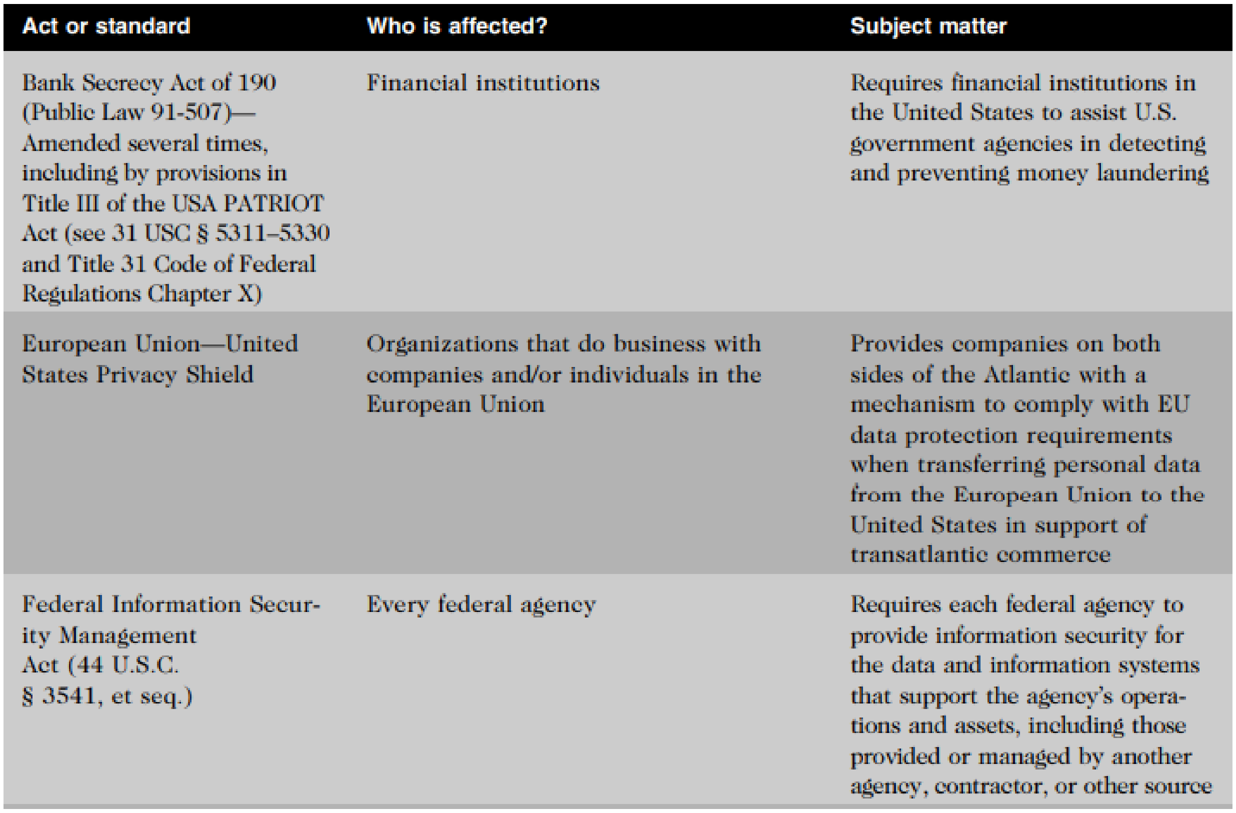
One result of a good audit is a list of items that needs to be addressed in order to ensure that the security policy is being met. A thorough security audit should also test system safeguards to ensure that they are operating as intended. Such tests might include trying the default system passwords that 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

