OpenVuln Security Framework

A Complete Reference for your Information Security needs

Compiled by

RAJHESHWAR V

SHARAT N

VISHAL S

Introduction

Information technology has become an integral part of our daily lives, and businesses and organizations rely heavily on data to make informed decisions, drive innovation, and stay competitive in their respective industries. However, with the increasing use of technology and the rise of cyber threats, the need for robust information security measures has become more critical than ever.

The proposed framework for information security aims to cover all aspects of information security, including methodology, practices, strategies, analysis, and technical details. This framework provides a comprehensive set of guidelines and best practices that organizations can use to define their own information security policies and frameworks.

The framework includes various components, such as risk assessment, access control, incident management, and encryption, among others. It also provides guidance on how to implement and manage information security measures effectively, such as security awareness training, security monitoring, and security audits.

By using this framework, organizations can tailor their information security policies and frameworks to their specific needs and requirements, ensuring that they have the necessary controls and measures in place to protect their sensitive data from cyber threats. This framework also provides a wealth of resources and knowledge that organizations can use to improve their information security posture and stay up to date with the latest security trends and threats.

Overall, the proposed framework for information security is an essential resource for organizations looking to establish or enhance their information security practices. It provides a comprehensive approach to information security and ensures that organizations have the necessary tools and knowledge to protect their valuable data assets from cyber threats.

Index

Part One

Fundamentals

1.1) Information Security Overview

What is information?

Information is a valuable resource. Information is frequently one of the most valuable assets a firm has. Information can occasionally give an organization a competitive advantage that it can use to outperform its rivals.

Information can be categorized into groups such as

• *Unclassified information*, which is information that is not protected by a classification system and can be shared or distributed without restriction.

• *Controlled Unclassified Information (CUI)* is information that needs to be protected or made available under certain conditions in accordance with the laws, rules, and government-wide policies.

• *Confidential information* is data that must be kept private and accessible only to authorized staff members. Examples include research and development plans, manufacturing procedures, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, PII (Personal Identifiable Information), PHI (Personal Health Information), or even something as basic as your ATM login credentials.

• *Specialized/secret information* is data whose privacy must be strictly upheld, such as trade secrets, formulas, production information, and other intellectual property, as well as proprietary techniques and processes that specify how services are offered, encryption keys, etc. It may result in significant loss or harm to a company, government, or organization if it is revealed or leaked.

Building a Security Program

Now that you know what information is, what kinds of information there are, and why information security is important. Learn what a security programme is and why an organization would require one.

The security policies, methods, tools, and controls used by an organization are listed in a document called a security programme. When it comes to any area of information technology and organizational security, it may be considered the "holy-grail."

When developing a solution, you need to answer the questions “What” and “Why?” In building a security program, you should begin with describing what is needed and why, and to proceed to define how it will be implemented, when, and using which particular methods.

The components in building a security program

- Authority
- Framework
- Assessment
- Planning
- Action
- Maintenance

Let’s look at each component in detail

Authority - A security programme establishes the goals, duties, and scope of the security organization and grants authority for the program. Information protection, risk management, monitoring, and response are often the purview of the security organization. It might also be in charge of enforcement, which includes reprimanding or even firing employees or contract workers. Physical security, disaster recovery and business continuity planning, regulatory and internal compliance, and auditing may be added to the list of duties. Yet, the security program is what grants the organization the right to take such measures.

Framework - An organization's security is governed by its security policy. Regarding what must be done to comply with the business needs, the framework specifies the policies and processes around the implementation and administration of information security measures. The security framework should specify rules and regulations. It is ideal to have a security framework established before beginning any implementations.

Assessment - An assessment helps you discover and implement important security controls in apps with the help of an assessment. Additionally, it emphasizes avoiding application security flaws and vulnerabilities.

Planning - This stage entails creating a plan that outlines the significant events and milestones that will occur throughout the course of the subsequent time period. One component of the

planning stage is designing the security architecture and how systems are organized inside the design.

Action - Actions explain how procedures are carried out continuously by individuals to deliver the desired results of the security programme in a repeatable, dependable manner. The incident response plan specifies the steps that should be done when a security event happens. Planning beforehand for what to do in the event of a security problem reduces reaction time and offers repeatable, dependable, and efficient steps to contain an incident's scope and harm.

Maintenance - As part of a typical lifecycle of planning, updating, reviewing, and improving, maintenance and support are part of supporting the continuing operations of the security programme and its associated technology.

In order to ensure that the management's intentions are carried out by the many individuals accountable for the behavior and activities outlined in the security rules, policy enforcement is also a component of maintenance. This enforcement frequently involves the cooperation of Human Resources, business management, and security management.

Strategy and Tactics

A security strategy is a comprehensive plan for defense, detection, and deterrence that defines all the architectural and policy elements that go into it. The daily routines of the people and tools tasked with protecting assets are known as security techniques. To put it another way, tactics are frequently reactive whereas plans are typically proactive. Both are equally crucial, and a successful security programme must combine tactical and strategic elements.

1.2) Risk Analysis

Risk mitigation is the goal of a security programme. Mitigating risks does not mean eliminating them; it means reducing them to an acceptable level. You must plan for the different types of incidents that can happen in order to ensure that your security controls are successfully reducing the risks in your environment. Also, you must specify what you are attempting to defend and who from. Risk analysis, threat definition, and vulnerability analysis are used in this situation.

Let's look at some of the terms and definition,

Threats include anything that poses a risk or can do so. Risk analysis includes evaluating threats as a key component. By identifying threats, you can focus your security strategy and lessen the possibility of missing crucial risk areas that might otherwise go unprotected. Threats can come in many different forms, so a security strategy must be thorough enough to handle the biggest ones if it is to be effective.

You must take into account all potential threats in order to prevent missing significant threat sources. Threats should be considered in light of the following factors:

- Threat vectors
- Threat sources and targets
- Types of attacks

Threat Vectors

A threat's origin and route to its target are both described by the term "threat vector." An illustration of a threat vector is an email sent from outside the company to an internal employee that has a tempting subject line and an executable attachment that is actually a Trojan programme that, if opened, will compromise the recipient's computer.

There are numerous threat vectors. For instance, viruses and Trojan horses infect computers connected to a reliable internal network. Trojan programmes are pieces of software that are secretly installed and use the privileges of authorized users to carry out tasks.

Threat Sources and Targets

Threats can come from a variety of sources and have a range of targets within an organisation. It might enter the company through its Internet-facing public face, or it might even be a nefarious insider looking to steal or discredit the company in question. Speaking of the targets, they could be an employee of the company or the servers that power it.

Attack Types

Attacks can be carried out manually by an attacker or automatically by malicious, mobile code that roams networks looking for exploit opportunities. In some cases, an attacker will use an automated programme to identify vulnerable hosts before manually attacking the targets. Attacks that involve entirely automated programmes are always the most effective in terms of the number of computers they compromise. Any computer that can be accessed via the Internet is also vulnerable to attack. Attackers and malicious software will continuously probe it in an effort to find vulnerabilities.

1.3) Compliance with Standards, Regulations, and Laws

Standards, Laws, and Regulations

The fourth layer of security management has been described as information security governance. Technical issues were addressed in the first layer, management issues were addressed in the second layer, organizational issues were addressed in the third layer, and governance issues were addressed in the fourth layer. Information security governance must be a concern for everyone involved in information security, including the board of directors, chief executive officers, information technology and information security professionals, and organization employees.

Information security professionals must contend with developing technologies, crafty and determined cybercriminals, a complex threat environment, and heightened compliance demands resulting from fresh corporate governance initiatives. Even security professionals who work in unregulated settings are expected to adhere to a common set of standards, guidelines, laws, and rules, and it is essential that they comprehend them.

Standards for Information Security

Information security frameworks, also referred to as standards, are a collection of best practices that have been created by and approved by the information security industry as a whole.

The most well-known of these are

- Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO) 27001 and 27002
- National Institute of Standards and Technology (NIST) standards

COBIT

ISACA, the Information Systems Audit and Control Association, is the publisher of COBIT. ISACA is a well-known independent IT governance group, and many organizations use its COBIT guidelines to define and oversee processes based on maturity models like the Capability Maturity Model (CMM). COBIT is a general IT standard that incorporates some information security best practices, but it is not just about information security. Compared to the ISO 27000 series, COBIT contains a higher-level set of information security recommendations.

The COBIT procedures undergo regular updates, and new versions are released by ISACA. COBIT 4.1 is divided into four domains, which are conceptual areas. These four domains are expanded

upon in COBIT 5, which also adds a fifth domain for governance. Versions 4 and 5's domains are as follows:

Governance:

• (v5) Evaluate, Direct, and Monitor (EDM)

Management:

• (v4.1) Plan and Organize (PO) and (v5) Align, Plan, and Organize (APO)

• (v4.1) Acquire and Implement (AI) and (v5) Build, Acquire, and Implement (BAI) • (v4.1) Deliver and Support (DS) and (v5) Deliver, Service, and Support (DSS)

• (v4.1) Monitor and Evaluate (ME) and (v5) Monitor, Evaluate, and Assess (MEA)

Key information security–related components of COBIT 4 (which are carried forward into version 5) include

• PO2.3 Establish an information classification scheme based on the criticality and confidentiality of data, and include ownership information, protection, retention, and destruction requirements.

• PO4.8 Establish an IT security and risk management function at a senior level of an organization's management.

• PO6, PO7.4 Implement a security awareness program along with formal security training for employees, service providers, and third parties.

PO9 Perform risk assessment and management via a risk management program that analyzes and communicates risks and their potential impact on business processes.

• PO10.12 Ensure that security requirements are embedded into the project management process.

• AI2.4 Include security requirements in the application development process to ensure security and availability in line with the organization's objectives.

• AI3.2, AI3.3 Implement security in the configuration, integration, and maintenance of hardware and software to provide availability and integrity.

• AI5.2 Ensure that third-party suppliers of IT infrastructure, facilities, hardware, software, and services comply with the organization's security requirements, and this is reflected in any contracts with those third parties.

• AI7.1–AI7.9 Follow a well-defined change control process that includes testing, production migration, and backout planning.

• DS1.3, DS2.2 Include security requirements in Service Level Agreements (SLAs).

• DS4.1–DS4.10 Perform Business Continuity Planning (BCP) with periodic testing, and ensure that backups are preserved in a safe offsite location.

• DS5.1–DS5.11 Manage security according to a specific plan, perform identity management and user account management, perform security testing and monitoring, perform incident detection and response, implement security protections, employ cryptographic key management, protect against malicious software, secure the network, and protect data exchanges.

• DS12.1–DS12.5 Control physical security and access to important assets with access controls, escorts, and monitoring of activities.

ISO 27000 Series

The ISO 27000 series of information security standards provides a set of frameworks for developing a security program from concept to maturity. It is divided into several manageable parts; each part, like COBIT, prescribes a set of activities that belong to phases similar to those in the Plan-Do-Check-Act (PDCA) cycle.

• ISO 27001 is a high-level specification for the management of an information security program. This is referred to as an information security management system (ISMS). High-level statements about management duties like goal-setting, performance evaluation, and compliance auditing are found in the ISO 27001 standard. It includes instructions for conducting a risk assessment first to identify which controls are most crucial for each organisation and how thoroughly they should be implemented. This is conceptually related to the COBIT "Plan and Organize" idea or the "Plan" phase of the PDCA cycle. Audits can be performed in accordance with this standard (voluntarily, for organisations that aspire to a high level of maturity)

ISO 27002 is a detailed set of information security controls that would ideally be driven by the output of the risk assessment performed as part of ISO 27001. This standard serves as a comprehensive reference for all potential organisational actions. You can think of it as a collection of best practises, and it's up to each organisation to choose which ones apply to their particular industry. This can be compared to the "Acquire and Implement" principle of COBIT or the "Do" phase of the PDCA cycle.

ISO 27003 is intended to offer suggestions and best practises for putting into practise the ISMS management controls outlined in ISO 27001, or how to deliver the security programme. This

can be compared to the PDCA cycle's "Check" phase or the COBIT concept of "Deliver and Support."

ISO 27004 covers measuring the effectiveness of the ISMS put in place by the first three ISO 27000 standards using metrics and key performance indicators. This information is used to assess how well the information security controls are performing. This can be compared to the "Adjust" phase of the PDCA cycle or the "Monitor and Evaluate" concept of COBIT.

ISO 27005 defines a risk management framework for information security that can be used to inform the decisions within ISO 27001 that lead to selection of controls for ISO 27002.

• ISO 27006 is a standard that provides guidelines for professional organizations that provide certification to be properly accredited.

Some significant examples from ISO 27002 that most organisations would probably find interesting include

• 4.1, 4.2 Establish a formal risk management program to assess and treat risks to the organization’s assets.

• 5.1 Publish an information security policy that reflects senior management’s expectations with regard to security, and make sure it is available to all stakeholders.

• 6.1 Establish an internal security organization with appropriate, well-defined responsibilities and relationships with third parties.

• 6.2 Use confidentiality agreements to protect information when working with third parties, to protect access to confidential information.

• 7.1 Identify and document assets, assign ownership, classify according to criticality, and establish an acceptable use policy.

• 7.2 Establish an information classification scheme that includes labeling and handling guidance.

• 8.1–8.3 Perform background checks on employment candidates, communicate security responsibilities to all employees, provide information security awareness and training, and ensure that the correct security behaviors are enforced through a disciplinary process.

• 9.1, 9.2 Establish physical security controls, including perimeters, access controls, separation of critical areas, and protection of equipment.

• 10.1 Establish a change control process along with separation of duties to separate development and production environments and activities.

• 10.2 Manage third-party service delivery.

• 10.3 Perform capacity planning and resource monitoring for proactive allocation of resources.

• 10.4 Protect against malware.

• 10.5 Establish reliable backups.

• 10.6 Establish network security controls.

• 10.7 Manage the handling and disposal of data and the media it resides on, and transport data securely so it can't be intercepted.

• 10.9 Protect online systems, data, and transactions and maintain accurate audit logs to identify issues.

• 11.2–11.6 Manage user access rights to control access to data.

• 12.2 Make sure that applications are correctly processing information and that they check their inputs to avoid misuse, and use encryption to protect that information.

• 12.5 Manage source code development and access, and use a formal change control process to promote code from development into the production environment.

• 12.6 Establish a vulnerability management program.

• 13.1, 13.2 Establish an incident response program.

• 14.1 Perform business continuity management, including regular testing.

• 15.1–15.3 Establish a compliance management program to comply with all legal and regulatory requirements. Perform audits to ensure compliance.

NIST

The National Institute of Standards and Technology (NIST) provides a set of "Special Publications" to assist industry, government, and academic organizations with following best practices.

With the exception of 800-53, the group of security-specific publications known as the "800 series" is very specific to individual technologies. To specify security control organization and structure, security control baselines, common controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls, 800-53 was created primarily for the U.S. Federal Government.

800-53 is organized into 18 “security control families,” which are conceptual categories that represent important components of a complete security program.

1. Access Control

2. Awareness and Training

3. Audit and Accountability

4. Security Assessment and Authorization

5. Configuration Management

6. Contingency Planning

7. Identification and Authentication

8. Incident Response

9. Maintenance

10. Media Protection

11. Physical and Environmental Protection

12. Planning

13. Personnel Security

14. Risk Assessment

15. System and Services Acquisition

16. System and Communications Protection

17. System and Information Integrity

18. Program Management

Each remaining 800 series publication provides guidance on specific subject areas such as WLANs, public cloud, VPNs etc.

Regulations that affect Information Security Professionals

There are other regulations and standards that apply to specific kinds of information and technologies such as HIPAA that provides guidance on different areas such as protection, securing etc.

Health Insurance Portability and Accountability Act (HIPAA) and companion HITECH Act Applies to the healthcare sector, regarding the protection of patient information

Sarbanes-Oxley Act of 2002, Section 404 a.k.a SOX , applies to all publicly traded companies to guarantee data integrity against financial fraud

Gramm-Leach-Bliley Act (GLBA) Applies to the financial sector, including banks and lenders, for the protection of customer and financial information

Payment Card Industry (PCI) Data Security Standard (DSS) Applies to any organization that processes, transmits, or stores credit card information

The Need to Care

Information technology strategy is heavily influenced by information security regulations and the risk of liability that comes with not meeting industry standards for anticipating, preventing, and responding to security breaches. The majority of these new federal and state regulations are focused on protecting electronically stored, personally identifiable information, and they typically only apply to specific business sectors. The regulations lay the groundwork for accountability and liability for organizations that don't implement the necessary safeguards. An emerging duty of care for any entity that obtains or maintains personally identifiable information electronically has been created as a result of the cumulative impact of security breaches. A discussion of the existing regulations provides some shape and contour to the measures that organizations should now consider essential to secure their systems.

The Need for Laws that affect Information Security Professionals

Information security professionals need to be familiar with the components of the various computer crimes listed in state and federal statutes. This is not only because it enables

information security professionals to lessen their organizations' liability for actions taken by their own employees, but also because it helps them protect their organizations' data, products, and communications from outside threats.

It assists in determining whether to alert other members of the organization to a particular act. The likelihood of information security staff raising an alarm in response to unactionable events significantly decreases when they are aware of the essential characteristics of criminal behavior.

Information security experts can use it to set up their businesses to make reliable criminal referrals (or to build solid civil cases). Computer crime laws are a bit special in that they place a lot of responsibility on the victim to take actions to prove that a cybercrime was committed, such as defining access permissions and documenting damage. Information security professionals can design their network defense posture and gather and document crucial evidence when responding to incidents by being aware of this responsibility. The majority of the time, information security managers will take the initiative to draught the information security policies for their organizations, and those policies can include recognition of the main components of computer crime.

It will help to prevent overly forceful responses to incidents that could make a system administrator liable.

1.4) Secure Design Principles

Security Models

Let's compare some of the security models that were proposed previously and still have a significant place in the world of information security.

CIA triad - Confidentiality, Integrity, and Availability is a venerable, well-established conceptual model that deals with the most important aspects of information protection. Security experts are well aware that information security is not just about information and that the CIA only concentrates on three aspects of information protection. Even though the model isn't perfect, it's still beneficial to be aware of it.

Confidentiality – *It* refers to the restriction of access to data only to those who are authorized to use it. Generally speaking, this denotes that a particular set of data is only visible to one or more authorized users or systems. For instance, a password is private because it should only be known by one person, whereas a patient record is confidential because it can be accessed by several members of the patient's medical team.

Integrity - It is the guarantee that the data has not been changed without authorization. It means that unauthorized parties shouldn't change, alter, or even completely delete the data.

Availability - It is the guarantee that a specific service, like network, storage, or compute, is always accessible when required. Implementing high-availability (or continuous-service) controls on computers, networks, and storage is typically done to protect service availability.

The Onion Model

Onion model is a defense security model which is a layered strategy that considers "security" as layered approach where the attacker has to break his way layer by layer just like how a onion is peeled away layer by layer. The better the protection against a failure of any one of those layers, the more layers of controls there are. The layered security approach can be used at any level where security controls are installed. It not only makes it harder for an attacker to get past the defenses, but it also lowers the possibility of an unintended failure of a single technology. It is possible to layer authentication controls for systems, networks, and applications.

Zones of Trust

Different parts of a network have varying levels of mutual trust. Some regions, or what we refer to as "zones," have completely trustworthy services and communication, while others do not.

Zones of trust are a term used to describe how trustworthy a network or computer system is. You can start dividing those functions into zones of trust once you have determined the risks and threats to your company and the necessary functions. You must do this by putting different levels of trust on each group of network resources. Zones of trust are interconnected, and as business needs change, communication between various dissimilar networks, systems, and other network entities is necessary. You can start to develop a plan for containing those systems into zones once you have an understanding of how systems on the network must communicate with one another. Certain areas enjoy greater levels of trust than others, and different areas have varying degrees of mutual respect. A crucial first step in minimizing the vulnerabilities that could jeopardize a security implementation is to list these areas.

Separating the resources into zones of trust enables you to vary the levels of security for these resources according to their individual security needs. A more trusted resource can be shielded from attack by a less trusted one by using multiple zones, which allows access between two zones to be controlled.

Each zone (aside from perhaps a "untrusted" zone) requires that the devices in it have a specific, equivalent level of security; this level of security is determined by the technologies and procedures that are in place to check for attacks, intrusions, and security policy violations. This level of security is required to establish a minimum level of trust.

To keep trust zones apart from one another, network access control devices and technologies such as firewalls, routers, virtual LANs (VLANs), and others can be used (as the walls in the castle analogy did). Based on the authorization rules specified in the security architecture, access control lists (ACLs) and firewall rules can be used to regulate communication between these levels.

The perspective of a transaction can also be used to view trust. Several systems may communicate with one another during a specific transaction through different zones of trust. In a transaction-level trust model, systems can be classified into functional groups according to the kinds of transactions they handle rather than being divided into different trust zones based on where they are on the network.

Even though a transaction may cross multiple network boundaries, all systems involved in it must have equal trust in one another. As a result, security measures at the system and network levels should permit each of these systems to carry out the tasks for which they have been authorized while preventing access to these resources by systems not involved in the transaction.

Some network defense best practices

Physically securing the devices

PCs and laptops may need to be physically fastened to their desks depending on your environment. Lockdown devices come in a variety of forms, from thin rubber-coated wire lanyards to hardened metal jackets specifically designed to enclose a PC. Someone should secure their laptop if they plan to leave it on their desk over night.

UEFI/BIOS password protection

Since the CMOS/BIOS settings of a computer contain many potentially secure settings, such as boot order, remote wake-up, and antivirus boot-sector protection, the majority of CMOS/BIOSs allow you to set up a password to prevent unauthorised changes. It's best if the password is different from other administrative passwords. This is especially important for portable computers, such as laptops and smartphones. The most likely targets for theft are personal computers with small form factors. On a tablet or smartphone, resetting the boot-up password frequently necessitates erasing the data as well, guaranteeing confidentiality and privacy.

Disable booting from optical and USB drives

By preventing boot viruses from USB storage devices and optical drives, as well as attackers from installing a different operating system on the computer, operating system security can be bypassed.

Boost operating system security

Always ensure that the operating system is hardened by taking precautions such as allowing the installation of only secure software, patching and updating the system frequently, configuring the settings securely, limiting the number of administrators and their privileges, and bolstering the authentication processes.

Antimalware programs should be used.

Anti-malware programs are crucial in the modern world. It ought to be installed on desktop computers with compelled automatic updates and enabled for real-time security.

Firewalls are essential.

Firewalls are capable of performing a wide range of security tasks, from straightforward port filtering to stateful inspection systems that can analyze threats occurring anywhere in layers three through seven with computer-based software.

Desktop firewall software, also referred to as host-based firewalls or personal firewall software, is used to protect individual PCs from external and internal threats. It typically has the added benefit of preventing unauthorized software programs, like Trojans, from initiating outbound traffic.

Secure Network Share Permissions

A network share (like NetBIOS or SMB) with no password or a weak password is one of the most popular ways an attacker or worm gains access to a system. The principle of least privilege should be used to apply discretionary ACLs (DACLs) to folders and files that can be accessed remotely over a network, and strong passwords should be used.

Use encryption

Every opportunity should be taken to use encryption. SSH should be used by Linux and Unix administrators to manage their computers instead of Telnet or FTP. If you must use FTP, think about using an FTP service that encrypts traffic using SSL and digital certificates. Both the client and the server must support the same encryption mechanism for encrypted FTP to function. Windows includes the Encrypting File System (EFS) feature. It instantly encrypts and decrypts password-protected files and folders. EFS will automatically create public/private encryption key pairs for the user and the recovery agent once it has been activated by a user. Every encryption and decryption operation is carried out silently in the background. Unauthorized users will not be allowed access to files that are protected by EFS. In some cases, such as when a worm attack is rampantly corrupting every data file it can find on a file server, this could stop malicious activity (like the VBS.Newlove worm does). While the authorized user is logged in, EFS won't stop malware occurrences because it encrypts and decrypts data on the fly.

Securely Configure Applications

Applications should be set up with the recommended security settings from the vendors. However, in end-user PC environments, you want to maintain the applications while reducing the risk. To achieve this, make sure security settings are set at the vendor's suggested levels, if not higher, and apply security patches on a regular basis.

