Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 08 August-2024, Page No.- 4848-4862

DOI: 10.47191/etj/v9i08.34, I.F. – 8.227

Solutions for Mobile Devices Security Concerns, Aden Refinery Company (A.R.C) Case Study

Eng. Mohammed Badeh[1], Dr. Nabil Munassar[2]

[1]Lecturer at University of Science and Technology (U.S.T), Staff at Aden Refinery Company (A.R.C)

[2]Professor at University of Science and Technology (U.S.T), Dean of Electronic and Distance Learning

ABSTRACT: Companies that allow their employees to use mobile devices for work purpose, they suffer from cybersecurity challenges such as virus or malware, download illegal content, poor authorization and authentication, etc. These challenges need solutions or controls to solve or mitigate them. In this paper, there are two objectives. The first aim is to know which of the security controls were asked in the questionnaire used in the A.R.C. The second objective is to know which security scenarios the IT department uses to protect the information from potential mobile device security concerns. A descriptive methodology was employed in this study. Data were collected from forty people in the IT department at Aden Refinery Company through a questionnaire. The results show that some security controls, such as antivirus/ antimalware, backups, firewalls, and policies, are used in the A.R.C.

KEYWORDS: Mobile Devices; BYOD; Cybersecurity Solutions.

1. INTRODUCTION

In many cases, BYOD presents a serious risk to an organization if the IT department does not appropriately control it. "Shadow IT" describes equipment that poses a security risk but has not received company certification. These devices' incapacity to be watched over or shielded from malicious software and other security risks is the root of the security problem. Because of this, a security policy is necessary to establish when employees should use company-provided devices and whether or not personal devices may be used at work **[1]**. With the emergence of new features and technologies, mobile devices are becoming indispensable parts of every aspect of day-to-day business operations. Furthermore, taking into account that mobile networks are now fully connected to the Internet. Using BYOD can lower IT infrastructure expenses and improve employee satisfaction. Mobile devices are not well-secured compared to computers and computer networks, and people rarely consider updates and patches. Because employees use their personal mobile devices to access company data and apps, mobile safety has become a major issue with BYOD **[2]**. Employees can now access corporate information systems through their devices, which presents a serious security risk to confidential data in the event that the device is stolen or shared with malevolent individuals **[3]**. Based on the security controls that the IT department staff has employed, this study offers A.R.C. a comprehensive strategy. The goal of this study is to know which security scenarios are used in the IT department to protect the information from potential mobile device security concerns. The Aden Refinery Company (A.R.C.) contracted with Symantec to use its antivirus / antimalware to protect its desktop and laptop computers. The IT department uses a Dell Sonic Well firewall, which includes IDS/IPS, to protect the connection to the internet and also to implement the policies in it. All the switches, the Layer 3 core switch, and the servers are from the HPE company. The rest of the paper is organized as follows: The study's literature is presented first, and then the methodology is explained. Next, the results of the study are presented and discussed. After that, the conclusion of the study is outlined. Lastly, the limitation of the study.

2. RELATED LITERATURE:

2.1. Mitigation and Solution of BYOD IT Risk

The landscape of mobile technology is evolving quickly, and enterprises need to get ready for a new Mobile Device Management (MDM) era. The process of getting ready will involve creating a policy for managing personal mobile devices that are utilized for work. MDM is essential for safeguarding devices used in BYOD adoption. The device can be provisioned via MDM via Over-The-Air (OTA) or alternative techniques. "OTA" describes the process of sending provisioning data or update packages for firmware or software updates to a mobile device via wireless mechanisms. In order to improve visibility throughout the company, other types of MDM communicate with directory services like Microsoft Active Directory (MAD). The device should have the necessary configurations, software, and certificates installed in order to support BYOD security standards and controls. By depending on comprehensive software solutions

that businesses can use to lock down, control, encrypt, and enforce policies, MDM will help support the mobile device [4].

It's possible to monitor activity and implement policies. Employers can prioritize information delivery based on user needs and maintain control over the resources made available to their staff by instituting a BYOD policy [5]. Organizations can manage risks, safeguard mobile devices, and handle any potential legal ramifications more methodically and comprehensively with the help of a BYOD policy [6]. The following section explains the importance of a BYOD policy.

2.1.1. Mobile device policy

It is possible to monitor and enforce policies. Employers can manage the resources that employees have access to and prioritize information delivery based on user needs by putting in place a BYOD policy [7]. According to Phyllis and Moore [8], the implementation of a Bring Your Own Device (BYOD) policy will furnish the organization with enhanced systematization and integration of protocols for handling potential legal implications, managing threats, and maintaining mobile devices. The significance of incorporating controls into the current information security policy or having a policy for mobile devices will guarantee that risks are taken into consideration and handled properly. Prior to deciding on the policy's parameters and the types of mobile devices that will be covered, Prior to deciding on the policy's parameters, the company should ascertain the kind of mobile devices that its employees are utilizing for work. The company can then choose which kind of device to cover under the policy and make it obvious which devices it will and won't support, along with the data that can be accessed on those devices [9]. The limitations of access control and protection of organizational information resources by both internal and external users must be addressed by the BYOD policy [10] The implementation of a BYOD policy can aid an organization in effectively accounting for and managing risks and controls.