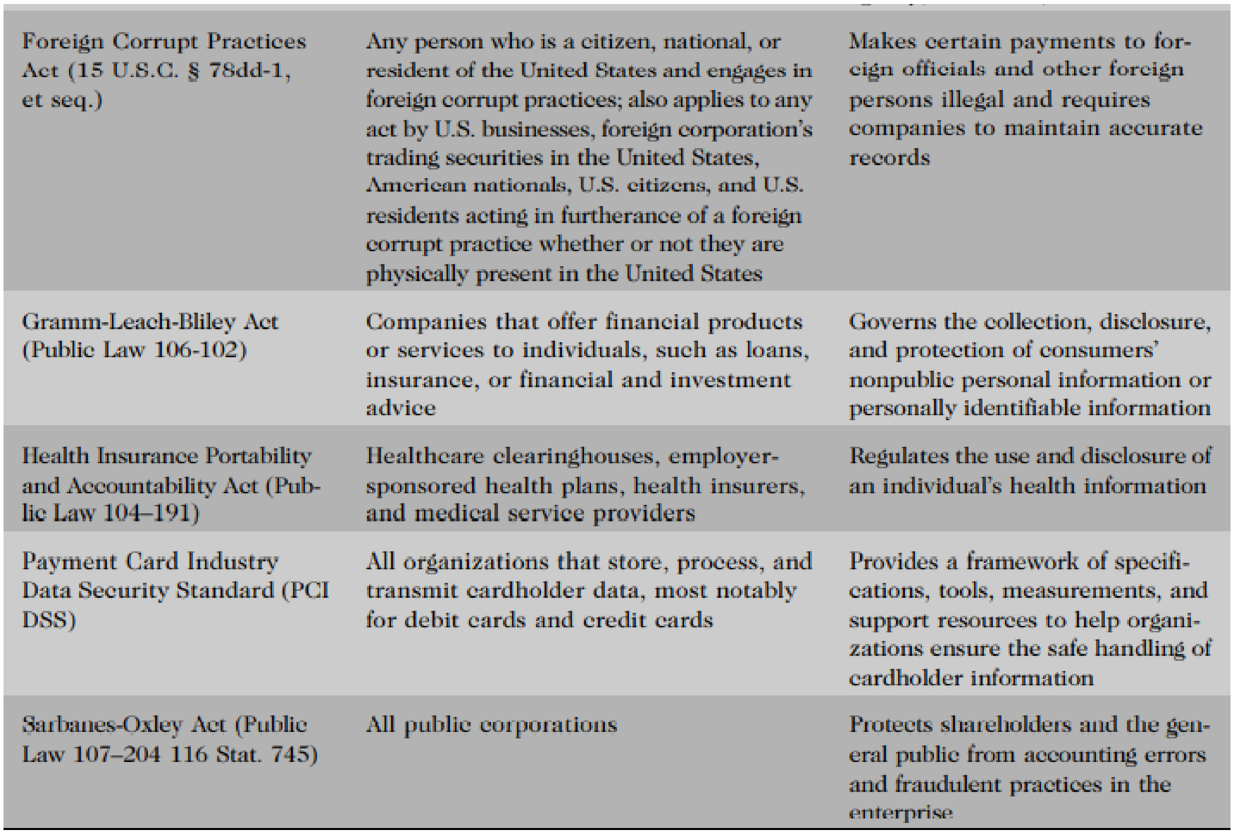
In addition to the requirement to comply with your own security program, your organization may also be required to comply with one or more standards defined by external parties. In that case, your organization's security program must include a definition of what those standards are and how the organization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

Regulatory standards that might affect your organization include those shown in Table 3-4

TABLE 3-4 Additional standards your organization may be required to meet



Act or standard	Who is affected?	Subject matter
Bank Secrecy Act of 190 (Public Law 91-507)—Amended several times, including by provisions in Title III of the USA PATRIOT Act (see 31 USC § 5311–5330 and Title 31 Code of Federal Regulations Chapter X)	Financial institutions	Requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering
European Union—United States Privacy Shield	Organizations that do business with companies and/or individuals in the European Union	Provides companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce
Federal Information Security Management Act (44 U.S.C. § 3541, et seq.)	Every federal agency	Requires each federal agency to provide information security for the data and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source

