Dublin Business School

excellence through learning

Computer Systems Security Assignment(B9IS103)

Security Solutions for DevTech

Module Title: Computer Systems Security (B9IS103)

Module Leader: Mr. Gordon Reynolds

Student Name: Manik Mahashabde (10518579)

Date: 05/04/2020

ACKNOWLEDGMENT

I would like to express my sincere gratitude to our module leader Mr. Gordon Reynolds for providing his invaluable guidance, comments, and suggestions throughout the entire project. I faced various difficulties in understanding some concepts used in the project but all those were clearly explained by Mr. Gordon.

TABLE OF CONTENTS

LIST OF FIGURES

1. SUMMARY

The report is divided into various sections that are overview, audit for DevTech, security policies for DevTech, recommendations for DevTech and then finally the conclusion. In the overview importance of network security is discussed. Some famous hacker attacks which happened due to the absence of cybersecurity and network security are discussed. Purpose of the report is also discussed and then finally scope is briefly covered which explain various audits, policies, and recommendation covered in details in later part of the report.

In the next section, a security audit is discussed and the steps are covered in the appendix section A1. How an audit is conducted in DevTech is discussed by implementing steps such as defining all managed devices and common threats, after this compliance of DevTech is discussed with Role-Based Access security model. Then, the assessment of the current security posture is discussed with the BitLocker encryption strategy and finally, responses and remediation actions are discussed to complete the audit.

After this comes security policies such as Acceptable Use Policy, Access Control Policy, Information Security Policy, Remote Access Policy, Disaster Recovery Policy and Incident Response Policy. Solutions of important concerns raised by directors of DevTech such as malware attack, data loss, and IT security interference with productivity are covered here.

Then some recommendations for DevTech such as using different hosts of the given subnet for guest wifi and employee wifi, implementing Active Directory instead of workgroups, adopting CIA and DiD security models in DevTech, using stack-wise topology structure for switches instead of daisy-chained, better server management techniques, non-business hours to be given to IT security team for software updates, data backups, antivirus update to avoid downtime are covered here.

Finally, in the conclusion brief of general issues at DevTech and how they're fixed by the implementation of audit, policies are covered in brief along with recommendations.

2. OVERVIEW

Due to the rise of Globalization and Industrialization, more and more companies are opening businesses. As a result, there is an increase in the new form of threats from hackers. A hacker tends to identify vulnerabilities in an organization to gain unauthorized access. Once a hacker is successful in breaching the system the confidential data of the company such as customer details, employee details, transaction details, etc. are compromised. Due to such unwanted circumstances, companies have to bear huge data loss, financial loss, etc. To deal with such situations, a company needs to have network security in place. Therefore hiring a network security officer is an essential thing now for any new organization.

For one such start-up company **DevTech**, security audit has been conducted and necessary security policies have been recommended to the company along with that the suggestions have been given to reduce security mitigation. All of these details are present in the main content of the report.

2.1 BACKGROUND

In the early days, there had been several network security attacks due to vulnerabilities of Information Security in the companies. Several attacks such as Morris Worm Attack(1988) caused $10-$100 Million

loss, Mafiaboy(2000) caused $1 Billion US Dollar damage, Google China Cyber Attack(2009), Teen of age 15 hacked NASA and US Defense Department(1999) caused $41000 loss where he was able to access confidential Emails, Data breach at Yahoo(2013) caused $35 Million where hackers stole the data of 3 Billion users*(Top 10 most notorious cyber attacks in history, 2020).* Hence due to these kinds of attacks, the strong Information Security of an organization plays an essential role.

2.2 PURPOSE

DevTech a start-up founded by four college friends has grown from 4 employees to 38 employees. They are expected to grow in the next 18 months with an employee strength of 70. The founders and directors of the DevTech are concerned about the Information Security of their company. Hence the purpose of this project is to conduct a security audit for DevTech for the next 12 months, implementing some of the security policies for them and suggesting to them some better alternatives to reduce security mitigations.