2.1.2. BYOD Security Solutions

The implementation of safety programs, worker behavior codes, and well-structured administrative guidelines are the three key components that increase the adoption rate of BYOD in businesses. According to A. French, C. Guo, and J. Shim [11], each of these elements plays a part in the overall success of BYOD. Organizations need to use both technical and non-technical technologies to address the security issues posed by BYOD. According to studies, businesses could also reevaluate the effectiveness of worker awareness campaigns, technical controls, policies, procedures, and safety and privacy regulation mechanisms in order to address the growing list of legal, safety, and privacy concerns related to BYOD implementation [12].

2.1.3. Non-technical approaches

Non-technical approaches that can be used include security culture, security awareness education, security strategies, and policy.

2.1.3.1. Security Awareness Education

When it comes to BYOD, there is a deficiency in knowledge regarding security and privacy [12]. Security awareness and education programs improve policy adherence throughout an organization by increasing worker knowledge of BYOD hazards and acceptable applications [13]. Businesses need to set up security and education policies to protect their data on people's devices. If workers are not informed about the risks associated with BYOD, they may commit numerous mistakes that could result in cyberattacks and security flaws. According to M. Ratchford, P. Wang, and R. Sbeit, [14], security and privacy awareness and education programs are essential in reducing BYOD security concerns. Employees should understand the consequences of breaking the BYOD policy, as well as the privacy trade-offs associated with it, such as monitoring personal devices, [15].

2.1.3.2. Security Culture

Security culture is the collective behavior, relationships, and attitudes of employees toward safety and risk mitigation. According to research, it is essential to create a safety compliant principle for workers to understand the importance of protecting information assets and their role in doing so, as different value systems can have an impact on how people think and act about security [6]. Employees may choose to ignore policies because they believe that safety procedures impede their ability to complete their work. This human mistake could lead to security lapses. Employees can carry out their designated tasks and utilize BYODs in a manner that improves risk mitigation and information asset preservation by endorsing a company culture that places a premium on security [13], [16].

2.1.3.3. Policies

BYOD-specific policies will cover authorized utilization, surfing, worker obligation, and incident management. These policies will set the framework for the management and upkeep of the initiative [13]. To maintain the policy, organizations must use essential technologies to draw a line between work and personally identifiable data. These tasks will be carried out by device management systems, which will support device collaboration and the security of shared resources [6] states that BYOD policies ought to contain instructions on data classification, antivirus software, encryption, user passwords, mobile device security, and wireless access. Protection of privacy and remote working, along with a security breach and its reaction. One important strategy for managing the BYOD environment is to establish explicit information security and privacy policies and to integrate or support the other BYOD control domains [15].

2.1.3.4. Security Strategy

One study claims that IT teams can save expenses and improve employee morale and motivation by implementing a well-thought-out BYOD strategy. According to David

Njuguna and Wambui Kanyi [13], a well-defined strategic BYOD plan fosters innovation, employee satisfaction, cost savings, and asset protection through the evaluation of opportunities and risks, selection of an appropriate platform, enforcement of policies and controls, recovery plans, mitigation, and business continuity.

2.1.4. Technical approaches

Various methods and strategies have been devised to provide software tools and security measures that aid in reducing the risks and obstacles. Enterprise Mobility Management (EMM), Network Access Control (NAC), Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Information Management (MIM) are some of the methods and strategies used for BYOD security management. These initiatives support worker-owned device management for both personal and work-related purposes [17]. Other steps are taken in addition to BYOD management strategies to guarantee information integrity, confidentiality, and authenticity when BYOD is implemented in the workplace. These actions consist of;

2.1.4.1. Secure browsing

While a virtual private network is a great way to safeguard company information, managers can also let employees access corporate intranet sites by using the AirWatch Browser on their devices. With a single sign-on and app tunneling, users can connect the AirWatch Browser to corporate intranets and external Web filters [18].

2.1.4.2. Separation Techniques

Methods based on virtualization and the operating system (OS) that divide work and personal space have demonstrated potential. In a BYOD, sensitive company information and private applications are restricted and run on the same device. A BYOD program needs to make sure that the security of the company workspace is not compromised by the personal workspace of each employee. The privacy of the personal user area should never be compromised in an enterprise work environment. Being able to separate the two environments on the same mobile device becomes essential for a successful BYOD design. Techniques including virtual mobile platforms, dual boot, and virtualization must be used in order to meet the separation goal [18].