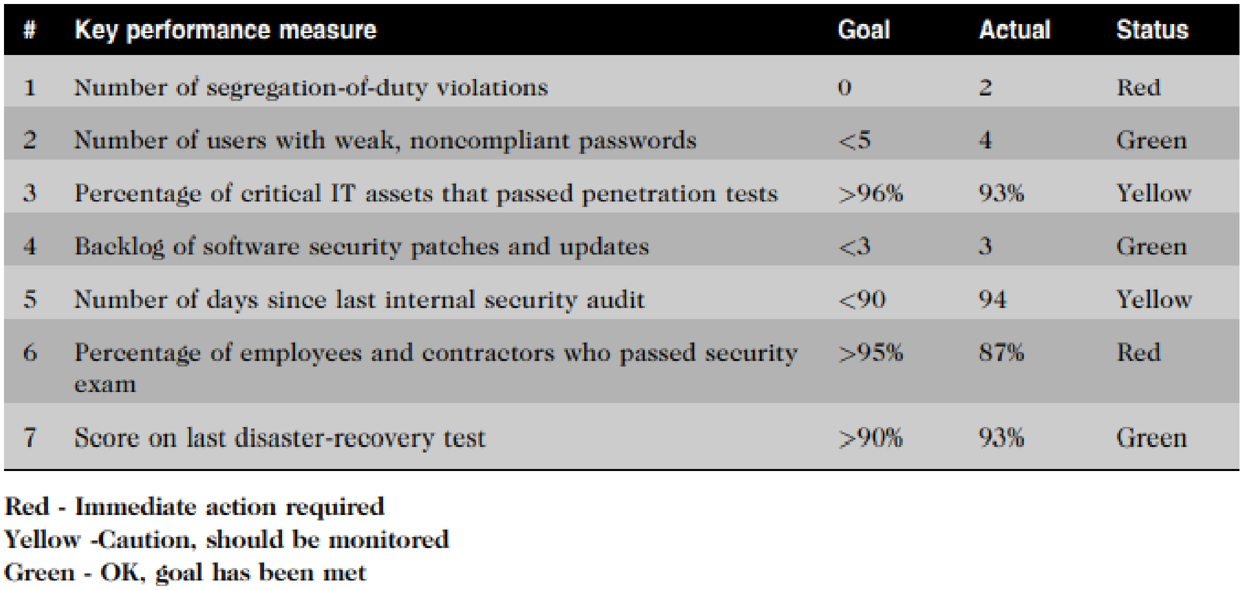


Foreign Corrupt Practices Act (15 U.S.C. § 78dd-1, et seq.)	Any person who is a citizen, national, or resident of the United States and engages in foreign corrupt practices; also applies to any act by U.S. businesses, foreign corporation's trading securities in the United States, American nationals, U.S. citizens, and U.S. residents acting in furtherance of a foreign corrupt practice whether or not they are physically present in the United States	Makes certain payments to foreign officials and other foreign persons illegal and requires companies to maintain accurate records
Gramm-Leach-Bliley Act (Public Law 106-102)	Companies that offer financial products or services to individuals, such as loans, insurance, or financial and investment advice	Governs the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information
Health Insurance Portability and Accountability Act (Public Law 104–191)	Healthcare clearinghouses, employer-sponsored health plans, health insurers, and medical service providers	Regulates the use and disclosure of an individual's health information
Payment Card Industry Data Security Standard (PCI DSS)	All organizations that store, process, and transmit cardholder data, most notably for debit cards and credit cards	Provides a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information
Sarbanes-Oxley Act (Public Law 107–204 116 Stat. 745)	All public corporations	Protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise

Security Dashboard

Many organizations use security dashboard software to provide a comprehensive display of all key performance indicators related to an organization's security defences, 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. Figure 3-5 shows an example of a security dashboard.



#	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

FIGURE 3-5 Organizational security dashboard

Algoma Central Corporation, a leading Canadian shipping company, owns and operates the largest Canadian flag fleet of dry-bulk carriers and product tankers operating on the Great Lakes—St. Lawrence Seaway system. The firm recently implemented a security dashboard from Avaap, Inc., to improve access to security information and alleviate the complexity of managing security data for its shipping operations.

Implementing CIA at the Network Level

The Internet provides a wide-open and well-travelled 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 resentful 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.

Authentication Methods

To maintain a secure network, an organization must authenticate users attempting to access the network by requiring them to enter a username and password; inserting a smart card and entering the associated PIN; or providing a fingerprint, voice pattern sample, or retina scan etc. A number of other 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.

Firewall

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, such as those whose content is based on sex and violence. Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities.

