2722-1666807763397-Unit 05 - Providing a Suitable Security Solution for Metropolis Capital BANK

Web Development (ESOFT Metro Campus)

Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS			
Programme title	BTEC Higher National Diploma in Computing		
Assessor	Miss. Iresha Jayarathne	**Internal Verifier**	
Unit(s)	**Unit 05: Security**		
Assignment title	Providing a suitable security solution for METROPOLIS CAPITAL Bank		
Student's name	G.D.N. Abeywickrama		
List which assessment criteria the Assessor has awarded.	**Pass**	**Merit**	**Distinction**

INTERNAL VERIFIER CHECKLIST		
Do the assessment criteria awarded match those shown in the assignment brief?	Y/N	
Is the Pass/Merit/Distinction grade awarded justified by the assessor's comments on the student work?	Y/N	
Has the work been assessed accurately?	Y/N	
Is the feedback to the student: Give details: • Constructive? • Linked to relevant assessment criteria? • Identifying opportunities for improved performance? • Agreeing actions?	Y/N Y/N Y/N Y/N	
Does the assessment decision need amending?	Y/N	

Assessor signature		**Date**	
Internal Verifier signature		**Date**	

Programme Leader signature (if required)		**Date**	

Confirm action completed			
Remedial action taken Give details:			
Assessor signature		**Date**	
Internal Verifier signature		**Date**	
Programme Leader signature (if required)		**Date**	

Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	G.D.N. Abeywickrama (E172195)		
Unit Title	**Unit 05: Security**		
Assignment Number	1	**Assessor**	
Submission Date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	

Assessor Feedback:		
Grade:	**Assessor Signature:**	**Date:**
Resubmission Feedback:		
Grade:	**Assessor Signature:**	**Date:**
Internal Verifier's Comments:		
Signature & Date:		

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Pearson

Higher Nationals in

Computing

Unit 5 : Security

General Guidelines

1. A Cover page or title page – You should always attach a title page to your assignment. Use previous page as your cover sheet and make sure all the details are accurately filled.
2. Attach this brief as the first section of your assignment.
3. All the assignments should be prepared using a word processing software.
4. All the assignments should be printed on A4 sized papers. Use single side printing.
5. Allow 1" for top, bottom , right margins and 1.25" for the left margin of each page.

Word Processing Rules

1. The font size should be **12** point, and should be in the style of **Time New Roman**.
2. **Use 1.5 line spacing**. Left justify all paragraphs.
3. Ensure that all the headings are consistent in terms of the font size and font style.
4. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each pag**e. This is useful if individual sheets become detached for any reason.
5. Use word processing application spell check and grammar check function to help editing your assignment.

Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for the compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Avoid using page borders in your assignment body.
3. Carefully check the hand in date and the instructions given in the assignment. Late submissions will not be accepted.
4. Ensure that you give yourself enough time to complete the assignment by the due date.
5. Excuses of any nature will not be accepted for failure to hand in the work on time.
6. You must take responsibility for managing your own time effectively.
7. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.

8. Failure to achieve at least PASS criteria will result in a REFERRAL grade .

9. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.

10. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You have to provide both in-text citation and a reference list.

11. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course

Student Declaration

I hereby, declare that I know what plagiarism entails, namely to use another's work and to present it as my own without attributing the sources in the correct way. I further understand what it means to copy another's work.

1. I know that plagiarism is a punishable offence because it constitutes theft.
2. I understand the plagiarism and copying policy of the Edexcel UK.
3. I know what the consequences will be if I plagiaries or copy another's work in any of the assignments for this program.
4. I declare therefore that all work presented by me for every aspects of my program, will be my own, and where I have made use of another's work, I will attribute the source in the correct way.
5. I acknowledge that the attachment of this document signed or not, constitutes a binding agreement between myself and Edexcel UK.
6. I understand that my assignment will not be considered as submitted if this document is not attached to the attached.

www.nadishaabeywickramaslac@gmail.com

Student's Signature: **Date:**

(*Provide E-mail ID*) **(*Provide Submission Date*)**

Assignment Brief

Student Name /ID Number	G.D.N. Abeywickrama (E172195)
Unit Number and Title	Unit 5- Security
Academic Year	2022/23
Unit Tutor	
Assignment Title	METROPOLIS CAPITAL Bank
Issue Date	
Submission Date	
IV Name & Date	

Submission Format:

The submission is in the form of an individual written report. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide an end list of references using the Harvard referencing system.

Unit Learning Outcomes:

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organizational IT security.

LO4 Manage organizational security.

Assignment Brief and Guidance:

METROPOLIS CAPITAL Bank is one of the leading private banking service providers in Sri Lanka. It operates over 100 branches and 500 ATM machines across the island as well as 8 Branches overseas. In order to provide their services, METROPOLIS CAPITAL Bank has a primary datacenter located in Colombo and a Secondary datacenter located in Galle. Each branch and ATM must have connectivity to the core banking system to be able to operate normally. In order to establish the connectivity between datacenters, branches and ATM machines, each location has a single ISP link. This link provides VPN services between branches, ATMs and datacenters as well as MPLS services for the bank and it establishes connectivity between datacenters, ATMs, and branches.

METROPOLIS CAPITAL Banks Head Office is a 5 Story Building in Kollupitiya with the Ground Floor allocated for Customer Services, the First Floor allocated for HR, the Second Floor allocated for Meeting Rooms and Senior Executive Staff, the Third Floor is allocated for the Technical Support Team and the Fourth Floor hosts High Performance Servers running core banking systems. Fifth Floor is for some other outside companies that are not related with the METROPOLIS CAPITAL Bank. Other than this, METROPOLIS CAPITAL bank provides a lot of services to customers including online and mobile banking facilities. Therefore, their core banking system must communicate with several outside systems and all communication between outside systems, Data centers and the Head Office is protected by a single firewall. In Addition, METROPOLIS CAPITAL Bank has recently implemented a bring your own device (BYOD) concept for Senior Executive Staff and HR Departments and to facilitate this, they are providing employee WiFi as well as a guest WiFi Hotspot.

The bank has signed agreements, AMCs, contracts and NDAs with several Local and foreign IT service vendors. Some local vendors provide services and supports to foreign companies. METROPOLIS CAPITAL Banks Technical Support Team is a local third-party vendor, contracted by METROPOLIS CAPITAL Bank and managed by their Supply chain management officer. The Technical Support Team provides onsite and remote support for their customers.

METROPOLIS CAPITAL bank strictly follows the rules and regulations enforced by the government and the Central Bank. Therefore, they have obtained the ISO 31000:2009 certification. In addition to this, the areas of datacenters, branches, ATM and HQ is covered by CCTV and 24x7 monitoring is happening. Other security functions like VA scanning, internal auditing, and security operation done by

the bank employees. They have purchased a VA scanning tool, Privilege access management (PAM) system, Endpoint detection and respond (EDR) system, Data loss prevention (DLP) tool, Web application firewall (WAF) and Secure mail gateway which are managed by the Technical Support Team.

It has been reported that an emergency is likely to occur where a work from home situation may be initiated. Therefore, you have been employed by METROPOLIS CAPITAL Bank as a Network Security Analyst to recommend and implement a suitable Security solution to facilitate this situation.

Activity 01

Discuss and assess the security procedures and types of security risks METROPOLIS CAPITAL Bank may face under its current status and evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organizational IT security. You also need to analyze the benefits of implementing network monitoring systems for METROPOLIS CAPITAL Bank with valid reasons in order to minimize security risks identified and enhance the organizational security.

Activity 02

2.1 Discuss how an incorrect/improper configuration for network infrastructure such as firewall and VPN could impact METROPOLIS CAPITAL Bank. Assess IT security risks that may face by the employees of METROPOLIS CAPITAL Bank and propose how the organization can facilitate their employees with a "**Secure remote working environment**".

2.2. Discuss how following technologies would benefit METROPOLIS CAPITAL Bank and its Clients to increase network performance. (Support your answer with suitable illustrations).

i) Static IP,

ii) NAT

iii)DMZ

Activity 03

Review risk assessment procedures for METROPOLIS CAPITAL Bank to protect itself and its clients. Explain the mandatory data protection laws and procedures which will be applied to data storage solutions provided by METROPOLIS CAPITAL Bank. Explain the topic "ISO 31000 risk management methodology" and summarize the ISO 31000 risk management methodology and its application in IT security. Analyze possible impacts to organizational security resulting from an IT security audit. Recommend how IT security can be aligned with organizational Policy, detailing the security impact of any misalignment.

Activity 04

4.1 Design and Implement suitable security policy to prevent misuse and exploitations in line with METROPOLIS CAPITAL Bank using the Organizational policy tools for the given scenario,

While evaluating and justifying the suitability of the tools used in an organizational policy to meet business needs. Identify the stakeholders who are subject to the METROPOLIS CAPITAL Bank and describe the role of these stakeholders to build security audit recommendations for the organization.

4.2 Discuss and present a disaster recovery plan for METROPOLIS CAPITAL Bank for all their sites to guarantee maximum reliability to their clients. (Student must develop a PowerPoint-based presentation which illustrates the recovery plan within 15 minutes of time including justifications and reasons for decisions and options used).

Grading Rubric

Grading Criteria	Achieved	Feedback
LO1 Assess risks to IT security		
P1 Discuss types of security risks to organizations.		
P2 Assess organizational security procedures.		
M1 Analyze the benefits of implementing network monitoring systems with supporting reasons.		
D1 Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organizational IT security.		
LO2 Describe IT security solutions		
P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs.		
P4 Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.		
M2 Propose a method to assess and treat IT security risks.		
LO3 Review mechanisms to control organizational IT Security		

P5 Review risk assessment procedures in an organization.		
P6 Explain data protection processes and regulations as applicable to an organization.		
M3 Summarize the ISO 31000 risk management methodology and its application in IT security.		
M4 Analyze possible impacts to organizational security resulting from an IT security audit.		
D2 Recommend how IT security can be aligned with organizational Policy, detailing the security impact of any misalignment.		
LO4 Manage organizational security		
P7 Design a suitable security policy for an organization, including the main components of an organizational disaster recovery plan.		
P8 Discuss the roles of stakeholders in the organization in implementing security audits.		
M5 Justify the security plan developed giving reasons for the elements selected**.**		
D3 Evaluate the suitability of the tools used in an organizational policy to meet business needs		

Activity 01

Security risk

What is the meaning of security risk?

- The possibility or likelihood of an event or incident that could have a detrimental effect on the security of a system, organization, or person is referred to as a "security risk." It involves the potential for a vulnerability to be exploited, resulting in unauthorized access, sensitive data loss or theft, service interruption, infrastructure damage, or any other negative effects.

  Organizations can prevent potential security breaches and events by identifying security risks and taking preventative action to safeguard their assets, maintain the confidentiality, integrity, and availability of their systems and data. To effectively manage and mitigate security risks, this entails putting security controls in place, performing risk assessments, teaching staff on security best practices, keeping an eye out for suspicious activity on systems, and staying up to date on new threats and vulnerabilities.

Types of security risks to organizations

Careless employees of an organization

Because they are most knowledgeable with how a business operates, including where sensitive data is kept and how to access it, employees provide the greatest security risk to any company. Organizations must contend with a variety of cyber security issues in addition to hostile attacks by careless employees.

They use fairly simple passwords so they can remember them in addition to sharing passwords. Another problem that regularly occurs is when staff members open suspicious email attachments, click suspicious links, or visit risky websites that could allow malware to enter the system.

Password Theft

Companies that conduct a lot of their business online face a serious threat from password theft. Websites have complete knowledge about businesses, including the location of data storage, making them the greatest security risk to an enterprise.

This implies that a hacker can steal your password and then use it to profit the company from which he also stole it. When password theft spreads from one company computer to another, it can undoubtedly damage the organization's ability to do business as usual.

Password theft can occur in any business, even one that takes security safeguards, making untrained organizations particularly vulnerable to it. Passwords should be regularly changed to increase security.

If you don't change your passwords periodically, you put your firm at risk of occurrences that could disrupt its ability to conduct business.

Phishing Attacks

The purpose of a phishing attack is to trick employees into believing an email is from a trustworthy, trusted source. When users click a link in an email or open an attachment after that, their computer becomes infected. The phisher may be someone pretending to be the employee's employer or to be a company with which the employee does business. For instance, a communication from the employee's bank can refer to a request as something they want, need, or think they are going to need. A clever phishing attempt, regardless of the disguise, appears to be a real communication but actually includes serious harm.