2.1.4.3. Consolidated control

Compacted configuration control, data sanitization, and compliance control are all included in BYOD control mechanisms. An administrator can also effectively identify every activity. BYOD misuse is identified through a dashboard. This facilitates the BYOD policy's enforcement.

2.1.4.4. Blocking and wiping remotely

To protect the company's sensitive and intellectual property, restrictions are placed whenever people use their personal devices for work-related purposes. Remote wiping and blocking are carried out in response to lost or stolen devices, policy violations, and employee terminations. Nevertheless, wiping or disabling a device could lead to its destruction or result in the loss of a person's data. Employees need to be aware of the consequences when they remove or block data from apps installed on their personal devices. Permission forms and policies regarding the use of personal devices must include all of these terms [6]. Remote wiping is the last option in cases where a device is lost, confiscated, or the owner departs the company. The process involves first logging onto the device and then wiping out all of the company's data and applications [13]. Some commercially available MDM and MAM solutions already come with remote wiping capabilities [11].

2.1.4.5. Antivirus, anti-malware, and spyware

One of the most well-known first lines of defense for safeguarding information systems is the use of antivirus and anti-malware software. Basically, anti-virus or anti-malware software or applications are available for every device and security solution. Anti-virus and anti-malware programs range from freely available trial versions that can be downloaded from numerous websites to enterprise versions that require substantial financial outlays and extensive licensing. They also differ in that they can be heuristic or signature-based and sometimes even incorporate AI. But their effectiveness is only as strong as their capacity for updating. The competition between malware and viruses and anti-virus and anti-malware is head-to-head. New viruses and malware are racing to take advantage of any zero-day vulnerability. In order to minimize damage, anti-virus and anti-malware programs work to prevent attacks or identify them as they occur [19]. Anti-virus and anti-malware software are crucial to the defense-in-depth of an organization's information systems when it comes to BYOD in remote work environments. Organizations should pay for their employees' anti-virus and anti-malware software and ensure that it is updated on a regular basis, according to numerous security experts and researchers [20].

2.1.4.6. Identification & Authentication

Identification and authentication are effective ways to safeguard an organization's trusted network environment. The organization's trusted networks cannot be adequately protected by the current level and type of identification and authentication [4]. Guidotti, A., [21] asserts that employers require additional tools for employee identification and authentication. To secure digital transactions, digital identity and digital authentication became essential. Businesses were attempting to keep operations at the same level, but cybersecurity was a major problem. Guidotti, the author, enhanced identification and authentication with integrity. Different multi-factor authentication methods (something you know, something you have, something you are, where you are, something you do) were mentioned by Guidotti. Prior to the authentication process, Guidotti emphasized the significance of identification. Several methods of identification include the use of a picture ID (passport or national identity card), utility bills, real-time video, digital ID providers, and connections to other businesses (bank accounts, for example). The use of biometrics in the

authentication process was recommended by author Guidotti. An article about using identity verification to secure assets was published by Amper, R., [22] Organizations were attempting to manage and validate data, according to the article.

biometrics tools in the identification and authentication process for their customers and staff, as well as network access. In contrast to outdated techniques like using a PIN, the author contended that biometrics are difficult to hack and foster trust. But the author also raised concerns about user experience and privacy when utilizing biometrics. Engle, M., [23] concentrated on the topic of passwords in the identification and authentication process and employers' hopes that workers would remember them, not use them for personal or work-related access, and keep them safe from hackers. Additionally, he stated that two-factor authentication is merely a stopgap measure for this procedure. But he was adamant that we should stop depending on passwords. This article's password-less solution uses tokens and registered devices to authenticate users rather than the user's knowledge.

2.1.4.7. Virtual Private Networks (VPN)

Abhijith, M., and Senthilvadivu, K., [24] described how VPNs guarantee secure connections to the organization's trusted networks by utilizing a variety of technologies, including firewalls, authentication, encryption, and tunneling. VPNs do not include firewalls; instead, firewalls are typically part of commercial solutions that are made available to businesses. The authors emphasized that an organization runs the risk of cybersecurity when using VPNs without firewalls. In an article about Zscaler's [25] VPN Report and Venkat [26] revealed that 97% of the enterprises surveyed believed that VPNs are vulnerable to cyberattacks. The study evaluated numerous factors associated with VPN use and outlined numerous challenges that organizations encounter. It highlighted the fact that 95% of survey participants use a VPN service to gain remote access and that most companies have more than three VPNs. The report explained that 80% of the companies are working on switching to a zero-trust architecture to mitigate risks related to the use of VPNs.