2.3 SCOPE

The scope of the project is conducting an audit and implementing security measures for a start-up company DevTech. The security measures are undertaken in three steps:

1) **Audits**: This is the process that covers the scope of software and devices in all locations to define the security perimeters of the company. Then it defines the threat of different kinds of Malware such as trojan horse, ransomware, worm, etc. After this prioritizing and risk scoring is done which covers cybersecurity trends, industry trends, organization history. Then comes the assessment of current security postures to protect the organization from cyber-attacks. Finally, response and remediation actions are taken by updating software, antivirus, firewall, and giving training to employees.
2) **Policies**: Many security policies such as Acceptable Use Policy, Access Control Policy, Information Security Policy, Remote Access Policy, Disaster Recovery Policy, Incident Response Policy are also covered in the scope. These are implemented for the management of DevTech for better handling of security issues.
3) **Recommendation**: These are also provided to the management team of DevTech to reduce security vulnerabilities. Recommendations such as using the stack-wise method for connecting switches instead of the daisy-chain method. Using a centralized Active Directory instead of Microsoft Workgroup. Also different wifi subnets for employees and guests.

3. SECURITY AUDIT FOR DEVTECH

3.1 WHAT IS AUDIT AND STEPS INVOLVED IN IT.

A security audit evaluates the security of the organization's information system by measuring how well it conforms to a set of established criteria. An audit typically assesses the security of the system's physical configuration and environment, information handling processes, software update checking, and user practices. They are used to determine regulatory compliance(*What is security audit? - Definition from WhatIs.com, 2020).*

The steps involved in a security audit are covered in **appendix section A1**.

3.2 CONDUCTING AUDIT FOR DEVTECH

As per the audit steps mentioned in sub-section 2.1.

1) The first step for the security officer was **defining all the managed devices** such as laptops, desktops, servers, and printers within DevTech. The Security officer also identified the essentials software required for the company. The reason this was done as the security officer became aware of all the devices and software within an organization.
2) After this in the 2nd step of the audit, the security officer **defined all the common threats** which could occur in DevTech to reduce risk. Issues such as malware(worms, Trojan horses, spyware and ransomware) were identified. Officer made sure that anti-virus was weekly updated automatically for all desktops as well as laptops. The security officer also reduced the surface area for the website of the company by not exposing the ports where communication is not expected(*What is a DDOS Attack & How to Protect Your Site Against One, 2020*). This reduced the chances of **DDoS(distributed denial of service)** attacks.
3) The 3rd step was **setting up compliance for DevTech for risk scoring**. The compliance ensures that whatever data a company has, it needs to define who specifically has access to which systems. For this purpose security officer implemented the **Role-Based Access** security model. Through this model access to confidential company data such as revenue, business domains, etc. were given to directors or founders of DevTech. After this team leads and office staff were given access to project data, client data of DevTech. The security officer was responsible for handling servers, data backup from systems, installing software requested by the employees. Finally, employees consisting of developers or sales team members were given basic and non-confidential information access of DevTech. This can be depicted in figure 1 below.