Blocking Dangerous File Types

Given that sending viruses and worms via e-mail is currently the preferred method for doing so, the best way to prevent exploits is to block dangerous file attachments. It is possible to block harmful file extensions at the Internet gateway device, email server, or email client. A plethora of commercial and open source programs exist to block file attachments at the gateway and e-

mail server level. Additionally, the majority of antivirus suppliers provide an email server antivirus solution.

Lock Down Applications

The ability of an end user to install and run any software they desire poses one of the biggest risks to any environment. There are numerous tools available to restrict what a desktop user can and cannot run. In Windows, an administrator could set system policies to severely restrict the desktop, disable the user's Run command, and prevent the installation of new applications. Administrators can specify what software is permitted to run on a specific computer using Windows' Software Restriction Policies feature.

Secure P2P Services

Music sharing and other peer-to-peer (P2P) applications are likely to continue to be popular targets for attacks in the future. This is due to the fact that P2P applications frequently get installed in the corporate environment without the administrator's permission and have very little security, if any. Additionally, they are built to access files on the computer of the end user, which makes it much simpler to steal those files.

First, get rid of P2P if it isn't permitted in your corporate environment. Start by educating end users and establishing sanctions for unapproved software with management. Then locate the programs and uninstall them. Finding them requires checking firewall logs for known P2P port attempts, sniffing P2P packets with an IDS on the local network, or using P2P auditing software.

Second, confirm that your firewall is set up to specifically block P2P traffic. It can be challenging to block P2P traffic by port number alone because P2P software frequently uses port 80 as a proxy port, but there are steps you can take. Block the destination at the firewall if P2P clients connect to servers with a specific IP address or in a specific domain. Some firewalls permit the use of wildcards in domain names that are blocked, such as *irc* or *kaz*. Last, if your end users insist on using P2P, and it is authorized by management, insist on a more secure P2P application, if at all possible.

Make Sure Developers Code Securely

SQL injection and buffer-overflow attacks can only be defeated by programmers using secure coding practices. Using double quotation marks in place of single quotes can help prevent SQL injection attacks. Input validation is necessary to prevent buffer-overflow attacks. If the programmer makes the application well-designed and secure, other attacks of this nature could be easily avoided.

Back up the system

The most frequent sign of malware damage is frequently altered, corrupted, or deleted files. Viruses and worms frequently destroy files, reformat hard drives, or purposely corrupt data. Malware can maliciously modify a system even if it doesn't intentionally alter any files on the host system. Security professionals sometimes are unable to undo the harm and restore the system to its pre-exploit state. Therefore, it's critical to maintain frequent, verified system backups.

. At the very least, all of your data files should be included in the backup, and a full system backup ensures a speedier recovery in the event of a serious exploit event. Additionally, you need to confirm that your backups weren't contaminated by the malware.

Implement ARP Poisoning Defenses

One of the most frequent and potent threats to network infrastructures is ARP poisoning attacks (especially wireless networks). They are a type of man-in-the-middle attack (MITM) that enables an attacker to covertly intercept and change network traffic. Therefore, these attacks require unique defenses of their own. An organization can protect itself from an ARP poisoning attack in a few different ways. Static ARP tables, port rate limiting, or DHCP snooping with dynamic ARP inspection are a few examples of defenses (DAI). A mix of the latter two strategies is the best form of defense.

Configure Port Rate Limiting

Port Rate Limiting (PRL) restricts and tracks the volume of traffic that can pass through a port in a given period of time. When the configured threshold is tripped, the port automatically closes until it is manually enabled or until a predetermined amount of time has passed (usually 15 minutes).

It is simple to understand why PRL is a respectable line of defence when considering how an MITM attack with ARP poisoning operates. As previously mentioned, ARP poisoning operates by routing the victim system(s)' traffic through the attacker's tool. If an attack is launched against a port that has PRL, the volume of traffic should be sufficient to exceed the threshold and shut the port down. You have essentially prevented an attacker from performing ARP poisoning from that port if you make the port inaccessible to them.

If enabling the port requires manual intervention, this may serve as a warning to the organization, especially if it occurs on several ports at once.

Use Dynamic ARP Inspection and DHCP Snooping

DHCP snooping combined with dynamic ARP inspection is the most efficient way to combat ARP poisoning (DAI). This defense is based on the fact that it discards any ARP reply requests that are not in its table. Similar to PRL, this defense necessitates some environment research on the part of the organization before full implementation can take place. For two to three weeks, the organization must run DHCP snooping in order to properly compile a table of IP addresses and MAC addresses. Once that table has been created, DAI can be used. DAI offers a strong defense against ARP poisoning attacks once it is implemented.

1.5) Security Policies, Standards, Procedures, and Guidelines

The four components of security documentation are policies, standards, procedures, and guidelines. Together, these form the complete definition of a mature security program.

Security Policy

A security policy is a document that outlines the security requirements of an organization. A security policy outlines what must be done, not how to do it, and it doesn't name any particular tools or fixes. The security policy outlines a specific set of goals and requirements that will help safeguard an organization's resources and operational efficiency.

It serves as the fundamental framework for an efficient and thorough security program. A strong security policy should be a high-level, succinct, formalized declaration of the security procedures that management anticipates staff members and other stakeholders will adhere to. A security policy should be succinct and simple to comprehend so that everyone can adhere to the instructions provided in it.

A security policy outlines clear guidelines for management, technical staff, and staff members. What an organization does in response to a security violation will depend on its explicit and well-documented security policy. Organizations put themselves at risk and frequently struggle to respond to a violation when there is no clear policy in place.

For managers, a security policy outlines the senior management's expectations regarding the roles, responsibilities, and actions that management should take in relation to security controls.

For technical staff, a security policy specifies which security measures should be applied to computer systems, physical infrastructure, and networks.

For all employees, a security policy describes how they should conduct themselves when using the computer systems, e-mail, phones, and voice mail

The security practitioner is given a road map for efficient, reliable policy production by using a top-down approach to security policy development. The person creating the policy must take the time to comprehend the regulatory environment, corporate goals, and risk management issues, as well as the general policy statements of the organization.

Security Policy Development

When developing a security policy for the first time, one useful approach is to focus on the why, who, where, and what during the policy development process: 1. Why should the policy address these particular concerns? (Purpose)

2. Who should the policy address? (Responsibilities)

3. Where should the policy be applied? (Scope)

4. What should the policy contain? (Content)

Security policy must be developed in the following phases,

1. Requirements gathering
   - Regulatory requirements (industry specific)
   - Advisory requirements (best practices)
   - Informative requirements (organization specific)
2. Project definition and proposal based on requirements
3. Policy development
4. Review and approval
5. Publication and distribution
6. Ongoing maintenance (and revision)

To ensure a smooth implementation after the security policy has been approved, standards and procedures must be created.

Security Policy Contributors

The following contributor groups may be represented in a security policy:

Human resources - When it comes to employee rewards and punishments, the HR department is typically in charge of enforcing the security policy. When the company's policies are broken, HR imposes sanctions, up to and including termination. Additionally, HR gets a signature from each employee confirming that they have read and comprehend the organization's policies, so there is no doubt about who is to blame when employees don't follow the rules.

Legal - A company with an internal legal department or outside legal counsel will frequently want to have those lawyers review and explain any legal points in the document and offer advice on specific matters of appropriateness and applicability, both in the organization's home country and abroad. When their policies are applied to specific employees, all organisations are advised to have some sort of legal review and advice.

Information Technology - Computer systems, and more specifically the security safeguards integrated into the computing infrastructure, are frequently the focus of security policy. The biggest users of the policy information are typically IT staff.

Physical Security - The physical security controls listed in the security policy are typically implemented by physical security (or facilities) departments. In some circumstances, the physical security system's information systems components may be managed by the IT department.

Security Policy Audience

The intended audience for the security policies is all the individuals who handle the organization's information, such as:

- Employees
- Contractors and temporary workers
- Consultants, system integrators, and service providers
- Business partners and third-party vendors
- Employees of subsidiaries and affiliates
- Customers who use the organization's information resources

Policy Categories

Three main categories can be used to further divide security policies:

Regulatory - It is helpful to include this particular category for audit and compliance purposes. Typically, the policy is filled with a number of legal declarations that explain what is required and why it is required. It is possible to include the findings of a regulatory requirements assessment in this kind of policy.

Advisory - This type of policy informs all parties who may be impacted of business-specific rules, which may include rules pertaining to computer systems and networks, people, and physical security. Typically, this kind of policy is based on security best practises.

Informative - To ensure that policies not covered under Regulatory and Advisory are taken into account, this kind of policy is available as a catch-all. Specific business units, business partners, vendors, and clients who use the organization's information systems may be subject to these policies.

The security policy should be concise and easy to read, in order to be effective. It should consist of a few straightforward declarations of the intentions of senior management.

The following elements can be used as an outline to represent the structure and organization of security policies:

• *Author* - The policy writer

• *Sponsor* - The Executive champion

• *Authorizer* - The Executive signer with ultimate authority

• *Effective date* - When the policy is effective; generally, when authorized

• *Review date* - Subject to agreement by all parties; annually at least

• *Purpose* - Why the policy exists; regulatory, advisory, or informative

• *Scope* - Who the policy affects and where the policy is applied

• *Policy* - What the policy is about

• *Exceptions* - Who or what is not covered by the policy

• *Enforcement* How the policy will be enforced, and consequences for not following it

• *Definitions* Terms the reader may need to know

• *References* Links to other related policies and corporate documents

Additional Security Frameworks and Laws

There are numerous security frameworks that work well with specific information technology components.

For instance, the HIPAA act clearly outlines how PHI (Personal Health Information) and other patient health-related data should be handled, transmitted, protected, and stored.

Therefore, it would be more beneficial if we took into account other similar frameworks when developing a security policy.

An organization or a business entity may need to abide by a number of laws. Therefore, it is crucial to develop a security policy that complies with these laws and rules. The security policy's

author and contributors must make sure that it complies with all applicable laws and regulations.

Security Awareness

Frequently, trusted internal staff members who have been given access to internal resources serve as the first line of defense against an organization's assets. The human element is, as with most things, the least predictable and most vulnerable to abuse. Trusted workers are either deceived or corrupted into unintentionally divulging useful information that helps burglars. Employees are the weakest link in any security chain because of the high level of trust that is placed in them.

Education is one of the best ways to stop employees from disclosing information, according to research. Employees are less likely to unintentionally assist an attacker in information gathering when they understand why they shouldn't disclose private information, are aware of the reasons why, and are aware that they will be held accountable. Social engineering and information leakage threats are lessened by education and training.

Importance of security awareness

Even the most meticulously designed security infrastructure is frequently compromised by employees either intentionally or unintentionally. This is due to the fact that in order to perform their duties, they are given trusted access to information resources through firewalls, access control mechanisms, structures, phone systems, and other private resources. End users have access to the system accounts and passwords required to copy, modify, delete, and print confidential information as well as alter its integrity level and prevent access by authorized users. Most organizations have common practices that put the information security program at risk, including propping open doors, disclosing account and password information, and throwing away sensitive documents. A security awareness program aims to change and stop these behaviors as well. Employees who are well-versed in security principles and practices can contain the damage a security breach causes quickly.

Implementing the Awareness Program

Once staff members are aware of security issues, they can start considering how to carry out their duties in accordance with the security policy and how to respond to security-related events and incidents. Following security policy and incident response typical topics include

- What to do about unauthorized or suspicious activity. How to report potential security events, including who should be notified, what to do during and after an incident, the timeframe for such reporting, and what to do about those events. When an employee is acting suspiciously, a

computer system is being attacked, or email could be intercepted by an intruder, it may be necessary to communicate verbally rather than via email. These are just a few examples.

- Securing the use of information technology systems.

- How to handle email attachments, create and manage passwords, and transfer and download files securely.

The awareness campaign should make it clear that management places a high priority on security. It should be made clear that everyone in the company, from executive management to every employee, is accountable for security procedures. When executives set an example and employees can see that security procedures are important to the company rather than just another initiative, they will be more likely to take them seriously.

Enforcement

Perhaps the most crucial element of network security is enforcement. If policies, procedures, and security technologies are disregarded or used improperly, they will not function. Enforcing the security policy guarantees adherence to the values and procedures that the security infrastructure's designers intended.

There are numerous ways to enforce. Enforcement gives general employees the confidence that daily work activities adhere to the security policy. Enforcement ensures proper maintenance procedures are taken by system administrators and other privileged staff members and prevents abuse of the increased level of trust accorded to this group of employees. For managers, enforcement reduces the likelihood of conflicts of interest caused when managers give their employees orders that are against policy and prevents overriding of the security practices intended by the policy's authors.

Enforcement discourages people from inadvertently, deliberately, or casually breaking the law. Normally, Human Resources is directly responsible for enforcing the corporate security policy for employees and temporary workers. For egregious security policy violations, HR implements punitive measures, up to and including termination, and also makes an effort to change behavior through warnings and evaluations. HR may also use financial incentives and other forms of positive reinforcement, such as bonuses. The same standards of policy enforcement should be applied to every employee, without exception. When enforcing policy, it is crucial to avoid prejudice or distinction between employees. In management, this is especially true. Senior managers and corporate executives, in particular, ought to be held to the same standards of accountability as regular employees, if not higher. Senior management ought to be a role model for ethical conduct for the rest of the company and maybe even held to a higher standard than those who report to them.

Software can occasionally be used to enforce policy compliance and stop behaviors that are against the rules. Controls for web browsing like website blockers are one illustration of this. Each time a user tries to access a website, these programs consult a list of websites that are forbidden. The attempt is blocked if it is made to access one of the forbidden websites. The benefit of software-based enforcement is that staff members are physically unable to break the law. The operating system's Group Policy settings are among the others. This implies that, despite their best efforts, no one will be able to violate the policy. As a result, the organization is guaranteed complete policy compliance. Software enforcement is the easiest and most reliable method of ensuring compliance with security policy.

The corporate security policy and acceptable use policy should be thoroughly documented, communicated to employees, and signed by them to show that they have read, understood, and agree to the terms, regardless of the corporate culture or how software-based enforcement is used in the organization to control behavior and promote compliance. Software-based enforcement should only be one step in a chain of enforcement techniques that includes other levels, including termination, when it is used.

For this reason, businesses shouldn't just rely on software; they also need levels of deterrence that are understood by all employees. Employees should be aware that they may lose their jobs if they act in ways that go against the employer's ethics or principles because employment is typically an at-will relationship between the employer and the employee. Instead of using software as an escape or a way to avoid the challenges and hardships of enforcement, use it to help the organization reach its enforcement objectives.

Security Standards

A policy is less specific than a standard. Standards should be regarded as obligatory because they provide instructions on how to adhere to the policy and because they are connected to policies. Standards define specific technology settings, platforms, or behaviours and are the extension of policy into the real world. Typically, security managers who are in charge of the IT infrastructure spend more time writing standards than they do policy. Compared to policy, which anyone should be able to understand regardless of level of expertise, security standards are much more detailed.

Security Procedures

Security procedures are detailed instructions on how to carry out a particular task. The level of specificity is higher in security procedures than it is in policies and standards. A system administrator would follow the procedure while seated at the keyboard of the computer that is being built. This information is very specialized and only intended for system administrators, so

the majority of people won't understand it. A security procedure will typically contain specialized information that is highly job-specific.

Security Guidelines

Guidelines provide guidance. They are only recommendations on how to abide by the policy; they are not requirements. The purpose of guidelines is to help people understand how to achieve the objectives set forth in the security policy, which should make life easier for both the end user and the security manager who wrote the policy.

Ongoing Maintenance

The security guidelines, policies, and standards are ever-evolving documents. They are not written once and then left unchanged for years, in other words. In response to evolving business conditions, technologies, customer requirements, etc., these documents should be updated on a regular basis. To manage this lifecycle process, some kind of document version control technology may be useful.

Finalizing the Implementation with Audits

An audit may be carried out by external organizations or internal divisions once the security policies, standards, procedures, and guidelines are in place, well-established, and in a position to direct day-to-day operations. An audit contrasts current procedures with the goals of the policy. A disinterested party (not the security organization or the IT department) must conduct the audit in order to identify weaknesses or issues with the policy and its enforcement. This requires having an unbiased third-party perspective. Any frequency—monthly, quarterly, yearly, or at another interval—can be used for audits. Audits of security policy compliance should be performed at least once a year because longer time frames could allow for significant differences between the operations and the policy.

Part Two

Data Security

2.1) Introduction to Databases

Information security professionals' first and foremost responsibility is to secure the data. Therefore, it's crucial to establish policies, adhere to processes, and practice some discipline when it comes to data security.

Difference between Structured and Unstructured Data

Data that complies with a rigid data model is said to be structured data. The majority of IT and security experts define structured data as data that is stored in a database and is arranged according to the database schema and any corresponding database rules. The structure of the data itself typically makes it possible to classify it quickly. For instance, you could locate a person's medical history in a database and implement security measures in line with that discovery. You have complete control over who can access structured data. Structured data can be easily defined and applied security controls using either the structure's inherent features or third-party tools created for that particular structure.

Unstructured data is much harder to secure and manage. Unstructured data is mobile across all networks, can exist anywhere, and can take any form. Think about a patient record being pulled from the database, displayed in a web page, copied into a spreadsheet, attached to an email, and then sent to a different address. There is no set format for unstructured data. The original structure of the data has been changed as it moves between formats.
The key areas where unstructured data can reside can be broken down into the following categories:

- Databases
- Applications
- Networks
- Computers
- Storage
- Physical world (printed documents)

Databases

The hub of the data universe is the database. The majority of the data you are attempting to protect either exists in, was created and inserted into, or was retrieved from a database. You must protect the database's data while allowing authorised users and applications to access it for practical reasons. Databases were previously only used to store structured data, but new

advancements in database technology have led to an increase in the amount of unstructured data being stored in databases. For instance, a content management system or application that stores pictures, videos, and other unstructured data can use a database as its storage component.

Encrypting Unstructured Data at Rest in the Database

Encryption is the most popular method for protecting the data in a database. There are several methods for encrypting data that is stored in a database:

• Encryption of the data itself, allowing it to be kept in an encrypted state in regular data files. The encrypted data is passed to the application to decrypt because the database may not be aware of (or care about) whether or how the data is encrypted.

• Partial encryption of the database schema, whereby only particular rows, columns, or records are encrypted depending on where the data will be stored. In this instance, the database manages data encryption and provides the application with the decrypted data.

• Full encryption of the database data files, ensuring that all data contained therein is encrypted.

Database exports and backups may be protected without additional technology depending on the type of encryption used. Data masking technologies are frequently used to declassify data that must be used in development environments. These technologies scramble or randomize real data to create fake information that retains many of the same properties as the original data.

Implementing Controls to Restrict Access to Unstructured Data

Restricting access to data is largely accomplished through database access controls. The strategies employed by various databases range from simple username and password authentication to a complex set of rules that specify who is permitted to access what from where, when, and with what application for various levels of data classification.

The credentials that are used to authenticate and grant access to data can either be kept on the database platform itself or in a separate identity directory. This makes it possible to link data security to the enterprise directory store, making it simpler to manage the access control model by utilizing the already-existing access control infrastructure.

The trust that the process that is permitted to access the data is legitimate or that the data remains secure after it leaves the database still underlies all the work put into configuring controls to restrict access to the database.

Securing Data Exports

The ability to bulk export data into other databases is a feature offered by many databases. There are security issues as a result. Encryption can be used at the export stage to solve this issue. This mechanism typically differs from those used for system-wide database backups or the encryption of data in the schema. It is typically possible to provide a passphrase when exporting data, which will be used as the key for the export's one-time encryption. Because the encrypted export and passphrase are shared separately when given to the user importing the data into their own system, this enables sets of data to be protected in transit.

Keeping Database Storage Secure

Databases and storage have a lot in common. Security of the storage becomes just as crucial as security of the databases. Although storage security solutions primarily deal with data at rest, sometimes stored data is also in use or in transit. The contents of a PDF file, which the operating system pages to the disc and stores in RAM as an illustration, are an example of this.

Storage Encryption

Encrypting these locations is an obvious solution because data in databases, network storage, content management systems, and computers ultimately end up being stored on storage gadgets like hard disc arrays or USB flash memory. There are two types of encryption techniques for storage devices:

• Hardware-based or software-based disc encryption

• File-system encryption

- *Hardware-based/software-based disk encryption*
  Disk encryption is the process of encrypting the disk(s) and its contents using software or hardware in a way that is transparent to the operating system, the application, or the content format. Before any data on the drive can be decrypted and read, some type of authentication must occur.

- *File-System encryption*
  When data is encrypted at the file system level, it is said to be file system encryption. This implies that the approaches could change based on the operating system being used. The primary distinction between file and folder encryption and metadata encryption is that the former only secures files and folders. In other words, without the cryptographic keys, an unauthorized person can list the files, view their names, and determine who owns them. However, they cannot actually access the files. Like disc

encryption, file-system encryption only takes effect when the content is stored in an encrypted location. The data is no longer secure if it is transferred from the encrypted disc to an unencrypted disc.

Data Loss Prevention (DLP)

Data loss prevention (DLP) is the name given to a group of relatively recent technologies used to track, find, and safeguard data. Three categories of DLP technologies exist.

• *Network DLP* - Typically a network appliance serving as a bridge between significant network perimeters (most commonly between your corporate network and the Internet). Network DLP keeps an eye on the traffic that enters the gateway in an effort to spot sensitive information and take appropriate action, usually blocking it from leaving the network.

• *Storage DLP* - Software that performs the same tasks as network DLP, running either on an appliance or directly on the file server. Searching for sensitive data, storage DLP scans storage systems. Once discovered, it has the ability to remove it, place it in quarantine, or simply alert the administrator.

• *Endpoint DLP* - Endpoint systems run software that keeps track of operating system and application activity, keeps an eye on memory usage, and scans network traffic for the unauthorized use of sensitive data.

Information Rights Management (IRM)

Regardless of where data files are stored, transmitted, or used, information rights management (IRM), a relatively new technology, incorporates protection right into the data files. To permit authorized users to open files and to block unauthorized users, IRM uses a combination of encryption and access controls. IRM encrypts files using advanced encryption methods. Software is needed to check with a central authentication server (typically located somewhere on the Internet) and determine whether the requesting user is authorized to unlock the data when a request is made to open, copy, modify, or decrypt the file and the data.

Security risks related to storage

Malfunctions

Data integrity is harmed by computer and storage malfunctions that corrupt data. Make sure the storage infrastructure you choose has appropriate RAID redundancy built in and that important data archives are part of the service to avoid malfunctions. You can also use integrity checking software that verifies data using checksums or other methods.

Data Deletion and Data Loss

Due to malfunctions in computer systems or improper handling, data can be destroyed on purpose or accidentally. Financial, organizational, individual, and audit trail data are some examples of this type of data. If such important data can't be recovered, it's lost forever once it's lost. To prevent data deletion and data loss,

• Make sure your critical data is redundantly stored and housed in multiple locations to prevent data loss and deletion.

• Keep track of and analyse audit logs for data deletion.

• Continue to offer programs that educate and inform those who access and manage data. Make sure to assign data owners who will be in charge of the data, bear responsibility for its loss, and have authority over it.

Data Corruption and Data Tampering

Data that is invalid or damaged can have serious consequences because valid, trustworthy data is the basis of every computing system. The integrity of data can be harmed by alterations brought on by faulty computer or storage systems, malicious individuals, or malware. A person who alters data with the intention of defrauding another party can harm integrity. To avoid data tampering and corruption,

• Maintain archive copies of important data before it is modified by using version control software. Make sure antivirus software is protecting all data. Maintain least privilege, role-based access control over all data in accordance with job function and need to know.

• Use integrity-checking software to track and notify changes to important data.

• Continue to offer programs that educate and inform those who access and manage data. Make sure to assign data owners who will be in charge of the data, bear responsibility for its loss, and have authority over it.

Denial of Service (DoS) attacks

A denial of service (DoS) attack or distributed denial of service (DDoS) attack aims to prevent the intended users from accessing a computer resource. This type of attack typically entails overwhelming the target machine with too many communications requests, rendering it ineffectively unavailable or unable to respond to legitimate traffic. The majority of DoS and DDoS attacks use compromised systems all over the world, making them difficult to track and vulnerable to defenses because they flood system and network resources. To prevent DoS attacks,

• Pick a storage platform with strong defenses against network intrusions. At the storage network's edge, install firewalls, an IPS, and network filtering to prevent attacks.

• Always keep an eye on intrusion detection systems.