2.1.4.8. Updates & Patches

Employees of organizations who work remotely and use their personal devices for work are required to update and patch these devices on a regular basis. Companies do not apply the required updates and patches to their workers' devices in a timely manner, which could lead to the incorrect correction of bugs that could compromise their reliable networks. [4].

2.1.4.9. Encryption

To secure information, organizations encrypt employee devices, data in transit, and internal communications as needed. Encryption is not used by organizations to secure information in internal communications, employee devices, or data in transit. [4].

3. METHODOLOGY

This study employed a descriptive methodology using a survey. The research questions were addressed through a descriptive method to view the risks in the IT department and the challenges that impede the adoption of BYOD. The participants of the study consisted of IT department professionals. Data were collected from forty people through a questionnaire instrument. The collected data was analyzed using descriptive statistical analysis.

4. RESULTS AND DISCUSSIONS

4.1. BYOD Solutions:

The targeted population was asked which of these ten security controls is used by their company to protect its information, and the answers are shown in Table 1.

Table: Technical security controls

NO	Q.1. Technical Security Controls in the Protection of BYOD	YES	NO	Median	Std. Deviation
1	Antivirus/Antimalware	40	0	20	28.3
2	Backups	40	0	20	28.3
3	Data loss prevention	28	12	20	11.3
4	Disabling Administrator Accounts / Limiting User Account Privileges	36	4	20	22.6
5	Encryption	4	36	20	22.6
6	Firewall	40	0	20	28.3
7	Identification / authentication	37	3	20	24
8	Secure Internet Connection and Wi-Fi	32	8	20	17
9	Strong Passwords	23	17	20	4.2
10	VPN	23	17	20	4.2

The first security control was antivirus, which has been chosen by all the participants, and this represents 100%. The median of the first security controls equals 20, and the standard deviation equals 28.3. The second control was backups, which have been chosen by all the participants, and this represents 100%. The median of the second security

control equals 20, and the standard deviation equals 28.3. The third security control was data loss prevention, which has been chosen by twenty-eight people, and this represents 70%. The other twelve people did not choose data loss prevention, which means that control wasn't implemented in the company, and this represents 30%. The median of the third security control equals 20, and the standard deviation equals 11.3. The fourth security control was disabling the administrator account / limiting the account privileges. It has been chosen by thirty-six people, and this represents 90%. The other four people did not choose disabling the administrator account / limiting the account privileges, which means that the company didn't implement this control, and this represents 10%. The median of the fourth security control equals 20, and the standard deviation equals 22.6. The fifth security control was encryption, which has been chosen by four people and represents 10%. The other thirty-six people did not choose encryption, which means that control wasn't implemented in the company, and this represents 90%. The median of the fifth security control equals 20, and the standard deviation equals 22.6. The sixth security control was the firewall, which has been chosen by all the participants, and this represents 100%. The median of the sixth security control equals 20, and the standard deviation equals 28.3. The seventh security control was identification/authentication, which has been chosen by thirty-seven people, and this represents 92.5%. The other three people did not choose identification or authentication, which means that control wasn't implemented in the company, and this represents 7.5%. The median of the seventh security control equals 20, and the standard deviation equals 24. The eighth security control was a secure internet connection and Wi-Fi, which have been chosen by thirty-two people; this represents 80%. The other eight people did not choose a secure internet connection and Wi-Fi, which means that control wasn't implemented in the company, and this represents 20%. The median of the eighth security control equals 20, and the standard deviation equals 17. The ninth security control was strong passwords, which have been chosen by twenty-three people and represented 57.5%. The other seventeen people did not choose strong passwords, which means that the company didn't implement this control, and this represents 42.5%. The median of the ninth security control equals 20, and the standard deviation equals 4.2. The tenth security control was VPN, which has been chosen by twenty-three people, and this represents 57.5%. The other seventeen people did not choose VPN, which means that the company didn't implement this control, and this represents 42.5%, as displayed in Figure 1

.