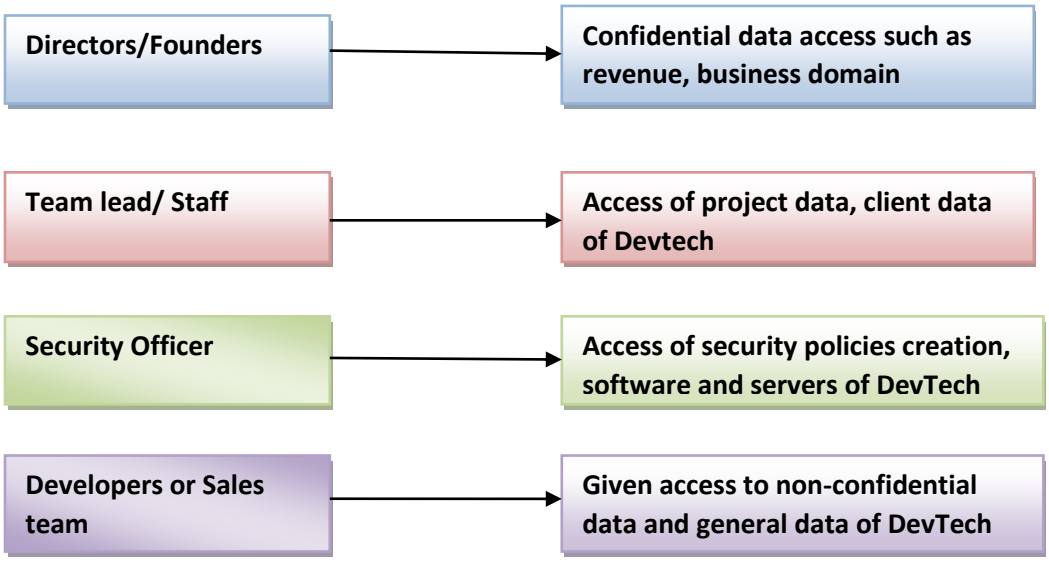

Figure 1: RBA Security Model for DevTech

4) In the 4th step i.e **assessing the current security posture** security officer made sure that data of every employee of DevTech is encrypted using **BitLocker** software. Instead of the director's and founder's data only being encrypted as per previous policy. BitLocker is Microsoft's encryption

program for Windows that can encrypt your entire drive, as well as help, protect against unauthorized changes to your system such as firmware-level malware (*Paul*, *2020*). If data of all employees are not encrypted and the system got stolen then it is very dangerous.

The security officer also changed an existing policy in DevTech by not permitting employees to install software on their own because sometimes employees might be accessing data from **untrusted websites** and **malicious attacks** can occur at that time. Instead, all essential Softwares are already pre-installed on their systems. If they needed any new software they have to raise a request for it and that particular software will be installed by the security officer.

The administrator rights were also revoked for all employees of DevTech so that in case of malware attack, the hacker cannot get admin privileges, install new programs on their own, moving sensitive data to a different drive. The security officer also revoked the C-drive access for all employees. The security officer also made sure that all the essentials files on the were also stored on all the servers.

5) The final step for audit completion i.e **responses and remediation actions** was done by the security officer consists of implementing automatic weekly data backups of laptops and desktops because if in case there is a loss of system due to damage then data can be recovered from the backup. **Employee training** was organized in which they were told to **change the password every 3 months** and guides were given to set up a complex password, how to detect and avoid phishing emails. The security officer makes sure that everyone on the network has the latest software updates and patches, firewalls, etc.

4. SECURITY POLICIES FOR DEVTECH

Once the audit was completed security officer reviewed and implemented some security policies suitable for DevTech.

4.1 ACCEPTABLE USE POLICY FOR DEVTECH

An AUP stipulates the constraints and practices that an employee using organizational IT assets must agree for accessing the corporate network or the internet. The new employees joining DevTech have to **read the AUP policy** and **sign it** to get access to the network ID. In this policy employees of DevTech are *not allowed to access social media websites* such as Facebook, Instagram, etc. from the company network. Apart from this employee are also *not allowed to have lunch at their desk*. The reason for implementing this policy is that employees should not put any sensitive data of DevTech on social media and employees also maintains hygiene at the workplace.

4.2 ACCESS CONTROL POLICY FOR DEVTECH

The ACP outlines the access available to employees regarding an organization's data and information systems. Employees are given guidelines on rules involved in setting up the password such as the use of **special characters** and a **minimum length** of the password to be set. They have been also told to use at least one **upper case alphabet** and some **lower case alphabets**. They have been also guided the use of **numeric value** in the password. Through this policy, DevTech employees who use corporate systems such as laptops are told to lock them properly in the office drawers while leaving. The reason for

implementing this policy is that employees should have a set of guidelines for the password set up and they should also know about the proper handling of unattended systems.

4.3 INFORMATION SECURITY POLICY FOR DEVTECH

This policy ensures that all employees who use information technology assets of the DevTech within the network or breadth of the organization comply with the stated rules and guidelines. The policy states that if there is a **loss of any asset** by an employee then he or she will be **held responsible** for it. They are also not allowed to email any company data to any non-corporate or personal email ID to prevent loss of sensitive information.

The reason for implementing this policy is if in case the employee forgot to lock the laptop while leaving the office or employee lost the office laptop while taking it home then the employee is held responsible for it and the employee also should not share project or company data on their home email.