• Collaborate with your legal team to find and bring charges against the attackers.

Outage

Any unplanned downtime or unavailability of a computer system or network is referred to as an outage. Storage infrastructures may be unavailable for as long as it takes to switch to the disaster recovery environment because unexpected outages can happen even when every device and network path is fully redundant.

Redundancy is the main safeguard against any service interruption. Make sure that each system, piece of hardware, and network link is clustered or configured to use high availability. Calculate the cost of downtime and use that figure to support investing in the extra equipment required for redundancy. Use a reliable disaster recovery plan as well to make sure you are prepared for prolonged outages and to enable automatic switching of storage environments to alternative locations in the event of an outage.

Utilize monitoring tools to continuously keep an eye on the storage environment's availability and response times. Little can be done to prevent outages because they typically result from software issues, making them difficult to prevent.

Instability and Application Failure

Applications may freeze, lock up, crash, or become unresponsive due to issues with software or firmware, which can also cause a computer or network to completely fail or lose functionality. To prevent instability and application failure,

- Ensure that all software updates are regularly applied to the infrastructure in order to prevent instability and application failure.
- Use service monitoring to find and notify you when an application is not responding as it should.

Slowness

When the response time of a computer or network or storage is considered unacceptably slow, its availability is affected. Slowness can continue and cause efficiency loss and useful downtime. To prevent slowness of storage,

- Configure the architecture using redundant storage and network connections so that application access will automatically switch to the fastest environment. Make sure you've also implemented high-capacity services with demand-driven resource expansion.
- Constantly check the applications' response times, and make sure alerts are delivered to support staff outside of the system to prevent delivery issues.
- Write clauses into contracts with storage manufacturers that offer rewards for late responses.
- Despite best efforts, slowness can continue, leading to lost efficiency and ineffective downtime.

High Availability

When a device has a problem, a service that is supposed to switch over to other, working devices might not actually switch over properly. This might occur, for instance, if a primary device gradually becomes less responsive to the point where it is effectively unresponsive, but the HA software doesn't actually recognize this as a "down" state. To prevent HA failure,

- Run recurring failover tests
- Monitor the health of backup systems or all the systems in a HA cluster.
- There isn't much that can be done to ensure that systems will switch over when they should.

Backup Failure

Data loss occurs when you realize the backups you were counting on aren't actually any good, either because the backup media is damaged or the backup data is corrupted or missing. Backups fail, but multiple paths to recovery can reduce the risk to a large extent. Data backups are one of the most dependable security practices because they have been done for a long time. Data can last an eternity if it is properly replicated. In order to stop backup failures,

- Use storage elasticity to avoid using conventional offline backups (on tape or in optical form).
- Repeat recovery tests frequently to confirm the data's resilience.
- Include a data-loss clause in the agreement with the storage manufacturer so that they will be motivated to assist with an unexpected data loss.

Few Things to Remember

Last but not least, it's critical to make sure that the server environment itself is under control and observation. Security of the storage infrastructure alone is insufficient. Any server that is accessed could be dangerously exposed, as could the storage environment. Server configuration must be secure, and the equipment must be kept in a facility that is monitored and secure with access control. The security of the storage environment should be taken into consideration when performing change management and activity monitoring to keep track of system changes and the actions of administrators on the server. Not only on the servers hosting the data, but also on the management servers used to manage the arrays and switches, these actions must be taken.

Solid understanding of storage security procedures should be part of the required skill set when hiring people to manage and secure the storage environment. An important requirement should be to have knowledge of computer security, networking, and storage techniques.

A crucial step in any organization's business continuity process is offsite (secure) data storage. To guarantee accountability for all data sent offsite, these facilities should undergo regular audits. Whether on disc or tape, the data should be encrypted for security reasons. End-to-end encryption should be used for all forms of online data backup.

2.2) Database Security

Databases play an important role in businesses as organizations typically deal with humongous amount of data that gets stored in databases either in a simple row-column format or complex non-relational format.

There are many uses for databases, including:

• Application support

Relational databases are the most widely used method for storing data, and can be used to store anything from basic employee lists to enterprise-level tracking software.

• Secure storage of sensitive information

One of the safest ways to store crucial data centrally is with relational databases. In regulated industries, these techniques can be used to comply with legislative requirements.

• Online transaction processing (OLTP)

Client applications and other servers access information that is stored and processed by OLTP systems. High levels of data modification are a defining characteristic of OLTP databases (inserting, updating, and deleting rows). As a result, they are enhanced to support dynamic data. They typically hold large amounts of data, which if not properly managed, can quickly grow.

• Data Warehousing

Platforms for relational databases can act as a central repository for data gathered from a variety of internal data sources. Then, "decision support" systems and centralised reporting can both use this database.

Database Security Layers

Database Server-Level Security

A database application's security depends entirely on the server it is installed on. Therefore, whether the servers are located locally or off-site, it is crucial to secure the servers on which your databases will be hosted.

- Choose which programs and users should have access to it.

- Make sure the databases are physically secure to prevent unauthorized individuals from accessing database files and data backups.

- Direct physical access to a database is rarely necessary because modern database platforms can be managed remotely.

Database Network Security Layer

Database security at the network layer is also crucial. These are a few best, typical practices

- Implement routing rules and packet filtering to make sure that only specific users on the internal network will even be able to communicate with a server.

- Modify the server's default port of listening.

Database Encryption Layer

Since databases store numerous types of information, including credit card numbers and passwords, which may or may not be sensitive and confidential, data encryption is a crucial security feature in areas outside of the network layer.

- A database can make effective use of data encryption

- Only the calling application will be able to decipher and make use of the encrypted values that are obscured in the data to allow authorised users to access and modify the data as needed.

On the majority of platforms, operating system security and database security are mutually exclusive. Database security can be affected by a variety of factors, including operating system encryption capabilities, file system permissions, network configuration settings, and authentication procedures. It's crucial for systems administrators to keep permissions settings current and to make sure that unused accounts are promptly deactivated.

Database-level security

Users have various types of permissions based on their job functions, and databases are frequently used to host a wide variety of databases and applications. Although any user may be able to connect to a database, each user will only be given the permissions they need.

In most cases, which databases a user has access to is determined by the first type of database-level security. Database administrators can specify whether or not a user login is required to access a particular database. Additional permissions must be assigned after a user has been given access to a database in order to specify the actions that user is permitted to perform there.

Database Roles and Permissions

Choosing the database(s) to which a login may connect is the first step in the general process. The database must then be assigned permissions. Typically, "groups" or "roles" are created by database administrators, and each of these contains users. The roles each have a set of permissions. Database administrators can easily manage which users have which permissions by using roles.

Object-level security

Relational databases can store a wide variety of objects. But the fundamental unit for storing data is a table. In general, each table is made to refer to a specific kind of entity. Information about each of these items is stored in columns within these tables. The ability to use one or more of the most popular SQL commands is granted. These commands are

• SELECT - Retrieves information from databases. SELECT statements can obtain and combine data from many different tables, and can also be used for performing complex aggregate calculations.

• INSERT - Adds a new row to a table.

• UPDATE - Changes the values in an existing row or rows.

• DELETE - Deletes rows from a table.

The ANSI Standard SQL language provides for the ability to use three commands for administering permissions to tables and other database objects:

• GRANT - Specifies that a particular user or role will have access to perform a specific action.

• REVOKE - Removes any current permissions settings for the specified users or roles.

• DENY - Prevents a user or role from performing a specific action.

Improvising Database Security

It's wise to refrain from granting permissions directly on database tables as a general rule. Instead, you should give users access to other database objects by giving them permissions so they can access the data they require. We'll take a broad look at the three frequently used database objects in this section and discuss how they can be used to more effectively manage security settings.

Views

A view is a logical relational database object that actually refers to one or more underlying database tables. In general, views are defined as the output of a SELECT query. This query can then retrieve data from numerous different tables and process the data using standard mathematical operations. One of the most popular techniques for limiting access to data is the use of views. Database administrators now have a way to define granular permissions settings that were previously impossible. After a view has been created, it can be given object-level permissions. The view will then allow database users to access any necessary information. A chain of objects based on business rules can be created by views by querying other views.

Stored Procedures

Database stored procedures allow different users to carry out common tasks. By using objects called stored procedures, databases allow developers to write and reuse SQL code. Any operation that can be carried out with the aid of common SQL commands can be performed using stored procedures. They can also consider arguments (much like functions and in other programming languages). Regarding security, stored procedures let users make changes to data kept in tables without granting direct access.

Triggers

Triggers are intended to be activated automatically whenever certain actions occur within a database. Triggers can be applied in various ways in terms of security. To start, you can conduct thorough auditing using triggers. For instance, you might want to alert a senior manager whenever certain information in a table is changed, or you might write a row logging this action to another table. Triggers can also be used to enforce complex database-related rules. For instance, if you want to guarantee that a particular set of actions is always performed whenever data is changed, you can create the necessary trigger to accomplish this.

In addition, you can customize the permissions that each web application has on the database by creating multiple accounts for each web application that tries to access the databases.

Securing databases from internet based applications

Web servers are used by many internet-based applications to access databases. It is crucial to protect the web applications that are running on these web servers so that they don't offer a route for attacking the databases. Some of the preventive measures that you could take against such risks,

- Prevent direct access to the databases from all but the most trusted servers (or, sometimes, networks)

- Web and standard-client applications often use a “connection string” to store authentication information. For administration purposes, this information is often stored in configuration files that can be modified, as needed. Ensure that these files are properly protected (through the use of encryption and file system permissions)

- To prevent errors, data corruption, or system crashes and attacks such as SQL injection, data validation must be done.

Database Backup and Recovery

Database Recovery and Backup

Accidental human error, flawed application logic, flaws in the database or operating system platform, and, of course, malicious users who are able to get around security measures are all potential causes of data loss. The only real way to recover data in the event that it is incorrectly altered or completely destroyed is from backups.

Choose the databases and tables you want to backup first. It's time to consider how to implement a data protection strategy once you have a good idea of what your company needs to back up. Prior to looking at the technical requirements for any type of data protection solution, it is imperative that you define your business requirements. You might also have a preliminary budget cap that can be used as a benchmark for comparing solutions in addition to these requirements. Additionally, you should start considering your staff and the kinds of expertise you'll need to have on hand in order to implement a solution.

Additionally, it's critical to remember that the goal of data protection is not to produce backups. The ability to recover information in the event that it is lost is the true goal. To that end, it's a good idea to start designing a backup solution based on the data you need to recover. The cost of downtime, the worth of the data, and the maximum amount of allowable

data loss in the worst-case scenario should all be considered. Also consider the likelihood of specific catastrophes.

Auditing and Monitoring Databases

When it comes to network and database security, the concept of accountability is crucial. Keeping track of data changes and permission usage is part of the auditing process. Before much harm is done, users who are attempting to violate their security permissions (or users who are not authorised at all) can frequently be identified and dealt with; alternatively, once data has been altered, auditing can provide information about the extent of loss or changes. Users may be less likely to try to snoop around your databases if they are aware that certain actions are being tracked. This method can therefore act as a deterrent.

Unfortunately, auditing often goes unnoticed in settings. You can track particular actions based on user roles or actions on particular database objects in the majority of relational databases. Too much information auditing frequently has a negative impact on system performance. Audit logs may also consume a sizable amount of disc space. Therefore, auditing systems need to be properly configured.

Most database administrators ought to configure logging of both successful and unsuccessful database login attempts, at the very least. This measure will provide some level of accountability even though it will only provide limited information on its own.

Reviewing Database Audit Logs

System and database administrators should routinely review the data gathered in order for auditing to be truly useful. Only by engaging in this activity can potential security settings issues be identified before they worsen. As a result, you might want to check the audit logs and establish specific responses to unusual activity that is logged. Additionally, reading through logs can be overwhelming; therefore, any techniques for filtering the gathered data can be useful.

Monitoring Databases

Sometimes all you need is a quick snapshot of the server's users and their activities. The majority of databases offer simple ways to view this data. Starting with the most recent activity information may not be the best way to discover potential security breaches, but it can give you a better understanding of how your database is being used. You will be able to quickly spot any potential system abuse by creating a performance and usage baseline. Additionally, based on typical activity, you can set up alerts that can be used to alert you when performance or other statistics are "out of bounds."

Part III

Network Security

3.1) Secure Network Design

Network design frequently overlooks the importance of security. When the security of an existing network needs to be upgraded, it becomes even harder and more likely to be disregarded.

Budgets, availability requirements, network size and scope, anticipated future growth, capacity needs, and management's risk tolerance are all factors in network design.

Each component of a network carries out unique tasks and houses data with unique security needs. Some devices hold extremely sensitive data that, if disclosed to unauthorized parties, could harm a company. Depending on where they are on the network, other devices are more exposed. Internal file servers, for instance, will be protected differently than web servers that are accessible to the general public. It is useful to recognize key security controls and be aware of the repercussions of a failure in those controls when designing and implementing security in network and system architectures.

For example, by restricting which services users can connect to on a given system, firewalls safeguard hosts. It's critical to secure the network as a whole in addition to its individual components. The network perimeter is a definite inner boundary within the electronic security perimeter and consists of all the external-most points of the internal network. Every connection to another network, including the Internet and any external third parties (such as business partners, data providers, and so on), creates a point of entry into the perimeter that needs to be protected. Implementing firewalls to allow only the communications necessary for conducting business and conducting periodic audits of the external networks are both good practices for reducing risks.

Impact of Wireless Networks on Network Security

Companies using wireless solutions must be aware of and take precautions against the risk of an unauthorized person connecting to the corporate LAN through wireless signal leakage outside of corporate-controlled premises. While the wireless access point signals quickly deteriorate when travelling over distance and through walls, more potent and specialized directional antennas like Yagi antennas can pick up signals at considerable distances. In addition to issues with signal leakage, weaknesses in the encryption techniques used to secure wireless traffic have been found.

As a result, there is a big chance that unauthorized parties could intercept and monitor network communications on wireless networks. Segregating wireless connectivity from the rest

of the corporate LAN has become standard practice to reduce the risks brought on by inadequate encryption and signal monitoring. VPN solutions can provide strong wireless traffic encryption and authentication as a temporary fix.

Network design must also take into account the impact of the explosion of mobile devices on wireless networks, the ways in which wireless designs must support and accommodate a greater variety of devices, and the ways in which this is driving the development of technologies like mobile device fingerprinting and identity management. The sheer number of mobile devices has led to unexpected risks for the wireless network as well as significant security challenges, creating a new dynamic that has expanded the network beyond its conventional boundaries.

Setting up Remote Access

The majority of corporate networks enable remote user access to internal resources. In the past, this was accomplished through a dial-up connection, but today, remote access is typically offered via a VPN solution. In contrast to a site-to-site or LAN-to-LAN VPN, which connects two networks together, a remote access VPN (also known as RA VPNs) connects people who are physically located outside of the organization to its network. VPNs affect the corporate network perimeter significantly despite being useful. Depending on how they are set up, VPNs can allow remote workstations to connect as if they were physically connected to the local network, even though they are not under the corporate security infrastructure's umbrella of protection. The security of the corporate network as a whole is dependent on the security of the employee's remote PC when VPN peers are remote users connecting to the corporate network via the Internet. The VPN may be used to tunnel traffic around corporate firewalls and the security they offer if a hacker manages to access an unprotected PC.

Security administrators need to make sure that adequate endpoint security is in place when VPNs are used for remote user access to the corporate network. The majority of significant firewall and VPN vendors integrate firewalling capabilities into their clients. When using their external email and the Internet, home users are not covered by the most recent corporate antivirus infrastructure. When deploying VPNs, these risks should be taken into account and minimized. Before allowing a remote system to connect to the network, posture validation, a feature of many remote access VPN products, performs a security software and configuration check on the system. It's an effective way to lessen the danger of vulnerable, infected, or compromised systems introducing threats to the company's network.

Internal Network Security Practices

Internally initiated attacks, which are currently the most prevalent threats, are vulnerable to organisations that only use firewalls to protect the perimeter of their networks. In order to add additional security for particularly sensitive resources like research networks, repositories for intellectual property, and databases used for payroll and human resources, internal controls like firewalls and early detection systems like IDS, IPS, and SIEM should be placed at strategic points within the internal network.

If there is no reason for two specific networks to communicate with one another when designing internal network zones, explicitly configure the network to block traffic between those networks, and track any attempts that hosts make to communicate between them. This can be difficult with modern VoIP networks because VoIP streams are typically endpoint to endpoint, but you should think about only allowing traffic that you are certain is legitimate between any two networks. Targeting a less secure area of the network and then slowly gaining access by "jumping" from one area of the network to another is a common tactic used by hackers. By blocking and logging the communication attempts between those networks, such threats can be avoided.

Intranets, Extranets, and DMZs

Organizations divide the networks into three categories for the purpose of applying security policies, practices and rules to the devices within these “nets”. Let’s take a deeper look into these network categories.

Intranets

Giving internal users access to applications and information is the main goal of an intranet. Internal applications, such as knowledge bases, organization bulletin boards, and time and expense tracking systems, are housed on intranets where they are typically inaccessible to outside parties. An intranet's primary function is to facilitate employee sharing of company data and computing resources. Intranet systems are combined into one or more dedicated subnets and firewalled to increase security.

Extranets

Extranets are application networks that are under the control of a company and made accessible to reliable outside parties like partners, clients, and vendors. Extranets, however, require additional security processes and procedures beyond those of intranets because these

users are external to the company and the security of their networks is beyond the company's control.

DMZs'

A company might decide to make some of its systems publicly accessible via the Internet. For instance, the email server needs to be accessible from the Internet in order for an organization to receive Internet mail. Deploying these systems on a specific subnet, also known as a demilitarized zone (DMZ) or screened subnet, apart from internal systems, is a good idea. These systems can and will be attacked by malicious users because they are publicly accessible. A successful attack against these systems still leaves a firewall between the successful attacker and more sensitive internal resources because they are housed on a separate network.

A single application system's components can be divided using a number of DMZs. For instance, a business that separates its web servers and email system into separate DMZs shields each system from a flaw in the other. Even if a hacker is successful in exploiting a web server vulnerability, a firewall still prevents them from accessing the email system.

Web Access Considerations

Proxy servers can be set up to prevent connections to URLs that are thought to be potentially harmful or not required for normal operation, such as those that contain specific scripts or other executable files. Proxy services are fortified procedures that can be offered independently by a dedicated server or internally on a firewall. When regulating user traffic, a company has a number of extra options when using a proxy service. For instance, the business might want to check downloaded files for viruses before sending them to the end user. Additionally, a proxy server can log, record, and compile information about user Internet activity, which can discourage workers from wasting their time browsing websites or going to pages that are irrelevant to their line of work. For example, high-bandwidth music and video downloads can quickly saturate an organization's Internet link, slowing other critical business systems that share the connection.

Outbound Filtering

By allowing users to access services that do not adhere to corporate security policies or that do not have valid business purposes, users run a number of serious risks to the company and its infrastructure if outbound access is not restricted.

3.2) Securing Routers and Switches

In this sub-topic, we will be learning on how to secure network devices especially routers and switches that constitute a major part of the network.

Switches

The network hub's evolved offspring are switches. Switches are layer two devices, despite some layer 3 features like QoS and basic routing being implemented in the newest switches.

Switches are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to. In addition, switches provide a security benefit by reducing the ability to monitor or "sniff" another workstation's traffic. A switched network cannot absolutely eliminate the ability to sniff traffic. By means of ARP poisoning and gratuitous ARP attacks. To reduce a network's exposure to ARP poisoning attacks, segregate sensitive hosts between layer three devices or use virtual LAN (VLAN) functionality on switches. For highly sensitive hosts, administrators may wish to statically define important MAC entries, such as the default gateway.

ARP-learned MAC entries will be subordinate to statically defined MAC entries. Although it is time-consuming and does not scale well, statically defining ARP entries can safeguard small networks that demand high security. Make sure to first ascertain whether any of the devices on your network use ARP spoofing for any HA functionality or for other valid functional reasons, such as new host redirection to a captive portal.

Routers

Routers operate at layer three, the network layer of the OSI model, and Internet Protocol version 4 is the most popular layer three protocol today (IPv4). Routers are primarily used to transfer traffic among networks and between different parts of a single network. Routers can locate various networks either manually or dynamically using administratively defined static routes or routing protocols. To ensure reliable connectivity between all required networks, networks typically combine the two.

Additionally, there may be a risk with dynamic routes. An important security concern is regulating which devices can advertise routes for your network. Network rogue or malicious routes can stop legitimate communications or reroute sensitive data to unauthorized parties. The Border Gateway Protocol (BGP) and a number of other routing protocols, including RIPv2, OSPF, and Open Shortest Path First (SSPF), can all perform authentication; however, a typical solution is to block or filter routing protocol updates on essential router interfaces.

Hardening the devices

Patching

Patches and updates that the product vendor releases should be applied promptly. The distinction between a minor inconvenience and a serious security incident can be made by prompt detection of potential issues and the installation of patches to address recently discovered security vulnerabilities. Subscribe to your vendor's email notification services as well as mailing lists for general security to make sure you are promptly informed of such vulnerabilities. Keep a close eye out for knowledge base (KB) articles and release notes that detail changes in device behavior and default settings from one code version to the next, as well as any vulnerabilities or bugs that were fixed. By invalidating prior measures you've taken to secure your devices, ignoring these details can result in potential security issues on your network.

Switch Security Practices

Hosts cannot send traffic directly to switches because they do not keep track of layer three IP addresses. The ARP poisoning attack is the main strategy used against switches. Switches can still be used as security control devices despite the threat of an ARP attack. When physical access over the network port cannot be trusted, such as in public kiosks, switches can be configured to allow only certain MAC addresses to send traffic through a particular port on the switch.This feature is known as port security.

With port security, a malicious person cannot unplug the kiosk, plug in a laptop, and use the switch port because the switch would deny the traffic because the laptop's MAC would not match the kiosk's MAC. Even though a MAC address can be faked, locking a port to a particular MAC makes it more difficult for a potential intruder. Virtual local area networks (VLANs), layer two broadcast domains that are used to further divide LANs, can also be built using switches. VLAN boundaries are generally useful for controlling and managing network segmentation as well as providing a foundation for applying various security levels to various networks depending on the particular security requirements.

Access Control Lists

Filtering IP packets is a function of routers. The source or destination address, or both, as well as other factors like the TCP or UDP port numbers present in a packet, can be used to permit or deny TCP, UDP, or other types of traffic using access control lists (ACLs). ACLs on routers placed carefully can greatly improve network security. ACLs, for instance, can be used on edge or border routers to filter out traffic that is obviously unwanted (like RFC 1918 traffic coming from an Internet source), relieving the load on border firewalls. Additionally, WAN links can use ACLs

to filter out broadcast and other unnecessary traffic, thereby consuming less bandwidth. ACLs are frequently used for other more sophisticated purposes as well as for protecting the router itself. The best practice is to use an ACL to restrict access to the administrative services (like Telnet, SSH, or HTTP) on a router to the management stations or hosts on a network used by administrative staff members who are permitted to log in to the network devices. The ACL engines in many vendors' products have special features built in.

Disabling Unused Services

Proxy ARP

One host can respond to ARP requests on behalf of the real host using proxy ARP. This is frequently employed on a firewall when traffic for protected hosts is being proxied. Proxy ARP is enabled by default on Cisco routers, which may make it possible for an attacker to launch an ARP poisoning attack against a host that is not connected to the local subnet or VLAN.

Network Discovery Protocols

There are a number of automatic discovery protocols; some are vendor-specific, like Cisco Discovery Protocol (CDP), while others are open standards, like Link Layer Discovery Protocol (LLDP). In all cases, even though they might make network administration a little easier, they also give anyone sniffing the network the chance to discover a lot of information about the network topology. When not in use, these protocols should be disabled, and when they are, special care should be taken to keep them as secure as possible.

Other Extra Unnecessary Services

These extra services can be secured or altogether disabled if unused.

Diagnostic Services

For some UDP/TCP services, routers have a number of diagnostic services enabled, including ICMP echo request, reply, and discard. When not in use for diagnostic testing or troubleshooting, these services ought to be turned off. These services may expose a vulnerability for a denial of service (DoS) condition by accessing a compromised router and activating a debug process that uses all of the device's resources. The same way, an administrator could unintentionally cause an outage.