When a hacker has access to your credit card information, password, or other personal online information, phishing assaults take place. An impact from a phishing attack can be felt at the highest levels of an organization.

- **How to prevent phishing?**

Training and awareness campaigns are among the most successful preventive interventions. Employees should receive training and education about various security dangers in general as well as specific phishing tactics.

Data breach

A data breach is a security issue that exposes private or protected information when data is accessed from a system without the owner's permission.

Customer information, trade secrets, credit card details, and other delicate, private, or proprietary information could be included.

-

Computer virus

A piece of software known as a virus spreads across computers or across networks without the user's awareness and conducts hostile attacks. It is capable of erasing files, formatting hard drives, and destroying or ruining a company's sensitive data.

- **How to prevent computer virus?**

We can use the advanced virus guard for pc.

Ransomware

Cybersecurity Ventures estimates that by 2031, the damage caused by ransomware would have cost $265 billion. According to their analysis, as ransomware offenders improve their malware payloads and related extortion schemes, there will be a new attack every two seconds.

In this kind of assault, the victim's computer is usually encrypted and locked, preventing them from accessing it or anything stored on it. The victim is required to pay ransom, frequently in the form of virtual money, in order to regain access to the gadget. There are various forms that spread these hazards. However, malicious email attachments, infected software programs, compromised websites, and infected external storage are how ransomware is typically propagated.

Until a ransom is paid, malicious software known as ransomware prevents users from using their computers and may also threaten to steal or leak victims' data. Ransomware has emerged as one of the biggest concerns in network security due to its capacity to take down huge enterprises and even whole cities, including Baltimore and Atlanta in recent years. Often, the infection starts when someone clicks on what seems to be an innocuous link or attachment, but it swiftly worsens

into a calamity for businesses of all sizes when important documents and data are suddenly unavailable and held for ransom. But sometimes, paying the ransom won't make things better. Sometimes hackers will demand a ransom even after the data they stole has been destroyed.

- **How to prevent Ransomware?**

- Back up computing devices and update software
- Avoid links in emails from unknown sources
- Avoid opening email attachments
- Do everything possible to avoid paying ransom
- Couple a traditional firewall that blocks unauthorized access to computers or networks
- Limit the data a cybercriminal can access

Computer worm

A computer worm is a type of malicious software or a program that spreads over the network it is attached to by duplicating itself from one computer in an organization to another computer in the same organization.

It has the capacity to propagate automatically, exploit software security holes, and try to get access in order to steal sensitive information, corrupt files, and install a back door giving remote access to the system.

DDoS (Distributed Denial of Service) Attack

An attempt to prevent users from accessing a computer or network resource entails temporarily or permanently halting the services of a host that is connected to the internet. DDoS frequently involves saturating the targeted computer with pointless requests from various sources in attempt to overwhelm systems and prevent some or all legitimate requests from being performed.

Spyware

Spyware is a security problem that is unwanted to businesses since it is installed on users' computers and discreetly collects sensitive data including credit card numbers, login credentials, and personal or corporate data.

These risks monitor online activity while monitoring login information and listening in on sensitive information. It might be a secret component of software packages, a computerized installation, or it could be installed using more typical malware tricks like misleading you with ads, emails, and instant messages.

Therefore, any company or person should take the necessary precautions to safeguard themselves from spyware, including using antivirus software, a firewall, and only downloading software from reliable websites.

Botnet

A botnet is a combination of the words "robot" and "network" and refers to a group of infected personal computers that are managed collectively without the users' awareness. They are routinely used to launch DDoS attacks, disseminate massive amounts of spam, and steal passwords. Botnets can act as a force multiplier for parties attempting to interfere with or hack targets' systems due to their combined computing power.

Trojan Horse

Trojan horses are malicious programs or codes developed by hackers to pass as reliable software and access a company's systems. The network or data may be damaged, blocked, erased, altered, or undergo other detrimental activities. Any malicious code contained therein may begin to run as soon as the user clicks on the attached file. In that case, neither the victim nor anybody else involved suspects or knows that the attachment is actually a Trojan horse.

Most Common Types of Trojan Horse

The following are examples of the most typical sorts of Trojan horses:

- **Backdoor trojan:** A backdoor trojan can give an attacker remote access and control of a device. This enables the hacker to access your systems and perform any actions they desire, including deleting files, restarting computers,

stealing data, and downloading viruses. Using a backdoor malware, a network of zombie computers is frequently used to create a botnet.

- **Banker Trojan:** A Trojan banker is designed to target users' bank accounts and financial information. It aims to steal information on credit and debit cards, e-payments, and online banking.
- **Distributed Denial of service (DDoS) Trojan:** Attacks carried out by this Trojan software involve overburdening a traffic network. It will bombard a target web site with multiple requests from a system or collection of machines, resulting in a service denial.
- **Trojan-Downloader:** An compromised PC is the target of a Trojan downloader, which downloads and installs additional malware. This also contains further trojans or other sorts of malware, such adware..
- **Exploit Trojan:** A computer program called a "exploit trojan" contains code or data that takes advantage of weaknesses in other programs or applications. By deploying a phishing attack to target specific people, the cybercriminal takes use of a known vulnerability in the software.
- **Remote Access Trojan:** Similar to a backdoor Trojan, this kind of malware gives an attacker total control over a user's machine. Through a remote network, the cybercriminal keeps control of the device, which is then utilized to steal or snoop on the user's information.
- **Trojan Game thief:** This Trojan is made primarily to steal user account information from people playing online games.

Drive - by Downloads attacks

In a drive-by download attack, malicious code is unknowingly or unlawfully downloaded from a website via a browser, application, or built-in operating system. Without the user clicking on anything, the download could begin. Visiting or viewing a webpage alone could trigger a download. Drive-by downloads can be used by cybercriminals to steal and acquire personal information, insert banking Trojans, install exploit kits or other malware on endpoints, and more.

Crypto jacking

Crypto jacking is the practice of secretly mining cryptocurrencies on someone else's computer. Hackers frequently force their targets to click on a malicious email link that installs crypto mining software, or they infect a website or online advertisement with malware that runs anytime the target browser loads it. Unaware victims continue to use their computers as usual while the crypto mining software is still active in the background. Reduced performance could be noticeable to the victim when they are using the computer, but otherwise it might go unnoticed. 2019 will see an increase in crypto jacking due solely to the promise of greater money for less risk.

Man in the Middle attacks

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. Cisco claims that they might filter and seize data after interfering with the transmission. MITM attacks commonly occur when a visitor uses an unprotected public Wi-Fi network. Attackers block access to the network and the visitor before using malware to install harmful software and access data.

SQL Injection

SQL injection, a type of injection attack that is one of the most often used internet hacking techniques, allows hackers control over the back-end database so they may add, remove, or change data.

Because the application doesn't thoroughly sanitize the SQL statements, there is a security hole that enables an attacker to include their own malicious SQL commands to access the company database. The attacker inserts malicious code into SQL queries by using web page input.

Rootkit

In order to gain administrator-level access to a computer or network system, malicious software called a rootkit installs and executes damaging code on a system without the user's awareness.

Among the many different types of rootkit viruses are Boot kits, Firmware Rootkits, Kernel-Level Rootkits, and Application Rootkits.

Exchanging contaminated disks or gadgets can cause it to infect a computer. It is frequently deployed using passwords that have been compromised or covertly exploiting phishing, social engineering, and system weaknesses.

Cloud attacks

Cloud services are become indispensable in our daily lives. We should be mindful, nevertheless, that not all cloud services offer secure encryption and authentication. Numerous problems, including attacks, network weaknesses, and data spills, can be brought on by misconfiguration.

Over half of cloud security breaches, according to IBM, are the result of straightforward problems. While examining configurations could help to prevent two-thirds of cloud security issues.

How to prevent cloud attacks?

- Educate/Train your employees
- Secure a data backup plan
- Identify who can access your data
- Use penetration testing
- Establish cloud governance policies and procedures

Malvertising attacks

Malvertising, often known as malicious advertising, is a relatively new and developing type of cybercrime. By using this method, thieves insert dangerous code inside digital adverts, sending users to rogue websites or infecting their devices with malware. Identification by internet users and publishers is exceedingly challenging. As a result, customers typically receive these through trustworthy advertising networks. Any online advertisement can put visitors at risk for infection.

Even well-known companies from throughout the world have unintentionally included harmful advertising on their websites.

How to prevent malvertising?

Once again, awareness is crucial. To decrease the danger of infection, certain procedures must be followed. These consist of:

- Ensure that software and extensions are updated

- Install antivirus software and ad blockers
- Avoid using Java or Flash programs

Publishers, on the other hand, are obligated to safeguard web users against harmful advertising. The following actions should be taken by them to lower risk:

- Evaluate third-party ad networks responsible for choosing, inspecting, and running ads
- Scan ads that they plan to display
- Avoid using Flash or JavaScript in ads

Organizational security procedures

A security procedure consists of the actions and duties required to provide security throughout regular business operations for an organization. In order to execute instructions for safety operations within any firm, security procedures operate in conjunction with security policies, regulations, and guidelines.

A security procedure can also install, enable, or enforce security controls outlined in the policies of your firm. Every safety process adheres to these security rules, regulations, guidelines, and procedures. Additionally, security rules serve as the cornerstone of a company's security program.

In terms of the level of specificity, there are fundamental ideas and elements to understand for security procedures.

- Security policies
- Standards
- Baselines
- Procedures

Types of organizational security procedures

Organizational security procedures are implemented to protect the confidentiality, integrity, and availability of sensitive information and assets within an organization. There are various types of security procedures that organizations can adopt,

depending on their specific needs and industry regulations. Here are some common types of organizational security procedures:

1. **Access Control**: These procedures make ensuring that only people with the proper access can access particular locations, systems, or data. Strong passwords, authentication methods (such biometrics or two-factor authentication), user access management, and role-based access restrictions are examples of access control techniques.
2. **Physical Security**: Protecting an organization's physical assets and facilities is done through physical security methods. To do this, security precautions including video monitoring, locks, alarms, visitor management systems, secure entrance points, and limited access to sensitive areas are used.
3. **Information Classification and Handling**: Organizations frequently categorize their information based on how sensitive or important it is. Security policies should outline the labeling, storing, transmitting, and safely disposing of various forms of information. This comprises data backup, encryption, secure file storage, and secure data disposal.
4. **Incident Response**: The steps to be done in the case of a security incident or breach are outlined in incident response procedures. This include identifying and assessing security incidents, minimizing their effects and threats, and recovering from them. Plans for responding to incidents should cover communication procedures and collaboration with pertinent stakeholders.
5. **Network Security**: Computer networks within an enterprise are shielded against illegal access, threats, and interruptions by network security protocols. These processes involve setting up firewalls, segmenting networks, implementing intrusion detection and prevention systems, doing frequent vulnerability scans of the network, and configuring network devices securely.
6. **Security Awareness and Training**: Organizations should have policies in place to inform staff members of security concerns, recommended practices, and their duties. Employees that participate in security awareness and training programs learn how to spot possible dangers, steer clear of social engineering scams, and appreciate the value of adhering to security rules and procedures.

7. **Data Backup and Disaster Recovery**: Critical data is frequently backed up and can be restored in the case of data loss or system failure thanks to procedures for data backup and disaster recovery. Setting up backup schedules, storing backups offsite, conducting recurring recovery drills, and using redundant systems are all required for this.
8. **Change Management**: A controlled and secure implementation of changes to a company's systems, applications, or infrastructure is guaranteed by change management methods. This entails evaluating the impact of changes, securing the necessary approvals, testing changes in a non-production setting, and keeping an eye out for any negative impacts.
9. **Security Monitoring and Logging**: Organizations should have policies in place for keeping an eye out for security-related events on their systems, networks, and applications. In order to detect and address possible security issues, this involves putting in place security information and event management (SIEM) systems, intrusion detection systems, log analysis, and real-time monitoring..
10. **Vendor and Third-Party Management**: For a variety of services, organizations frequently use outside providers. The selection, evaluation, and monitoring of suppliers for compliance with security standards should all be outlined in security protocols. This involves establishing security obligations in contracts and carrying out routine security audits or assessments.