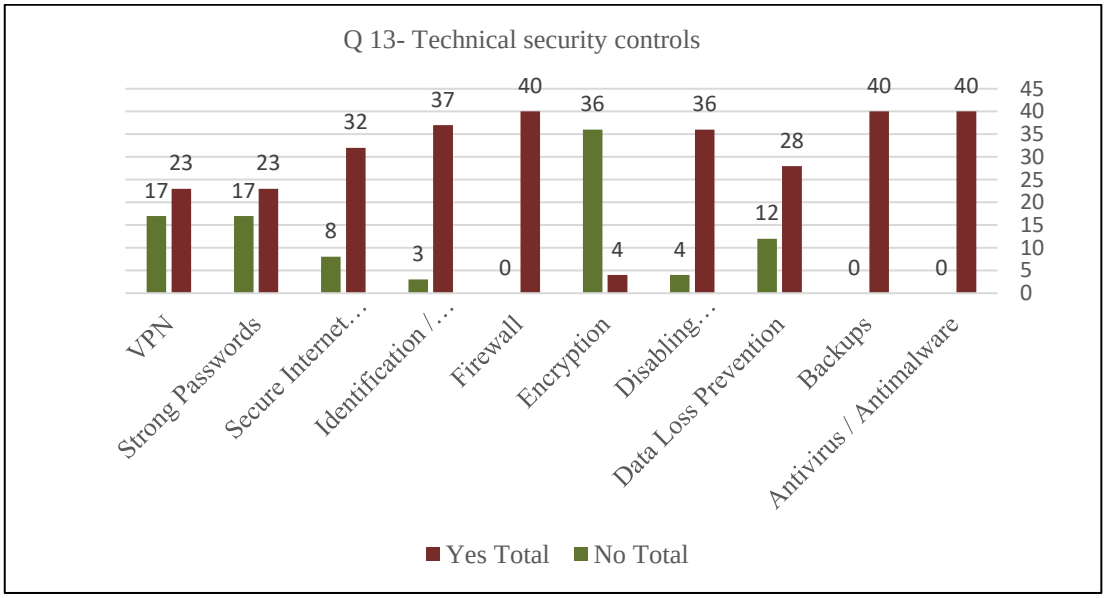


Figure 1: Technical security controls

The median of the tenth security control equals 20, and the standard deviation equals 4.2.

The participants have been asked which of the following identification and authentication tools your organization is using. The answer is shown in Table 2.

Table 2: Identification and Authentication tools

Q 2: Which of the following identification and authentication tools is your organization using?	
Tools	Total
- Strong passwords (8 characters minimum, upper case, lower case, number, special characters)	18
-Multi-Factor Authentication	5

-Biometrics	31
Median	18
Std. Deviation	13

The first option was strong passwords (8 characters minimum, upper case, lower case, number, special characters). This option has been chosen by eighteen people, and this represents 45%. The second option was multi-factor authentication. This option has been chosen by five people, and this represents 12.5%. The third option was biometrics. This option has been chosen by thirty-one people, and this represents 77.5%, as presented in Figure 2.

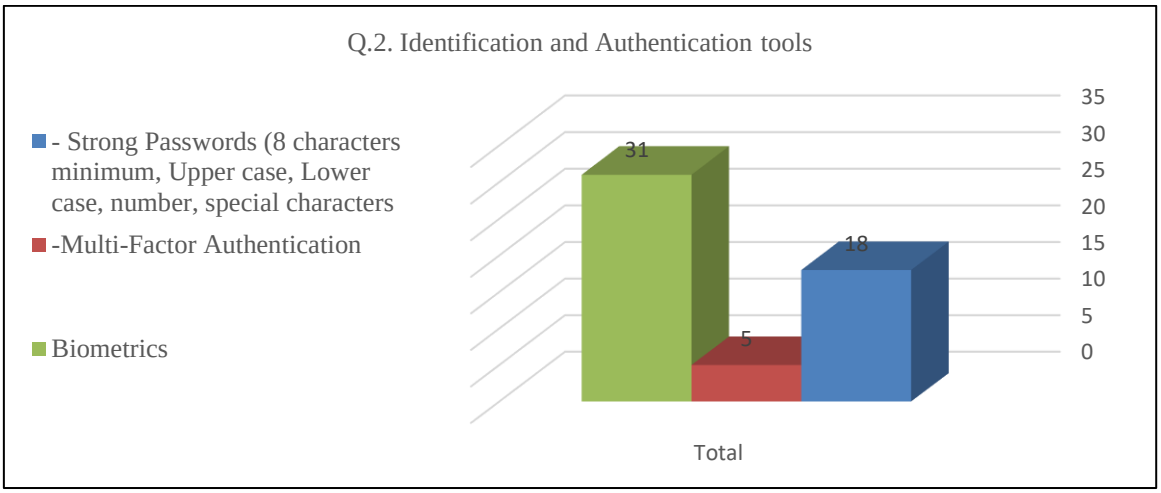


Figure 2: identification and authentication tools

The median of the identification and authentication tools equals 18, and the standard deviation equals 13.

The participants in the questionnaire were asked to give their opinion about the phrase "Using antivirus / antimalware on your mobile devices is very important ", and the answers are shown in Table 3.

Table 3: The important of using antivirus / antimalware

Q. 3.	Using antivirus / antimalware on your mobile devices is very important.	Agree	Slightly Agree	Disagree	Median	Std. Deviation
		31	8	1	8	15.7

Thirty-one people agreed to this phrase, and this represents 77.5%. Eight people slightly agreed, and this represents 20%. One person only disagreed, and this represents 2.5%, as displayed in Figure 3.