BOOTP Server

DHCP addresses can be distributed to clients via the BOOTP service using BOOTP Server Routers. The router frequently serves as the DHCP server in residential and small office/home office (SOHO) configurations, but this is less common in enterprise settings. Disable the unnecessary service if it's not in use.

TFTP Server

To transfer configuration files and software updates to and from the router, use a trivial file transfer protocol (TFTP) server. However, TFTP doesn't offer services for authorization or authentication. Most administrators keep a TFTP server running outside of the router and turn it on as necessary.

Web Server

A web server is offered by many vendors so that configuration changes can be made. The web server can be disabled if the router won't be managed in this way. While they are active, these services, along with a number of others, put the router's regular operation at risk for security breaches. Many times, security breaches can be prevented by simply becoming aware of and adhering to a manufacturer's best practice recommendations regarding its equipment. If in doubt, disable the services until you need them.

Administrative Practices

There are several techniques for managing routers. Telnet or the Secure Shell protocol can be used to remotely access a command-line interface from a console (SSH). Telnet is sent over the network in cleartext, so SSH is advised. In addition, a browser can access a web interface, and the Simple Network Management Protocol can be used to monitor and control the router (SNMP). Configuring a login banner or message-of-the-day (MOTD) banner, which is shown whenever a connection is established as part of the login process, is another crucial step in hardening network devices.

. A warning message about unauthorized use of the device should be included in the banner in addition to making sure that it doesn't contain any vital information that could reveal the device's type or operating system. This makes it impossible for someone to claim that they were unaware that their use was prohibited. Along with following these best practices, it's a good idea to omit information about the device's location or the organization it belongs to. Essentially, you want the banner to be a strong warning while remaining as generic as possible.

Remote Command Line

SSH is a protocol that is supported by the majority of routers. The same access and interface are offered by SSH as by Telnet, but all communications are encrypted. It is possible for an attacker to intercept sensitive data, including passwords and configuration parameters, while it is being transmitted over the network if administrative connections to network routers are not encrypted. The configuration of host and domain names on the router, the creation of an encryption key, the configuration of accounts, and the setting of necessary SSH parameters are all required on many network devices in order to enable SSH.

Many network devices keep two passwords by default—one for device access and another for configuration commands, also known as "privileged" or "enable" access. It can usually be configured even if this is not the default behavior.

Individual user accounts can and should be created to provide granular authorization and full accountability, though not always locally on the device; the method and choice to use named accounts on an individual basis is much more crucial than where the accounts are created and stored. Another vital factor to take into account is how these passwords will be stored—locally or in a central authentication server.

Centralizing Account Management (AAA)

It is difficult to synchronize and maintain separate user accounts on each network switch, router, and device in large-scale environments. The majority of network devices can be set up to use authentication, authorization, and accounting to verify their identity against a central account repository (AAA). The removal of usernames and passwords from local configurations is facilitated by this. While AAA is the mechanism, a sound methodology for administrative device account creation and use policy is equally important. As you can take extra precautions like more frequent password rotation for admin accounts or more stringent password complexity requirements, requiring administrators to have a separate account specifically for administrative purposes will help protect crucial network equipment.

The only real drawback to the strategy is that if one of these accounts with elevated privileges is compromised, an attacker would gain access to resources they might not otherwise have.

RADIUS and TACACS (now TACACS+) are the two most widely used protocols for these access devices to conduct device-level AAA communication. Some devices can directly query an LDAP or Active Directory service in addition to those that use RADIUS and TACACS+.

Administrative control can be precisely tailored for particular needs using the granular controls and variables provided by these protocols.

A remote authentication server shouldn't be used for all aspects of network device authentication. No one could log in if the server was down or unavailable. Consequently, maintaining a local backup account is a wise preventative measure.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP), which offers a centralized mechanism for monitoring and configuration, can also be used to monitor and manage network devices. Through the use of Management Information Base Object Identifiers (MIB OIDs), a structured format database that describes objects within a device that can be monitored or managed by SNMP or another management protocol, SNMP can be used to monitor things like link operation, port status and statistics, and CPU load. By configuring an ACL on each device to regulate who is permitted to query the device via SNMP and what they are permitted to do, it is possible to protect SNMP communications. RW SNMP should only be used if a particular automation or functionality needs read-write access. If not, use RO for node managers that are only collecting statistics.

Internet Control Message Protocol (ICMP)

Protocol for Internet Control Messages (ICMP)

TCP/IP communication issues can be reported using the Internet Control Message Protocol (ICMP), which also offers tools for evaluating IP layer connectivity. When analyzing network issues, it is a crucial tool. ICMP, however, can also be used to gather crucial data about network topologies and accessible host services. Messages are a general term for a wide range of defined ICMP communication types. When used maliciously, the following ICMP functions pose a number of risks.

ECHO and Traceroute

Pings, also known as echo requests and replies, are used to check whether a host is available and reachable over the network. One host's ability to successfully ping another host indicates that the hosts' networks are functioning properly up to and including layer three of the OSI model. This does not ensure that there are no additional restrictions or barriers in place, but it does show reachability. However, there are occasionally exceptions to this rule.

Attackers with more experience avoid ping and employ more covert techniques for host identification. However, an attacker can use ping to scan publicly accessible networks to find available hosts. Because it is believed that nothing bad can be contained in an ICMP packet, ICMP echo and echo reply have also been used to make covert channels through firewalls that permit malicious traffic to pass through unchecked. At the network perimeter, ICMP echo requests and responses should be dropped. TTL packets can be used by an attacker to find open ports in perimeter firewalls.

Attackers have developed a technique for scanning networks using UDP, TCP, and ICMP packets that expire one hop past the perimeter firewall using this method. Dropping TTL Exceeded packets can prevent such attacks since they rely on receiving ICMP TTL Exceeded messages from firewalled hosts.

Unreachable Messages

A Type 3 Destination Unreachable message is another classification of ICMP message. When a router is unable to forward a packet because the specified destination address or service is unavailable, it will respond with an ICMP Type 3 message. Dropping all messages marked as Destination Unreachable has a significant impact. For a network to function properly, the message Code 4, "Fragmentation Needed," is crucial. If hosts are not informed that the amount of data they are transmitting into the network exceeds its maximum transmission unit (MTU), disruptions may result.

Directed Broadcasts

A packet sent to a network's first and last addresses is equivalent to sending a separate packet to every host connected to that network. A class of attacks known as bandwidth amplification attacks are based on this functionality. In such attacks, the attacker inserts the victim's source address into UDP ECHO packets or ICMP traffic sent to a number of large networks' broadcast addresses. This is done to ensure that the victim and not the attacker receives the ICMP responses. Due to the way that some services that use the UDP protocol behave, these packets will elicit responses from every system that is reachable and responding within the network range. Modern firewalls are capable of spotting and preventing these attacks, but frequently rely on being configured to do so.

Redirects

In the normal course of network operation, ICMP redirects are used to inform hosts of a more effective route to a destination network. On networks where several routers are present on the same subnet, this is typical. Redirects on router interfaces to untrusted and external networks should be disabled because a malicious user may be able to manipulate routing paths.

Anti-Spoofing and Source Routing

Attackers spoof or insert information into TCP/IP packet headers in an effort to pass for a more reputable host. Internal packets should obviously not be arriving inbound on border routers, as address spoofing is an attempt to get past external defenses by posing as an internal host. Inbound packets with source IP addresses that match the internal network can be dropped by border routers to protect the network from such attacks. Additionally, broadcast packets and packets with source addresses that match RFC 1918 "private" IP addresses should be dropped by routers. Routers should be set up to reject packets that contain source routing information in addition to spoofed packets.

The route a packet should take through a network is determined by source routing. By forcing a lot of traffic through one router and overloading it, such information could be used to circumvent known filters or create a denial of service situation. An administrator might occasionally want to use source routing. In these circumstances, source routing may be enabled solely for that goal.

Logging

Both system-related and ACL activity-related information can be logged by routers. Although the majority of routers lack large discs for locally logging data about network and system activity, they do offer the ability to log remotely to a syslog server. A single repository can be created by centralizing and aggregating all of the scattered network logs using the syslog facilities. Syslog can play a crucial role in conducting forensic investigations or in troubleshooting network-related issues. Choosing the appropriate level of logging and the duration of log retention gives you a window into the past and enables you to look back at what was happening in various locations throughout the network at a specific time. Security Information and Event Management (SIEM) is a cutting-edge security technology that gathers, examines, and correlates logs before either taking action or recommending action based on the event information.

3.3) Firewalls

The first line of defense between a company's internal network and unsecured networks like the Internet is a firewall. For layer three traffic, first-generation firewalls were merely permit/deny engines, operating similarly to an appliance with an access control list. They were only able to "allow or deny" traffic from "this predefined source IP address to this predefined destination IP address on these predefined TCP and UDP ports." They were unable to perform any other "intelligent" operations on the traffic. By keeping track of running network sessions, second-generation firewalls effectively operated at layer four. Stateful firewalls or, less frequently, circuit gateways were the names given to these devices.

By being able to monitor network sessions, the firewall was able to prevent man-in-the-middle (MITM) attacks coming from other IP addresses. In some sophisticated firewalls, a high-availability (HA) pair could swap session tables, allowing a network session to continue through the other firewall in the event that one failed. The application layer, or layer 7, was first entered by the third generation of firewalls. Some well-defined, preconfigured applications, like HTTP, DNS, and older, computer-to-computer protocols like FTP and Telnet, could be decoded by these "application firewalls," which could also decode data inside network traffic streams for other applications. They were created with the World Wide Web in mind, which made them well suited to identifying and preventing web site attacks like cross-site scripting and SQL injection, which were causing a lot of concern at the time.

Additionally, advanced application-layer firewalling capabilities, antivirus, intrusion detection and prevention, network content filtering, and other security features have been combined in unified threat management (UTM) devices. These are genuine devices at layer seven. Application-layer gateways, which are specifically created to comprehend how a specific application should function and how its traffic should be constructed and patterned, can be run on fourth-generation firewalls.

The majority of network appliances you will find today fall under the commonly accepted definition of a fourth-generation firewall. Fifth generation firewalls are internal to hosts and protect the operating system kernel. Some sixth generation firewalls (meta firewalls) have also been described.

Firewall Features

Application Awareness

At the very least, traffic from OSI layers three through seven must be able to be processed and interpreted by the firewall. In order to effectively manage communications between

applications, it should be able to filter at layer three by IP address, layer four by port, layer five by network sessions, layer six by data type, and, most importantly, layer seven.

Accurate Application Fingerprinting

Applications should be correctly identified by the firewall not only based on their external appearance but also by the internal contents of their network communications. To guarantee that all applications are properly covered by the firewall policy configuration, accurate application identification is required.

Granular Application Control

The firewall must be able to recognize and classify the features of applications in order to manage them effectively, in addition to allowing or blocking communication between applications. Examples of potentially undesirable features that the firewall should be able to control include file transfer, desktop sharing, voice and video, and in-application gaming.

Bandwidth Management (QoS)

The firewall can control the Quality of Service (QoS) of preferred applications, such as Voice over IP (VoIP), based on the current network bandwidth availability. To guarantee the highest level of availability for the most important services, the firewall should integrate with other network devices.

Core Firewall Functions

Network Address Translation (NAT)

RFC 1918 designates specific network ranges as "private" networks that will never be used on the Internet in order to conserve IPv4 addresses. As a result, businesses can use these blocks for their internal corporate networks without having to worry about tripping over an Internet network. But in order for these networks to be routable when they are connected to the Internet, they must translate their private IP network addresses into public IP addresses (NAT). This allows a large number of hosts protected by a firewall to access the Internet alternately or by sharing a small number of public addresses. In a firewall, NAT is typically implemented independently of the policy or rule set. It is important to keep in mind that just because a NAT has been set up to translate addresses between two hosts, it does not guarantee that the hosts can talk to one another. The policy specified in the firewall rule set governs this.

Static NAT

The address translation that results from a static NAT configuration is constant. The host is defined with a fixed 1:1 relationship between a single local address and a corresponding global address. As each packet passes through the firewall, the static NAT translation rewrites the source and destination IP addresses as necessary. Nothing else in the packet is impacted. This is typically used for internal servers that require a stable IP address so they can be accessed from the Internet. This straightforward strategy will enable most protocols to pass through a static NAT without incident. Static NAT is most frequently used to give a trusted host inside the firewall perimeter access to the Internet or to grant inbound access to a particular host, like a web server that needs to be reachable via a public IP address.

Dynamic NAT

A group of internal local addresses can be mapped to one or more external addresses using dynamic NAT. From the standpoint of an Internet-based attacker, dynamic NAT has the advantage of offering a constantly changing set of IP addresses, which makes it more challenging to target specific systems. The limitation on the number of concurrent internal users who can access external resources at once is dynamic NAT's biggest drawback. Simply put, the firewall will exhaust its supply of global addresses and won't be able to assign new ones until the idle timers begin releasing global addresses.

Port Address Translation

The entire inside local address space can be translated to a single global address using port address translation (PAT). In addition to changing the source and destination IP addresses, this is accomplished by altering the communication port addresses. Due to the firewall's ability to keep track of which ports correspond to which sessions, multiple communications can use a single IP address. PAT offers a higher level of security because incoming connections cannot be made using it. PAT has the drawback of restricting connection-oriented protocols like TCP.

Auditing and Logging

A firewall makes a great auditor. They have the ability to record any traffic that passes through them if given enough disc space or remote logging capabilities. Attack attempts will leave traces in the logs, and if administrators are vigilantly monitoring the systems, attacks can be stopped before they succeed. Firewalls should keep track of both successful and unsuccessful system events. In order to assist the network and security administrators, it is best to send the logs to a Security Information and Event Management (SIEM) system, which can filter, analyze, and perform heuristic behavior detection.

Firewall Design

Software-based firewalls are an option, but purpose-built appliances are far more prevalent. Sometimes a group of various devices work together to perform the firewalling duties. One of the most important aspects of securing a network is the design of the network where the firewall resides and its specific features. Firewalls must be properly configured and installed in the appropriate places on the network for them to be effective. Best practices include

- All communications must pass through the firewall. The effectiveness of the firewall is greatly reduced if an alternative network routing path is available; unauthorized traffic can be sent through a different network path, bypassing the control of the firewall
- The firewall permits only traffic that is authorized. If the firewall cannot be relied upon to differentiate between authorized and unauthorized traffic, or if it is configured to permit dangerous or unneeded communications, its usefulness is also diminished.
- In a failure or overload situation, a firewall must always fail into a "deny" or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.
- The firewall must be designed and configured to withstand attacks upon itself. Because the firewall is relied upon to stop attacks, and nothing else is deployed to protect the firewall itself against such attacks, it must be hardened and capable of withstanding attacks directly upon itself.

Firewall Strengths

- Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.
- Firewalls are used to restrict access to specific services.
- Firewalls are transparent on the network—no software is needed on end-user workstations.
- Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities, they can log interesting traffic that passes through them.
- Firewalls can alert appropriate people of specified events.

Firewall Positioning

A firewall is typically placed at the edge of the network, directly in front of any external connections. However, more firewalls can be installed inside the network perimeter to protect specific hosts with higher security needs with a more focused defense.

Firewall Configuration

When building a rule set on a firewall, consider the following practices:

- Develop rules in descending order of specificity. The majority of firewalls run through their rule sets in order, stopping once a match is found. A general rule cannot obscure a specific rule further down the rule set by being placed above it.

- A rule set's most active rules should be placed near the top. Screening packets requires a lot of processing power, and as was already mentioned, a firewall will stop processing a packet after it matches a rule. CPU savings could be significant in situations where millions of packets are being processed and rule sets can have thousands of entries.

- All firewalls should be set up to reject "impossible" or "unrouteable" Internet packets, such as broadcast packets, packets coming from an external interface whose source addresses match those of the internal network, and packets with RFC 1918 "private" IP addresses. All of these represent unwanted traffic, such as that created by attackers, because none of them would be anticipated from the Internet.

3.4) VPNs

By encrypting and isolating traffic at the packet level while using standard Internet services for transport, VPNs offer virtual network links. Connecting branch offices or distant sites (known as LAN-to-LAN tunnelling, or L2L) and granting remote access to office environments are the two most popular uses of VPN (called remote access [RA] VPN).

L2L tunnels are frequently used for confidential communications between corporate networks and other reputable networks, such as third parties, remote offices, or other corporate-controlled networks. The L2L tunnel can be compared to the "industrial-strength" VPN method and is typically utilized similarly to a point-to-point circuit or private network link. Since all settings on both endpoints of a VPN must be identical for a tunnel to be created, L2L VPNs typically call for a device that can support the same features and capabilities on both sides of the connection.

Internet-based VPNs are quick, easy, and secure, but there is no way to provide Quality of Service (QoS) because the layer three pathway still decides how to route the traffic. Users of RA VPN services can conduct business virtually in an office while working from a remote location. As telecommuting and third-party system access become more crucial to a variety of businesses, RA VPN services are expanding in popularity for both cost- and convenience-related reasons.

Remote Access VPN Security

The security of the devices on the other end of the VPN tunnel is crucial because they can access the internal network when remote sites and clients are allowed to connect to the corporate network over public networks. When designing a RA VPN solution, the following security issues should be taken into consideration.

It is impossible to predict the past or settings of the clients unless the organization provides all remote systems and demands that only these be used. All network-connected entities must be managed, supported, and secured in accordance with the organization's policies, standards, and procedures in order to manage and maintain the network's security. Patch management, antivirus management, firewall management, and other security measure management are not permitted on systems that are not owned and managed by the organization. Even if a specific third party takes care to maintain clean systems, the absence of enterprise management renders these systems dangerous for the network. Remote third party systems might not be able to "call home" for security updates and fixes, third party systems might not be able to

receive updates and changes to comply with new organization standards, and malware can be introduced into the network by external systems.

Some remote access solutions make it difficult to enforce the requirement that remote clients join the domain or do not allow for seamless awareness of Microsoft domains. As a result, you won't be able to implement login scripts or group policies to make sure that clients abide by the corporate security guidelines. Some products have developed methods to handle this depending on the remote access solution, but many have not. Additionally, there are still a lot of issues with cached credentials and password management that are primarily the responsibility of the designer.

It can be challenging to specify scripts or security settings for remote access solutions because they frequently need to provide connectivity solutions for various client types. It is more difficult to define the corporate standard for software like personal firewalls and antivirus programs because some programs might support a platform before others.

If a client computer is not connected to the corporate network, it is difficult to predict what will happen to it. This fact can be a big liability, especially when combined with the variety of local administrators and privately owned computers. This is an important issue to address during the design phase of any remote solution because Bring Your Own Device (BYOD) programs, which encourage employees to bring their own personal computing devices to work, are becoming more common.

Additionally, the organization has only a small amount of control over how the network is set up near the client. Organizations must give their end users freedom to choose the consumer networking technologies they use for remote access.

Authentication Process

Even when using certificate exchange as the connection security method, many authentication procedures for remote clients still rely on a username and password. Since usernames and passwords are simple to set up and use and have been around for such a long time, nearly all client operating system implementations offer excellent support for this type of authentication. Enterprise remote access techniques are shifting towards two-factor authentication procedures in the IT sector. This typically involves a certificate-based smart card for Windows-based environments. Other options include biometric scanners and token-based one-time password (OTP) systems. Regardless of the back-end server, the default behavior for VPN clients using the native L2TP over IPSec support in Microsoft Windows is to demand a certificate to begin the security association between the client and the server. This is typically either a machine

certificate or an IPSec specific certificate (typically for non-domain users) (normally for computers that are domain members). Windows systems also support creating the security association using a shared secret, also known as a pre-shared key.

In a VPN environment, authentication ultimately serves two purposes:

- *Identifying the device* - The system is recognized as a legitimate system for establishing the IPSec security association by the machine certificate (or, to a lesser extent, the shared secret).

- *Identifying the user* - The basic task is determining whether the user has permission to establish a connection. The user proves their identity using a username, OTP, certificate, or another mechanism.

Before granting full access, the majority of remote access vendors use methods to first authenticate the user and then check the client configuration. The term for this is posture validation (PV)

Configuring the Clients

The targets of almost all attacks are the tunnel endpoints. Any remote access plan must take into account the state of the tunnel endpoints. The focus of security strategy used to be limited to whether a user had authorization to connect to the remote access service, but nowadays it's common to demand additional client system configurations. The amount of security patches and software updates that must be installed on the client system in order to harden it against endpoint attacks makes this a necessary step. When deploying remote access solutions, many organizations take the logical course of trying to purchase one VPN solution for all types of clients. This is fairly simple for organizations with a small number of client types, but it can be difficult for those with a diverse clientele. Although it would be ideal to find a unified solution for all clients, it frequently happens that only some clients can be supported, or that some clients can be supported more effectively than others. The remote access architect must assess these problems and their implications for the organization before determining the best course of action. Early VPNs were typically designed to connect Windows systems, but the proliferation of different end-user operating systems and devices (including mobile devices) has made the situation more complex today.

Before allowing a connection, an organization would typically want to demand three things from a remote client:

• Service packs and security patches must meet a minimum standard.

• There needs to be a host-based software firewall in place.

• Antivirus software that uses the most recent virus definitions is required.

Since many tablets and smartphones and other endpoint devices do not support these kinds of applications, an administrator may want to specify additional requirements for client compliance before allowing a connection to the network. In order to quarantine or segment the client into a portion of the network where it can be checked and scanned but cannot access any corporate resources, the majority of systems perform posture validation at the head-end system level. In this case, the head-end system will typically permit a limited connection from the client. If the client successfully completes the validation without any errors, it will then send a message to the remote access server letting it know everything is fine and lifting the quarantine. When the logic of the login process is increased in this manner, two problems occur. The first is that clients will have a wide range of patch levels unless there are adequate methodologies and componentry in place to support up-to-date patching across the enterprise, and it can be a significant burden on the remote access system to validate large volumes of client connections. The second is that supporting various client operating systems and devices on the same network access device becomes more challenging as more logic is required of the clients. . It is feasible to assemble kits for various clients, and many vendors and significant implementations are now supporting this. Depending on the requirements of the organization, a decision will need to be made regarding whether this will be done and how. It appears likely that this capability will eventually become a standard feature of any enterprise that still permits full client connections, based on the growth of BYOD and the mobile computing revolution. Although each product in the PV market has a unique set of capabilities, the main objective is to determine the condition and safety of the client configuration. . Although there have been some attempts, there has not yet been a standardization of these checking processes in the login or authentication process. Because vendor remote access products' client-checking features aren't always interoperable, the remote access architect must base design choices on the remote access goals.

Client Networking Environment

Another factor to be taken into account when creating a remote access design is how the client is set up to handle the network connection for the virtual tunnel. Split-tunnel routing, or simply split tunnelling, is the term used when the client can connect to multiple remote networks at once. In its most popular form, a remote client can connect to the company's network and the Internet simultaneously. Given that the security perimeter and Internet ingress/egress points are extended to the client device, it is essential to rely on any client with a split-tunnel configuration to be secure. Each client is a part of the corporate network's perimeter, making them crucial to the security of that network. . The client determines the traffic's path regardless

of any add-on software that can modify the routing parameters because the client controls how the TCP/IP stack behaves. For the tunnel session, many vendors demand client-side add-on software that can track unauthorized routing table changes and, in most cases, will cut the connection if they occur. On client systems, it's crucial to restrict end-user privileges to just those necessary for proper operation.

There are really only a few advantages of a split-tunnel environment:

• Remote clients may be given access to more resources when the routing table permits a direct connection to a destination rather than requiring the connection to go through corporate firewalls and proxy servers. For instance, the organization's firewall policies might forbid external traffic from terminal servers, but since the firewall would not filter client traffic, users could connect to the destination directly with terminal service traffic.

For Internet websites, direct connections can increase speed. The network architecture and the connection to the VPN services will really determine the speed difference. Many designers use caching servers to help with this problem, and in many cases they are able to improve performance by utilizing both the large Internet links of an organization and speeding up the speed to match the direct connection.

• If you have a small office LAN hidden behind a connection-sharing device, you might not be able to transfer files or print when the tunnel is connected because some VPN software disables the ability to print or access local resources on any subnets. For users who want to print to a local printer, this causes issues.

• Lastly, home users who use their own systems might not want the company to monitor their movements. This is understandable, but when they want to work on personal material they should instead log off of the corporate resources.

In order to maintain acceptable performance, the infrastructure will need to be watched over by the remote access team. You must establish what you believe to be a well-protected client as the remote access architect.