Technical requirements and hiring practices

The first security precaution that needs to be done is making sure the website satisfies the required technological standards. These consist of selecting an appropriate web host, putting an SSL certificate on the server, and enabling automated updates.

Verify the website is additionally secured with the necessary security measures. Think about setting up accounts that have been approved by the firm, making secure passwords, and keeping the server secure.

These technical requirements will help the company secure the website, but they won't be very helpful if no one is aware of them and doesn't follow them. As a result, METROPOLIS CAPITAL bank's recruiting methods must follow industry standards.

Access Control

The first step in building efficient security in a company is to manage server accessibility. You can restrict access to only the chosen people using the access control system on your server, making sure that nobody else has access to it. The likelihood of attacks from outside sources will be lessened by doing this.

Two-Factor Authentication

The final important step you may take is to implement two-factor authentication. Many have adopted this security measure since it increases protection by requiring more than just a password to access your account.

Online business security is a critical element that needs further comprehension. The best way to safeguard the METROPOLIS CAPITAL bank is to have all the necessary technology requirements and precautions.

URL Filtering and Blocklisting

A crucial extra step you can take is to implement URL filtering and blocklisting. Given that they can access the server in a variety of ways due to their existence, bad actors will try to create information that they can use to do so. An attacker can try to make up information to be added to or even removed from the list of users on your server.

SSL Certificate

The next essential step in ensuring the security of your website is to obtain an SSL certificate. Verified website owners can use a digital signature to securely confirm their identity to everyone by using an SSL certificate.

It's crucial to keep in mind that these are generic categories of security processes, and the particular ones that a company implements may differ depending on its industry, legal requirements, and risk assessments.

Network monitoring

Monitoring a network's infrastructure to ensure its availability, performance, and security is known as network monitoring. To obtain insights into network behavior, identify problems, and make well-informed decisions for network management, it entails gathering data from network devices including routers, switches, and servers. Following are some crucial elements of network monitoring.:

1. **Monitoring Tools**: Take use of network monitoring solutions that offer capabilities including real-time network traffic analysis, device performance monitoring, log analysis, and security event detection. Nagios, Zabbix, PRTG, and SolarWinds are a few well-liked network monitoring software.
2. **Performance Monitoring**: Keep track of network performance indicators like device resource usage, latency, and packet loss. This enables proactive troubleshooting and optimization by assisting in the identification of bottlenecks, congestion, and performance deterioration.
3. **Availability Monitoring**: Monitor the network's hardware and services for availability and uptime. This include keeping an eye on system availability generally, service response times, device reachability, and port status. It assists in quickly locating and fixing network failures or service disruptions.
4. **Traffic Analysis**: To obtain insight into usage trends, spot abnormalities, and spot potential security issues, analyze network traffic patterns and flows. Packet analysis, flow-based analysis, or specialist network monitoring tools can all be used to accomplish this.
5. **Event and Log Monitoring**: To spot security issues, system failures, and configuration changes, keep an eye on network events and logs. Various network devices and systems' logs can be collected and analyzed with the use of centralized log management systems, such as SIEM (Security Information and Event Management) solutions.
6. **Security Monitoring**: Utilize tools and techniques for network security monitoring to identify security lapses, intrusions, or unusual network behavior

and take appropriate action. In order to do so, it is necessary to keep an eye on firewall logs, use intrusion detection systems (IDS), and scan network traffic for suspicious behavior.

7. **Alerting and Notifications:** Set up alerts and notifications to notify network managers of important events, problems with performance, or security risks. This facilitates quick reaction and cuts downtime.

A robust, effective, and secure network architecture depends heavily on network monitoring. It enables network managers to proactively manage network resources, address problems, enhance performance, and guarantee the network's overall safety and security.

Importance of network monitoring to METROPLIS CAPITAL bank

Most network monitoring software keeps a real-time check on a network. This suggests that it can find and alert users to performance issues before network staff members do. If you want to properly resolve network performance issues, it's imperative to reduce the time between when a problem occurs and when METROPOLIS CAPITAL bank learns about it. You will also be informed of any network performance issues, especially those that network teams cannot recognize. Even a little issue that marginally reduces performance has the potential to become considerably more problematic. You must therefore be conscious of any performance issues that are slowing down your network.

Network monitoring is of utmost importance to METROPLIS CAPITAL bank for several reasons:

1. **Security:** The bank can identify and stop security lapses and unwanted access attempts thanks to network monitoring. It offers real-time visibility into network traffic and can spot any unusual or malicious activity that could jeopardize the infrastructure or critical data of the bank. METROPLIS CAPITAL can quickly respond to any threats by keeping an eye on the network and putting the required security measures in place to protect their systems.
2. **Performance Optimization**: METROPLIS CAPITAL bank uses network monitoring to guarantee optimal network performance. They can use it to keep an eye on things like network latency, bandwidth usage, and general network

health. By monitoring these indicators, the bank can find and fix any performance problems or bottlenecks, guaranteeing efficient operations and positive user experiences for both staff members and clients.

3. **Troubleshooting**: METROPLIS CAPITAL can proactively find and fix network faults thanks to network monitoring. It offers information about device status, network connectivity, and application performance. By keeping an eye on the network, the bank's IT staff can rapidly pinpoint the source of any issues and take the necessary steps to reduce downtime and interruptions.
4. **Compliance and Regulatory Requirements**: Various compliance and regulatory obligations, such as those relating to data protection and privacy, are imposed on banks, including METROPLIS CAPITAL. By keeping an eye on network traffic for any potential infractions or unauthorized access attempts, network monitoring helps to assure compliance. It enables the bank to produce audit logs and keep track of network operations, both of which are important for compliance audits and investigations.
5. **Capacity Planning**: METROPLIS CAPITAL can properly plan for future expansion and scalability thanks to network monitoring. The bank can spot locations that might need more resources or capacity increases by examining network traffic patterns and consumption trends. With this proactive strategy, METROPLIS CAPITAL is able to optimize its network architecture and prevent performance snags as their company grows.

In conclusion, METROPLIS CAPITAL bank needs network monitoring because it improves security, maximizes performance, helps with troubleshooting, assures compliance, and enables efficient capacity planning. The bank can maintain a safe and dependable IT infrastructure by constantly monitoring their network, giving its staff and customers access to a steady and effective banking environment.

Benefits of network monitoring

Maintaining full network visibility

It is hard to effectively understand the network's performance without full network visibility. Each piece of network traffic that flows through METROPOLIS CAPITAL bank, as well as every linked device and standard performance indicators, must be

able to be monitored. Any network monitoring program worth its salt includes in-depth monitoring capabilities that cover every aspect of the network. On the network, performance-degrading problems won't exist in this way.

Discovering security threats.

Even though their primary function is performance monitoring, network monitoring tools can help you find security threats that are lurking within the system. Some malware and viruses are designed to remain on a network after they have gained access to it without doing anything at first, while others can be performing little, covert actions. The METROPOLIS CAPITAL bank will be alerted to any anomalous or suspicious network behavior (a hint that a security threat is utilizing network resources) via network monitoring technologies.

Predicting and preventing network downtime

Although you can never guarantee 100 percent service availability, even with the most comprehensive network monitoring system, they can nevertheless aid in preventing unexpected network outages. One of the primary functions of network monitoring systems is to find network activity that indicates a device or network is about to crash. This helps the METROPOLIS CAPITAL bank to minimize service interruptions and avoid any unplanned outages whenever possible.

Observing bandwidth utilization

The majority of network managers believe that bandwidth use is one of the most important performance indicators to take into account. As much bandwidth as is practical should be used by the METROPOLIS CAPITAL bank while ensuring that each service is performing at its highest level. A network monitoring system will notify the network and ensure that the quality-of-service (QoS) protocols are working properly when bandwidth use approaches critical levels.

Reducing mean time to repair

Network performance difficulties don't just have a monetary cost; instead, the time it takes the network employees of the METROPOLIS CAPITAL bank to resolve a problem could be employed on other, more important tasks. Therefore, it is essential

for companies to reduce the time between a performance issue's occurrence and resolution. As soon as performance issues are discovered, network monitoring tools alert the personnel, enabling the METROPOLIS CAPITAL bank to begin resolving them straight away. Numerous monitoring packages also include diagnostics features that enable your personnel to quickly assess the issue without having to conduct a thorough investigation.

Testing changes to a network or device

Any modifications you make to a device or the network must be tested to ensure they function as intended. The rest of your network could become unusable if adding or changing a device is done incorrectly. You may test new or updated connections and equipment to see if they might cause problems before your network is seriously harmed with the aid of network monitoring tools.

Generating network performance reports.

Performance data is continuously tracked by a network monitoring system, which displays it visually on their dashboard. Monitoring systems can also convert them into other printed file types, in addition to providing reports that the METROPOLIS CAPITAL bank may study. These reports may be generated by the solution on a weekly, monthly, quarterly, or any other schedule that the METROPOLIS CAPITAL bank selects.

Finding performance issues that occur after business hours.

Performance issues can arise at any time, even when no one is around to resolve them. Network monitoring software can uncover these problems for you because they continuously monitor a network. A problem must be reported to the METROPOLIS CAPITAL bank if it occurs after business hours. However, a trustworthy network monitoring system won't immediately send out notices for these issues because these cautions can be overlooked by the time the staff arrives at work. The patch would ideally delay the alert until a time that the network administrator specifies.

Network monitoring offers several benefits to organizations:

1. **Early Issue Detection**: Organizations can use network monitoring to find flaws and anomalies in their network infrastructure before they become serious concerns. It gives IT staff immediate access to information about

network traffic, device condition, and performance indicators, enabling them to quickly detect and fix problems. Early detection reduces user impact, cuts downtime, and maintains a stable network environment.

2. **Improved Network Performance**: Organizations can improve their network performance by tracking network measurements and traffic. IT teams can discover bottlenecks and optimize network resources thanks to the information it provides into bandwidth utilization, latency, packet loss, and other important data. Organizations can improve network efficiency, deliver faster and more consistent connectivity, and offer a better user experience by tracking and analyzing performance data.
3. **Enhanced Security**: A crucial part of recognizing and thwarting security threats is network monitoring. It enables businesses to keep an eye on network traffic for viruses, shady activity, and illegal access attempts. IT staff may identify and respond to security problems in real-time, preventing potential breaches or data leaks, by analyzing network data and utilizing security analytics. Additionally, network monitoring aides in ensuring adherence to rules and standards for security.
4. **Capacity Planning and Scalability**: Organizations are able to prepare for future development and scalability thanks to network monitoring, which offers insightful information on network usage and trends. IT organizations can identify peak usage periods, forecast resource needs, and schedule capacity expansions by tracking network traffic patterns. Organizations can minimize performance snags, guarantee network availability, and maximize resource distribution with this proactive method.
5. **Troubleshooting and Faster Problem Resolution**: Network monitoring speeds up problem solving by simplifying troubleshooting procedures. IT staff can use it to assess network connectivity, keep tabs on device condition, and evaluate application performance. When problems occur, network monitoring offers useful information to locate the underlying cause, conduct efficient troubleshooting, and apply the proper solutions. This lessens downtime, limits productivity losses, and boosts the effectiveness of IT operations.

6. **Compliance and Auditing**: Network security and data privacy compliance and legal requirements vary widely by industry. By logging network activities, network monitoring assists companies in meeting these demands. These logs act as an audit trail, documenting compliance and assisting with security inquiries. Monitoring the network helps to uphold industry standards, preserve sensitive data, and ensure data integrity.
7. **Cost Optimization**: Organizations may optimize their network resources thanks to network monitoring, which reduces costs. Organizations can plan for resource allocation and capacity by identifying underutilized resources, tracking bandwidth usage, and reviewing network performance. This enhances network infrastructure, cuts down on wasteful spending, and increases the return on IT investments.

Physical and virtual security measures that can be employed to ensure the integrity of organizational IT security

What is a physical security?

A common definition of physical security includes security measures designed to limit access to authorized individuals, as well as any resources that protect personnel from hard and property from damage.

So, in the simplest term, physical security is defined as the securing and protecting of organizational assets from coming to harm as a result of physical events. These events can range from natural disasters such as fires and floods, to human-inflicted dangers including theft and vandalism. Accidents and accidental damage also fall under the umbrella of events that may be covered by a physical security plan.