Routers

A router is a networking device that connects multiple networks together and forwards data packets from one network to another. Often, an ISP installs a router in a subscriber's home to connect the ISP's network to the network within the home.

Routers enable you to create a secure network by assigning it a passphrase so that only individuals who have the passphrase can connect to your network. However, a skilled and committed attacker can break the passphrase to gain access to your network. So, as an additional layer of security, the router provides you the capability to specify the unique media access control (MAC) address of each legitimate device connected to the network and restrict access to any other device that attempts to connect to the network.

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. Great harm could be done and chaos could ensue if these data were to fall into the wrong hands. Encryption is one means of keeping these data secure.

An encryption key is a value that is applied (using an algorithm) to a set of unencrypted text (plaintext) to produce encrypted text that appears as a series of seemingly random characters (ciphertext) that is unreadable by those without the encryption key needed to decipher it. There are two types of encryption algorithms: symmetric and asymmetric. Symmetric algorithms use the same key for both encryption and decryption. Asymmetric algorithms use one key for encryption and a different key for decryption.

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 as shown in Figure 3-6 below.

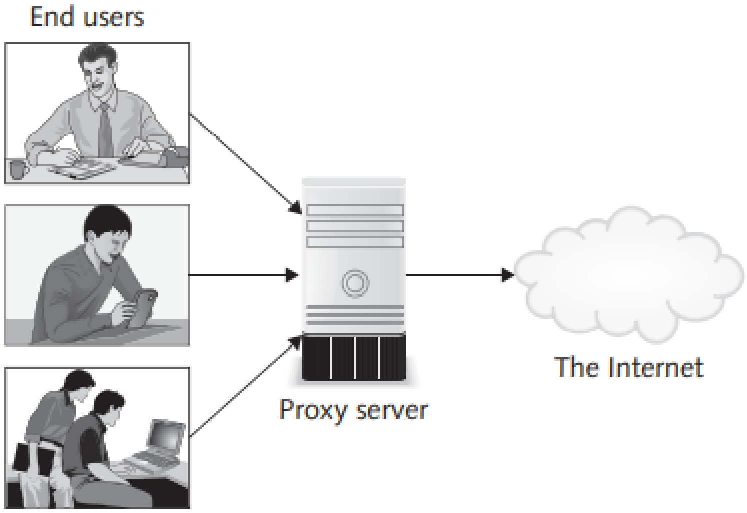


FIGURE 3-6 Proxy server

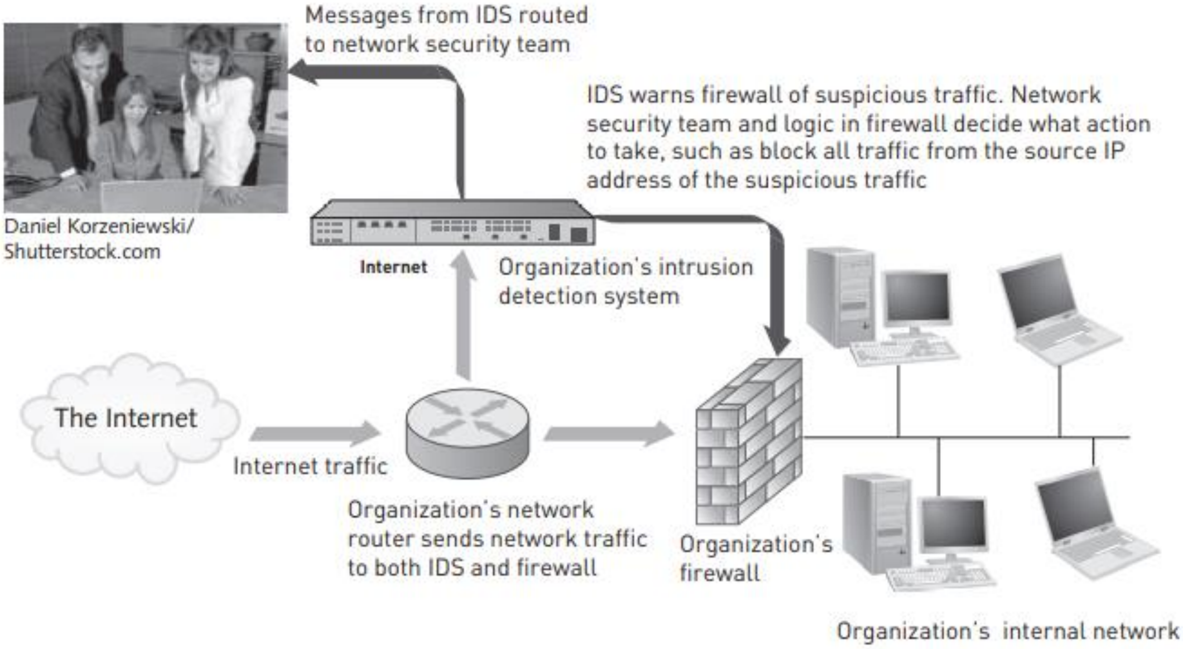
When you enter the URL for a website, the request is forwarded to the proxy server, which relays the request to the server where the website is hosted. The homepage of the website is returned to the proxy server, which then passes it on to you. Thus, the website sees the proxy server as the actual visitor 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 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 as shown in Figure 3-7 below.