A client can be quarantined if it doesn't follow the rules that must be followed in order to establish a VPN connection. There are several ways the client can be quarantined from the rest of the corporate network:

• Break off communication Some vendors have opted to merely explain the issue to the client in a message before cutting off communication. Without access to the corporate network, this will stop any potential infection but may also make the task of fixing the client more difficult.

• Limit the connection's duration. In this case, the user receives a message outlining the issue and is then given a window of time to resolve it before the session is cut off. When there are large patches and slow connections, this poses a potential issue and is generally more challenging to support. The benefit of this solution is that it is simpler to configure on the back end.

• To "sandbox" the client, create access control lists (ACLs) for the session. In this scenario, the client will be informed of the issue and filters will be applied to the connection session to limit traffic to specific ports or internal locations. This is ideal because it gives the client the chance to resolve the issue on their own dime without endangering the company as a whole. The remote access team must be very clear about the minimum client requirements, both at first and as changes and upgrades are required, as this can get rather complex to configure and maintain.

Normally, service packs and security patches are checked once, at client login time, though some systems monitor the client environment continuously throughout the session. Network Access Controls [NAC], a product that combines all client validation into a single, manageable solution, is available to help with the task of client integrity/posture validation.

All clients should be required to have a router or router/firewall combination in home networks with always-on connections (like DSL and cable), which fixes a number of issues like these:

- The connection-sharing device resolves a number of ISP Dynamic Host Configuration Protocol (DHCP) problems, such as short lease duration, in which client IP addresses from the ISP are frequently changed. Instead of the client handling the renegotiation, the device can do so while still maintaining the tunnel.

- It shifts the front line of the network from the client maintaining the VPN session to the connection-sharing device, even if it only has a minimal stateless firewall.

- It allows for multiple VPN sessions and the use of multiple systems to access the same Internet connection.

Offline Client Activity

Most businesses allow non-company client systems to access remote services and log in. Unless the exposed services are intended for such use and are adequately protected, the condition of the client must be assessed at the time of connection because the organization won't be aware of the state of these other client systems. All service packs and security patches must be installed at the time of connection, the virus scanner must be current and running, and the firewall software must be installed and configured in order for the client and the network to

remain secure. Some businesses decide to give every client a router or other device that keeps the tunnel endpoint on it rather than the client. This replaces the client VPN with an L2L approach, making each of the remote client sites identical to a branch office. Although it comes with its own set of support, design, and cost considerations, in many cases, this is a good way to ensure the security and capabilities of the clients.

Site-to-Site VPN security

Site-to-site links, or B2B connections, are those where a corporation only owns one side of the link. This frequently occurs when business partners' networks are connected to those of the organization. It is up to the remote access architect to specify the minimum requirements for the partner tunnel endpoint or to bring the connection in through a location in the network where it is isolated and there is visibility into what is happening since there is currently no quarantine type solution that will check this type of connection. It's crucial to keep an eye on link traffic and, if at all possible, limit it to just the essential internal destinations. Since multiple users can frequently share a site-to-site connection, the remote access architect can afford to spend more money on the connection's ends. In fact, many businesses install stateful firewalls at their branch offices, loaded with corporate rules. Because it ensures the same rules are applied regardless of the client location, having distributed firewall rules offers a very good security model. Stateful distributed firewalls are ideal for all remote locations, including corporate endpoints and home user endpoints, but they are typically too expensive. The security and cost of this strategy for the specific environment will need to be assessed by the remote access architect. Additionally, it's crucial to make sure that branch offices aren't merely using NAT devices as VPN endpoints. This is sometimes done in small offices and businesses, but because the network is inside a private network, setting up a NAT device without firewall features gives users and administrators a false sense of security. Although it is useful, NAT is not sufficient to protect a network on its own.

3.5) Wireless Network Security

Through the use of cutting-edge encryption and access control techniques, wireless security has significantly improved over the past few years. Today, it is possible to secure a wireless network using the Wi-Fi products' built-in features, making your wireless network likely more secure than your wired LAN.

Layer One Security Issues

By adjusting the transmitter's output power, picking the proper frequency, selecting the right antennas, and positioning those antennas in the most effective way to provide a quality link where needed, while limiting your network's "fuzzy" borders, you can usually resolve issues with wireless network layer one security. Knowledge of RF behavior, transmitter power estimation and calculations, and aerial concepts are necessary for proper implementation of these measures. The majority of enterprise controller-based systems with lightweight access points (LWAPs) have features like auto frequency switching/hopping, which enables access points to select the best radio frequency based on current conditions, and dynamic power sensing and adjustment, which raises or lowers the signal's power so that communication is optimized without being too weak or strong. LWAPs are essentially dummies that take all commands from a central controller. Even some systems have supplementary parts that can perform real-time frequency management.

Antenna Placement

The placement of antennas is a crucial issue because wireless access points occasionally broadcast their wireless networks outside of a safe area, which can provide an opportunity for an attacker to attack that network. So it becomes crucial to pick the proper aerial and configure the broadcasting range.

Here are some tips for choosing antennas for wireless networks:

• Only employ omnidirectional antennas when absolutely necessary. Be inventive; in many cases, a sectored or panel antenna with the same gain can be substituted, reducing the LAN's perimeter and detectability.

• Use ground plane omnis when deploying a wireless network inside a tall building to reduce the "visibility" of your LAN from the lower floors and streets. The downward signal is reflected by the ground plane, which eliminates the bottom of the omni irradiation "doughnut."

• Put your indoor omnis in the heart of a business structure. Instead of placing an array of omnis along a long corridor to deploy a wireless LAN connecting multiple offices, think about placing two panel antennas on either end of the corridor.

• Take antenna polarization into account. Place your omni or semi directional antenna horizontally if the majority of client device antennas are horizontal (like built-in PCMCIA wireless card antennas). Vertical polarization is used in Bluetooth built-in to microchips and CompactFlash (CF) wireless cards. The magnetic mount omni, a favorite of the war driver, is always mounted vertically using the vehicle as a ground plane. It is less likely that war drivers will detect your signal using the magnetic mount omni if your access point's antennas are horizontally polarized.

Common Wireless Intrusion Scenarios

• Installing USB adapters, access points, bridges, and other wireless equipment without enterprise IT management's consent

Solution: Make sure that your company's security policy clearly prohibits the use of unauthorized wireless devices and that all employees are aware of its provisions. Utilize wireless sniffers or other specialized wireless tools and appliances to find any nearby wireless devices. Remove any discovered unwanted devices and look to see if the traffic coming from them resulted in any log alerts.

• Wireless access points installed by intruders to provide a back channel into the corporate LAN, effectively getting around the firewall's egress filtering.

Solution: The best course of action in this situation is to treat it as a physical security breach. Consider the rogue device as significant evidence in addition to locating and removing the device and reviewing logs (as in the previous point). Place it in a sealed bag, label the bag with a note indicating the time of discovery and the credentials of the person who sealed it, and handle it carefully to preserve the attackers' fingerprints. Examine the CCTV footage and ask around to see if anyone has seen the potential intruder.

• Attackers use external wireless access points and bridges to launch man-in-the-middle attacks.

This is a "red alert" situation and shows that the assailant was skilled and determined. The attacker may be utilizing the access point from a nearby apartment or hotel room, or they may have it installed in their vehicle and connected to the vehicle accumulator battery. An alternative is to configure a PCMCIA card to function as an access point, which is more convenient for an attacker. To steal the login names and passwords of unwary users, an attacker aiming for a public hotspot might try to mimic the user authentication interface.

Solution: The most important thing to remember is that these attacks show that either the network under attack was vulnerable or that user authentication and data encryption were disregarded. Use caution when setting up your wireless network and take the security precautions. Consider taking down the wireless network and physically locating the attacker if the attack continues. Contact a specialized wireless security company with attacker triangulation capabilities to accomplish the latter goal.

802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats

The primary issue with layer two wireless protocols is that the management frames in 802.11 and 802.15 standards are neither encrypted nor authenticated. Anyone can record, examine, and transmit them without having to be a part of the target network. Despite the fact that eavesdropping on management frames is not the same as eavesdropping on sensitive network data, it can still yield a wealth of data, such as network SSIDs (basically, the network name), wireless hosts' MAC addresses, active DSSS LAN channels, FHCC frequency hop patterns, and more. Each Bluetooth device has a distinct ID that is transmitted in the management frames in clear text. Therefore, listening in on these frames can aid in locating such a device and its user. Short of completely turning off the Bluetooth device, preventing this is difficult. Unfortunately, the data provided by management frames only represents a small portion of the issue. De-authenticate and disassociate frames can be sent by the attacker to quickly take wireless hosts offline. Even worse, the attacker can use a different channel to associate with the target host, spoof the real access point's MAC and IP addresses, and then send a disassociate frame to the host in question (s).

Closed-System SSIDs, MAC Filtering, and Protocol Filtering

Closed-system SSIDs, MAC address filtering, and protocol filtering are examples of common nonstandard wireless LAN security measures. A common feature of higher-end wireless access points and bridges is closed-system SSID. It alludes to the removal of the SSID from the beacon frames and/or probe response frames, necessitating the use of a valid SSID on the client hosts in order to establish an association. As a result, SSID now functions as a shared authentication password. However, management frames other than beacons and probe responses can also contain closed-system SSIDs. Wireless hosts can be made to disassociate in order to capture the SSID in the management frame's underlying reassociation process, just like in the case of shared key authentication mode. Using de-association/de-authentication frames, attackers can quickly get around closed-system SSID security.

Contrary to closed-system SSID, MAC filtering is a standard feature that almost all current access points support. It is easily circumvented and does not provide data confidentiality (again,

an attacker can force the target host to disassociate without waiting for the host to go offline so its MAC address can be assumed). MAC filtering, however, might prevent script kiddie (non-sophisticated) attackers from connecting to the network.

Finally, protocol filtering is less frequent than closed systems and MAC address filtering; it is only effective when it is sufficiently selective and only in certain circumstances. For instance, you can filter all other protocols and use the built-in encryption capabilities of web and mail servers to provide a sufficient level of data confidentiality when the wireless hosts only require web and mail traffic. SSH port forwarding is an alternative. Wireless LANs designed for mobile users with low-CPU power devices limited to a single task may benefit from protocol filtering in conjunction with secure layer six protocols (barcode scanning, browsing the corporate web site for updates, and so on).

Wireless Vulnerabilities and Mitigations

Most attacks on Wi-Fi take place at layer two because that is where it primarily functions in the OSI stack. However, wireless layer one attacks like jamming are also possible. Five different wireless attack types are discussed in this section.

Wired Side Leakage

Reconnaissance on wireless networks entails a wireless sniffer being used to promiscuously listen for wireless packets so the attacker can start to create a wireless network footprint. Since we are not connected to (associated with) an access point, we will ideally concentrate on layer two packets. The attacker could sniff layers three and above if they were connected to an access point. Thanks to protocols like NetBIOS, OSPF, and HSRP, among others, which were created to be chatty about their topology information because they were intended to be used only on protected internal networks, broadcast and multicast traffic are rampant on the majority of wired networks.

Many network administrators are unaware that if their wireless connections to their wired networks are not properly segmented and firewalled, broadcast and multicast traffic may leak into the wireless airspace. The majority of wireless switches and access points permit this traffic to enter the airspace without being blocked. Sometimes internal protocol communications may be leaked onto the airwaves when the attacker connects to an AP that is also connected to a network device. Unfortunately, this traffic might expose usernames, passwords, device types, and even network topology! ! For instance, multicast packets are sent by Cisco's Hot Standby Router Protocol (HSRP), which is used for gateway failover. By default, these packets send back and forth heartbeat messages that contain the router's hot standby password in plain text.

These packets leak information about the network topology and the password when they travel from the wired network to the wireless airspace. You must make sure that, similar to a firewall, ingress and egress are taken into account when deploying wireless. To stop this sensitive wired traffic from leaking into the nearby airspace, broadcast traffic on the wireless switch and access point should be properly filtered out of outbound traffic. By checking packets for indications of data leakage, a wireless intrusion prevention system (IPS) can assist in identifying this wired-side leakage, allowing administrators to stop any leaks on their access points, wireless switches, or firewalls.

Rogue APs

Unauthorized wireless access points connected to your physical network are known as rogue APs. An access point that is nearby is any other visible AP that is not yours. It's necessary to have some prior knowledge of the authorized access points and the legal wireless environment in order to vet out potential rogue APs. The best effort approach is used in this method of rogue AP detection because it involves identifying the environment's anomalous access points. The physical connection between the access points and your network may not always be verified by this method. To do that, you must also evaluate the wired side and then compare it to the wireless assessment. If not, your only other choice is to examine each actual access point to see if the suspect AP is linked to your network. For a big assessment, this may not be feasible. Because of this, wireless IPSs are much better at finding malicious APs. An IPS that uses wireless sensors compares what it sees to what it sees from the wired side. It determines whether the access point is actually a rogue access point or one that is physically connected to the network using a variety of algorithms.

Misconfigured Access Points

Misconfigurations can be common in enterprise wireless LAN deployments. Misconfigurations can result from a number of factors, including human error and inconsistent administrators installing the access points and switches. For instance, if a device reboots during a power outage, an unsaved configuration change could enable a device to revert to its factory default settings. And numerous other errors can result in a wide range of weaknesses. As a result, these devices need to be checked for compliant configurations with your policies. With WLAN management tools, some of this monitoring can be done on the wired side. If you predefine a policy within the wireless IPS to monitor for devices not compliant with policy, mature wireless IPS products can also keep an eye out for incorrectly configured access points. Modern systems take different factors into account; while the controller-based methodology largely avoids this problem, some organizations, particularly smaller ones, may still experience it. There is a greater and more significant risk from human error on the controller side because all access points will have a problem or configuration vulnerability, not just one.

Wireless Phishing

Trends show that wireless users have become the low-hanging fruit as businesses become more focused on securing their wireless networks. It can be challenging to enforce secure Wi-Fi usage when it comes to human behavior. The risks associated with connecting to an open Wi-Fi network at a local coffee shop or airport are simply unknown to the average wireless user. Users may also unwittingly connect to a wireless network that they think is the authentic access point but is actually a honeypot or open network that has been set up to lure unsuspecting victims.

Client Isolation

Especially when it comes to Wi-Fi, users are typically the easiest target for attackers. Users who are connected to an access point can observe other users who are attempting to connect to it. The majority of users connect to the access point to access the corporate network or the Internet, but they can also become targets of another malicious wireless network user. As long as they are connected to the same access point, malicious users can also directly target other users in addition to listening in on their conversations. In particular, after user authentication and association with the access point, user receives IP address and consequently layer three access. The other users of that access point are now directly targets for an attack because, similar to a wired network, the malicious wireless user has joined the same network as them. Wireless manufacturers have made product features available to provide client isolation for public and private networks in response to this vulnerability. Client isolation essentially removes the LAN capability while still allowing users to access the Internet and other resources made available by the access point. Isolation is essential for Wi-Fi network security. Make sure the feature is enabled across all access points because it is typically disabled by default.

Part IV

Security Operations

4.1) Security Operations Management

The process used in-person to manage security incidents, implement and maintain security controls, and supervise those who have more access to systems and data is known as security operations management.

Communication and Reporting

Providing management with metrics and key performance indicators to measure success is one of the most crucial duties of security operations (KPIs). Metrics are numerical indicators that show whether security controls are in compliance with a desired goal (for instance, the number of complete and current antivirus installations) or whether the controls are working as intended (for example, the number of attacks blocked by a firewall). Numbers, counts, and sums are the most common formats for metrics. Metrics frequently contain a vast amount of information that, while helpful to the security team, is difficult for executives to comprehend. Metrics are therefore mainly applied internally to improve performance and identify issues. Although they are much simpler, key performance indicators, or KPIs, are based on metrics. They exemplify the data's meaning. KPIs typically take the form of a percentage or a straightforward red-yellow-green score, like a pass-fail statistic, that is similar to a dashboard. KPIs frequently lead to a remediation plan because they concentrate on highlighting things that are noncompliant and require attention.

Heat Maps

In this kind of diagram, green, yellow, and red are used to indicate areas that are under control and those that need attention. A heat map contains more data than a straightforward chart or table of numbers, but it is also much simpler to comprehend at a glance. The heat map is especially useful for identifying the precise locations of the issues. The heat map assists an executive in determining which part of the process needs attention, as opposed to a simple score for the entire process area, which may indicate a problem without outlining a solution.

Change Management

Change management processes are meant to manage risks associated with planned changes by carefully analyzing and reducing the impact of each change. Change management, a subset of information security, is concerned with safeguarding both the integrity and availability of data. Software and system modifications, such as patches, updates, new releases, and reconfigurations, sometimes have unanticipated and unintended effects. In addition to

minimizing these effects, a change management process makes sure that the appropriate individuals are aware of any potential issues and prepared to take appropriate action.

ITIL, a framework for service-oriented information technology service delivery provides a set of highly formalized and rigorous best practices for change management. You should consider the complexity and resource availability of your environment when evaluating change management processes to decide how to implement change management in your organization. This will help you determine how much process is actually necessary in your situation. A very comprehensive reference model for change management with a wide variety of best practices is offered by ITIL (version 3). In the ITIL framework, incident management and service management—the method by which IT services are provided and charged to end users—are complementary processes (the process of handling errors and outages). ITIL change management components include

- Change - Not just a change, but also the addition or removal of a part of an IT service that could have unanticipated effects.
- Change advisory board (CAB) - Stakeholders from the business and IT communities make up the group that reviews and approves changes. Prioritizing and/or scheduling changes may also fall under the purview of the CAB (in more dynamic environments with a high level of change activity).
- Change request (CR) or request for change (RFC) - a thorough explanation of a proposed change that includes a business case, risk analysis, and a plan to address any unexpected outcomes. The term RFC is preferred in ITIL version 3, though CR is also frequently used.
- Change model - a repeatable procedure, frequently preapproved for straightforward, risk-free changes, for putting into practice known changes that have been successfully implemented in the past.
- Change management system - a repository (or knowledge base) of each change that has ever been requested, implemented, or otherwise affected the process.
- Change schedule/forward schedule of changes (FSC) - the list of upcoming adjustments that have been authorized and are expected to take effect.

For mature IT organizations in sizable, mature environments, the full nine-step process is provided at the top. The steps are streamlined in a condensed version that is displayed at the bottom.

The first step is to record the change request (RFC). The request is entered into the system of records at this stage so it can be monitored and assessed. This change request should come from an incident or service request that is being tracked somewhere else in the system in a full

ITIL implementation. In other words, change requests are never the result of nothing; they are always prompted by a difficulty or a desire for improvement.

The change request is then quickly assessed by a change manager to ensure that it is properly documented and classified. This is just a quick check to make sure all fields are filled out and that this request for change is genuine and not just a misclassified piece of data.

The request is then categorized in accordance with the information given, including impact, severity, complexity, the requirement for downtime, and other elements that establish the extent of review and approval required. The request can now be given a priority ranking in relation to other change requests already present in the system. Based on the change calendar and the urgency of the business need driving the request for change, the change is then planned.

The CAB assesses the change and determines whether it is approved or denied based on the information that has been provided thus far. When an ITIL-based change management process is fully implemented, this evaluation and approval take place in a meeting with participation from all stakeholders following presentation by the change requestor and discussion with the CAB. In smaller settings, replacing the in-person meeting with email can streamline the process.

After approval is received, the build, test, and implement steps are carried out. These phases represent a typical IT methodology for deploying and testing changes in development, staging, and testing environments before fully deploying them in the production environment. Smaller environments might need to condense these steps because not all organizations have the luxury of having multiple environments that are exactly like production environments. When testing opportunities are scarce, a change can be implemented gradually among a smaller group; however, a strong backout plan, outlining the steps necessary to reverse the change, must be in place.

The process's last step, evaluation, can be conducted in front of the CAB during a meeting or, in smaller environments or for low-impact changes, separately via email or in the change management system.

Acceptable Use Enforcement

Every organization should have an acceptable use policy (AUP) that specifies what staff members are permitted to do with the computers they use, as well as the networks and data they have access to, as part of an overall security policy programme. The security operations division and HR typically work together to enforce this policy. Security operations is in charge of

identifying violations, notifying authorities, and conducting follow-up investigations; HR is in charge of prosecuting offenders. This division of responsibilities is crucial and resembles law enforcement, where police gather evidence (and occasionally stop a crime in progress), but judges determine the consequences.

The following list includes some policies that might be found in an AUP pertaining to a company's employees.

- Do not post confidential information on Internet message boards, chat rooms, or other online forums, nor give unauthorized people or locations access to, store, distribute, or otherwise process confidential information.
- Do not access company records, files, information, or any other data If there is no legitimate, authorized need for the information for your job.
- Do not send or forward offensive emails or visit offensive websites.
- Never connect any equipment that belongs to you personally to the network of the business.

The security operations team may be required to keep an eye on employee e-mail, external websites for access to company information resources and the disclosure of any confidential information, web site categories, network connections, and software installations. In these situations, the team would employ security instruments to generate reports and alerts, which the security operations staff would then review and escalate in accordance with their established procedures.

Proactive Enforcement

AUP enforcement entails more than just disciplining offenders of a policy through administrative means. Enforcement also refers to actively seeking out violations and putting a stop to them before they happen. Filtering technologies are used by technologies like URL blocking, web content filtering, email filtering, and application control to prevent access to websites or even to keywords that a company deems unacceptable. Email may be automatically scanned for regulated topics by filtering software. Other products might adopt a more obedient strategy, like merely logging each page visited and enabling reports to monitor user activity on the Internet. A database of URLs segmented into these categories can be used by web content filtering applications, for instance, to block access to sites with adult content, gambling, file-sharing, political, shopping, and other content that might be considered objectionable. Application control products can control how employees use media-rich network protocols, instant messaging, streaming media, and other services. They can control access by allowing

access when there is enough bandwidth and blocking access when the company needs that capability for work-related activities.

Administrative Security

Think about the potential advantages an authorized administrator has compared to a less privileged regular user when considering controls that determine the availability and integrity of computing systems, data, and networks. Within your network, people with elevated privileges include systems administrators, backup operators, database administrators, maintenance technicians, and even help desk support staff. You must also take into account the controls that can stop administrator abuse of privilege if you want to ensure the security of your systems. Without administrative task control, the automated controls that regulate access to regular transactions and data within your organization are unable to guarantee integrity and availability. Any other controls are weakened if the controls governing the use of administrative authority are not strong enough.

Preventing Administrative Abuse of Power

The logical infrastructure of the network, including domain controllers and other central administration servers, is managed by service administration. They also divide users into groups, assign privileges, and manage the specialized servers on which these controls are installed. On the other hand, data administration involves managing servers that house files, databases, websites, and other types of content. Even within these structures, authority can be further decentralized; specifically, roles and privileges can be established. The people with access rights to back up the database server and the file server should not be the same people.

As with file and print server administrators, database administrators may only be allowed on specific servers. These roles can be further broken down in large organizations, with some help desk representatives having the ability to reset passwords and accounts while others are only allowed to assist with the operation of specific programs. The idea is to acknowledge that while elevated privilege administrators should all be trusted, some should be trusted more than others. The number of people who can abuse their all-inclusive or all-encompassing privileges decreases as the number of those people decreases.

Management Practices

The management techniques listed below can support administrative security:

• Implement controls on out-of-band access to devices, like serial ports and modems, and physical controls on access to sensitive devices and servers.

• Place controls on remote access, access to consoles, and access to administrative ports.

• Limit the number of administrators who can physically access these systems or log in at the console. An employee's authority can still be limited even though they have administrative status.

IT administrators have a great deal of control over an organization's resources. Before hiring, reference checks and background checks should be performed on every IT employee with these privileges.

• Employ techniques for automated software distribution. Automated OS and software installation techniques are a good practice for preventing the abuse of power because they not only guarantee standard setup and security configuration, preventing accidental compromise. Back door programs and other malicious code or configuration are less likely to be installed when systems are automatically installed and configured.

• Use scripts and procedures for administration that are standard. The use of scripts can increase productivity, but rogue scripts can cause harm to systems. Scripts can be standardized to reduce the likelihood of abuse. Additionally, scripts may be digitally signed to guarantee that only approved scripts are executed.

Accountability Controls

Accountability controls make sure that system and network activity can be linked to a specific person.