4.4 REMOTE ACCESS POLICY FOR DEVTECH

The remote access policy outlines and defines acceptable methods of remotely connecting to an **organization's internal networks**. Through RAP policy employees of DevTech are not given permissions to give remote access of their system to someone outside of the DevTech network. The reason for implementing this policy is that the outsider should not have access to DevTech data.

4.5 DISASTER RECOVERY POLICY FOR DEVTECH

Disaster recovery policy in DevTech ensures that if in case of any disaster such as physical damage, malware attack, data loss. Then data is taken from the backup servers of DevTech. This policy is implemented to **reduce** the **director's fear of data loss and malware attacks**. Through this policy, DevTech ensures that there is no major business impact.

4.6 INCIDENT RESPONSE POLICY FOR DEVTECH

The reason for implementing this policy in DevTech is having a good response for incident creation and handling for limiting the damage to business operations, customers and reducing recovery time and costs in case of any issue to the organization.

The security policies recommended for DevTech are shown in figure 2:

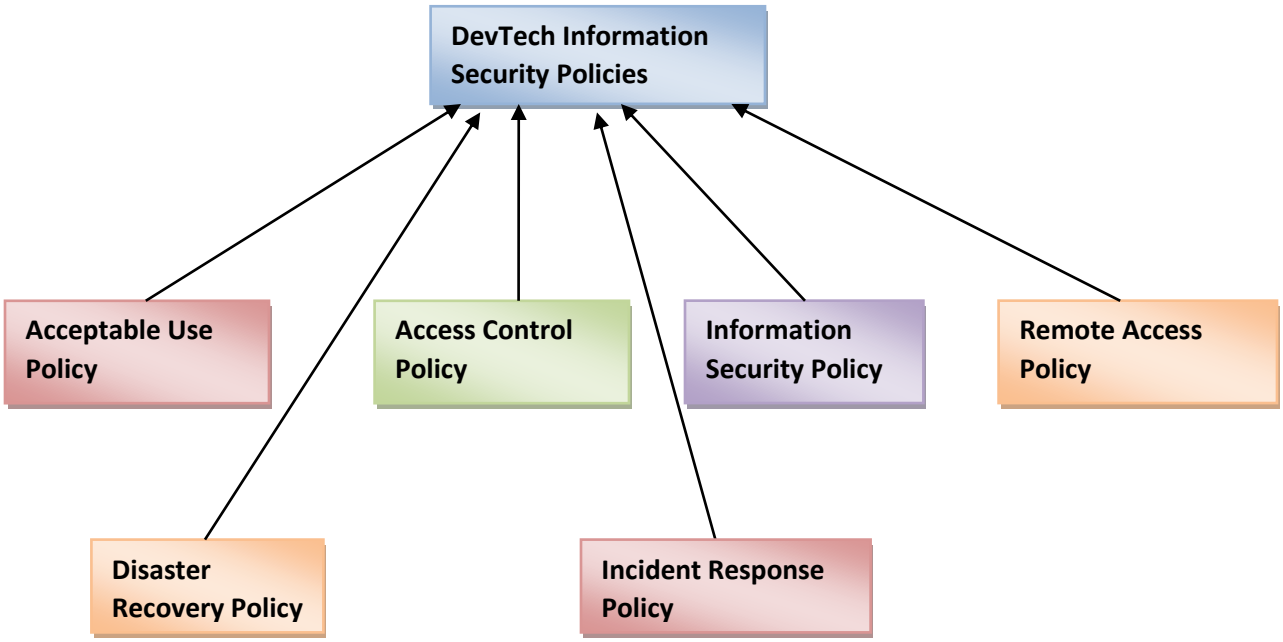

Figure 2: Security Policies in DevTech

All the above policies are used as part of official IT documentation for DevTech. This includes operational guides, company IT policies, company IT processes and other general IT documentation for future perspectives.

5. RECOMMENDATIONS FOR DEVTECH

After completion of the audit and policies, the security officer gave the following recommendations.