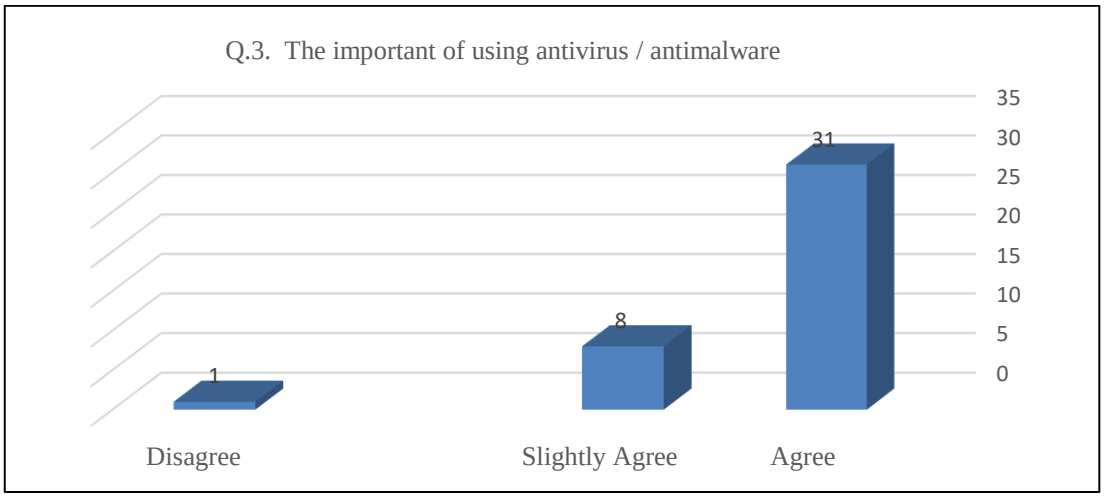


Figure 3: The important of using antivirus / antimalware

The median of the identification and authentication tools equals 8, and the standard deviation equals 15.7.

The thirty-one people who agreed that antivirus and antimalware are very important were asked which kind of antivirus they used, and the answers are shown in Table 4.

Table 4: kind of Antivirus

Q.4. Kind of Antivirus	Total
Symantec	7
Default Protection	2
Avira	5
Avast	5
Kaspersky	6
Nod	3
AVGI	1
Nova	1
No Answer	1

Seven people used Symantec, six people used Kaspersky, five people used Avira, and five people also used Avast. Three people used Nod. Two people just used default protection. Only one person used AVGI, and another person used Nova. The last person didn't answer, as shown in Figure 4.

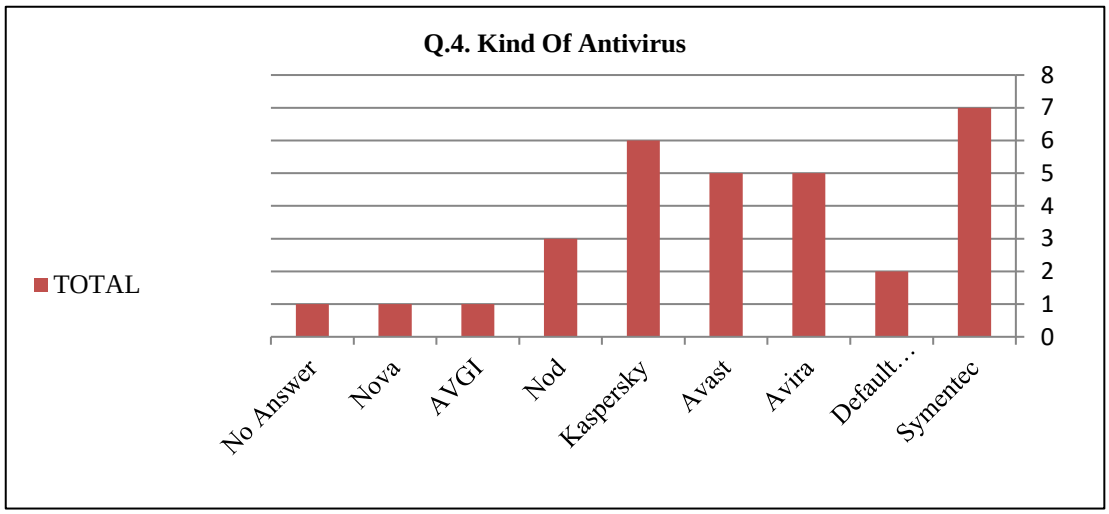


Figure 4: kind of Antivirus

The participants of the questionnaire were asked to give their opinion about the phrase "You must update your application, operating system, and antivirus regularly", and the answers are shown in Table 5.