These controls include

Authentication controls - Smart cards, passwords, biometrics, accounts, and other similar tools and algorithms that adequately protect the authentication process

Authorization controls - Devices and settings that limit access to particular users and groups

Accounts, passwords, and authorization controls can be effectively used to hold users accountable for their actions on your network. For a system to be used properly, each employee who is permitted to use it must have at least one account assigned to them. All administrative staff members ought to have a minimum of two accounts: one for "regular" use, with regular privileges, for things like checking email, searching the web, and doing other

menial tasks, and another for performing administrative tasks. Some highly privileged tasks may be assigned to a single account, with the password being jointly created by two trusted employees. As a result, neither can complete the task on their own; they both must. Additionally, each will observe the other performing the duty because both may be held accountable. An administrative account on the root certification authority could be another special account. Two IT staff members must be present to log on when using this account, for example, to renew this server's certificate, reducing the likelihood that the keys will be compromised.

Security Monitoring and Auditing

It is crucial to track and audit system activity for two reasons. First, monitoring activity provides the systems administrator with information on which systems are performing as they should, where failures are occurring, where performance is a problem, and what kind of load the system is currently carrying. These specifics identify areas that require additional research and enable proper maintenance as well as the identification of performance bottlenecks. The sage administrator assesses the overall network and system health using every available tool and then takes appropriate action. The disclosure of suspicious activity, audit trails of normal and abnormal use, and forensic evidence that can be used to diagnose attacks or misuse as well as possibly apprehend and prosecute attackers are the second and related security concerns. Suspicious activity can include outward signs, such as well-known attack codes or signatures, or it can take the form of patterns that, to the knowledgeable, indicate potential tries or successful intrusions. You must comprehend the types of information available and how to obtain them in order to take advantage of the data found in logs and other monitoring techniques. You must also be aware of how to use it. Three types of information are useful:

- Activity logs
- System and network monitoring
- Vulnerability analysis

Activity Logs

Each device, operating system, and application may offer a lot of logging functionality. However, administrators do have to choose how much activity to record. There is no simple solution for what should be logged, and the range of information that is logged by default

varies as well as what is available to log. The answer depends on the log-in purpose and the activity.

Determining What to Log

In general, you must answer the following questions:

• What is logged by default? This includes not just the typical security information, such as successful and unsuccessful logons or access to files, but also the actions of services and applications that run on the system.

• Where is the information logged? It may be logged to several locations.

• Do logs grow indefinitely with the information added, or is log file size set? If the latter, what happens when the log file is full?

• What types of additional information can be logged? How do you turn these options on?

• When is specific logging activity desired? Are there specific items that are appropriate to log for some environments but not for others? For some servers but not others? For servers but not desktop systems?

• Which logs should be archived and how long should archives be kept?

• How are logs protected from accidental or malicious change or tampering?

Activity logs must be given a size and can be set to overwrite previous events, pause logging until manually cleared, or, in Security Options, shut down the system when the log file is full. Activity logs do not automatically archive themselves. A large log file should be created, and events should be allowed to be overwritten, but best practices advise monitoring file fullness and frequently archiving to ensure that no records are lost. The security log contains one or more records as a result of auditable events. Information dependent on events is included in every record. Although an event ID is included in every event, the type of event will determine the event's brief description, date, time, source, category, user, type, computer, and other details.

Log File Summarization and Reporting

Early security and systems administrator guidance emphasizes the need for daily log reviews and presupposes that the time is available to do so. We now understand that, barring

exceptional circumstances, this does not occur. The following actions are recommended according to current best practice:

- Regularly, collecting copies of security event logs, archiving them in a database, and then writing SQL queries to generate reports or using a commercial product to directly query this database for particular log types.
- Investing in a third-party security management tool that collects and analyses specific types of log data.
- Putting in place a Security Information and Event Management (SIEM) system that gathers alerts and log data from a variety of sources, including security logs, web server logs, IDS logs, and so on.
- Making use of the log management features of platforms or services for systems management or service management tools.

System and Network Activity

System and network activity can also notify the knowledgeable administrator of potential issues, in addition to log data. In addition to allowing for the investigation and remediation of performance bottlenecks and the repair of critical systems, system and network monitoring enables you to determine whether everything is operating normally or whether an attack is in progress. Many management tools report on system activity, while some SIEM tools also aim to provide a picture of network activity. Continuous monitoring is perhaps the best defense for security operations.

Log files like host logs, proxy logs, authentication logs, and attribution logs must be able to be produced, collected, and queried by security operations. Deep packet inspection must be performed by security operations that cover all of the network's crucial "choke points" (ingress and egress). There are numerous commercial monitoring tools and event correlation engines available. A significant task is choosing what to monitor and how to monitor it. The National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," is a good resource for security professionals. The strategies for continuous monitoring are outlined in this document. Targets (assets) with high value require priority monitoring.

Vulnerability Analysis

Vulnerability scanners are a necessary component of every security toolkit. These tools offer an audit of the systems that are currently in use in comparison to known configuration flaws, system vulnerabilities, and patch levels. They may be thorough and able to scan a variety of platforms, operating system-specific, or specifically focused on a single vulnerability or service, like a malware detection tool. They may be highly automated and only need a simple start command, or they may demand complex knowledge or the accomplishment of a lengthy list of tasks. Prior to using or commissioning a vulnerability scan, take some time to consider what the results might reveal. Even straightforward, single-vulnerability scanners might fail to find vulnerabilities. Instead, they might just say that a machine is running the particular vulnerable service. Some of them might be false positives, others might require highly technical expertise to comprehend or mitigate, and still others might be flaws that you have no control over. Although there are different vulnerability scanning products, it's important to remember that a simple vulnerability assessment and mitigation do not call for expensive consultants or fancy tools. There are numerous free sources of vulnerability lists as well as free tools like the OpenVuln Scanner we suggested. Operating system vendors have lists specific to their products available online.

Keeping Up with Current Events

The challenge of staying current with the security landscape is one that security professionals must overcome. You should stay informed about current threats and the corresponding countermeasures that apply to the key business operations and high-value targets in your organization. To find out more about the current threat landscape, you can use a variety of resources. Leading security companies such as Symantec, which releases an annual Internet Security Threat Report, McAfee Labs, which offers a quarterly threat report, IBM X-Force, which generates threat and trend risk reports, and Cisco, which releases security threat whitepapers, are all good sources for staying up to date on the threat landscape. Additionally, a number of organizations provide threat intelligence, such as the Computer Security Institute (CSI), the SANS Institute, the United States Government Emergency Readiness Team (US-CERT), and the Carnegie Mellon Software Engineering Institute (CERT), which publishes a list of the top cyber security risks and conducts long-term security studies. Professional organizations like the International Information Systems Security Certification Consortium, Inc. (ISC2) offer vendor-neutral training, education, and certifications for security professionals, including the CISSP, in addition to these resources. The COBIT standards and CISA certification are just a couple of the industry-leading knowledge and practices for information systems that are being developed, adopted, and used by the Information Systems Audit and Control Association (ISACA). You are in charge of implementing the suggested security precautions for every asset noted. The

challenge faced by security professionals is determining when a system or application needs to be patched or fixed. When a maintenance subscription is purchased, the majority of vendors offer a mailing list for security updates and provide security alerts and information. Although there are many security mailing lists, Insecure.org's Bugtraq and Full Disclosure lists have become the most well-liked in recent years. Keep in mind that the most recent hacks and exploits are never published online, and vendors are never made aware of "zero-day exploits" before they happen. But by joining these mailing lists, you can stay as informed as it is possible to be.

Incident Response

The efficiency and skills of an incident response team determine how well a company can identify and address a sophisticated attack. Since the response to an incident will be carried out by a variety of roles ranging from managers to employees and internal to external professionals, such as IT staff, business partners, security operations, human resources, legal, finance, audit, public relations, and law enforcement, this team is made up of more than one person. Any security operations function should include a Computer Security Incident Response Team (CSIRT). The CERT program at Carnegie Mellon provides a great example and practical resources for incident response. A handbook for computer security incident response teams is available from CERT (CSIRT). Everything from a suggested framework to common problems faced by response teams is covered in the guide. The steps for creating your own incident response team are listed below and are available on the CERT website at www.cert.org.

As with most security initiatives, the first step is to secure senior management support for your project. This support is necessary for funding, resources, and the team's ability to hire employees from different organizational departments on a temporary basis. In the end, top management's backing is related to the team's success. The high-level strategic plan for the incident response team must be defined as the next step. A road map and project plan are provided for implementing the CSIRT by carefully planning the objectives, timelines, and team composition while taking into account the dependencies and limitations the team must deal with.

The crucial next step in determining the role of the CSIRT and the resources it will require is gathering data from the organization. This step involves discovering which other organizations have the resources you require and how to make use of them. You will choose which external resources, like law enforcement and public CSIRT organizations, need to be involved during the information gathering phase. The team's vision, mission, charter, and plan must then be developed and communicated. By giving the team members a clear direction, they can better

understand their responsibilities and how the organization works with the CSIRT. Budgeting is also a part of this step according to CERT.

After all the planning is finished, the team must be assembled. In this phase, personnel are assembled, trained, and equipment is acquired to support the tasks outlined in the team charter. A communication program is implemented after announcements are sent to the entire organization and the team is operational.

The team's effectiveness is evaluated as the last step to identify areas for improvement in the spirit of a plan-do-check-act cycle. A single organization's incident response team will not be adequate to provide the necessary coverage in the blended threat environment of today. In order to be effective, security operations must partner with a reputable incident response group. Additionally, due to the high demand for this skill set, security operations must have some level of in-house or outside malware analysis. In order to meet the challenges posed by today's complex, networked, global economy, security operations must prioritize continuous monitoring and incident response.

4.2) Disaster Recovery, Business Continuity, Backups, and High Availability

Business continuity planning and disaster recovery are two distinct but related ideas. Disaster recovery actually forms a part of business continuity. Disaster recovery (DR) is the process of restoring the technical elements of your company, including its computers, software, network, data, etc. Disaster recovery is a component of business continuity planning (BCP), which also includes steps to restart daily operations at your place of business as well as the foundational functionality of the infrastructure required to support it. Planning for business continuity is essential to ensuring that operations continue after a disaster and that things return to "business as usual." Professionals in DR and BCP collaborate to guarantee the continuity and recovery of all aspects of an organization that are impacted by an outage or security event. According to DRI International, a disaster is "any event that creates an organization's inability to provide critical business functions for some predetermined period of time" or "any sudden, unplanned calamitous event causing great damage or loss." The disaster recovery planner or business continuity specialist would sit down with all of the organization's leaders and create a map of what would constitute a disaster for that organization with this general definition in mind. This is the first phase of a business impact analysis (BIA), which is a crucial component of planning service reliability and resumption.

Disaster Recovery

When creating a disaster recovery plan, you must comprehend how the network, applications, and information technology (IT) infrastructure of your company support the operations of the enterprise from which you are recovering. When a disaster strikes, the DR planner may need to collaborate with (and inform) the business unit in order to help them comprehend why they must pay for a day-one recovery rather than a day-three recovery. The business unit may believe that any efforts to ensure business continuity or disaster recovery will be prohibitively expensive because the business unit's budget typically includes a sizeable expense for the IT department. You can occasionally find a way to get around a specific electronic feed or file dependency by working with the IT subject matter experts (SMEs). This may be necessary to continue the recovery of your system. If you are aware of who and what you are recovering from, everything will go smoothly. To operate a fine, successful, and profitable organization, the responsible business continuity or disaster recovery professional should collaborate with the IT group and the business unit. By bringing together experts, such as the programmer, business analyst, system architect, or any other SME that is required, you can learn who and what you are recovering. When it comes to developing your DR plan, these professionals will be of utmost value. They are the ones who understand the technical requirements for managing the in question business systems and can justify why a particular disaster recovery procedure

will cost a certain sum. For the business unit manager to be able to make wise decisions, this information is crucial.

Business Continuity Planning

The business continuity specialist is more focused on the employee-performed business functions than on the underlying technologies. The business continuity specialist must collaborate closely with each business unit in order to determine how the company can carry on as usual during a disaster. As a result, they must meet with the decision-makers in the management team, those who implement those decisions, and finally the "technical workers" who carry out the work. The business unit management team is essential because its members view the business unit from a business perspective—at a higher level—and will aid in determining the significance of the application because they are familiar with the business unit's mission. The business unit must keep a disaster recovery plan in mind as it introduces new or upgraded program applications. It is crucial to communicate these changes to the disaster recovery and/or business continuity professional. As you can see, the business continuity specialist needs to be good friends with every executive in the division so that the knowledge and capability to recover the product will be taken into account in the event that a new product is introduced.

The Four Components of Business Continuity Planning

Business continuity planning consists of four main parts, each of which is crucial to the overall BCP initiative:

- Plan initiation
- Business impact analysis or assessment
- Development of the recovery strategies
- Rehearsal or exercise of the disaster recovery and business continuity plans

Every business unit needs to have its own strategy. A comprehensive plan for the organization as a whole, including all the business units, is required. A business continuity plan (recovery of the people and business function) and a disaster recovery plan ought to be two plans that cooperate (technological and application recovery).

Initiating a Plan

At the start of the plan's development, everyone is on the same page thanks to the plan's initiation. From the viewpoint of the specific business unit or the entire organization, a disaster or event is defined. What one business unit or organization views as a disaster might not be regarded in the same way by another business unit or organization, and the opposite is also true. A BIA is crucial for a number of reasons. It offers a monetary impact for an unexpected event to an organization or business unit. This shows how long a company's operations can be disrupted before going out of business entirely.

Analyzing the Business Impact

You must first identify the crucial business function when conducting a business impact analysis. Only the crucial employees in the business unit can decide this. Since the business unit will ultimately be responsible for funding the disaster recovery project and business continuity plan, the BIA should be completed and reviewed by upper management.

Developing Recovery Strategies

Create your recovery strategy as your next step. The business unit needs to be aware of the options available to them for various types of recoveries since they will be responsible for paying for it. You can offer a quick recovery or one that takes place right away. Everything depends on the business functions that must be recovered and the maximum amount of time the business unit can function without them. Written procedures must be available for all employees in your business unit to quickly access, comprehend, and follow in a business recovery situation. The business function that must be carried out requires information to be easily accessible. To guarantee that they are available in a disaster scenario, the procedures should be kept in several easily accessible locations. This list must be of the current employees to contact, and it should include members of the Human Resources, Facilities, Risk Management, and Legal departments. The list of contacts should also include the local fire and rescue department, police department, and emergency operations center.

Rehearsing Disaster Recovery and Business Continuity Plans

Rehearse, exercise, or test the plan is the fourth and most important BCP component. Even if the other three elements are in place, the plan is insufficient if you are unsure of its viability. Testing your strategy is crucial. All the effort you put into creating the plan will be for naught if it hasn't been tested and fails in the event of a disaster. However, if a test of the plan ends in failure, you can refine it and conduct another test.

Third-Party Vendor Issues

Most organizations make use of various third-party vendors (Enterprise Resource Planning [ERP], Application Service Provider [ASP], et al.) in their recovery efforts. In these situations, knowing the details of the third-party vendor is just as important for your company's or your technology's recovery. It is advantageous, if not essential, to learn more about the third party's operations before implementing its product or services when you need to use such resources. In the real world, the disaster recovery and/or business continuity specialist must incorporate the vendor's data into the continuity plan for the business unit. You can't get your operation back up and running if a third-party vendor isn't ready to help you if a critical path in your DR plan depends on their involvement. The strength of your recovery will also depend on how quickly the vendor can recover from a failure. Even if your recovery is technically sound, you still need to be able to conduct business. The third-party vendors you work with should adhere to the same standards as your own company. You should be able to do business with them. The appropriate inquiries with third party vendors should be made by the disaster recovery or business continuity coordinator to confirm that they can support a DR scenario.

Awareness and Training Programs

An awareness program is a crucial component of business continuity and disaster recovery planning. Each business unit can meet with the business continuity or disaster recovery specialist to conduct tabletop exercises. These activities are crucial because they force the members of the business unit to consider a specific event and how to first stop it or lessen its impact, then how to recover from it. The occurrence could be anything from workplace violence to a category 3 hurricane. It is up to the management team to create or develop an action plan or business continuity plan because any work stoppage could potentially impede the organization's recovery or resumption of services. This procedure must be facilitated by the business continuity or disaster recovery specialist, who must also inform the business unit that certain events have the potential to bring the operation to a complete halt.

Backups

Backups can be used to restore the entire system, but they can also be used to recover specific data, like the contents of a mailbox or a "accidentally" deleted document. Backups can be expanded to include saving data that isn't just digital. Specifications and configurations, policies and procedures, equipment, and data centers can all be backed up as part of a backup process. It won't solve the issue, though, if the backup is inadequate, too dated, or the backup media is damaged. It's not always enough to have a backup plan in place to provide protection. Additionally, many businesses can no longer rely on conventional backup procedures because

performing an offline backup is unacceptable, performing an online backup would significantly impair system performance, and recovering from a backup would take too long for the business to resume operations. Such businesses use redundant systems and cloud services as alternatives to traditional backups. Therefore, backup systems and processes reflect both an organization's availability needs and its recovery needs. This section explains conventional data backup procedures and gives details on more recent technologies.

During a traditional backup, data is predictably and methodically copied to backup media, primarily tape, for safe on- and off-site storage. Thus, backup media can be made available in case a system fails and needs to restore data to new or repaired systems. Modern operating systems and application configurations are backed up in addition to data. When applications that support data are tightly integrated with a particular system, this enables faster restore capabilities and occasionally might even be the only way to restore those systems.

Backup Types

There are several standard types of backups:

• *Full* - Backs up all data selected, whether or not it has changed since the last backup. On various systems, a full backup is defined differently. On some systems, a full backup contains the essential operating system files required for a system's complete rebuild, but on other systems, it only backs up user data.

• *Copy* - Data is copied from one disk to another.

• *Incremental* -- The archive bit on a file is disabled during data backup. The archive bit is reset when changes are made to the file. Using this data, an incremental backup backs up only the files that have changed since the previous backup. The archive bit is turned off once more by an incremental backup, and the subsequent incremental backup only backs up the files that have changed since the previous incremental backup. This method of backup saves time, but it also necessitates that every incremental backup made after the last full backup be restored.

• *Differential* - Similar to an incremental backup, a differential backup only archives files that have changed since the last backup and have the archive bit set. A differential backup does not, however, cause the archive bit to be reset, unlike an incremental backup. All files that have changed since the last differential backup that reset the bits are backed up with each differential backup. With this method, differential backups are done after a full backup. The last differential backup made is the only backup that is restored after the full backup. However,

depending on your system, creating differential backups takes longer than creating incremental backups, which can slow down the restore process.

Backup Alternatives and Newer Methodologies

Many backup strategies are available for use today as alternatives to traditional tape backups.

• *Hierarchical Storage Management (HSM)* - HSM is a legitimate method of data preservation that can be taken into account as part of a data retention strategy even though it is more of an archiving system than a strict "backup" strategy per se. The least-used files are transferred automatically through HSM to progressively farther-flung data storage. In other words, data that is frequently used and changed is kept online on fast local discs. Data is transferred to more distant storage locations, like disc appliances, as it ages (because it isn't accessed or changed). The user can still easily access the data though it is still catalogued. If accessed, the data can be automatically made available by being transferred to local discs, returned through network access, or, in the case of offline storage, operators can be prompted to load the data. For the more distant data storage, online services or cloud storage can be used; email archiving solutions frequently employ this strategy.

• *Windows shadow copy* - A working volume is captured by this Windows service, and after that, a regular data backup that includes open files can be created. The shadow copy service only fixes a point in time and then stores subsequent changes in a hidden volume; it does not create a copy. Closed files and disc copies of open files are both stored with the changes when a backup is made. When files are kept on a Windows system, the service continuously monitors file changes while running in the background. Any user who has permission to read the file can access older versions of it if a special client is loaded and restored them.

• *Online backup or data vaulting* - A person or organization can hire an online service that connects to a host or hosts automatically and frequently and copies specific data to an online server. Usually, plans can be made to back up everything, just data, or just certain data sets. Payment plans can include full data backups of entire data centers and are based on both the amount of data backed up and the number of hosts.

• *Dedicated backup networks* - If parallel disc and tape systems are offered and their combined throughput capacity is greater than the LAN's, an Ethernet LAN may turn into a backup bottleneck. Additionally consuming bandwidth, backups hinder the efficiency of other network operations. A Fibre Channel storage area network (SAN), Gigabit Ethernet network, and Internet Small Computer Systems Interface are frequently used to implement dedicated backup networks (iSCSI). Data transfer at wire speed is possible with iSCSI and Gigabit Ethernet. Backups are stored on SAN servers or disc appliances.

• *Disk-to-disk (D2D) technology* - Servers may be able to provide data faster than the tape system can record it, making a slow backup system a bottleneck. Both backups and restores may be quicker with D2D servers because they don't require a tape drive and discs can be delivered over high-speed dedicated backup networks. Dedicated backup networks can be provided for D2D, or it can use conventional network-attached storage (NAS) systems supported by Ethernet connectivity and either the Network File System (NFS, on Unix) or Common Internet File System (CIFS, on Windows) protocol.

Backup Policy

Having a backup policy that is both enforceable and followed is the best way to guarantee that backups are created and protected. The procedure's objectives should be stated in the policy, including frequency, the need for on-site and off-site storage, and specifications for formal procedures, authority, and documentation. Then, using the most recent software, data sets, hardware, and technological resources, procedures can be created, approved, and used to interpret policy.

The following topics should be specifically detailed in the policy:

• *Administrative authority* - Name the person with the power to physically begin the backup, move and check out backup media, carry out restores, sign off on activity, and approve changes to procedures. The criteria for selecting people should also be included. Separating responsibilities for backing up and restoring, for approval and activity, and even between systems, should all be recommended.

• *What to back up?* - Choose the data that needs to be backed up. Should only application data be backed up, or also system data? What about the level of version, patch, and configuration information? How will operating systems and applications be replaced? Are both the original and backup installation discs offered? These specifics ought to be mentioned.

• *Scheduling* - Identify how often backups should be performed.

• *Monitoring* - Specify how to ensure the completion and retention of backups.

• *Storage for backup media* - Indicate the ideal backup media storage method from the many options available. Are media files kept both on and offsite? What specifications apply to each type of storage? Are there, for instance, fireproof vaults or cabinets? Do they remain closed? What location are they in? Although it may be ineffective to keep backups close to the original

systems, onsite backup media must be accessible. A disaster that destroys the primary system might also destroy the backup media.

• *Type of media and process used* - Describe the backup process. How many and what kind of backups are created? How frequently do they get made, and how long do they last? How frequently is backup media changed?

High Availability

Redundancy and the idea of high availability go hand in hand. Redundancy guarantees the accuracy and accessibility of information, ensuring the survival of a company or organization. To determine where and how much redundancy is required, there are two methods that can be used. The first, more conventional method involves comparing the cost of downtime without redundancy to the cost of providing redundancy. Direct comparisons between these costs are possible (is the cost of downtime higher or lower than the cost of redundancy?). The second approach involves making a choice based on the likelihood that customers will choose the company that can offer the best availability of service, which is harder to calculate but getting easier to justify. This is based on the rising expectations that online services, in contrast to traditional services, be accessible 24/7/365. A selling point that directly generates more business is high availability. Indeed, some customers will demand it. There are automated methods for providing system redundancy, such as hardware fault tolerance, clustering, and network routing, and there are operational methods, such as component hot-swapping and standby systems.

Automated Redundancy Methods

• *Clustering* - Systems or computers as a whole are duplicated. When one system fails, the other systems take over automatically. Clusters may be configured as active-active or active-standby, where one system is live and the other is idle, or as dynamic load sharing, where multiple systems are kept perfectly in sync. The best configuration is active-active because no system is ever left unattended and the combined power of all systems is always used. There are simply fewer systems available to carry the load in the event of a system failure. Load balancing changes when the failed system is replaced. However, clustering does have drawbacks. Duplicating systems is costly when active-standby is used. When systems are under heavy load, the failover time for these active-standby systems can take several seconds. However, active-active systems might need specialized hardware as well as additional, specialized administrative knowledge and upkeep.