5.1 DIFFERENT HOSTS OF GIVEN SUBNET

In the current methodologies of DevTech, it is mentioned that the network is based on a single IP 192.168.10.0/24. This subnet is used for company laptops, servers, printers, wifi, and guest wifi. But for security purposes, the subnet for guest wifi should be at a different host than DevTech's internal wifi.

The given IP address 192.168.10.0/24 is a class C IP address. After doing the subnetting of this IP, the security officer found that it has only one valid subnet(2^0 as no 1 in the last byte) **192.168.10.0** as per given **CIDR(/24)**. Furthermore, **254 valid hosts**(8 zeros in the last byte) are possible ranging from **192.168.10.1** until **192.168.10.254**. Finally, the broadcast address is **192.168.10.255**. Hence, the security officer recommended the directors to have different hosts for guest wifi and company wifi and also to keep a **firewall between both the hosts** for additional security. The reason for this recommendation is to perform load managing capability at different hosts and also the better security during wifi access by guests as well as employees of DevTech.

5.2 SWITCH TOPOLOGY STRUCTURE CHANGE

The current 16-port daisy-chained network hardware of switches is inefficient as if one among the three 16-port network switch is failed the other two network switches won't be able to communicate. Hence, the security officer recommended the **stack-wise topology protocol** for connecting switches. Stack-Wise operates as a switch-to-switch Ethernet link and supports quite higher speeds than the daisy-chained on the switch. Because SW ports can pass management-plane information as well as data-plane, the two separate devices can operate as one (*Question: What is the difference between Daisy-Chain and Stack-wise (stack-able switches)? 2020*). The reason for this recommendation is to increase efficiency in a network topology.

5.3 DEDICATED TIME SLOT FOR IT SECURITY

The security officer also recommended DecTech directors that a separate time slot to be dedicated to the IT security for the software update, software backup, antivirus update, firewall update, system update so that the security officer or IT security does not interfere with productivity and/or system usability. This time slot should be during non-business hours or weekends so that there is no business impact. During this time slot, the security officer will also ensure that all PC are in the same state regarding updates.

5.4 ACTIVE DIRECTORY INSTEAD OF WORKGROUPS

In DevTech the operating systems are connected using four workgroups. This method is in-efficient as a workgroup is a peer to peer network with no central authentication. Each computer in the workgroup acts as a client as well as a server. When a user in a workgroup wants to access another user's computer or even a shared resource like a file, they need to create their username and password on the other user's computer.

Whereas Active Directory ensures better security as it is possible to set up degrees of permissions for different users or groups of users. If a user wants to access another computer on the domain, they don't need to create another account on that computer. All login and access requests by users are managed by a domain controller (DC) that runs AD. A DC is a centralized server that responds to all such requests and is effectively a security gatekeeper for the network. Both authentication and authorization are done by DC (*Fundamentals of Active Directory*, *workgroups and domains*, *2020*). Hence, this is the reason the security officer recommended the use of AD-DS instead of workgroups. There also needs to be a regular backup of the centralized server so that company's data loss doesn't occur in case of any issue at the primary server. Figure 3 is shown as:

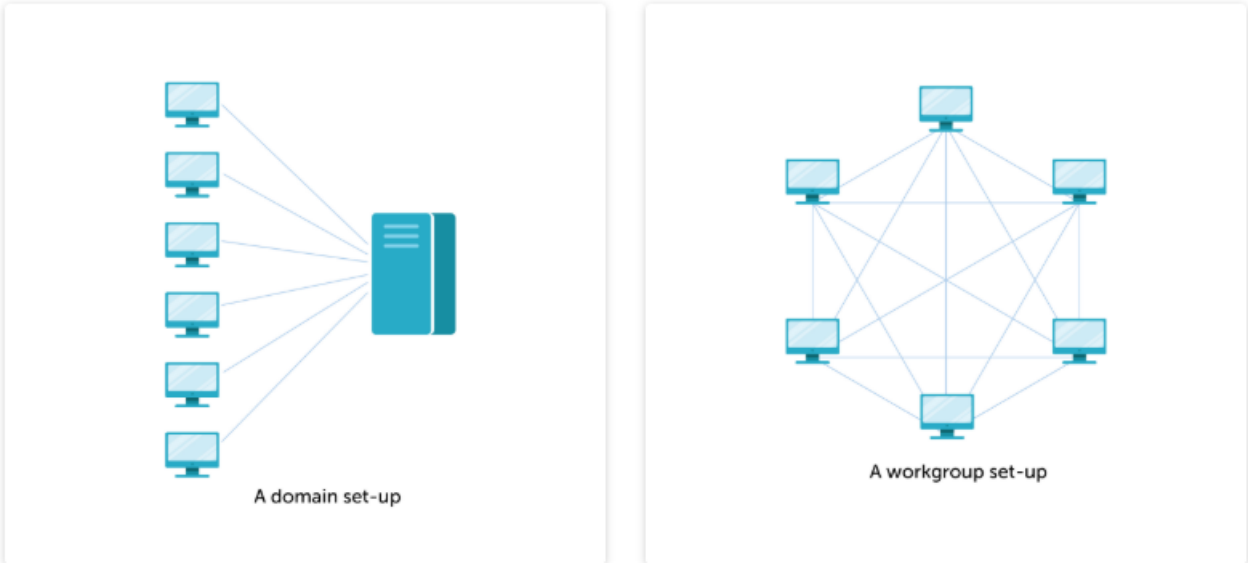

Figure 3: AD-DS vs Workgroup

5.5 BETTER MANAGEMENT OF SERVERS

The security officer also suggested that there needs to be a separate room for all the 6 servers storage. Employees should not be allowed to enter the room for security purposes. Only the security officer should have the key to the room and apart from this only officer should have administrator access to the server and not the employee of Devtech. Instead of storing the data into the server by using an external hard disk, AD-DS should be installed on all the servers for data synchronization(original data can be restored) as there can be a security breach in case of damage or loss of external hard drive. The security officer should only be responsible for data storage and retrieval from the server every weekend during non-business hours.

5.6 CIA and DiD SECURITY MODEL IMPLEMENTATION

Security officer strongly suggested the use of the CIA and DiD security model within DevTech. CIA stands for Confidentiality, Integrity, and Availability (*What is the CIA Triad?*, *2020*). Confidentiality means information kept must be available only to authorized individuals. Confidentiality can be managed by including access control lists, volume and file encryption, and Unix file permissions in DevTech. Integrity ensures that systems are designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an unauthorized person makes a change it shouldn't damage the system and can be reverted. Finally, Availability refers to the availability of data to authorized users.

DiD stands for defense-in-depth which ensures multiple layers of security by using different defenses together, such as firewalls, malware scanners, intrusion detection systems, data encryption, and integrity auditing solutions, which effectively close the gaps that are created by relying on a singular security solution (*What is Defense in Depth?*, *2020*). Although most of the security principles of these security models were already covered by the security officer in audit and policies. The security officer

told the directors that these security models need to be implemented even after a 12 months (*Sheehan, 2020*).

6. CONCLUSION

This report concludes that the security officer hired by directors and founders of DevTech has successfully conducted a security audit. Before hiring the security officer, there were various flaws in the existing methodology of DevTech. Administrative rights of systems, as well as servers, were given to employees. The antivirus was not updated regularly. Employee data was not encrypted. Regular data backup was missing. As DevTech planned to expand to 70 employees in the next 18 months directors were concerned about malware attacks, data loss, business impacts for DevTech. But after the audit issues like anti-virus updates, system state, data backups, malware protection, employee data encryption, etc. were fixed.

Official IT documents and policies were absent in DevTech earlier. Hence, the security officer implemented 6 policies which are Acceptable Use Policy, Access Control Policy, Information Security Policy, Remote Access Policy, Disaster Recovery Policy, Incident Response Policy. These policies make sure that employees of DevTech are aware of the rules and regulations of DevTech.

Finally, there are some recommendations given by the security officer regarding having different hosts of the given subnet for guest wifi and employee wifi, implementing Active Directory instead of workgroups, adopting CIA and DiD security models in DevTech, using stack-wise topology structure for switches instead of daisy-chained, non-business hours to be given to IT security team for software updates, data backups, antivirus update to avoid downtime.