Messages from IDS routed to network security team
IDS warns firewall of suspicious traffic. Network security team and logic in firewall decide what action to take, such as block all traffic from the source IP address of the suspicious traffic
Internet
Organization's intrusion detection system
The Internet
Internet traffic
Organization's network router sends network traffic to both IDS and firewall
Organization's firewall
Organization's internal network

Daniel Korzeniewski/ Shutterstock.com

FIGURE 3-7 Intrusion detection system

Such activities usually signal an attempt to breach the integrity of the system or to limit the availability of network resources.

Knowledge-based approaches and behaviour-based approaches are two fundamentally different approaches to intrusion detection. 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 behaviour-based IDS models normal behaviour 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 credentials 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 centres, 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

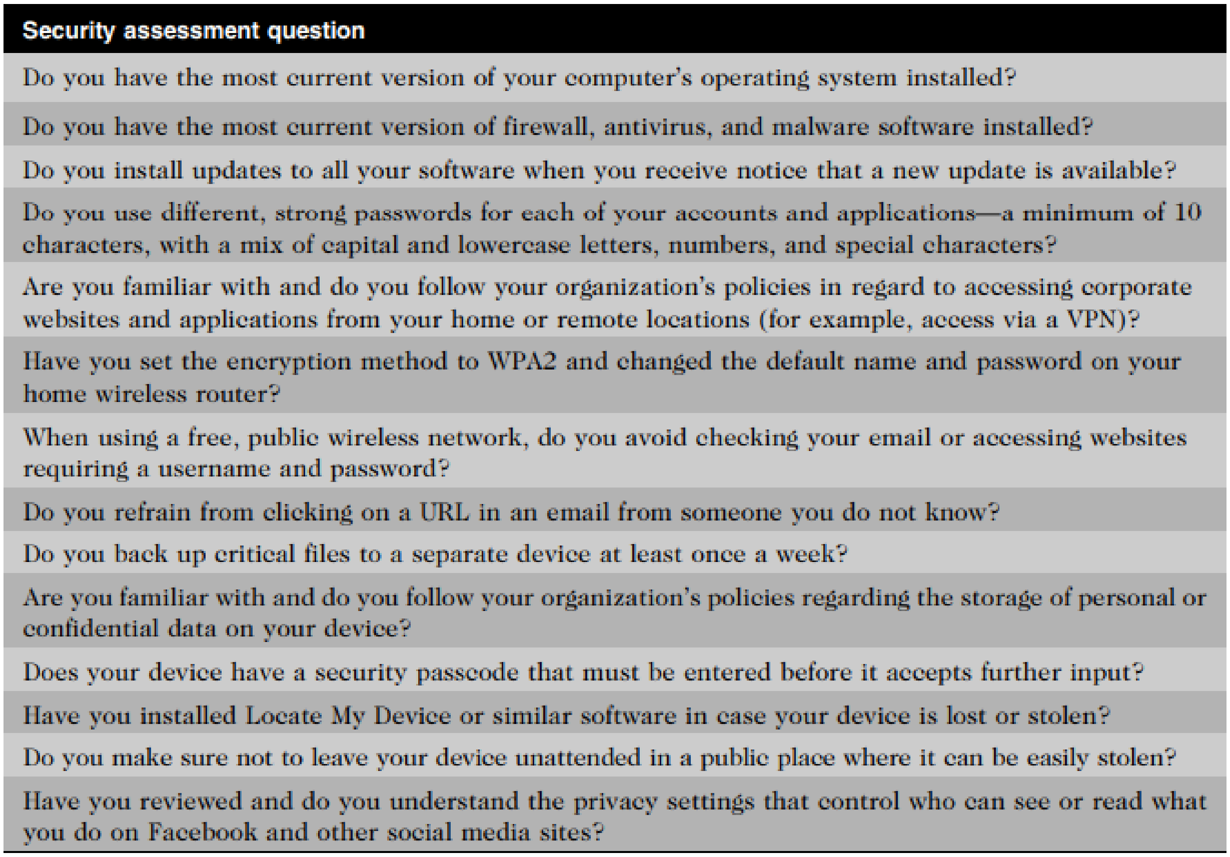
Creating and enhancing user awareness of security policies is an ongoing security priority for companies. Employees and contract workers must be educated about the importance of security so that they will be motivated to understand and follow security policies. This can often be accomplished by discussing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