• *Fault tolerance* - Components may be equipped with backup systems or sections of systems that enable them to recover from errors or continue to function even when they occur. For instance, fault-tolerant CPUs employ a number of CPUs that operate simultaneously and share the same processing logic. Three CPUs are typically used, and the outcomes from each CPU are compared. One CPU is deemed to have failed and is not used again until a replacement is found if its output differs from that of the other two CPUs.

• *Redundant System Slot (RSS)* - One unit contains entire hot-swappable computer units. Although every system has a unique operating system and bus, they are all connected and share other parts. RSS systems, like clustered systems, can be either active-active or active-standby. RSS systems function as a unit and cannot be separated from it and continue to function.

• *Cluster in a box* - A single unit combines two or more systems. These systems differ from RSS systems in that each component is equipped with its own CPU, bus, peripherals, operating system, and applications. Its advantage over a conventional cluster is the ability to hot-swap components.

• *High-availability design* - On the network, there are two or more complete components, one of which acts as an active node or as a standby system (with traffic being diverted there in the event of a primary system failure) (with load balancing being used to route traffic to multiple systems sharing the load, and if one fails, traffic is routed only to the other functional systems).

Operational Redundancy Methods

In addition to technologies that provide automated redundancy, there are many processes that help you to quickly get your systems up and running, if a problem occurs. Here are a few of them:

• *Standby systems* - Systems, whether whole or in part, are kept ready. The standby system can be activated in the event that a system or one of its subsystems fails. This method has a lot of variations. The clustered system is ready to go but idle because some clusters are deployed in active-standby state. A hard drive may simply be moved to another, duplicate, online system in order to quickly recover from a CPU failure or other serious system failure. A backup system outfitted with database software may be kept available to enable quick recovery from database system failure. The export and import features or replication are used to update the database on a regular basis. The backup system, though it might be missing some recent transactions, can be made online if the primary system fails.

• *Hot-swappable components* - Nowadays, replacing a lot of hardware doesn't require shutting down the system. Current hardware components that can be added include hard drives,

network cards, and memory. Modern operating systems immediately recognize the addition of these devices, and operations proceed with few, if any, service interruptions. For instance, a RAID array's built-in redundancy may be able to cover a drive failure. The array will resume its pre-failure state if the failed drive can be replaced without shutting down the system. There won't be any service interruptions, but depending on the load at the time, performance might be affected.

Compliance with Standards

Here are some guidelines from a few standards

ISO 27002

ISO 27002 has an entire section devoted to business continuity management (Section 14), which contains the following provisions:

• 14.1.1 - Information security should be included in the business continuity management process. A managed process should be put in place to develop and maintain business continuity throughout the organization, which includes information security requirements. The business continuity plan should be formalized, and regularly tested and updated.

• 14.1.2 - Business continuity and risk analysis should include consideration of events that could cause interruptions to business process such as equipment failure, flood, and fire. A risk assessment should be conducted to determine impact of such interruptions, and a strategic plan should be developed based on the risk assessment results to inform the overall approach to business continuity.

• 14.1.3 - The development and implementation of business continuity plans should include information security, and plans to restore business operations within the required time frame following an interruption or failure should be regularly tested and updated.

• 14.1.4 - There should be a single business continuity plan framework, maintained to ensure that all plans are consistent and priorities are identified for testing and maintenance. Consideration should also be given to conditions for activation of the plan, and individuals should be assigned responsibility for executing each component of the plan.

• 14.1.5 - Business continuity plans should be tested regularly to ensure that they are up to date and effective, and they should be maintained by regular reviews and updates to ensure their continuing effectiveness. In addition, the organization’s change management program

should include measures to ensure that business continuity is addressed when systems are modified, introduced, and retired.

COBIT

COBIT contains the following provisions,

• DS4.1 - A framework should be developed for IT continuity to support business continuity management for the organization, using a consistent process. The objective should be to assist in determining the required fault tolerance of the infrastructure and to drive development of disaster recovery and IT contingency plans. The framework should address the organizational structure for continuity management, including the roles, tasks, and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test, and execute the disaster recovery and IT contingency plans. The plan should also identify critical resources, key dependencies, monitoring and reporting of availability of critical resources, alternative processing, and backup and recovery.

• DS4.2 - IT continuity plans should be developed based on the framework, and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk analysis of potential business impacts and they should address requirements for resilience, alternative processing, and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and testing.

• DS4.3 - Attention should be focused on items specified as most critical in the IT continuity plan, to build in fault tolerance and establish priorities in recovery situations. Less-critical items should not be recovered first, and response and recovery should be done in line with prioritized business needs while ensuring that costs are kept at an acceptable level, and regulatory and contractual requirements are met. Availability, response, and recovery requirements should be specified for different tiers, including outage tolerances such as 1 to 4 hours, 4 to 24 hours, more than 24 hours, and critical business operational periods.

• DS4.4 - IT management should define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Changes in procedures and responsibilities should be clearly and timely communicated.

• DS4.5 - The IT continuity plan should be tested on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed, and the plan remains relevant. This

requires careful preparation, documentation, reporting of test results, and, according to the results, implementation of an action plan. Recovery testing should proceed from single applications, to integrated testing scenarios, to end-to-end testing and integrated vendor testing.

• DS4.6 - All stakeholders should be provided with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Training should be improved based on the results of the contingency tests.

• DS4.7 - A distribution strategy should be defined and managed to ensure that continuity plans are properly and securely distributed and available to appropriately authorized parties when and where needed. Consideration should be given to making the plans accessible under all disaster scenarios.

• DS4.8 - Actions to be taken for the period when IT is recovering and resuming services should be planned in advance. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. The business should understand IT recovery times and the necessary technology investments to support business recovery and resumption needs.

• DS4.9 - All critical backup media should be stored offsite along with documentation and other IT resources necessary for recovery and business continuity plans. The scope of backups should be determined in collaboration between business process owners and IT personnel. Management of the offsite storage facility should adhere to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed for content, environmental protection, and security. Compatibility of hardware and software should allow archived data to be restored, and backups should be periodically tested and refreshed.

• DS4.10 - IT management should have established procedures for assessing the adequacy of the plan concerning the successful resumption of the IT function after a disaster, and the plan should be updated based on the results.

4.3) Incident Response and Forensic Analysis

Computer and network systems' regular operations can and will be interrupted. An incident will be deemed any interruption of a computer system's regular operation for the purposes of this chapter. Organizations need systems and procedures to detect these disruptions, as well as plans and guidelines for how to react and recover. When a problem is discovered, organizations should coordinate their response and recovery using their incident response plans. You may occasionally need to reconstruct system activity and extract data from impacted computer systems. Identification, extraction, preservation, and reporting of data taken from a computer system constitute the process of forensic analysis. A failed system's critical data can be recovered using forensics; unauthorized employee activity can be documented; and evidence can be gathered for potential criminal prosecution.

Incident Response

Any incident response (IR) plan's ultimate objective is to quickly and painlessly contain, recover from, and resume normal operations. Regardless of when a problem arises, thinking through and creating a plan of action can help avoid panic and costly errors. Additionally, developing, reviewing, and testing response protocols will expose gaps and failures in the organization's detection, response, and recovery capabilities. Organizations can recover from a variety of incidents with the help of an effective IR plan. Personnel with the knowledge to assess the situation, plan a course of action, and implement solutions are needed for the initial response. The initial responders may also find that the incident's scope is greater than they initially believed or that it affects additional systems, in which case they will require more personnel or teams. Responders may find it easier to locate and contact such resources if escalation lists are clearly defined. To handle the incident's non-technical aspects, it might be necessary to reach out to other departments in addition to the technical ones, like public relations, legal, or human resources. The IR strategy should also take into account the fact that the person who finds a problem is probably unable to solve it and will therefore need to report it. For many IR plans, defining how and where incidents should be reported is a good place to start. The main components of the IR plan's details are how personnel are notified, what the escalation procedures are, and who has the authority to make decisions in relation to a specific incident. The phases of an effective IR plan are broken down into the following sections, each of which is covered in detail:

- Incident detection
- Response and containment
- Recovery and resumption

• Review and improvement

Incident Detection

There are several ways to detect incidents. It might originate from an Intrusion Detection System (IDS) or Security Information and Event Management (SIEM) system, a user phone call, or an alarm-sounding dedicated system. However, a public service may also issue a notice or caution. Finding an actual incident, such as a process failure or security breach, is the first barrier to effective incident response. Simple Network Management Protocol (SNMP)-based systems are frequently chosen for monitoring. Using a centralized console, SNMP management systems can be used to regularly monitor system response times and check the availability of processes. These systems have the capacity to email or page designated personnel to alert them when an alarm is triggered. Should a serious fault arise that needs attention, the monitored systems themselves can use SNMP to send urgent messages called traps to a console. Organizations need systems to identify security-related events and alert the appropriate parties in addition to SNMP monitoring. SIEM systems collaborate with IDSs to correlate, summaries, report, and alert on issues at a higher level, saving the system administrators from having to sift through voluminous logs. Intrusion detection systems (IDSs) have been developed specifically for the purposes of detecting malicious activity.

Response and Containment

The organization's response strategy should be started as soon as a potential incident is identified. An organization must act quickly to assign the appropriate individuals to the issue. There should be a clear and easy method for informing the proper staff members of the changing circumstances. The IR plan must include up-to-date contact information. A ticketing system with multiple queues that automatically contact designated staff when a ticket is assigned to that queue may be maintained by larger organizations. Whatever mechanism is used, it should be a trustworthy and effective way to get in touch with whoever the organization wants to be working on the issue. Keep in mind that a prompt and well-planned response could mean the difference between a minor incident and a serious disaster. After the appropriate parties have been informed, their main objective is to quickly assess the situation and determine any immediate actions needed to contain and stop further system damage. They must respond to the following questions right away:

• Is this a security incident?

• If it is a security incident, has the attacker successfully penetrated the organization’s systems, and is the attack still actively in progress?

• If it is not a security incident, what is causing the alert?

Determine whether the attack is active or not and whether it is obviously successful if the incident appears to be a security breach. The response will have more time to be planned if it is not active or successful. If the attack seems to have been successful or is still going on, prompt action must be taken to close the hole. The ultimate objectives of the organization have an impact on the actual actions taken. Response strategies should take care to preserve and gather evidence in the event that an organization decides to prosecute an intruder. To have system evidence that is admissible in court, a number of legal requirements must be met. The best course of action may be to immediately shut down affected systems and block the attacker's network path if an organization is only concerned with recovery and has no interest in pursuing legal action.

You might need to communicate with the affected systems as you evaluate the severity of the security breach. When working with a potentially compromised system, the most crucial thing to understand is that you shouldn't put your trust in it. Remember that logs may have been changed to hide the attacker's activity and do not rely on system commands to report accurate information. When responding to an incident, effective communication between response personnel, decision makers, system owners, and affected parties is essential to avoid duplication of effort and people working incompatibly.

IR plans should include the necessary documentation for securing emergency preapproval to make changes outside of regular change windows in the event of system failures. The system vendor should be contacted to report the issue and to gain access to the vendor's support staff if the root cause is not immediately apparent. IR plans should contain the vendor's contact information as well as the information required to access support.

Recovery and Resumption

The organization can enter recovery and resumption mode once the incident has been contained in order to resume normal operations. This mode includes installing patches, changing the configuration, or swapping out malfunctioning hardware for system failures. It concentrates on securing systems, locating and closing security gaps, blocking access for intruders, and restoring systems to a trusted state in the event of security breaches. To maintain and conceal their access, intruders can and will install software and back doors (often using rootkits). Therefore, closing the security hole that allowed them access may not be enough to close the system's back door.

Rebuilding affected systems from scratch after an intrusion is the best option for recovery. The only way to guarantee that the system is free of Trojans and tampering is to rebuild. Use a reliable backup tape to restore important data once the system has been rebuilt (one created

before the intrusion occurred, not necessarily the backup from the previous night). However, forensics may be necessary to recover the data if it has been deleted and cannot be recovered from a backup. In this case, it's crucial to keep the disc media intact to improve the chances of data recovery. Make sure to fix the security flaw that allowed the intrusion in the first place once the system has been restored to its prior operating state. Applying a patch, changing the vulnerable service's configuration, or providing it with stronger firewall protection are all possible ways to accomplish this.

Review and Improvement

Review should make up the process's last step. The organization can find areas for improvement in its response by conducting an overall assessment of the incident. The following components should be part of the review process:

• Perform a damage assessment. How long were systems unavailable? Could systems have been recovered quicker if better backups or spare hardware was available? Did monitoring systems fail? Was there evidence of the impending failure that was not reviewed in a timely manner?
• For security breaches, was critical data accessed, such as trade secrets or credit card data? If so, does the organization have a legal responsibility to notify the stakeholders? If the attack was not successful, significant work may not be required. Even if the attack was unsuccessful, however, the organization may wish to increase its monitoring, especially if the intruder was aggressive and persistent.

• Determine how the intrusion happened and why it wasn't discovered sooner, ideally before it succeeded. If necessary, search past firewall and IDS logs for any indications of an initial intrusion by the hacker.

• Ensure that the necessary steps are taken to patch the security hole on the affected machine and to locate and similarly protect any other servers that may contain the same hole.

•Examine processes to determine how the security gap might have developed. A security hole can have a variety of causes, such as the failure to recognize and apply a crucial patch, an incorrectly configured service, or lax password security.

• Beyond a simple review of the technical aspects of the attack, the organization should review its performance to identify areas of improvement. For example, how long did it take critical personnel to begin working on the problem? Were they reachable in a timely and simple fashion? Did they encounter any roadblocks while responding?

• If legal action is being considered, make sure that all evidence has been properly gathered, marked, and stored.

Forensics

Identification, extraction, preservation, and reporting of data obtained from a computer system are the focus of the field of computer forensics. There are many applications for forensic analysis, including reconstructing or recording user activity on a specific system and gathering proof of a computer break-in. In addition, forensics can be used to restore deleted or corrupted data, as well as copies of deleted data from failed systems. The National Institute of Standards and Technology defines a process for performing "digital forensics" in Special Publication 800-86 as follows:

• *Collection* - Identifying, labeling, recording, and acquiring data from sources while following procedures to preserve the integrity of the data.

• *Examination* – Forensically processing collected data, identifying relevant data, and extracting it while maintaining data integrity. Working from a copy rather than the original is the norm in this situation.

• *Analysis* - Utilizing techniques and methods that have been approved by the law to analyse the examination results in order to extract data that responds to the inquiries that served as the basis for data collection and examination.

• *Reporting* - Reporting the findings of the analysis may include outlining the steps taken, elaborating on the tools and methods chosen, identifying additional steps that must be taken, and making suggestions for the forensic process's improvement.

Legal Requirements

To be admissible in criminal proceedings, forensic evidence must meet a number of legal requirements. It's crucial to comprehend these prerequisites before getting into the specifics of computer forensics. In essence, forensic evidence must meet the same standards for gathering evidence as other types of evidence. According to these standards, all collected data must be accurate and undamaged. Additionally, the evidence must be taken directly from the crime scene. The analysis must also be carried out without changing the data. An examiner should be diligent in his or her procedures and documentation even in situations where the ultimate use of the evidence is unknown or even if there is a very slim chance that the case will ever go to court. If the case actually goes to court, improper evidence handling practices cannot be corrected.

The requirement that the evidence be presented unedited applies to every stage of the evidence's lifecycle, including collection, examination, storage, and eventual presentation in a court of law. You must always be able to account for the whereabouts and ownership of evidence once it has been taken into custody. The chain of custody refers to the record of who has custody of the evidence. When you give a testimony about the reliability of the evidence, you must be able to provide a verified, unbroken chain of custody. When not being analyzed, evidence should be physically secured in a safe or evidence locker to preserve its integrity. In addition, a thorough log of each person who accesses the evidence, the reason for the access, and the timestamps of when it was taken out of storage and put back should be kept.

Evidence Acquisition

Perhaps the most delicate and important step in the entire process is gathering evidence. Potential evidence might be misplaced, overlooked, or ruled inadmissible by the courts if handled incorrectly. Data from computer forensics can be categorized as either host-based or network-based. Network-based data is obtained from communications that network-based systems like firewalls or IDS, for example, have recorded. Some IDS products come with the ability to automatically record network traffic for later playback. This function may be helpful in tracing the sequence of events leading up to a computer break-in. Firewall logs on a network can also reveal information and evidence about network activity. The evidence uncovered on a particular system is referred to as host-based data, and depending on the subject under investigation, it may include a wide range of different things.

An examiner must take control of the area around the target computers before touching them and record the surroundings. Make a note of the location of crucial components, such as portable storage units, power adapters, and various wiring (so you can easily disassemble it and move it to another location, if necessary), and if the display is still functional, make a note of its contents.

Unquestionably, taking pictures is a quick and efficient way to record the scene. The harder it is to refute the veracity and accuracy of the evidence, the more thorough the documentation is. Grab anything and everything that might contain evidence, including laptops, storage devices, CDs, and DVDs, when gathering evidence from a crime scene. Each item that is removed from the scene should be marked with a seal and labelled with the time and date it was removed as well as the precise location it was found.

If the computer has not yet been turned off, the examiner must make a crucial decision regarding whether to leave it running or unplug it. Make sure the machine stays off until the necessary images are created if it has already been turned off. The boot process of an operating system causes numerous changes to the drive media, including updates to file access times and

changes to swap space and temporary files. Evidence must be presented without tampering. The most appropriate strategy depends on the specific circumstances, though both have advantages. In most cases, cutting the power and freezing the system is the safest course of action, so it should never be viewed as a mistake.

The examiner cannot be charged with contaminating the system contents because they turned the machine off. Additionally, once the system is frozen, the examiner has more time to come up with a plan without worrying that additional system damage might happen. But occasionally, management may have refused to allow the machine to be taken offline, leaving only the evidence stored in memory. The server may perform tasks that are too crucial to the operation of the company for it to be offline for even a brief period. The examiner may be able to monitor the intrusion and gather more evidence if the machine is allowed to continue operating. An examiner ought to be adaptable and ready for either situation.

Creating a Forensic Backup

A forensic backup has a different objective than a standard system recovery backup. A routine backup is intended to restore the system to a working state as quickly as possible and targets intact files. The contents of the entire drive—including the empty or "unused" space—are an exact duplicate in a forensic backup, also known as a system image or bit-stream backup. The bit-stream technique records all previously created partitions, whether or not they are in use, including unallocated space (drive space that has not yet been partitioned). As a result, all data written to disc that is not part of the file system or file slack will also be collected.

In this manner, deleted files and data fragments that might have found their way onto one of these locations can be recovered when looking at the forensic image (the original is rarely examined directly). In reality, hard drives are made up of numerous nested data structures. A partition will be the largest structure on the drive. A hard drive may have one or more partitions, and the operating system may refer to each one separately. Partitions are frequently used to keep different operating systems on the same drive apart or to improve the utilization of a single, very large drive.

The partition table is a specific region of the disc where information about the available partitions is kept. A file system can be installed on the partition after it has been created. The operating system makes use of the file system to store and access files in a straightforward and orderly manner. The file system must be divided into units of equal size in order for it to operate. These components are referred to as blocks on a Unix system and clusters on a Windows system. These units, which can range in size from 4 bytes to several hundred bytes depending on the size of the file system, are the smallest chunks in which a file or piece of data can be stored. Slack refers to the unoccupied space left when a file doesn't fill the entire

cluster. As a result, there are 64 bytes of file slack when a 64-byte file is stored in a 128-byte cluster.

A forensic investigator is interested in file slack because of what it might contain. There might be traces of the larger file in the file slack if a smaller file overwrites a larger file. Furthermore, a knowledgeable user may purposefully conceal data in file slack to avoid detection. When a file is copied to another drive or backed up in a non-forensic way, file slack is not also transferred with it. There are numerous ways to create bit-stream backups. One drive to another can be copied using specialized hardware designed for disc duplication. You must boot the system into a different operating system and mount the disc as read-only if dedicated hardware is not available. Even though there are numerous software tools available to create a useful forensic image of a system, you might need to show the courts that the backup is actually identical and the software you used is trustworthy. Make sure to capture the entire drive when creating an image with software, not just the file system in the primary partition.

It is best practice to calculate the hash value of the untouched original media in order to support an examiner's assertion that the image is an exact replica of the original drive. The contents of the drive are subjected to a cryptographic algorithm, which yields a hash value. The two most popular hash algorithms at the moment are MD5 and SHA1. It is a good idea to generate hashes using two different algorithms so that, in the event that a vulnerability or attack is found in one hash, making it unreliable, the other hash can still be used to verify the authenticity of data. To make sure the hash values match, compute a hash value for the newly created image in addition to hashing the original media. If not, the image is not a perfect replica of the original, and a new image needs to be made. Examiners frequently use an image of the image rather than working directly with the original backup. In this manner, the original image can be securely locked up, and in the event that a mistake is made or the evidence is tainted, a new, unaltered copy is still available.

Working with a Live System

Working with a live system has the purpose of capturing items that won't make it through the power-off procedure. These can include things like the contents of physical memory and swap files, active connections, and currently running processes. Additionally, writing files to the local file system has the potential to obliterate evidence. Be ready to attach a local storage device that can record the output or write output to remote systems over a network.

Capturing System Contents

Computer memory and a portion of the hard drive both contain highly volatile data. When working with a live system, your first actions should be to gather data starting with the most volatile. These are the main things that need to be recorded:

• *System memory and CPU activity* - One of the most erratic and challenging things to accurately measure is CPU activity. Thankfully, CPU activity is not very helpful to forensic investigators and is not really worth the effort. On a Unix system, the contents of the /dev/mem and /dev/kmem files can be dumped to another system in order to record the contents of system memory.

• *Running processes* - The examiner can better comprehend what was happening on the system at the time by recording the active system processes. Both the Windows Task Manager and the Unix command ps allow you to record processes.

• *Network Connections* - Understanding what systems are currently connected to the network and figuring out whether any unidentified processes are waiting for connections are the two main benefits of documenting network connections. Such listeners are an obvious indication of an intrusion. Use the netstat command to record network connection details on Unix and Windows platforms. Use the arp command to capture the contents of the system's Address Resolution Protocol (ARP) table in addition to using netstat with the -r switch to capture the system routing table.

• *Open files* - Using the lsof command on a Unix system, you can record open files (list of open files). Use the Handle program from www.sysinternals.com for Windows.

Evidence Analysis

You can start your analysis once you have a set of supporting evidence. There are several stages to evidence analysis, and evidence can be found in various places. The most obvious location for evidence to be found on the file system is in a file. However, if the examiner is recording instances of computer systems being used without authorization, it may be necessary to piece together evidence from temporary and swap files, identify recently used files and pertinent e-mails, reconstruct Internet browser caches and cookies, and recover deleted files and pieces of data from local and possibly remote file systems. Examiners for forensics must be adaptable. They come across a wide range of systems and circumstances that put their knowledge and skills to the test.

Examining the File System

A forensic examination searches the entire disc for evidence when looking at a file system for potential evidence. The ever-growing storage capacities of modern discs pose a growing challenge to forensic experts today. Additionally, computers might be linked to a terabyte-capable storage area network (SAN) or even an external storage device. Unfortunately, the most important source of evidence will be files on the file system, so you might need to manually inspect each file and look through every byte for possible signs of tampering. On a

large disc, such a task could keep the examiner busy for months. The majority of files on a system are actually safe and can be deleted right away. To confirm that common files haven't been altered or are actually what the filenames claim they are, both general forensic software and specialized software can be used. The trusted MD5 and SHA1 hash algorithms used to authenticate drive images are the same ones that these programs employ. In order to obtain a cryptographic hash for each file on the trusted system, an examiner can construct a system with the same operating system, patch level, and installed programs as the suspect machine. The cryptographic hashes of the files on the target system can be compared to the hash values of a trusted database once it has been created. Files whose hashes match those of the trusted system have not been altered and can be deleted, while those whose hashes don't match require further investigation. A well-designed database might make it unnecessary to look through more than 50 or 60 percent of the system's files. Examine the remaining files after you've reduced the population of files. The most recently accessed files will likely be of significant interest when attempting to reconstruct and document the activity of the system owner. On the operating system, each file has a timestamp that shows when it was last accessed. Going through each file one by one can take a lot of time given the potential size of the system's file storage. There are numerous tools available to make bulk file and directory content inspection easier. Using a tool that can read and open a variety of file formats is another way to save time. This may save you a lot of time. The examiner may also be interested in a user's past Internet usage as a source of information. To find out which websites a user recently visited, an examiner will want to look through the browser cache, bookmarks or favorites, and cookie files.