BIBLIOGRAPHY

ARN. 2020. Top 10 Most Notorious Cyber Attacks In History. [online] Available at: <https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/> [Accessed 5 April 2020].

SearchCIO. 2020. *What Is Security Audit? - Definition From Whatis.Com*. [online] Available at: <https://searchcio.techtarget.com/definition/security-audit> [Accessed 5 April 2020].

Amazon Web Services, Inc. 2020. *What Is A DDOS Attack & How To Protect Your Site Against One*. [online] Available at: <https://aws.amazon.com/shield/ddos-attack-protection/> [Accessed 5 April 2020].

Paul, I., 2020. *A Beginner's Guide To Bitlocker, Windows' Built-In Encryption Tool*. [online] PCWorld. Available at: <https://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html> [Accessed 5 April 2020].

reddit. 2020. *Question: What Is The Difference Between Daisy-Chain And Stack-Wise (Stack-Able Switches)?*. [online] Available at: <https://www.reddit.com/r/ccna/comments/8ks6bd/question_what_is_the_difference_between/> [Accessed 5 April 2020].

Windows-active-directory.com. 2020. *Fundamentals Of Active Directory, Workgroups And Domains*. [online] Available at: <https://www.windows-active-directory.com/fundamentals-of-active-directory-workgroups-and-domains.html> [Accessed 5 April 2020].

Forcepoint. 2020. *What Is The CIA Triad?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/cia-triad> [Accessed 5 April 2020].

Forcepoint. 2020. *What Is Defense In Depth?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/defense-depth> [Accessed 5 April 2020].

Sheehan, K., 2020. *Security Architecture: CIA, CVSS, Cpus And Defense In Depth*. [online] SecureDBA. Available at: <https://www.securedba.com/securedba/2009/05/security-architecture-cia-cvss-cpus-and-defense-in-depth.html> [Accessed 5 April 2020].

APPENDIX

A1 STEPS IN AUDIT

The audit is generally done in 5 steps:

Step 1: The scope of the security perimeter.

This step includes defining all the managed devices (computers, machines, devices, and databases that belong to the company directly) and unmanaged devices(personal laptops, gadgets or BYOD, IoT connected devices and machines). Finally, it includes all wired, wireless and VPN connections.

Step 2: Defining the threat.

Common threats to be defined are:

- Malware(worms, Trojan horses, spyware and ransomware).
- Employee exposure(frequent password change by the employees, protection against phishing attack and scams.
- Malicious Insider:- Risk of theft or misuse of sensitive information.
- DDoS attack:- It happens when multiple systems flood a targeted system such as a web server, overload it and destroy its functionality.
- BYOD and IoT:- these devices tend to be somewhat easier to hack and therefore must be completely visible on the network.

Step 3: Prioritising and risk scoring.

Common factors for priorities and risk scoring are:

- Compliance:- It includes the kind of data that is to be handled, whether the company stores/transmits sensitive financial or personal information.
- Organization history:- – If the organization has experienced a data breach or cyber-attack in the past.
- Industry trends:- understanding the types of breaches, hacks, and attacks within your specific industry should be factored in when creating your scoring system.

Step 4: Assessing the current security posture

It refers to the overall security status of the organization's assets.

- These assets include hardware, software, networks, services, and information.
- Controls in place to protect the organization from cyberattacks.
- An initial security posture should be available for each item included in the initial scope definition.
- With the right access control systems in place, no internal biases affect your initial audit.
- Finally, making sure that all the connected devices have the latest security patch.

Step 5: Responses and Remediation actions

Based on the result of steps 1-4, several solutions to be included are:

Network monitoring:

- To protect from cyber offenders certain software that gives alerts, monitors, security patches, the antivirus should be used.
- Establishing continuous automated monitoring and creating automated risk assessments will lead to improved risk management.

Software Updates:

- Making sure that everyone on the network has the latest software updates and patches, firewalls, etc.

Data backups:

- Data Backups and Restore Testing is crucial and can be relatively simple to establish. This will ensure minimal damage to the organization in case of malware or physical cyberattack.

Employee education:

- Training such as how to stop phishing campaigns, password and password complexity, multi-factor authentication should be given to employees.