So, what do physical security systems and plans entail? On the surface, physical security measures include locks, gates, video security cameras and security guards. Although these are excellent strategies, there are deeper layers that you should take into account when creating a physical security plan.

An effective plan should include equipment and technology, and can work alongside these areas:

- **Training:** Ensure your staff has the proper knowledge in implementing your physical security strategy.
- **Site design and layout:** Equipment and physical security components should be strategically placed to complement the design and layout of your facility.
- **Emergency response readiness:** Staff in your facility should be trained on what to do during certain situations and emergencies.
- **Access control:** Understand how you will assign access to your staff and limit access for restricted spaces.

- **Environmental components:** Create safety measures to mitigate damage from intentional or unforeseen natural disasters that may happen.

Key physical security measures

When it comes to preventing different types of physical security threats in any facility, there are many types of innovations that you can use—from encrypted access cards and security cameras to mobile credentials and temperature sensors. But before you use any of these systems, it's important to understand the different elements that can contribute to your overall plan.

When creating a physical security strategy, you need to have all your security measures complementing one another. This means that you need to use different types of physical security measures in a layered approach to ensure that you're protected from every angle.

So, what is good practice for physical security? Here are the most common elements in an effective physical security plan:

1. **Deterrence:** This type of physical security technology focuses on keeping unwanted people, vehicles or animals away from a certain area. Deterrence can encompass various equipment such as signage, security cameras and access control systems. It also includes physical barriers such as doors, locks and walls. It is essentially any security systems or equipment that can help deter intruders from entering sensitive areas.
2. **Detection:** Deterrents can only do so much. If you want to fully protect your facility, you need to have devices that can identify potential intruders and ways to alert the correct authorities. Some technologies you can use for physical security detection measures are sensors, alarms and automatic notifications.
3. **Delay:** Several physical security controls are created to slow intruders down when breaking into a facility. Simple security measures such as additional

doors, locks and security guards can help delay incidents. More advanced physical security technology, such as key cards and mobile credentials, can make it more difficult for unauthorized users trying to enter a building. With this technology in place, it's easy to mitigate a breach before too much damage is caused.

4. **Response:** Once a breach or intrusion happens, you must also have a response strategy in place, such as building lockdowns or automatically notifying emergency services.

Successful and effective plans should include these technologies to ensure that a facility can prevent physical threats and take necessary action if a security breach occurs. [CITATION avi23 \l 1033]

Physical security measures.

Physical security refers to the steps taken to protect the physical security of IT assets, such as structures, equipment, personnel, resources, and other assets, from physical injury and unauthorized access. Physical security measures are implemented to protect these assets from physical threats such theft, vandalism, fire, and natural catastrophes.

Physical security is usually given great importance in structures with a large concentration of assets, especially those that house vital technology for business operations. Since the hardware components and supporting infrastructure must be kept free of anything that could interfere with their proper performance, physical security is absolutely essential for IT resources. This includes unauthorized employee interference as well as unforeseen events like accidents and natural disasters.

Physical security measures are crucial for protecting people, buildings, and other physical assets against physical threats such as theft, damage, and unlawful access. Here are a few typical physical security measures used by businesses.:

1. **Perimeter Security**: First line of defense is to set up a safe perimeter around the property. Physical obstacles like fences, walls, gates, bollards, or barricades can be used to limit access and prevent unwanted entry.
2. **Access Control Systems**: Access control systems limit access to those who are permitted. This can involve PIN codes, combination locks, fingerprint, iris, or other biometric scanners, key cards, proximity cards, or combination locks.

Systems for access control might be installed at a facility's entrances, doors, parking lots, or other sensitive areas.

3. **Video Surveillance**: Cameras placed strategically around the space are used by video surveillance systems to record and monitor activity. In the event of a security incident, CCTV cameras can serve as a deterrent and a source of proof. Advanced systems might have capabilities for remote monitoring, facial recognition, and motion detection.
4. **Security Guards**: Employing qualified security staff can give possible dangers a physical presence. Security officers can patrol the area, respond to problems, patrol access points, and enforce security rules. Additionally, they can help in an emergency and respond quickly to security breaches.
5. **Intrusion Detection Systems**: Sensors, sirens, and other detecting techniques are used by intrusion detection systems (IDS) to locate and notify staff of unlawful entry or security breaches. This may include sensors on walls, doors, or windows that, if tampered with, sound an alarm or send a notification.
6. **Security Lighting**: Areas with enough lighting can help with monitoring and deter crime. Ample illumination helps reduce blind spots and increase visibility for security staff and cameras around entrances, parking lots, walkways, and other critical locations.
7. **Secure Storage and Locking Mechanisms**: Valuable items, delicate data, or confidential information can be protected in secure storage spaces with locks, safes, cabinets, or cages. These precautions aid in guarding against theft and illegal access to valuable resources.
8. **Emergency Preparedness**: In the event of calamities or natural disasters, it is essential to put emergency response plans into action, including evacuation protocols, fire safety systems, and designated assembly points.
9. **Employee Training and Awareness**: It is crucial to provide personnel with training on security processes, access control policies, reporting suspicious activity, and emergency response. Every employee in the firm should be alert and aware of their responsibility in preserving physical security, which can be achieved by fostering a culture of security awareness.

10. **Regular Security Audits and Assessments**: Regular security audits and assessments help find weaknesses, gauge how well current security measures are working, and make the required corrections. This include assessing risks, examining physical security procedures, and fixing any flaws that are found.

Types of physical security measures

1. **Locking the server room's door**

Make sure the server room door locks are in working order before you shut the servers down or even before you switch them on for the first time. Even the best lock won't help you if you don't use it, so you need laws requiring such doors to always be shut whenever a room is unoccupied. The policies should specify who has the key or keycode to get access.

The server room, which acts as the brain of your physical network, is home to servers, switches, routers, cables, and other equipment that may be physically accessed by anybody and cause serious harm.

2. **Establish surveillance**

Locking the server room door is a good first step, but someone might break in or someone with access might misuse that right. You require a system to keep track of who enters and leaves at what times. Using a log book for signing in and out is the simplest way to achieve this, but it has a number of drawbacks. A bad person would probably just stay away from it.

The doors must be unlocked using a smart card, token, or biometric scan, and everyone entering is required to provide identity. An authentication system integrated into the locking mechanisms is preferable to the log book as a substitute.

A video should be added to the logbook or electronic access system.

3. **Ensure that the devices that are most susceptible are in the secured room.**

In light of this, you shouldn't be focused solely on the servers. A hacker can use sniffer software to record network traffic by connecting a laptop to a hub. The majority of your network hardware ought to be in that locked room, or if they must be elsewhere, in a locked closet someplace else in the building.

4. **Utilization of rack-mount servers.**

Rack mount servers take up less room in the server room and are also easier to secure. Despite being smaller and possibly lighter than (some) tower systems, they can nevertheless be swiftly mounted into closed racks that can subsequently be fastened to the floor after being filled with several servers, making the entire setup nearly impossible to move, let alone steal.

5. **Remember the workstations.**

Hackers may use any unsecured device connected to the network to access or delete vital data for your business. Workstations at vacant offices, vacant desks (such as those used by absentee or departing employees who have not yet been replaced), or locations where visitors can easily enter the building, such as the front desk of the receptionist, are particularly vulnerable.

Computers that aren't in use should be turned off or removed, and offices that are vacant, even briefly while a worker is out to lunch or unwell, should have their doors secured. To make it harder for unauthorized users to log in, install smart card or biometric readers on computers that must remain in public areas, frequently concealed from employees' view.

6. **Prevent case opening by trespassers**

Servers and workstations should both be guarded against burglars who can open the casing and grab the hard disk. Much easier to smuggle out of a building than a full skyscraper is a hard disk in your pocket. To prevent case opening without a key, case locks are frequently incorporated with computers.

Locking kits, such as the one from Innovative Security Products, can be found everywhere for incredibly low costs.

7. **Guard the portables.**

With regard to physical security, laptops and other portable computers present unique challenges. A thief can easily access any data on the computer's HDD as well as any saved network login information. If employees use laptops at their workstations, they should either take them with them when they leave or secure them using a cable lock, like the one provided by PC Guardian, to a permanent fixture.

Handhelds can easily be tucked into a pocket and taken with you as you leave the area. Even a drawer or safe can be used to store them. Motion-sensing alarms are

another choice for alerting you if your portable is moved. The one from SecurityKit.com is one illustration.

Biometric scanners, full disk encryption, and "phones home" software

8. **Pack up the backups**

Backing up important data is an essential part of disaster recovery, but it's important to keep in mind that the information on those tapes, CDs, or discs could be taken and used against the company. IT professionals usually keep the backups in the server room, close to the server. They should be stored in a safe or drawer at the very least. The best practice is to retain a set of backups off-site, but you must take security measures to ensure their safety.

Remember that some workers might keep backup copies of their work on floppy disks, USB keys, or external hard drives. Have policies specifying that if this behavior occurs, the backups must always be locked up.

9. **Disable the drives**

If you don't want employees transmitting company data to removable media, you can disable or remove floppy drives, USB ports, and other connections for external devices. Cutting the wires might not be enough to deter technically competent staff. Some organizations will even go so far as to cover ports with glue or other materials in an effort to permanently restrict their usage, despite the fact that software mechanisms prohibit it. Disk locks, like the one from SecurityKit.com, can be installed to keep out other diskettes on computers that still have floppy drives.

10. **Keep the printers safe**

Even though you might not think of printers as a security risk, many contemporary printers now come equipped with on-board memory where they store document data. If a hacker steals the printer and gains access to its memory, they could be able to copy recently printed documents. In the same way that servers and workstations that house sensitive data are locked down and maintained in safe locations to prevent theft, printers should also.

Physical security measures encompass various types of safeguards designed to protect people, assets, and facilities from physical threats. Here are some common types of physical security measures:

1. **Perimeter Security**: In order to restrict access and prevent unlawful entry, perimeter security systems create a perimeter around a building or piece of property. Fences, walls, gates, bollards, obstacles, and vehicle barriers are a few examples.
2. **Access Control Systems**: Systems for controlling access to secure places regulate and keep an eye on admission. They include devices like key cards, proximity cards, PIN codes, facial recognition systems, and biometric scanners (fingerprint, iris, or iris recognition). Access control systems may be installed at building entrances, doors, elevators, parking lots, or certain locations.
3. **Surveillance Systems**: Cameras and other sensors are used in surveillance systems to see and document activity inside and outside a building. For monitoring, recording, and playback, closed-circuit television (CCTV) cameras are frequently used in conjunction with video management systems (VMS) and digital video recorders (DVR). Advanced systems might have capabilities for remote monitoring, facial recognition, and motion detection.
4. **Security Guards**: A physical presence and ability to respond to security incidents are provided by trained security personnel. They can patrol the area, keep an eye on access points, enforce security rules, and help in an emergency. Security officers deter potential intrusions and can react rapidly to threats.
5. **Intrusion Detection Systems**: Sensors and alarms are used by intrusion detection systems (IDS) to spot and notify staff of unlawful entry or security breaches. These systems may have earthquake sensors, glass break sensors, door/window sensors, or motion sensors. Alarms can be noisy or silent, and they can send notifications to central monitoring stations or security personnel.
6. **Security Lighting**: It is essential to have good illumination to deter criminal activity and improve surveillance. Areas with good lighting eliminate hiding places and enhance visibility for security guards and monitoring equipment. Around entrances, parking lots, sidewalks, and other sensitive locations, lighting can be added.

7. **Locking Mechanisms and Secure Storage**: Protecting priceless items, delicate information, or confidential data sometimes involves the use of locking mechanisms like locks, safes, cabinets, or access-controlled storage places. These security methods guard vital resources from unwanted access.
8. **Emergency Preparedness**: Fire safety systems, evacuation plans, designated assembly areas, and emergency communication networks are examples of emergency preparedness procedures. They guarantee that staff members can react correctly to crises or natural disasters.
9. **Security Signage and Markings**: Staff members and visitors can be directed by clear signage, warnings, and markings that identify restricted areas, emergency exits, or safety considerations. These aid in enforcing security regulations and raising security awareness in general.
10. **Physical Barriers and Reinforcements**: To defend against particular threats, extra physical barriers and reinforcements can be put in place. Examples include blast-resistant materials, security doors, reinforced glass, security film, and anti-ram barriers.