Table 5: Updating

Q 16	You must update your application, operating system, and antivirus regularly.	Agree	Slightly Agree	Disagree	Median	Std. Deviation
		26	14	0	14	13

Twenty-six people agreed, and this represents 65%. Fourteen people slightly agreed, and this represents 35%. No one disagreed, as shown in Figure 5

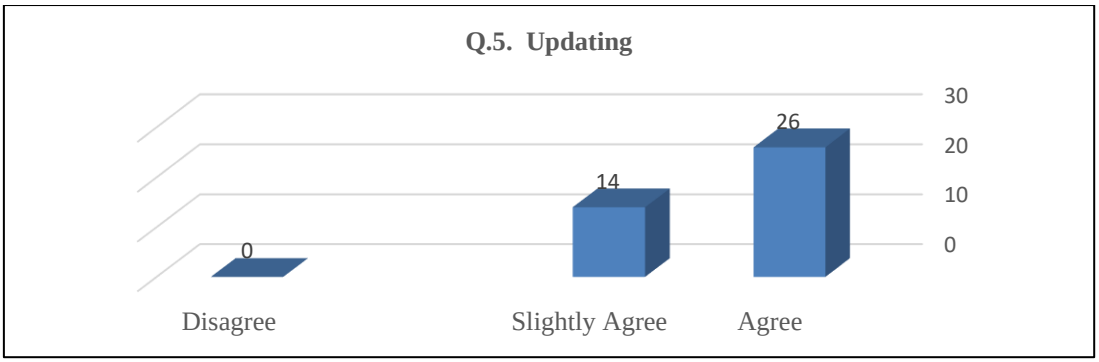


Figure 5: Updating

The median of the update equals 14, and the standard deviation equals 13.

The persons who agreed were asked about the period that they updated their applications, operating system, and antivirus. Some people who slightly agreed answered this question, and the answers are displayed in Table 6.

Table 6: Update Period

Q.6. Update Period	Total
Monthly	16
2 Months	4
3 Months	6
weekly	2
When prompted	1
No Answer	5

Two people update every week. Sixteen people update every month. Four people update every two months. Six people update every three months. One person updated when the antivirus was promoted. Five people from the agreed-upon group didn't answer, as shown in Figure 6

.

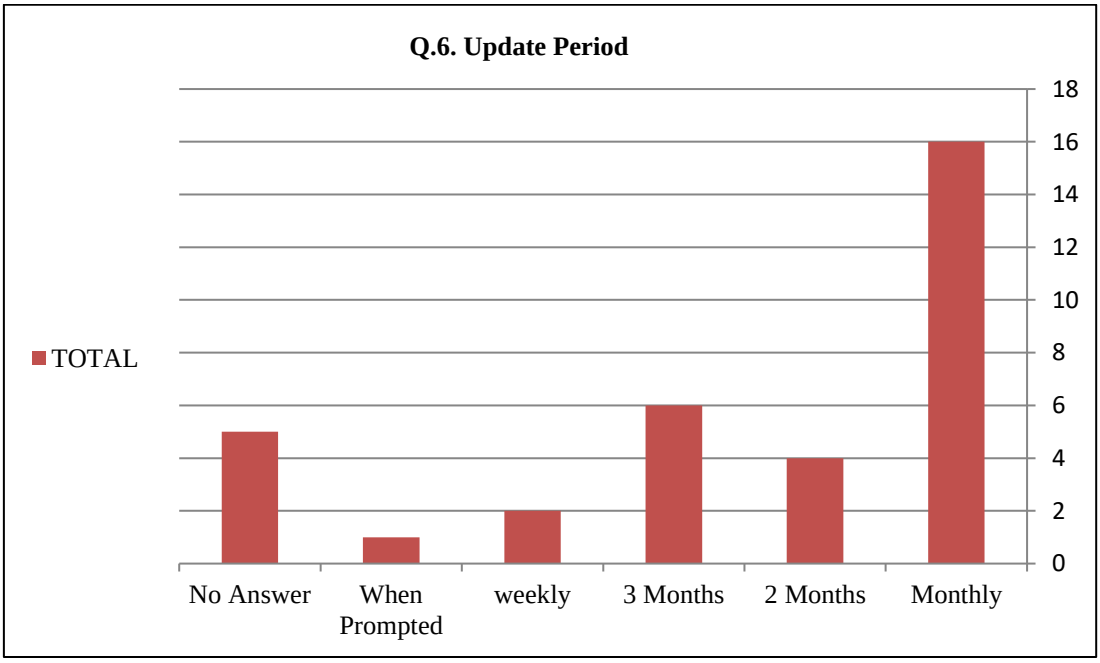


Figure 6: Update Period

The participants of the questionnaire were asked to give their opinion about the phrase "You should use backups to ensure minimum acceptable protection from mobile devices while working through the network ", and the answers are as shown in Table 7.