Table 3-5 provides a simple self-assessment security test that employees and contractors alike should be asked to complete.

TABLE 3-5 Self-assessment security test



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. Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.

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.

RESPONSE TO CYBERATTACK

An organization should be prepared for the worst - a successful attack that defeats all or some of a system's defences 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.

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 FBI be contacted?

Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and 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 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

Creating a detailed chronology of all events will also document the incident for possible later prosecution. To this end, it is critical to develop an estimate of the monetary damage. Potential costs include loss of revenue, loss in productivity, and the salaries of people working to address the incident, along with the cost to replace data, software, and hardware.

Another important issue is the amount of effort that should be put into capturing the perpetrator. If a website was simply defaced, it is easy to fix or restore the site's HTML (Hypertext Markup Language—the code that describes to your browser how a web page should look). However, what if the intruders inflicted more serious damage, such as erasing proprietary program source code or the contents of key corporate databases? What if they stole company trade secrets? Expert crackers can conceal their identity, and tracking them down can take a long time as well as a tremendous amount of corporate resources.

The potential for negative publicity must also be considered. Public discussion of security attacks through public trials and the associated publicity has not only enormous potential costs in public relations but real monetary costs as well. For example, a bank or a brokerage firm might lose customers who learn of an attack and think their money or records aren't secure. Even if a company decides that the negative publicity risk is worth it and goes after the perpetrator, documents containing proprietary information that must be provided to the court could cause even greater security threats in the future. On the other hand, an organization must consider whether it has an ethical or a legal duty to inform customers or clients of a cyberattack that may have put their personal data or financial resources at risk.

Using an MSSP

Keeping up with computer criminals—and with new laws and regulations—can be daunting for organizations. Criminal hackers are constantly poking and prodding, trying to breach the security defenses of organizations. Also, laws such as HIPAA, Sarbanes-Oxley, and the USA Patriot Act 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 reams 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 webbased 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.

Below mention describes the Manager's checklist for assessing an organization's readiness to prevent and respond to a cyberattack: -

Question

Has a risk assessment been performed to identify investments in time and resources that can protect the organization from its most likely and most serious threats?
Have senior management and employees involved in implementing security measures been educated about the concept of reasonable assurance?
Has a security policy been formulated and broadly shared throughout the organization?
Have automated systems policies been implemented that mirror written policies?