Advantages of physical security measures

Numerous alternatives with several advantages are available for physical security. Turnstiles, mantraps, fences, and electric fences make up the perimeter security system in the first place. safe locks with tricky to duplicate keys. Any employee must have a badge in order for their identity to be validated. Install the surveillance in areas where it won't be exposed to the attacker or vulnerable to tampering. Ensure the safety of any flimsy devices and portables. Put the backups in a place that is hard to access and is secure. In the event of an explosion, fire, or electrical problem, use the appropriate control approach to perhaps save some of the vital objects in the METROPOLIS CAPITAL bank.

Physical security measures offer several advantages for organizations:

1. **Deterrence**: Potential thieves and intruders are discouraged by the presence of obvious physical security measures, such as fences, security personnel, or

video cameras. It can deter unwanted access or illegal activity since it makes it evident that security is handled seriously.

2. **Prevention of Unauthorized Access**: Unauthorized people cannot access restricted locations because to physical security measures like access control systems, locks, and obstacles. Organizations can safeguard sensitive information, assets, and facilities from illegal access, theft, or manipulation by implementing access controls.
3. **Protection of Assets**: Physical security methods protect priceless resources against theft, loss, damage, and inventory theft. Asset protection measures including secure storage, locking mechanisms, and surveillance systems can also help find and recover lost or stolen objects.
4. **Safety of Personnel**: Physical security measures help to ensure the safety and wellbeing of a facility's tenants, visitors, and staff. Security officers can make people feel comfortable, deal with crises, and make sure everyone adheres to safety rules. People are protected during emergencies by emergency preparedness measures including evacuation plans and fire safety systems.
5. **Detection and Response to Security Incidents**: Alarm systems, surveillance cameras, and intrusion detection systems all aid in the real-time identification of security events. This enables security staff, law enforcement, or emergency services to react quickly. Threats or security breaches can be lessened in impact with early discovery and action.
6. **Evidence Collection and Investigation**: In the event of security events, accidents, or legal issues, physical security measures like surveillance systems can offer crucial evidence. In order to investigate occurrences, identify offenders, or give evidence for legal procedures, video footage, access records, or sensor data may be employed.
7. **Compliance with Regulations**: Organizations can comply with industry standards for security and safety and compliance needs by using physical security measures. Organizations can show their dedication to safeguarding sensitive information, client data, and keeping a secure environment by putting in place the proper physical security measures.

8. **Business Continuity**: Physical security measures reduce interruptions and downtime, which promotes company continuity. Organizations can continue to function even in the event of security crises or emergencies by protecting key infrastructure, facilities, and assets.
9. **Insurance Benefits**: Strong physical security measures can have a positive effect on insurance coverage and costs. Organizations that demonstrate good physical security measures may receive cheaper rates or better coverage alternatives from insurance providers, lowering the financial risks connected with security incidents.
10. **Peace of Mind**: Employees, clients, and stakeholders are all given piece of mind by physical security measures. Trust and confidence in the organization's dedication to safety and protection are fostered by knowing that adequate security measures are in place.

Disadvantages of physical security measures.

However, there are a few gaps. Intruders and animals could be damaged or harmed by some of the approaches. The intrusion could be accomplished by a leaping intruder. Validity could be compromised by both authentication and access control (AC). It is possible for hackers to steal smart cards or keys, which makes it easier for them to enter your computer and recover the missing USB. Users are left to figure out how to operate the highly complex security installations and systems of today on their own.

Staying up to speed with security technology is difficult because new updates and development plans are implemented every year. The issue is that despite the abundance of facilities, employees hardly ever know how to use them. For instance, the firm is equipped with fire extinguishers.

Physical security measures have many benefits, but there are also some possible drawbacks that organizations should take into account.:

1. **Cost:** It can be expensive to implement and maintain physical security measures. The initial installation of systems like access control, security cameras, and alarm systems, as well as continuous maintenance, upgrades, and

labor expenditures, are all included in the costs. Organizations with tight resources may struggle to cover the cost of physical security measures.

2. **False Sense of Security**: Physical security measures alone may give one a false sense of security. It's common for businesses to believe that their physical defenses, locks, or surveillance measures are adequate to fend off all dangers. Physical security measures are simply one part of an all-encompassing security strategy, it's crucial to keep in mind. Additionally crucial are elements like personnel training, cybersecurity, and procedural controls.
3. **Vulnerability to Physical Attacks**: Physical security measures may be there, yet determined intruders or criminals may find ways to get around or get beyond them. Physical security systems may be compromised by sophisticated methods, technologies, or social engineering strategies. In order to meet changing threats, organizations must routinely evaluate the efficiency of their physical security measures and adapt them as necessary.
4. **Privacy Concerns**: Employees, tourists, or people in public places may be concerned about their privacy when using some physical security measures like surveillance cameras or access control systems. It's critical to strike the correct balance between security and privacy. To ensure compliance with relevant privacy laws, organizations should develop explicit policies addressing the collection, storage, and use of personal data collected by physical security systems.
5. **Maintenance and Upkeep**: Physical security measures need to be maintained and kept up to date on a regular basis to ensure their efficacy. Barriers or locks may need to be repaired, access control systems may need to be updated, and surveillance cameras may need to be calibrated. These systems' dependability and the intended security benefits can be harmed by inadequate maintenance.
6. **Human Error and Insider Threats**: Human error or insider threats are possible with regard to physical security measures. An employee might unintentionally violate security protocols, open a locked door, or jeopardize access credentials. Through employee training, awareness campaigns, and

strict access control measures, organizations must address the human element in their physical security systems.

7. **Integration and Complexity**: Integrating many technologies and systems is frequently necessary when putting in place a thorough physical security system. It may take careful planning, coordination, and compatibility across several components to complete this integration, which can be challenging. Organizations may encounter difficulties addressing interoperability concerns or integrating physical security technologies with current infrastructure.
8. **Limited Flexibility**: Physical security measures may limit the comfort and flexibility of authorized workers. Strict access restrictions, complicated authentication processes, or time-consuming security measures may obstruct normal business operations, annoying staff members or visitors.
9. **Environmental Limitations**: Environmental considerations may have an impact on some physical security measures. For instance, bad weather might affect the efficiency of security cameras or access control systems. Specialized equipment or maintenance concerns may be necessary in extreme temperatures or severe situations.
10. **Psychological Impact**: Employees, clients, or visitors may occasionally feel uneasy or uncomfortable in the presence of conspicuous physical security measures like barricades, guards, or surveillance cameras. Striking a balance between maintaining a welcome and upbeat mood and offering a secure environment is crucial.

Virtual security measures

Virtualized security, often known as security virtualization, refers to software-based security solutions developed to operate in a virtualized IT environment. Contrast this with traditional hardware-based network security, which utilizes hardware such as traditional switches, routers, and firewalls and is static.

While virtualized security is flexible and dynamic, hardware-based security is rigid. It is frequently cloud-based and independent of any one device, allowing it to be put anywhere in the network. For virtualized networks, where operators launch

workloads and applications as needed, the flexibility of security services and operations is essential.

Virtual security measures refer to the steps and technologies implemented to protect virtual environments, such as computer systems, networks, and data, from unauthorized access, breaches, and other cyber threats. Here are some common virtual security measures:

1. **Firewalls**: Using pre-established security rules to filter incoming and outgoing network traffic, firewalls serve as a barrier between internal networks and external networks. They aid in guarding against network-based threats and preventing unwanted access.
2. **Antivirus and Antimalware Software**: Software like antivirus and antimalware is made to find, stop, and get rid of harmful programs like Trojans, worms, and spyware. In order to provide security against the most recent dangers, these programs must be regularly updated.
3. **Intrusion Detection and Prevention Systems (IDS/IPS):** IDS/IPS programs keep an eye on network traffic for unusual activity or well-known attack patterns. They can identify possible dangers and notify administrators of them, or they can automate the blocking of malicious activity.
4. **Virtual Private Networks (VPNs):** Secure remote access to networks is made possible via VPNs over the internet. Between the user's device and the network, they encrypt network traffic to protect the confidentiality and integrity of data exchanges.
5. **Access Controls:** To protect virtual environments, it is crucial to implement robust access controls. Enforcing distinct user accounts, secure passwords, and multi-factor authentication are some examples of this (MFA). By limiting user privileges in accordance with work requirements, role-based access controls (RBAC) can reduce the danger of illegal access.
6. **Data Encryption**: Data is changed by encryption into an unintelligible format that can only be unlocked with the right encryption key. Sensitive data is

protected by encryption both in transit and at rest (stored data) (data being transmitted between systems or networks).

7. **Regular Patching and Updates**: It's crucial to keep software, operating systems, and applications updated with the most recent security patches. Bug fixes and vulnerability patches that address well-known security flaws are frequently included in these releases.
8. **Security Audits and Penetration Testing**: Penetration testing and regular security audits can help find holes and vulnerabilities in virtual environments. To identify areas that need improvement, they entail assessing security precautions, simulating attacks, and analyzing the system's response.
9. **Backup and Disaster Recovery**: Regular data backups and a reliable disaster recovery plan are essential. Backups and recovery procedures help reduce downtime and data loss in the case of a security incident or system failure.
10. **User Education and Awareness**: It is crucial to encourage user education and understanding of best security measures. Overall virtual security is strengthened by teaching employees how to spot phishing emails, create secure passwords, and stay away from dubious websites or downloads.

It's crucial to remember that virtual security measures should be put into place using a tiered strategy, combining several defenses to offer complete protection against developing cyber threats.

Types of virtual security measures.

Implement named users and least privilege

For everyday activities, connect to ESXi hosts using just non-root user accounts. Create a named administrator user in vCenter Server and give specific users the administrator role so that you can keep track of who used what host, at what time, etc., and hold them accountable for the changes they make to your environment.

Secure every component of the infrastructure.

All parts of the infrastructure, including the physical parts (hosts, switches, routers, and physical storage), the virtual parts, the operating systems used by guests, and any cloud environments you use, must be adequately safeguarded. More specific.

- The installed firmware on hosts, as well as the virtualized infrastructure, should be updated with the most recent security patches (VMware vSphere or Microsoft Hyper-V). It's also critical to have the most recent versions of the VMware tools updated on your virtual machines.
- All active network components, such as switches, routers, load balancers, and other devices used to distribute workloads, should have the most recent firmware loaded.
- Every operating system should receive a complete fix via automated updates. The application of patches should be scheduled for after-hours and should include automatic reboots.
- Install antivirus and antimalware software designed for virtualized environments.

Based on their particular focal areas, virtual security measures can be divided into a number of different types. The following list of popular virtual security measures:

1. **Network Security**:
    - Firewalls
    - Intrusion Detection and Prevention Systems (IDS/IPS)
    - Virtual Private Networks (VPNs)
    - Network segmentation
    - Network monitoring and traffic analysis tools
2. **Endpoint Security**:
    - Antivirus and antimalware software
    - Host-based intrusion detection and prevention systems
    - Data loss prevention (DLP) tools
    - Device and application control
    - Patch management

3. **Application Security**:
    - Secure coding practices
    - Web application firewalls (WAF)
    - Secure software development lifecycle (SDLC) processes
    - Code analysis tools
    - Authentication and access controls within applications
4. **Data Security**:
    - Data encryption (at rest and in transit)
    - Data loss prevention (DLP) solutions
    - Database access controls
    - Data backup and recovery
    - Data classification and access policies
5. **Identity and Access Management (IAM):**
    - User authentication (e.g., passwords, biometrics, tokens)
    - Multi-factor authentication (MFA)
    - Role-based access control (RBAC)
    - Privileged access management (PAM)
    - Identity federation and Single Sign-On (SSO) solutions
6. **Cloud Security**:
    - Cloud-specific firewalls and security groups
    - Encryption of data in the cloud
    - Identity and access management for cloud services
    - Cloud workload protection platforms (CWPP)
    - Cloud access security brokers (CASB)
7. **Incident Response and Forensics**:
    - Incident response plans and processes
    - Security information and event management (SIEM) solutions
    - Log analysis and monitoring
    - Digital forensics tools
    - Incident investigation and reporting procedures
8. **Security Awareness and Training**:
    - User security awareness programs

- Phishing awareness and simulation training
- Security policies and procedures communication
- Social engineering awareness
- Ongoing security education for employees

Possess a reliable backup and disaster recovery (DR) strategy.