Hidden Files

Regardless of Windows and Unix systems, some files, users, or attackers may have hidden files. Therefore, make sure Windows Explorer is configured to display all hidden files in a Windows environment. In Unix, you can list hidden files by using the ls -la command. Take a backup of those files as well once you've located the hidden ones.

Deleted Data

When a user instructs an operating system to delete a file, the data is not actually erased from the disc. The space used by the file is merely marked as available for the operating system in order to conserve precious CPU cycles and disc operations. The data will be overwritten if a later need for the disc space arises, but up until that point, the actual data is left intact on the disc. There are a number of third-party applications made specifically to restore deleted files from Windows systems.

But first, make sure to look through the Recycle Bin to see if there's anything useful there. You might find pieces of the original file in the free space even if the disc space is reused. It is also possible to ascertain what was on the disc prior to the data being overwritten or erased using modern tools and techniques. A faint image of the original file is left behind on a disc, similar to a blackboard that has not been properly cleaned. You must use a file-wiping programme to completely overwrite the disc sector where the file was located in order to securely delete data from a disc. The wiping program overwrites the section of disk many times with binary ones and zeros to destroy all trace elements thoroughly from the drive.

Encryption and Compressed Data

Compression presents a challenge in that any data within a compressed file will be missed by a hard drive keyword search. The examiners cannot decompress and search such files if they are not aware of their existence, even though decompressing the file is probably a simple process. Similar issues arise with encryption, but it's probably not simple to decrypt files. You must decrypt and examine the contents of those files in addition to looking for the encrypted data. You might need to find alternative methods to decrypt the data if the suspect is unavailable or unwilling to grant access to the files. In addition to encryption, forensic investigators might come across password-protected files or need to decrypt operating system login passwords. People typically do not use strong passwords, which is unfortunate for security professionals but fortunate for forensic examiners because it gives the investigator the chance to guess the password and even makes a brute-force attack feasible.

Keyword Searching

Keyword searches on the hard drive are a great way to find evidence since examiners typically have a general idea of the topics that are pertinent to the investigation. A keyword search is a systematic drive-wide bit-level search that looks for matches. String searching can uncover evidence in file slack, regular or incorrectly named files, swap space, and data buried in alternative data streams even though it cannot decipher encrypted text. Finding an exact match and knowing what to search for are the challenges of string searching. Spelling variations may be beneficial when defining search terms. The majority of forensic software has fuzzy logic features that automatically look for words with similar spellings.

Law Enforcement Referrals—Yes or No?

Any entity responding to an information security incident must make a critical choice regarding whether to contact law enforcement. An entity may be forced to contact law enforcement as a result of the advent of reporting requirements in some states that require people with

knowledge of computer crimes to report them to law enforcement officials. However, there are frequently benefits and drawbacks to involving government officials in an incident when such contact is optional.

The advantages of contacting law enforcement authorities include the following:

• It conveys to potential predators a strong message that an organization will report incidents.
• Because some of the cost of the investigation is assumed by the government, there may be financial savings.

• It gives the government access to more potent investigative tools, such as grand juries and search warrants, whereas private parties are only allowed to use civil discovery.

• There is frequently no chance of recovery through civil litigation, so it allows for mandatory restitution for damages under the Mandatory Victims Restitution Act, where victims are entitled to recover the "full amount of each victim's losses".

Of course, involving law enforcement has disadvantages as well:

• By doing this, control over the procedure is given up, which may result in problems with timing, coordination, and interference.

• It increases the risk of internal information being revealed.

• It could result in negative publicity for the information security of your company.

• It might stop business operations.

• It might reveal any wrongdoing that the plaintiff herself may have committed.

• The client releases the attorney-client privilege. Any voluntary choice to involve law enforcement necessitates a cost-benefit evaluation of these and other factors. An organization with its own investigative resources may take into account whether those resources are adequate for the task, whether civil remedies are sufficient for the harm sustained, and whether involving law enforcement will restrict or completely prevent the ability to file a civil lawsuit.

Part V

Physical Security

5.1) Physical Security

The IT world and physical security have historically been completely separate, but as technology continues to replace paper-based and manual processes, physical security is becoming more and more IT-centric. In this section, we'll be learning some best practices and advice on implementing physical security in your organization.

Classification of Assets

In order to create clear controls and procedures that effectively protect physical assets, the process of classifying assets entails identifying those assets and putting a value and criticality on them. These asset categories have inherent and widespread traits that let you determine the minimum levels of protection for each one. Corporate physical assets will typically be categorized into the following groups:

• *Computer equipment* - Servers, network-attached storage (NAS) and storage area networks (SANs), desktops, laptops, tablets, pads, etc.

• *Communications equipment* - Routers, switches, firewalls, modems, private branch exchanges (PBXs), fax machines, etc.

• *Technical equipment* - Power supplies, uninterruptable power supplies (UPSs), power conditioners, air conditioners, etc.

• *Storage media* - Many older systems use storage media devices like CD-ROMs, and Zip drives, so it is still good to be familiar with them. Most systems today use hard drive arrays, solid-state drives or thumb drives, and the various types of memory cards such as Secure Digital (SD), microSD, Compact Flash, and Memory Stick, to name a few.

• *Furniture and fixtures* - Racks, NEMA-rated enclosures, etc.

• *Assets with direct monetary value* - Cash, jewelry, bonds, stocks, credit cards, personal data, cell phones, etc.

Assets should have their value and business criticality evaluated and documented. Your matrix should at the very least include the following criteria for critical assets: depreciation value, initial cost, replacement cost, asset owner, vendor, version, and serial number (if applicable). Normally, business continuity and disaster recovery documentation will contain this information. Asset protection priorities can be effectively assigned using a

"Low/Medium/High," "Not Important/Important/Critical," or a similar, numerically based scoring and weighing system.

Physical Vulnerability Assessment

Similar to its information security counterpart, a physical security vulnerability assessment depends on measurements of exposure to a relevant risk. An asset must already be categorized and have a monetary value to the organization. Once this has been done, a quick walk-through should be done to identify any potential weak points in physical security. Determine the issue, but also consider whether there is a business need that justifies it. It is a liability for that condition to exist and it should be remedied if there is no valid business need for it or if the risk is greater than any potential return. Any assessment of a person's physical vulnerability should cover these four areas: buildings, computing devices and peripherals, documents, and records and equipment. Your situation may vary, depending on various factors.

Computing Devices and Peripherals

Verify that systems and peripherals are locked down and accessible. Systems that are left unattended ought to be shut down or have their screens locked. The following minimum requirements are applicable for servers:

• Put crucial servers in a secure area that requires a card reader to enter. This records every entry into the room and restricts access to those who have permission. It might not always be possible to lock up all of your servers due to physical constraints or operational needs. Environments used for product testing or development could be an example of this. In cases like these, logical system isolation may be sufficient. Keep in mind that if this method is employed, it is essential to maintain mitigating controls at all times, such as data and network segmentation from critical data.

• Verify that a physical lock is present on the case.

• Secure the BIOS using a strong password.

• In the system setup, disable system booting from CD/DVD/USB drives.

• Set up the keyboard and monitor so that nobody but the operator can see them. When entering an administrative password, you don't want anyone to be watching.

• Shut off or remove unused network ports and modems.

• Separately store your tools, preferably locked up.

• Limit who has access to the server room, and keep track of who has it. Put a sign-in sheet inside the door, or use a card reader or biometric entry control to track access electronically.

Documents

As part of your data classification, information owner matrixes, and policies, documents should already be categorized. Inspect the area for Confidential or "Eyes Only" documents, Post-it notes with passwords and login information, documents that weren't collected from print jobs and faxes, and documents that should have been destroyed that are in the trash or recycling bin. Try "shoulder-surfing" for restricted or confidential information while out and about. Generally speaking, people will assume that you don't care what they are reading. This is a risky supposition. Spend some time educating your staff on corporate espionage tactics and making sure they are aware of the repercussions of what might initially seem like a harmless situation.

Records and Equipment

The same amount of thought should be given to the category of records and equipment as to any other important asset. There will always be the file cabinet with paper records, no matter how reliant we become as a society on electronically storing and processing records. Records are anything that is recorded, which distinguishes them from documents. Records include things like employee timesheets, receipts, accounts payable/receivable, and more. Ensure that only those with permission to access the documents can access them and that they are locked away when not in use. Depending on their intended use and location, equipment items like fax machines, printers, modems, copiers, and other equipment each have their own security recommendations.

Choosing Site Location for Security

Cost should not be the primary factor when selecting a site for a data center or office building. Sites with low costs could come with risks that outweigh the cost savings. There is a sizable chance that one of these events could result in significant and expensive damage if the site is in a flood zone, an area susceptible to tornadoes or hurricanes, an earthquake zone, or a high-crime area. You don't want to have to use the backup power generator, security guards, or other compensating elements that come with a well-designed and well-maintained site. If you do, they might be pricey. So, both from a financial and security standpoint, picking a trustworthy and secure site location makes sense.

When selecting a secure site location, there are many security factors to take into account.

• Accessibility

• To the site

• From the site (in the event of evacuation)

• Lighting

• Proximity to other buildings

• Proximity to law enforcement and emergency response

• RF and wireless transmission interception

• Utilities reliability

• For a data center, the loss of power may be overcome through the use of generators, but if the water supply is cut off, the AC units will be unable to cool the servers

• Construction and excavation (past and present)

Let's consider each of these briefly to address applicability to common business environments.

Accessibility

The site's accessibility is typically taken into account first, and for good reason. Usability and commutability are impacted if a site is too far away to be useful. On the other hand, if the website is simple for you to access, it probably is for others as well. On the other hand, you need to think about possible evacuation. Examples of potential evacuation triggers include bomb threats, fires, terrorist attacks, anthrax mailings, and SARS. Lighting A proper lighting evaluation and consideration should be made, especially for organizations that operate continuously. When the lighting is bad, there are more chances for burglaries and threats to employee safety. Create as many physical barriers as you can between your workplace and undesirable individuals and situations right away. Mirrored or highly reflective windows should face north-south rather than east-west to prevent glare from the sun entering busy areas. Lighting should never be placed so that it blinds people who are leaving the building at night.

Proximity to Other Building

A physical security incident is more likely to occur in close proximity to other buildings and businesses. Additionally, keep in mind that any issues with a nearby or connected building could end up affecting you as well.

Proximity to Law Enforcement and Emergency Response

The location's proximity to law enforcement and/or emergency response teams is another factor. Consider the possibility that the incident might not receive a response within a framework that you consider ideal if the area has a history of crime despite the fact that you chose the location. Similarly, consider the implications of any delays and whether they would

be acceptable if an emergency service unit were requested to respond to an incident at this location.

RF and Wireless Transmission Interception

Wireless hacking and hijacking are a growing threat as wireless networking usage increases, particularly in urban areas. In addition to radio frequency devices, cordless phones, cell phones, PIMs, and mobile e-mail devices, other "airborne" protocols should be taken into account. Scanners should be used to test existing protocols, and it is best to steer clear of heavily used frequency ranges. It is essential to encrypt sensitive traffic.

Utilities Reliability

Office buildings offer workspace for workers who must be reliable and productive at their jobs. Network and phone outages as well as power outages can severely hamper productivity. Some of these things can be made up for, but not all of them. For instance, UPS systems and a generator can be used to a certain extent to make up for power outages. UPS batteries have a limited lifespan, and in a serious emergency, generator fuel can be expensive and difficult to obtain. Service issues with the phone, network, and Internet can be more severe. You can frequently—but not always—change to a different provider if they go down. Problems always arise in the "last mile." There isn't much you can do until the wiring is fixed if the connection between your site and your provider has reliability issues because of outdated wiring, subpar fiber, or construction-related incidents like "backhoe failures" (in which a digging machine cuts through the communications cabling in your building). It can be expensive to be idle. Loss of power can have a negative effect on a data center. While UPSs and generators can provide power temporarily, the data center's systems must be constantly cooled to prevent meltdowns. Due to AC failure, numerous organizations have had to replace a lot of expensive equipment.

Construction and Excavation

Your network and communications infrastructure can be completely destroyed by construction and excavation in one swift motion of a backhoe's bucket. Examine previous construction projects that have been completed nearby and any effects they may have had on the neighborhood. You can typically find the information you need about any construction, excavation, or demolition, both recent and historical, in town or city records. Make it a point to inquire about any power or telecom outages with the locals.

Securing Assets: Locks and Entry Controls

The many different factors you should take into account when using physical security devices to protect your assets are covered in this section.

Locks

Locks are no longer only used on doors. You probably found a few unlocked laptops, smartphones, tablets, MP3 players, jewelry, keys, and other miscellaneous items during your physical security vulnerability assessment. Lock up the device or valuable and be sure to emphasize to the asset owner how crucial it is to secure the item.

Doors and File Cabinets

Where applicable, check for locked doors; you'll be surprised by the results. Make sure the door's lock operates properly and can withstand enough pressure. A damaged or dysfunctional lock is only marginally preferable to having none at all. When not in use, file cabinets that contain sensitive information or expensive equipment should be kept locked. Additionally, the keys to these should be kept out of public view.

Laptops

When not being transported, laptops at the office should be physically locked to the desk or in the docking station. Cable locks are a cheap price to pay to protect the laptop (and sensitive data) from falling into the wrong hands. Theft of laptops is at an all-time high; the majority happen right in front of the owner. It should be made clear to all staff to exercise extra caution when travelling with laptops. Software and operating system safeguards are only as effective as the physical security limiting access to the device. Half the battle is won if someone has unrestricted physical access to a system. After that, it will only be a matter of time before these protections are defeated.

Data Centers, Wiring Closets, Network Rooms

Because they all serve a similar purpose, all of these spaces should have a single set of access controls. Make sure to keep these spaces locked. Make sure an access log is kept if automatic entry-tracking mechanisms are not in use.

Entry Controls

Entry controls have unique security requirements that undoubtedly change depending on your security plan and business requirements. You must first take into account the location where the entry controls will be installed when evaluating the various options. The most typical deployment scenarios involve a high-rise building, a campus group of buildings with distinct public entrances, a suite in a multitenant building, and an existing structure with a single tenant.

Building Access Control Systems

There may be equipment in place for existing structures that can be recycled. Access control systems are frequently used in multi-tenant buildings to regulate entry into the structure or access to a designated parking area that is shared by the entire building. Multiple access cards might be required if you intend to implement an access control system that is incompatible with an existing system. Numerous card technologies are supported by many access control systems, and some cards can even support multiple technologies and operate on numerous incompatible systems.

The most crucial thing to remember when managing a multi-tenant building is to make sure that nobody from the unsecure side of the suite can enter the secured side unless they have permission to. In multi-tenant buildings without a "Z corridor," which connects two stairwells to the lift lobby, this can be challenging. This public area should also be the goods lift's exit. By doing this, you can prevent the general public and other tenants from having to enter your suite in order to access another area of the building. In most cities, high-rise buildings are required to have a Z corridor on every floor; however, in a building without this public corridor, there may be circumstances where you must allow people to enter your suite without restriction.

Mantraps

A mantrap is a space created to only allow one authorized person entry at a time. These are most frequently used in high-security areas, cash handling areas, and data centers as an anti-tailgating mechanism—to stop an unauthorized person from closely following an authorized person through an open door.

Building and Employee IDs

Giving new hires ID badges is typically one of the first things any organization does after making the hiring decision. Identification for the building and/or employees should always be visible, and anyone without one should be questioned.

Biometrics

In the past few years, biometric devices have advanced significantly and have gained popularity in both the entry control and network authentication markets. Any device that uses distinctive personally identifiable characteristics or distinctive physical traits to reliably identify a person is categorized as a biometric device. The use of any given biometric device will depend on the circumstances. The following traits or characteristics are used by some of the more popular devices to verify identification: fingerprint, voice, face, retina, iris, handwriting, hand geometry, and keystroke dynamics. Currently, fingerprint and hand geometry devices are the most widely used biometric technologies for entry control. The most recent fingerprint readers can now

read the corpuscles beneath the skin, making them nearly universally applicable, even to people with weak fingerprint ridges. This technology has become more affordable as a result of the recent trend of including fingerprint readers in commercial devices like laptops and time and attendance systems.

Security Guards

Security guards appear to be the most effective deterrent. However, security guards serve more than just a deterrent. An organization, business, or agency will hire a security guard to patrol, guard, monitor, preserve, protect, support, and maintain the safety and security of both people and property. Infractions of organizational rules, policies, and procedures are prevented, discovered, and reported by security guards. Security guards help limit or prevent unauthorized activities, including but not limited to trespass, forcible entry or intrusion, vandalism, pilferage, theft, arson, abuse, and/or assault. A security guard is a resource as well as a person. As a result, business needs and requirements will determine the use, number, and placement of guards. All security guards should undergo background checks, and wherever necessary, the necessary licences and clearances should be obtained.

Physical Intrusion Detection

Similar to its informational counterpart, physical intrusion detection needs advance thought, planning, and fine-tuning to function at its best. The following sections go over a few security factors for physical intrusion detection.

Closed-Circuit Television

The positioning of CCTV equipment should take operational and financial constraints into consideration. High-traffic areas, critical function areas (like parking structures, loading docks, and research areas), cash handling areas, and transition zones are a few examples of potential first locations for device placement (such as the hallway leading from a conference room to a sensitive location). Make sure the CCTV equipment's cabling is out of the way so that transmissions cannot be easily intercepted. The effectiveness of the camera will also be greatly influenced by lighting. If you're thinking about using a wireless CCTV setup, remember that anything sent over the airwaves was intended to be received as well and can therefore be intercepted.

Alarms

A test log should be kept, and alarms should be tested at least once per month. Alarms for intrusions should be installed at all points of entry and exit. Everyone who will respond to an incident needs to be aware of their roles and responsibilities, and there should be a response

plan in place. For areas that might need them, duress alarms should also be taken into consideration.

Compliance with Standards

Let's take a look at the ISO 27002 and COBIT guidelines on implementing physical security.

ISO 27002

ISO 27002 contains the following provisions, to which this chapter's contents are relevant:

• 9.1.1 - Physical security perimeter: Security perimeters (barriers such as walls, card controlled entry gates, or manned reception desks) shall be used to protect areas that contain information and information processing facilities. (Comparable to COBIT DS12.1 and DS12.2.)

• 9.1.2 - Physical entry controls: Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. (Comparable to COBIT DS12.2 and DS12.3.)

• 9.1.3 - Securing offices, rooms, and facilities: Physical security for offices, rooms, and facilities shall be designed and applied. (Comparable to COBIT DS12.1 and DS12.2.)

• 9.1.4 - Protecting against external and environmental threats: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. (Comparable to COBIT DS12.4.)

• 9.1.5 - Working in secure areas: Physical protection and guidelines for working in secure areas shall be designed and applied. (Comparable to COBIT DS12.3, PO4.14, PO6.2, and AI3.3.)

• 9.1.6 - Public access, delivery, and loading areas: Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. (Comparable to COBIT DS12.1, DS12.3, and DS5.7.)

• 9.2.1 - Equipment siting and protection: Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. (Comparable to COBIT DS12.4 and DS5.7.)

• 9.2.2 - Supporting utilities: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. (Comparable to COBIT DS12.4 and DS12.5.) 9.2.3 Cabling security: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. (Comparable to COBIT DS12.4 and DS5.7.)

• 9.2.4 - Equipment maintenance: Equipment shall be correctly maintained to ensure its continued availability and integrity. (Comparable to COBIT DS12.5, DS13.5, and AI3.3.)

• 9.2.5 - Security of equipment off-premises: Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises. (Comparable to COBIT DS12.2, DS12.3, and PO4.9.)

• 9.2.6 - Secure disposal or reuse of equipment: All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. (Comparable to COBIT DS11.4.)

• 9.2.7 - Removal of property: Equipment, information, or software shall not be taken off-site without prior authorization. (Comparable to COBIT DS12.2 and PO6.2.)

COBIT

COBIT contains the following provisions, related to physical security implementation,

• PO4.9 - Create and maintain an inventory of information assets (systems and data) that includes a listing of owners, custodians, and asset classifications. Include assets that are outsourced and those for which ownership should stay within the organization.

• PO4.14 - Require contractors to comply with the organization's policies and procedures, for example: requirements for security clearance, physical and logical access control requirements, and requirements for client and personnel equipment.

• DS5.7 - Ensure that all hardware, software, and facilities related to the security function and controls are tamper-proof.

• DS11.4 - Sanitize equipment and media containing sensitive information prior to reuse or disposal. Such processes should ensure that data marked as 'deleted' or 'to be disposed' cannot be retrieved (e.g., media containing highly sensitive data should be physically destroyed). To maintain an audit trail, log the disposal of equipment or media containing sensitive information. Define a procedure to remove active media from the media inventory list upon disposal. Transport unsensitized equipment and media in a secure way throughout the disposal process. Require disposal contractors to have the necessary physical security and procedures to store and handle the equipment and media before and during disposal.

• DS12.1 - Select a site for IT equipment that meets business requirements and the security policy. Take into account special considerations such as geographic position, neighbors, and infrastructure. Other risks that need consideration include, but are not limited to, theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, or explosives. Ensure that the selection

and design of the site take into account relevant laws and regulations, such as building codes and environmental, fire, electrical engineering, and occupational health and safety regulations.

DS12.2 - Define and implement a policy for the physical security and access control measures to be followed for IT sites. Regularly review the policy to ensure that it remains relevant and up to date. Limit the access to information about sensitive IT sites and the design plans. Ensure that external signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside. Confirm that organizational directories/site maps do not identify the location of the IT site. Design physical security measures to take into account the risk associated with the business and operation. Physical security measures include alarm systems, building hardening, armored cabling protection, and secure partitioning. Periodically test and document the preventive, detective, and corrective physical security measures to verify design, implementation, and effectiveness. Ensure that the site design takes into account the physical cabling of telecommunication and the piping of water, power, and sewer. The installation must be concealed, so it is not directly visible. The piping of water and sewer must also be redirected away from the server rooms. Define a process for the secure removal of IT equipment, supported by the appropriate authorization. Safeguard receiving and shipping areas of IT equipment in the same manner and scope as normal IT sites and IT operations. Define and implement a policy and process to transport and store equipment securely. Define a process to ensure that storage devices containing sensitive information are physically destroyed or sanitized. Define a process for recording, monitoring, managing, reporting, and resolving physical security incidents, in line with the overall IT incident management process. Ensure that particularly sensitive sites are checked frequently (including weekends and holidays).

• DS12.3 - Define and implement a process that governs the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorized by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access. Define and implement procedures to ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas, or zones) on job function and responsibilities. Define a process to log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site. Define and implement a policy instructing all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorization. Define and implement a policy requiring visitors to be escorted at all times while onsite by a member of the IT operations group. If a member of the group identifies an unaccompanied, unfamiliar individual who is not wearing staff identification, security personnel should be alerted. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. The devices record entry and sound an alarm in the event of unauthorized access. Examples of such devices include badges or key cards,

keypads, closed-circuit television, and biometric scanners. Define a process to conduct regular physical security awareness training.

• DS12.4 - Establish and maintain a process to identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities. Define and implement a policy that identifies how IT equipment, including mobile and offsite equipment, is protected against environmental threats.

. • DS12.5 - Define and implement a process to examine the IT facilities' requirement for protection against environmental conditions, power fluctuations, and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning. Regularly test the uninterruptible power supply's mechanisms and ensure that power can be switched to the supply without any significant effect on business operations. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorized personnel. Properly protect cabling against damage caused by fire, smoke, water, interception, and interference. Ensure that cabling and physical patching (data and phone) are structured and organized. Cabling and conduit structures should be documented, e.g., blueprint building plan and wiring diagrams. Analyze the facilities housing high-availability systems for redundancy and fail-over cabling requirements (external and internal). Define and implement a process that ensures that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents. Define and implement a process to record, monitor, manage, and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations. Define a process to ensure that IT sites and equipment are maintained as per the supplier's recommended service intervals and specifications. The maintenance must be carried out only by authorized personnel. Analyze physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.

• DS13.5 - Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel, and other relevant factors. Review all activity logs on a regular basis to identify critical hardware components that

require preventive maintenance, and update the maintenance plan accordingly. Establish maintenance agreements involving thirdparty access to organizational IT facilities for onsite and offsite activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorization procedures, to ensure compliance with the organizational security policies and standards.