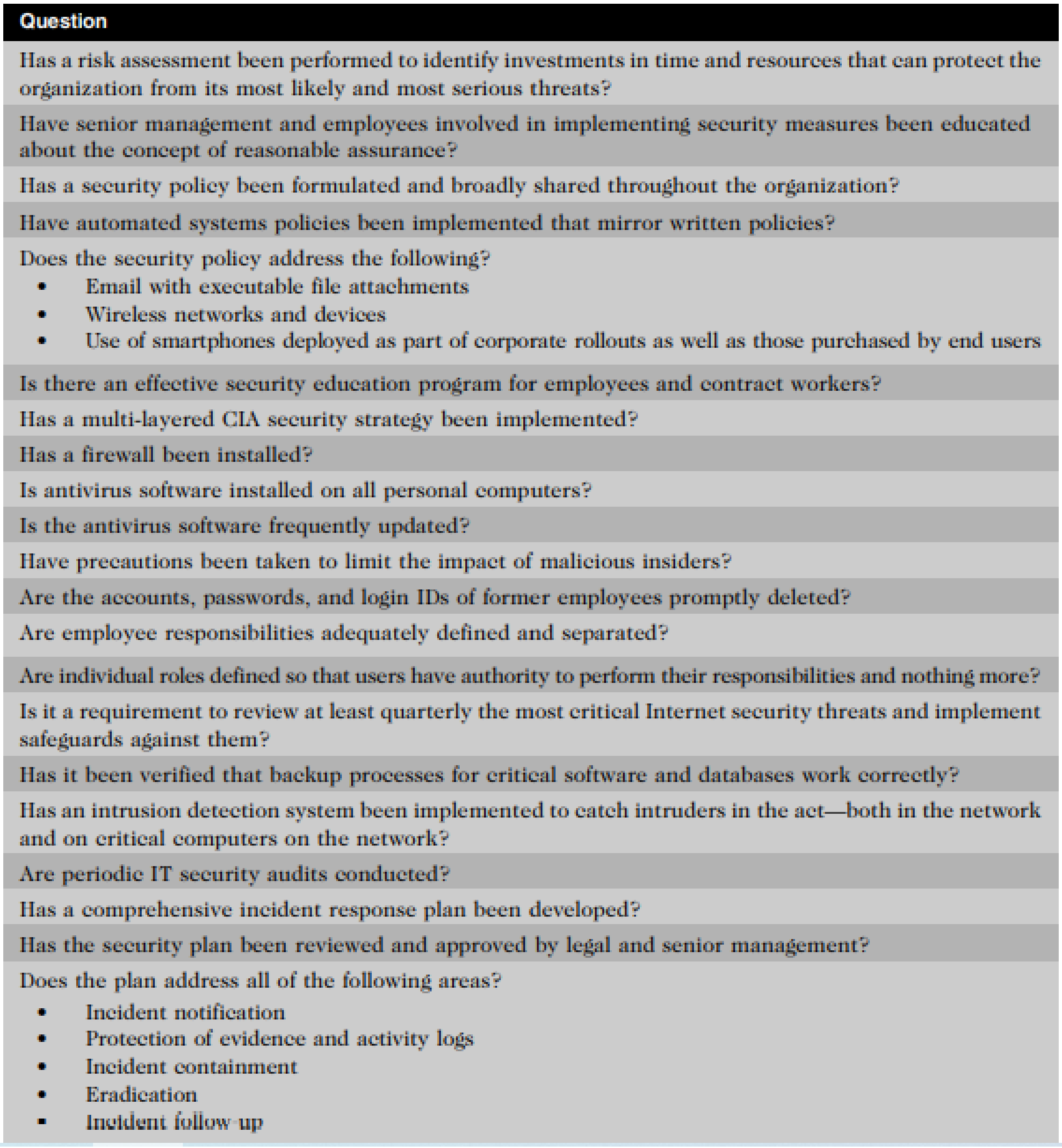
Does the security policy address the following?

- Email with executable file attachments
- Wireless networks and devices
- Use of smartphones deployed as part of corporate rollouts as well as those purchased by end users

- ➢ Is there an effective security education program for employees and contract workers?
- ➢ Has a multi-layered CIA security strategy been implemented?
- ➢ Has a firewall been installed? Is antivirus software installed on all personal computers?
- ➢ Is the antivirus software frequently updated?
- ➢ Have precautions been taken to limit the impact of malicious insiders?
- ➢ Are the accounts, passwords, and login IDs of former employees promptly deleted?
- ➢ Are employee responsibilities adequately defined and separated?
- ➢ Are individual roles defined so that users have authority to perform their responsibilities and nothing more?
- ➢ Is it a requirement to review at least quarterly the most critical Internet security threats and implement safeguards against them?
- ➢ Has it been verified that backup processes for critical software and databases work correctly?
- ➢ Has an intrusion detection system been implemented to catch intruders in the act—both in the network and on critical computers on the network?
- ➢ Are periodic IT security audits conducted?
- ➢ Has a comprehensive incident response plan been developed?