Having a solid backup and disaster recovery plan is essential for ensuring company continuity, regardless of whether you encounter a cyberattack or a storm takes down your production datacenter. The likelihood of a prolonged outage can be decreased with the use of a DR site in the cloud or at a remote datacenter. Two essential recommendations to keep in mind while you create your DR plan are as follows.:

- Backup physical servers and virtual machines — Although ESXi itself cannot be backed up, its settings can be utilizing the Power CLI scripting tool and the VMware command line. Nowadays, the same tools may be used to back up both physical computers running Windows or Linux and virtual machines running any OS.
- Use the fallback. Make at least three copies of your data, keep them up to date, and store two of them as backups—one of which should be offshore. This is known as the 3-2-1 rule.
- Consider replication: For further DR protection, you can replicate your production VMs to a different datacenter, where you can failover quickly if necessary.

Advantages of virtual security measures

Virtualized security not only meets the complicated security needs of a virtualized network better than traditional physical protection, but is also more flexible and effective. Here are a few of its unique benefits:

Virtual security measures have many benefits for protecting networks, computer systems, and data from online attackers. Here are several major benefits.:

1) **Protection against Unauthorized Access**: Virtual security measures assist in limiting unauthorized access to confidential data and resources. Virtual security measures make sure that only authorized people may access and

manipulate data and systems by establishing robust authentication processes, access controls, and encryption.

2) **Data Confidentiality and Integrity**: The confidentiality and integrity of data are guaranteed by virtual security mechanisms like as encryption, secure data transmission, and access controls. Secure transmission techniques stop data interception or tampering while in route, while encryption shields data from unauthorized access or change.

3) **Mitigation of Cyber Threats**: A wide range of cyber dangers, including malware, viruses, phishing scams, and network-based intrusions, are protected from by virtual security measures. The risk of data breaches and system compromises is decreased thanks to the assistance of security solutions such as antivirus software, firewalls, intrusion detection systems, and other.

4) **Regulatory Compliance:** Regarding data protection and security, several sectors have their own legislation and compliance standards. Organizations can achieve these compliance requirements and adhere to industry-specific rules and standards by using virtual security solutions.

5) **Business Continuity**: Maintaining business continuity requires the use of virtual security measures. In the case of a security issue or system failure, regular backups, disaster recovery plans, and incident response procedures assist reduce downtime and data loss. This guarantees that crucial business processes may be swiftly and effectively resumed.

6) **Enhanced Productivity and Efficiency**: By saving time and effort on handling security incidents and fixing system flaws, efficient virtual security solutions can increase productivity. With strong protection in place, workers can concentrate on their work without interruptions from online risks.

7) **Protection of Reputation and Customer Trust:** A security lapse can seriously harm a company's reputation and lose customer confidence. Virtual security measures show a commitment to securing sensitive information and assist prevent data breaches. Organizations may improve their reputation and develop trust with consumers and partners by putting robust security measures in place.

8) **Cost Savings**: Although putting virtual security measures in place costs money up front, they can save money over time. Organizations can avoid expensive legal fights, fines from the government, and reputational harm by preventing security incidents and data breaches. Strong security measures also lessen the need for costly incident response and recovery activities.

9) **Cost-effectiveness:** A business can maintain a secure network without incurring major additional costs for pricy proprietary hardware thanks to virtualized security. For companies that properly manage their resources, usage-based pricing for cloud-based virtualized security services can result in significant savings.
10) **Flexibility:** It is crucial in a virtualized environment that security operations can follow workloads wherever they go. It provides security in scenarios including many data centers, different clouds, and hybrid clouds, allowing a business to fully utilize virtualization while preserving data security.
11) **Operational effectiveness:** Because virtualized security doesn't require IT staff to set up and operate several hardware appliances, it may be deployed more rapidly and simply than hardware-based security. Instead, they may set up security systems using centralized software and swiftly grow them. When security technology is deployed, security-related tasks can be automated, giving IT staff more time to focus on other tasks.
12) **Regulation adherence**: Since traditional hardware-based security is static and unable to keep up with the demands of a virtualized network, virtualized security is crucial for enterprises that must maintain compliance with legislation.

Disadvantages of virtual security measures

The risk increases as a result of the virtualized security's increased complexity. It is more difficult to track workloads and applications as they move between servers in a virtualized environment, which makes it harder to keep track of security configurations and policies. Furthermore, the ease of setting up virtual machines could result in security weaknesses.

Regardless of whether security services are virtualized or not, it is imperative to remember that many of these risks can still occur in virtualized settings. Therefore, it can be concluded that the above-mentioned physical and virtual security measures can be applied to METROPOLIS CAPITAL bank to improve the security of the organization and to improve the integrity of the organization. These risks can be reduced by adhering to business security best practices (such as spinning off virtual machines when they are no longer required and employing automation to maintain security rules current).

Although virtual security measures have many benefits, there are also some potential drawbacks to take into account.:

1. **Complexity and Management Overhead:** Virtual security measures can be difficult and time-consuming to implement and manage. To manage security measures properly, organizations may need to make investments in expert IT personnel or outsource security services. Costs and resource allocation may go up as a result.
2. **False Positives and Negatives**: Antivirus software and intrusion detection systems, for example, may produce false positives or false negatives. When legal activity are mistakenly labeled as harmful, false positives happen, causing unneeded alerts and disruptions. False negatives, on the other hand, take place when real dangers go unnoticed or unidentified, leaving the organization open to attack.
3. **User Convenience and Productivity Impact**: Users may feel burdened by stringent security measures like multi-factor authentication or complex password regulations. The whole security posture could be jeopardized as a result of resistance or attempts to circumvent security measures. Furthermore, some security solutions could impose extra procedures or authentication requirements that could impede operations and lower productivity.
4. **Compatibility and Integration Challenges**: Virtual security measures must work with the current IT infrastructure and systems and be integrated into them. When adopting new security solutions, compatibility or integration issues may appear, causing disruptions or conflicts with current systems. Deployment and integration may take more time and effort as a result.

5. **Cost Considerations:** Virtual security measures can be expensive to implement and maintain. To guarantee the efficiency of security measures, organizations must make investments in hardware, software, licenses, and ongoing maintenance. The entire cost may also increase as a result of hiring professional security employees or outsourcing services.
6. **False Sense of Security**: A false impression of security may be produced by relying entirely on virtual security measures. These precautions are essential, but they are not impenetrable, and persistent attackers may discover a way around them. Organizations must create a thorough security strategy that addresses any weaknesses through proactive monitoring, training, and reaction as well as teaching and training.
7. **Evolving Threat Landscape:** New threats are continually developing, changing the cybersecurity landscape. To stay up with new threats, virtual security measures must be regularly updated and modified. Systems and data could become exposed to new attack vectors if updates are not made.

Activity 02

Configuration

Configuration, in the context of technology and computer systems, refers to the organization and selection of numerous hardware, software, and parameter settings that control how a system or device functions. It entails defining and modifying the precise properties and choices that control a system or application's operation, functionality, and presentation.

Hardware settings, network setups, software settings, user preferences, security settings, and other factors are all included in configuration. To adapt the system or application to particular needs or desired results, it entails specifying and modifying a variety of characteristics, options, and choices.

A system or application's initial setup, installation, as well as continuing management and maintenance, can all involve configuration. It frequently entails making decisions and modifications based on

Configuration can be carried out via configuration files, dedicated configuration tools offered by the system or application, graphical user interfaces (GUIs), command-line interfaces (CLIs), or any combination of these. In order to get the best performance, functionality, and security, it is crucial to make sure that the configuration settings are precise, consistent, and in line with the intended goal.

The practice of methodically maintaining and controlling configurations across different systems, devices, or applications is referred to as configuration management as well. To provide correct configuration integrity and control over time, it entails creating and maintaining a consistent and reliable configuration state, monitoring changes, and putting version control systems in place.

1) **In computers and computer networks**, Configuration describes how the components of a computer system are assembled. The specific hardware and software information, including the system's parts, capacity, and attached devices, are commonly referred to as a configuration. Configuration includes both software and hardware components. When discussing hardware configuration, people occasionally make explicit reference to software elements and hardware arrangement. Understanding computer setup is essential because some hardware or software programs call for a specific configuration.

Configuration describes the precise options and parameters that specify how hardware elements, software programs, and network components are set up and function in computers and computer networks. It entails modifying and altering a number of system components to guarantee optimal operation, connectivity, and security. Here are several illustrations of configuration in this situation.:

1. **Hardware Configuration:** Setting up and altering the physical settings of a computer system's CPU, RAM, storage, and peripheral devices is known as

hardware setup. Device-specific settings, hardware drivers, and BIOS configuration may all be included.

2. **Software Configuration**: Setting up software applications or operating systems entails adjusting their settings and options. This involves managing user profiles, setting default behavior, modifying preferences, and activating or disabling features. Graphical user interfaces, command-line interfaces, or configuration files can all be used to configure software.
3. **Network Configuration**: To create network connectivity and guarantee effective communication between devices, network setup involves setting up and configuring network devices, such as routers, switches, firewalls, and wireless access points. It entails allocating IP addresses, constructing routing tables, configuring network protocols, establishing security constraints, and administering network services.
4. **Server Configuration:** When a server is configured, the software and settings are set up and customized to match particular needs. It comprises setting up services like web servers, database servers, email servers, or file servers as well as server roles, security settings, access controls, and resource allocation.
5. **Security Configuration**: Security configuration entails putting in place the right security safeguards to safeguard computer networks and systems. This involves managing user authentication and authorization techniques as well as configuring firewalls, access controls, encryption, and intrusion detection and prevention systems.

2) **In a network**, The term "configuration" is frequently used to describe the topology.

3) **Configuration,** In installing hardware and software, which is occasionally the purposeful process of configuring options that are offered.

Misconfigurations

Security misconfiguration occurs when security settings are not properly configured during the configuration process or when they are maintained and deployed with default values. This could have an impact on any layer of the application stack,

cloud, or network. A significant cause of data breaches that wind up costing firms millions of dollars is improperly setup clouds.

Computer systems, software programs, or network component settings and configurations that are erroneous or unsuitable are referred to as misconfigurations. These errors can be brought on by human error, ignorance, oversight, or poor configuration management procedures. On the functionality, performance, and security of the system, they may have substantial detrimental effects. Here are some instances of incorrect settings:

1. **Security Misconfigurations**: Systems and networks that have security setup errors are more susceptible to online threats. This can include not updating security patches and updates, providing users excessive user access, misconfiguring firewall rules, and leaving default passwords untouched. These setup errors may disclose private information, permit unauthorized access, or aid virus dissemination.
2. **Network Misconfigurations**: Misconfigured networks can cause connectivity problems, subpar performance, or even complete network failure. Incorrect IP address assignments, subnetting mistakes, incorrectly configured routing protocols, and improperly configured network access control lists are a few examples (ACLs). These errors can impair data transfer, interfere with network communication, and interrupt services.
3. **Application Misconfigurations**: Software application configuration errors can present vulnerabilities or have an adverse effect on its functionality. This may involve lax access controls, insecure default configurations, insufficient authentication methods, or unsuitable database connection options. Misconfigured applications run the risk of compromising data, allowing unwanted access, or becoming unstable.
4. **Cloud Misconfigurations:** Misconfigurations in cloud settings, like platform as a service (PaaS) or infrastructure as a service (IaaS), can lead to security breaches or service interruptions. Common instances include incorrectly setup access controls, storage buckets that are accessible to the public, unsecure API configurations, or insufficient encryption options. Misconfigurations of the

cloud can disclose confidential information, jeopardize client data, or result in unauthorized access to cloud resources.

5. **Server Misconfigurations**: Misconfigurations on servers can affect its functionality, security, and reliability, including operating system settings, services, and permissions. Examples include misconfigured user accounts, enabled insecure protocols, inappropriate resource allocation, and erroneous file permissions. Misconfigured servers can lead to system vulnerabilities, interruptions in operation, or illegal access to confidential data.

Why do misconfigurations occur?

A misconfiguration can be caused by a variety of factors.

Due to the complexity and rapid development of modern network infrastructures, it is simple for enterprises to overlook important security settings, including new network equipment that can keep default defaults.

Even if the company has implemented secure endpoint configurations, they still need to regularly audit configurations and security protocols to detect configuration drift. Misconfigurations may occur when systems are updated, new hardware is added to the network, or when software changes are made.

Misconfigurations can happen for a number of reasons, such as human mistake, a lack of knowledge or competence, a deadline, the complexity of the system, and insufficient configuration management procedures. The following are some typical causes of misconfigurations.:

1. **Human Error**: Misconfigurations are frequently caused by errors committed by users, developers, or system administrators. Simple mistakes like wrongly inputting values, picking the incorrect options, or skipping over crucial configuration settings might cause this.
2. **Lack of Knowledge or Training**: Misconfigurations may result from a lack of comprehension of system setups, security best practices, or particular application requirements. Errors and oversights may occur due to inadequate training or expertise in managing complicated configurations.
3. **Complexity of Systems**: Modern computer networks, software programs, and systems are intricately interconnected and have a wide range of configuration possibilities. Config management in such complex setups increases the risk of mistakes or oversights.

4. **Time Pressure and Deadlines**: System administrators and developers may experience time pressures or deadlines in fast-paced environments, resulting in hurried configuration procedures. As a result, there may be a higher likelihood of mistakes or overlooking important settings.
5. **Lack of Standardization and Documentation**: It becomes challenging to guarantee uniform and secure setups across systems in businesses with uneven or poorly documented configuration standards. The possibility of mistakes or departures from best practices is increased by inconsistent methods and undocumented setups.
6. **Inadequate Change Management**: Misconfigurations may be caused by poor change management techniques, such as a lack of change control, testing, or approval procedures. Implementing changes without conducting adequate review and testing may result in configuration conflicts or mistakes.
7. **Lack of Automation and Configuration Management Tools:** Human mistake is more likely when manual configuration methods are used without automation or configuration management solutions. Automated tools can be used to verify setups, assure consistency, and look for potential configuration errors.
8. **Complexity of Security Requirements:** Configuring numerous levels of security controls is a common step in the implementation of effective security measures. Access controls, encryption, and authentication systems are examples of complex security configurations that might be difficult to set up effectively, increasing the possibility of configuration errors.
9. **Lack of Ongoing Monitoring and Auditing**: Misconfigurations may go undetected in the absence of ongoing monitoring and periodic audits. Misconfigurations can persist and expose systems to security vulnerabilities or operational problems if they are not quickly detected.

What causes security misconfiguration.

Even after you think your work is done, a secure environment built by a number of stakeholders (systems administrators, DBAs, or developers) may still have weak points because not all stakeholders are responsible for upholding the security of the web app and/or infrastructure. These security deficiencies expose the organization to

significant risks in the future, including costly fines and reputational damage. Ones of the most frequent configuration mistakes is:

- Unpatched systems
- Default/ out of the box account settings (i.e. usernames and passwords)
- Unencrypted files
- Old and out of date web applications
- Unsecured devices
- Web application and cloud misconfiguration
- Insufficient firewall protection

We are all aware that your business may be affected by these dangerous security anomalies and threats due to the challenges of operating in a heterogeneous environment for businesses and a lack of security awareness. In your heterogeneous environment, you must manage security weaknesses like improper configurations at every level.

Security setup errors can occur for a number of reasons, including the following:

1. **Lack of Secure Defaults**: Systems and software frequently have default settings that place more emphasis on usability than security. Systems may become susceptible if these settings are not correctly changed during installation or configuration. Security misconfigurations may occur if default passwords are not changed, necessary security measures are not enabled, or superfluous services are not disabled.
2. **Inadequate Patching and Updates**: Security misconfigurations can result from a delay in applying security patches and upgrades. These updates frequently include configuration adjustments and security fixes to address known vulnerabilities. Failure to update software, operating systems, and firmware can expose systems to known security flaws.
3. **Improper Access Controls**: Unauthorized access or excessive permissions may be the result of configuration errors with regard to access controls. This can happen when authentication mechanisms are shaky or incorrectly designed, user accounts have excessive rights, or access controls are improperly implemented. Unauthorized users may be able to access sensitive

data or carry out unlawful actions if access rights and permissions are not clearly stated.

4. **Insecure Communication Protocols**: Confidential information may be made accessible to interception or unauthorized access by improperly configuring communication protocols, such as by employing weak encryption settings or neglecting to enforce secure communication routes. The secrecy and integrity of data transmissions can be compromised by improper SSL/TLS configurations, feeble cipher suites, or the usage of antiquated or unsafe protocols.
5. **Poorly Configured Security Settings**: To satisfy certain security requirements, security settings within software programs, operating systems, or network devices may need to be customized. Inadequate password policies, insufficient firewall rules, and improperly configured security settings can degrade system security overall and open the door for future assaults.
6. **Mismanagement of Error Handling and Logging**: The discovery and reaction to security issues might be hampered by inadequate error handling and logging configurations. It may be challenging to recognize and look into security breaches or unauthorized actions if error messages are improperly configured or if logs are not enabled and reviewed.
7. **Cloud Service Configuration**: Data breaches or unauthorized access to cloud resources can result from setup errors in cloud settings, such as incorrectly configured access controls, unsecure storage rights, or faulty implementation of security groups. Cloud service configuration mistakes can leave sensitive data and assets vulnerable to outside attackers.
8. **Lack of Security Testing and Reviews**: Misconfigurations may go undetected as a result of inadequate security testing and reviews, such as vulnerability scanning, penetration testing, or code reviews. Security flaws and incorrect setups may go undetected without a thorough examination and validation of configurations, leaving systems open to attack.

Impact of security misconfigurations

Security errors, which might be the consequence of very simple mistakes, can make an application vulnerable to attack. Because misconfiguration can occasionally

expose data, a cybercriminal may not even need to initiate an active attack. As users' access to code and data is increased, the danger to application security grows.

For instance, an improperly configured database server can enable data access through a typical online search. If this data contains administrator credentials, an attacker may be able to access other data not contained in the database or launch another attack on the company's servers.

Due to inadequately designed (or nonexistent) security, many critical and personal bits of information may be made publicly accessible online.

Organizations that experience security misconfigurations may suffer from a number of detrimental effects, such as:

1. **Increased Vulnerability to Attacks**: Security setup errors can open doors for attackers to use. These errors can lead to sensitive data being compromised, illegal access, or privilege escalation. Attackers can use misconfigurations to conduct a variety of assaults, including remote code execution, cross-site scripting (XSS), and SQL injection, which jeopardize the availability, integrity, and confidentiality of systems and data.
2. **Data Breaches and Information Exposure**: Sensitive data, such as client information, intellectual property, or financial data, can be made vulnerable by configuration errors. Data breaches can result in financial losses, reputational harm, and legal repercussions. They can also be caused by inadequate access restrictions, improperly designed storage or databases, or weak encryption settings. Personal identifiable information (PII) disclosure can also lead to regulatory non-compliance and data protection law violations.
3. **Service Disruptions and Downtime**: Critical services may be interrupted by misconfigurations, which could even result in a total system shutdown. Network connectivity can be disrupted when apps or websites can't be accessed if DNS servers, load balancers, firewalls, or network devices are configured incorrectly. Such interruptions can have an adverse effect on how a business operates, cause financial losses, and erode customer confidence.
4. **Compliance and Legal Issues**: Misconfigurations may result in a breach of legal or contractual requirements or industry norms and regulations. Due to security misconfigurations that breach privacy laws, fail to protect sensitive

data, or jeopardize industry-specific compliance standards, organizations may be subject to legal action, regulatory fines, or loss of business contracts.

5. **Reputation Damage:** A company's reputation might suffer greatly from security misconfigurations that lead to data breaches, service interruptions, or other security events. The rapid dissemination of information about security events and breaches can erode consumer trust, harm a brand's reputation, and result in lost sales and missed business prospects.
6. **Financial Losses:** Due to a number of variables, security misconfigurations can cause financial losses. This covers the expense of responding to incidents, taking corrective action, filing lawsuits, paying regulatory penalties, compensating customers, and putting a stop to business. Long-term financial effects may result from the loss of clients and possible business possibilities.
7. **Operational Inefficiencies:** Misconfigurations can result in operational inefficiencies including subpar system performance, higher resource usage, or trouble managing and sustaining systems. Ineffective setups may cause resource scaling issues, system slowdowns, and longer response times, which can all have an adverse effect on user experience and productivity.

How to prevent security misconfigurations

"It is said that "prevention is better than treatment." Up to this point, we've discussed methods for identifying and correcting these setup mistakes.

According to a Cypress Data Defense post, there are several doable actions you may take to prevent security misconfiguration.

- It's crucial to implement a repeatable hardening procedure that makes it simple and quick to deploy another environment that has been completely prepared. To boost security, the development, production, and QA environments should all be configured similarly, but with unique passwords in each. This process can be automated to build a new secure environment while also saving time.
- Patches and software upgrades should be applied frequently to each environment. Patching a golden image before deploying it is an alternative. The company should have an application architecture that is robust enough to provide security and effective component separation.

- To keep a well-organized software development cycle and detect any security misconfigurations or missing upgrades, the business must often conduct periodic audits and scans. The importance of performing application security testing at each level of the development process cannot be overstated.
- Employers play a critical role in limiting vulnerabilities. Employee education and training discuss the significance of security settings and how they may affect the organization's overall security.
- Before introducing customized code into the production environment, run it using a static code security scanner. Security professionals should also run manual tests as well as dynamic tests.

It takes initiative and the application of certain recommended practices to prevent security misconfigurations. The following actions businesses can take will help them reduce the danger of security misconfigurations.:

1. **Follow Secure Configuration Guidelines**: Follow industry-accepted security configuration best practices and guidelines. These recommendations cover how to secure web servers, operating systems, databases, network devices, and other components. The CIS Benchmarks, NIST Special Publications, and vendor-specific security configuration manuals are a few examples.
2. **Implement Configuration Management Processes**: Establish reliable configuration management procedures to guarantee configuration control and consistency. To do this, standard configurations must be established, configuration settings must be documented, and change management processes must be put in place to monitor and control configuration changes. This procedure can be streamlined and automated with configuration management solutions.
3. **Regularly Update and Patch Systems:** Keep the most recent security patches and upgrades installed on your systems, programs, and firmware. Ensure that essential security updates are immediately applied to address known

vulnerabilities and misconfigurations by implementing a proactive approach to patch management.

4. **Harden System Configurations**: To reduce the attack surface, disable or delete superfluous services, ports, and protocols. Apply the least privilege concept when determining who gets what permissions and access controls. Set up security defaults like encrypted communications, strong passwords, and strong passwords.
5. **Conduct Security Audits and Assessments:** Conduct security audits and assessments frequently to find configuration errors. To find security flaws and incorrect configurations in systems and applications, this includes vulnerability scanning, penetration testing, and configuration audits. Validate configurations against secure configuration guidelines using automated tools and manual inspections.
6. **Provide Security Awareness and Training**: Teach secure configuration techniques to system administrators, developers, and other relevant staff. Give instruction on secure coding principles, secure deployment methods, and the potential repercussions of configuration errors. Encourage a culture of security awareness throughout the company.
7. **Implement Secure Defaults and Templates:** When feasible, configure systems, programs, and gadgets to secure default settings. Use hardened system images that have pre-configured security settings or secure configuration templates. This lessens the need for human configuration and lowers the possibility of oversight or mistakes.
8. **Employ Continuous Monitoring and Logging**: Put in place reliable logging and monitoring systems to spot suspicious activity and security setup errors. To gather and analyze logs, create alerts for suspected misconfigurations, and keep an eye out for signs of compromise, use security information and event management (SIEM) systems.
9. **Conduct Security Reviews in Development**: To find and fix misconfigurations early on, perform security reviews and testing during the development process. To identify unsafe configuration procedures in

applications and system designs, this comprises code reviews, static analysis, and security testing.

10. **Regularly Review and Validate Configurations**: Review configurations on a regular basis to make sure they're accurate and following security guidelines. Verify configurations against known-good configurations and secure baselines. To speed up this procedure, use automated configuration validation tools or scripts.