- Has the security plan been reviewed and approved by legal and senior management?

- Does the plan address all of the following areas?
  - Incident notification
  - Protection of evidence and activity logs
  - Incident containment
  - Eradication
  - Incident follow-up



Question
Has a risk assessment been performed to identify investments in time and resources that can protect the organization from its most likely and most serious threats?
Have senior management and employees involved in implementing security measures been educated about the concept of reasonable assurance?
Has a security policy been formulated and broadly shared throughout the organization?
Have automated systems policies been implemented that mirror written policies?
Does the security policy address the following? • Email with executable file attachments • Wireless networks and devices • Use of smartphones deployed as part of corporate rollouts as well as those purchased by end users
Is there an effective security education program for employees and contract workers?
Has a multi-layered CIA security strategy been implemented?
Has a firewall been installed?
Is antivirus software installed on all personal computers?
Is the antivirus software frequently updated?
Have precautions been taken to limit the impact of malicious insiders?
Are the accounts, passwords, and login IDs of former employees promptly deleted?
Are employee responsibilities adequately defined and separated?
Are individual roles defined so that users have authority to perform their responsibilities and nothing more?
Is it a requirement to review at least quarterly the most critical Internet security threats and implement safeguards against them?
Has it been verified that backup processes for critical software and databases work correctly?
Has an intrusion detection system been implemented to catch intruders in the act—both in the network and on critical computers on the network?
Are periodic IT security audits conducted?
Has a comprehensive incident response plan been developed?
Has the security plan been reviewed and approved by legal and senior management?
Does the plan address all of the following areas? • Incident notification • Protection of evidence and activity logs • Incident containment • Eradication • Incident follow-up

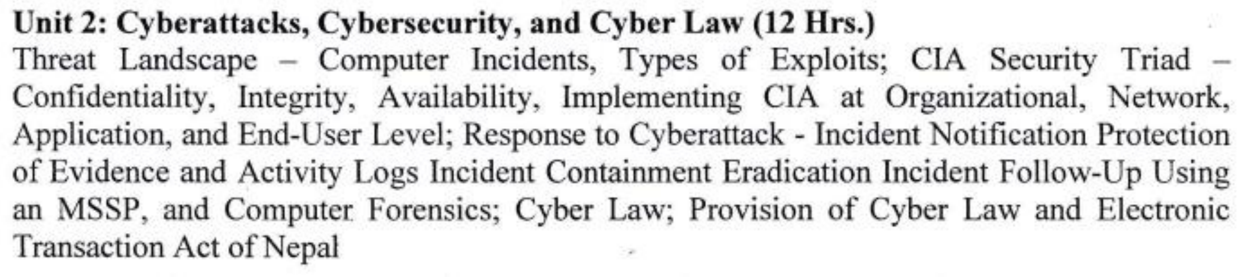
Cyber Law;

Cyber Law:

Cyber law is the part of the overall legal system that deals with the internet, cyberspace and their respective legal issues. Cyber law or internet law is a term that encapsulates the legal issues related to use of the internet. It is domain covering many areas of law and regulation. It is a term used to describe legal issues related to use of communication technology particularly cyberspace (internet). Cyber law is an attempt to apply laws designed for the physical world to human activity on the internet.

Provision of Cyber Law and Electronic Transaction Act of Nepal

========================= End of Unit-2 =================================



Unit 2: Cyberattacks, Cybersecurity, and Cyber Law (12 Hrs.)

Threat Landscape – Computer Incidents, Types of Exploits; CIA Security Triad – Confidentiality, Integrity, Availability, Implementing CIA at Organizational, Network, Application, and End-User Level; Response to Cyberattack - Incident Notification Protection of Evidence and Activity Logs Incident Containment Eradication Incident Follow-Up Using an MSSP, and Computer Forensics; Cyber Law; Provision of Cyber Law and Electronic Transaction Act of Nepal