Firewall

An internal network and an external network are separated by a firewall, which is a network security equipment or piece of software (such as the Internet). Its main objective is to watch over and manage incoming and outgoing network traffic in accordance with predefined security policies. For the purpose of safeguarding the internal network from unauthorized access, malicious activities, and potential risks, the firewall functions as a filter, allowing or blocking network connections depending on established criteria.

Network packets are examined by firewalls, which then apply rules to decide whether to accept or deny the traffic. Various variables, such as source and destination IP addresses, port numbers, protocols, or particular application signatures, can be used to base these rules. Firewalls can be set up to enact regulations like restricting access to specific ports or services, only permitting authorized connections, or monitoring for and stopping suspicious activity.

Firewalls can be used in a variety of ways:

1. Network Firewalls: Located at the network perimeter or within the network infrastructure, network firewalls are hardware or software-based devices. In order to manage access between various network segments or between the internal network and the Internet, they filter traffic based on IP addresses, ports, and protocols.
2. Host-based firewalls are software programs that are installed on particular PCs or servers. By regulating inbound and outbound traffic specifically for the host on which they are placed, they offer protection at the system level. In particular, host-based firewalls are helpful for protecting individual systems, especially when they are connected to unreliable networks.
3. Deep packet inspection (DPI), intrusion prevention system (IPS), application awareness, and user identity management are examples of extra security features that are combined with traditional firewall capabilities in next-generation firewalls (NGFW). Improved visibility, granular control, and threat prevention capabilities are provided by NGFWs.

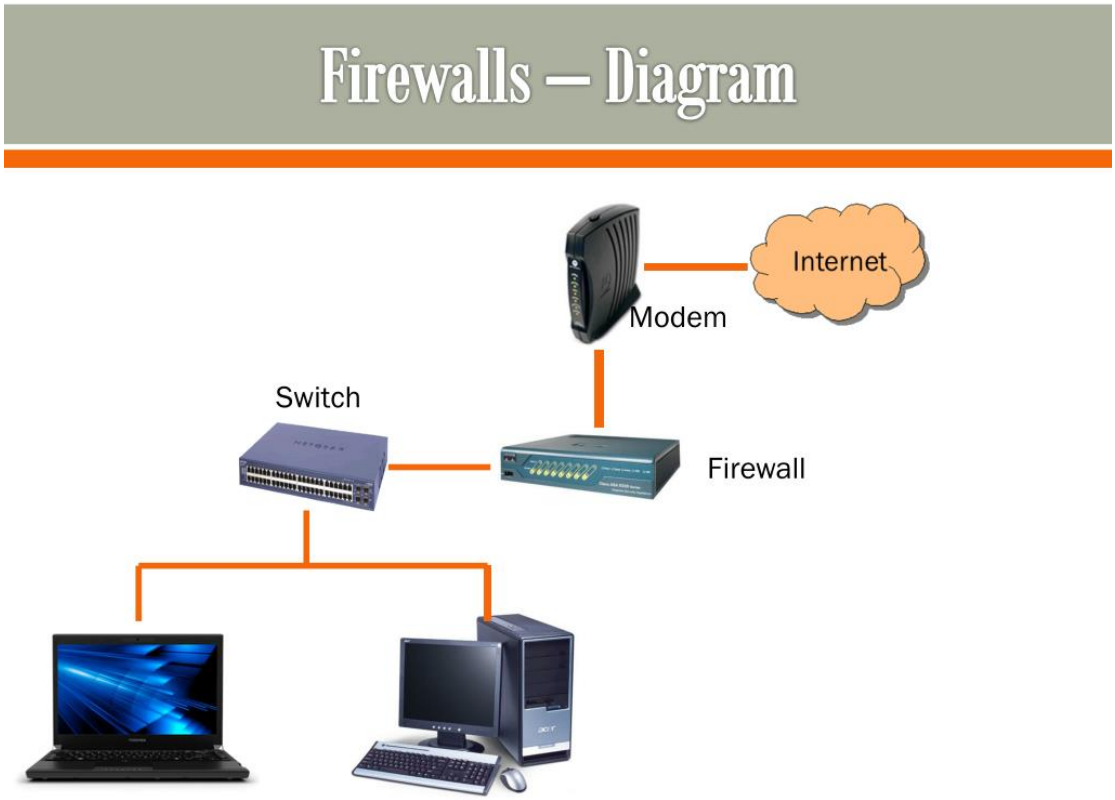

Figure 1 Firewall Diagram

How does a firewall work?

Firewall filters guard your PC from harmful data. Firewalls can protect your computer from backdoors, DoS attacks, macros, remote logins, spam, malware, and other frequent threats.

Attackers can enter vulnerable apps through backdoors, which act as "doorways." This includes operating systems that potentially have flaws that hackers could use to gain access to your computer.

When a hacker requests permission to connect to a server but the server is unable to identify the system when it responds, a denial-of-service attack is initiated. Repeating this causes the server to become overwhelmed and consume so much energy processing the numerous requests that it is unable to support actual users. In some cases, the server may need to be completely shut down. Some firewalls can authenticate connection requests, protecting your network from denial-of-service attacks.

Programs run macros, which are scripts, to do out tasks automatically. A macro may contain a series of linked operations all initiated by the same command. Hackers produce or purchase macros designed to work with particular software. It's possible for a macro to infiltrate your computer by hiding among seemingly benign data and wreck havoc on your system. Dangerous macros can be found when a firewall examines the data packets that try to pass through.

Occasionally, links to risky websites might be found in spam. These websites activate malicious software, which downloads cookies to the user's computer. The cookies create backdoors that allow hackers to gain access to the computer. Avoiding clicking on anything suspicious in an email, regardless of who the sender appears to be, can frequently stop a spam campaign. Your emails can be examined by a firewall, which can also prevent computer malware.

A firewall works by monitoring and controlling network traffic based on a set of predefined rules. It acts as a gatekeeper between the internal network and external networks, such as the Internet, examining network packets and making decisions on whether to allow or block them based on the configured rules. Here's a high-level overview of how a firewall operates:

1. **Packet Inspection:** The firewall examines the headers and content of network packets as they pass through it to learn the source and destination IP addresses, port numbers, protocols, and other pertinent information. The term "packet inspection" or "packet filtering" refers to this procedure.
2. **Rule-Based Decision Making:** The packet inspection data is compared by the firewall to a list of predetermined rules. These regulations outline the standards for approving or rejecting network connections. Various variables, such as IP addresses, port numbers, protocols, or particular application signatures, can be used to base rules.
3. **Filtering Decisions:** The firewall makes filtering judgments based on comparisons with the rules. A packet is allowed to flow past the firewall if it matches an allowed rule. A packet is lost or rejected and the connection attempt is ended if it matches a blocked or denied rule. Additionally, the firewall can be set up to log events for later analysis or auditing.

4. **Network Address Translation (NAT):** Network Address Translation (NAT) technology is frequently present in firewalls. In order to disguise the internal network architecture or save IP addresses, NAT enables the firewall to change the source or destination IP address and port numbers of packets.
5. **Stateful Inspection**: Stateful inspection techniques are used by several current firewalls. Stateful inspection monitors the state of network connections, recording details about existing connections and the sessions they are connected to. This strategy improves security and performance by enabling the firewall to make more informed filtering decisions depending on the context of the traffic flow.
6. **Application Awareness:** Application awareness is incorporated by next-generation firewalls (NGFWs). They have deep packet inspection (DPI) capabilities, which allow them to examine network packet content at the application layer. This gives the firewall the ability to comprehend particular apps and the protocols that go along with them, granting it greater granular control and the capacity to recognize and block dangers related to particular applications.
7. **Virtual Private Network (VPN) Support:** Virtual Private Network (VPN) functionality is often supported by firewalls. By tunneling network traffic across untrusted networks, this enables secure remote access or site-to-site communications.

Different types of firewalls

There are several different types of firewalls, each with its own characteristics and capabilities. Here are some of the commonly used types:

1. **Packet Filtering Firewalls:** The headers of network packets, including the source and destination IP addresses, port numbers, and protocols, are examined by packet filtering firewalls. They either permit or deny packets based on established rules. This kind of firewall is generally integrated into routers or other specialized hardware devices, operating at Layer 3 of the OSI model, which represents the network layer.
2. **Stateful Inspection Firewalls**: Stateful inspection firewalls combine the capacity to monitor the status of network connections with packet filtering.

They keep records of relationships that have been made and the sessions that go along with them. Stateful inspection firewalls can make more informed filtering judgments by comprehending the context of the traffic flow. They function at the OSI model's network layer (Layer 3) and transport layer (Layer 4).

3. **Application-Level Gateways (Proxy Firewalls):** Proxy firewalls, often referred to as application-level gateways, operate as a middleman between the client and the server. They create separate connections with the client and server and look at the OSI model's application layer (Layer 7). Advanced security features like content filtering, application-specific restrictions, and deep packet inspection can be provided via proxy firewalls (DPI). But because of the increased processing needed, they can cause latency to increase.
4. **Next-Generation Firewalls (NGFW):** Traditional firewall functions are combined with extra security measures in next-generation firewalls. They integrate advanced features like user identity management, deep packet inspection (DPI), intrusion prevention system (IPS), and application awareness. At various layers of the OSI model, NGFWs offer improved visibility, granular control, and threat prevention capabilities.
5. **Network Address Translation (NAT) Firewalls:** Network address translation (NAT) firewalls change packets' source or destination IP addresses and port numbers. They're frequently employed to protect public IP addresses and conceal the internal network layout. NAT firewalls can be used in routers or standalone firewall hardware.
6. **Host-Based Firewalls:** Host-based firewalls are programs that are installed on specific PCs or servers. They offer system-level security by regulating incoming and outgoing network traffic for the host on which they are installed. Particularly helpful for protecting individual systems while connected to unreliable networks are host-based firewalls..
7. **Virtual Firewalls:** Software-based firewalls called virtual firewalls are made to function in virtualized settings. They offer security controls for virtual networks and computers (VMs). Virtual appliances or firewalls are frequently used in conjunction with virtualization platforms.

Key components of firewall

A firewall is made up of several essential parts that cooperate to ensure network security. These elements consist of:

1. Firewall Policy: The firewall policy defines the rules and configurations that dictate how the firewall will handle network traffic. It specifies criteria such as allowed or blocked IP addresses, port numbers, protocols, and application signatures. The policy is based on the organization's security requirements and defines the behavior of the firewall.
2. Rule Base: The rule base is a collection of individual rules within the firewall policy. Each rule specifies a specific condition or set of conditions that incoming or outgoing network traffic must meet to be allowed or blocked. Rules can be based on source and destination IP addresses, port numbers, protocols, or other parameters. The rule base is evaluated sequentially to determine the appropriate action for each packet.
3. Network Interfaces: Firewalls have multiple network interfaces to connect to different network segments or zones. These interfaces enable the firewall to receive and send network traffic from and to different networks. For example, a firewall may have separate interfaces for the internal network, external network (such as the Internet), DMZ (demilitarized zone), or other network segments.
4. Packet Filtering Engine: The packet filtering engine is responsible for inspecting individual network packets and making decisions based on the defined firewall policy and rule base. It examines packet headers and, in some cases, packet contents to determine whether to allow or block the traffic. The packet filtering engine operates at the network layer (Layer 3) or transport layer (Layer 4) of the OSI model.
5. Stateful Inspection Engine: Stateful inspection engines maintain information about the state of network connections and sessions. They track the sequence and status of packets to identify established connections and ensure the integrity and security of the traffic. Stateful inspection allows firewalls to make context-aware filtering decisions and protect against certain types of attacks, such as TCP/IP-based attacks or session hijacking.
6. Logging and Monitoring: Firewalls typically have logging and monitoring capabilities to record and track network traffic and firewall activities. They generate logs that contain information about allowed and blocked connections, intrusion attempts, and other events. Monitoring tools provide real-time visibility into network traffic and firewall performance, allowing administrators to detect anomalies or potential security issues.
7. Management Interface: The management interface allows administrators to configure and manage the firewall settings. It provides a graphical user interface (GUI) or command-line interface (CLI) through which administrators can define the firewall policy, manage rules, monitor logs, and perform other administrative tasks. The management interface also includes features for software updates, firmware upgrades, and system maintenance.