Table 7: Backups

Q 17	You should use backups to ensure a minimum acceptable protection from mobile devices while working through the network.	Agree	Slightly Agree	Disagree	Median	Std. Deviation
		37	2	1	2	20.5

Thirty-seven people agreed, and this represents 92.5%. Two people slightly agreed, and this represents 5%. Only one person disagreed, and this represents 2.5%, as shown in Figure 19.

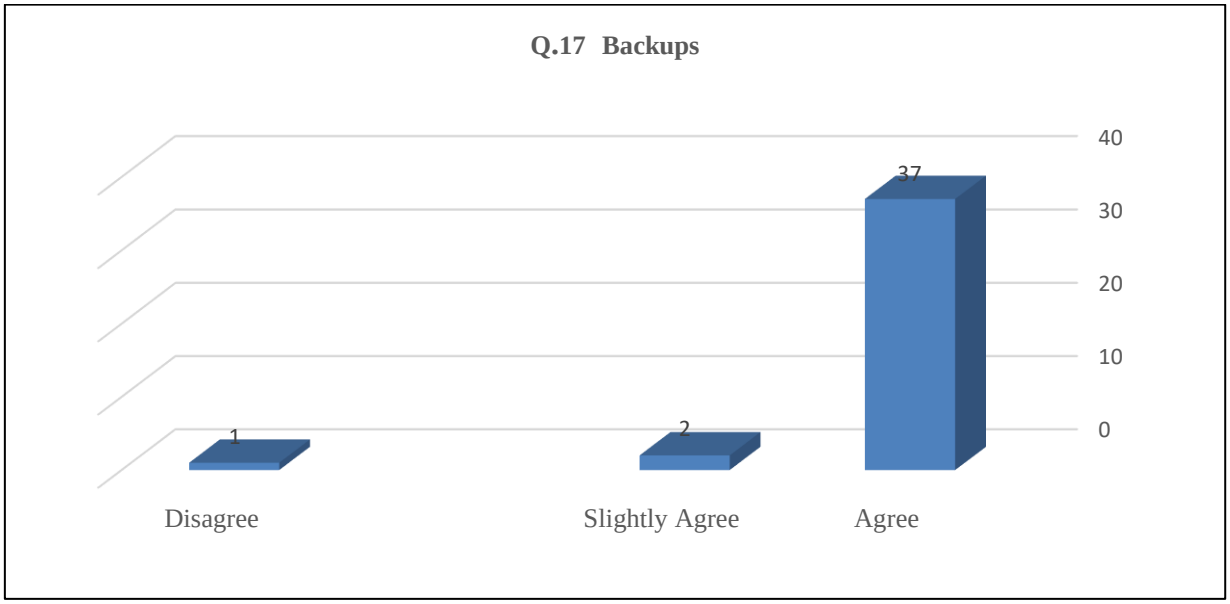


Figure 7: Backups

The median of the backups equals 2, and the standard deviation equals 20.5.

The participants of the questionnaire were asked to give their opinion about the phrase "You should implement policies (privileges, licenses) to ensure maximum acceptable protection from mobile devices while working through networking", and the answers are shown in Table 8.

Table 8: Policies

Q 18	You should implement policies (privileges, licenses) to ensure maximum acceptable protection from mobile devices while working through the network.	Agree	Slightly Agree	Disagree	Median	Std. Deviation
		35	3	2	3	18.8

Thirty-five people agreed, and this represents 87.5%. Three people slightly agreed, and this represents 7.5%. Two people disagreed, and this represents 5%, as shown in figure 20

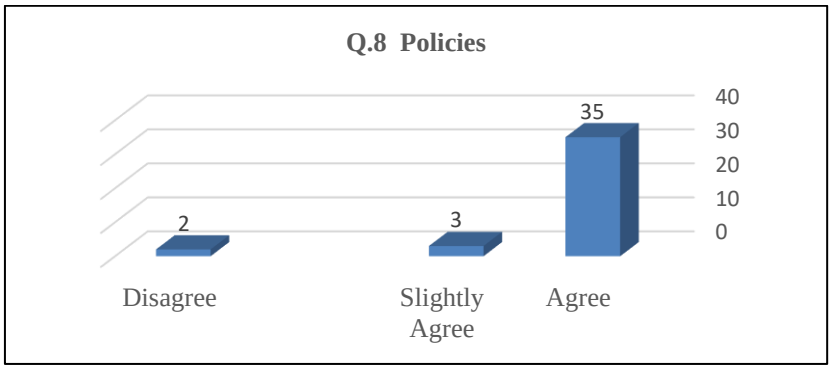


Figure 8: Policies

The median of the policies equals 3, and the standard deviation equals 18.8.

Solutions Scenarios in the IT department for mobile device security concerns:

3.2.1. Scenario one (1):

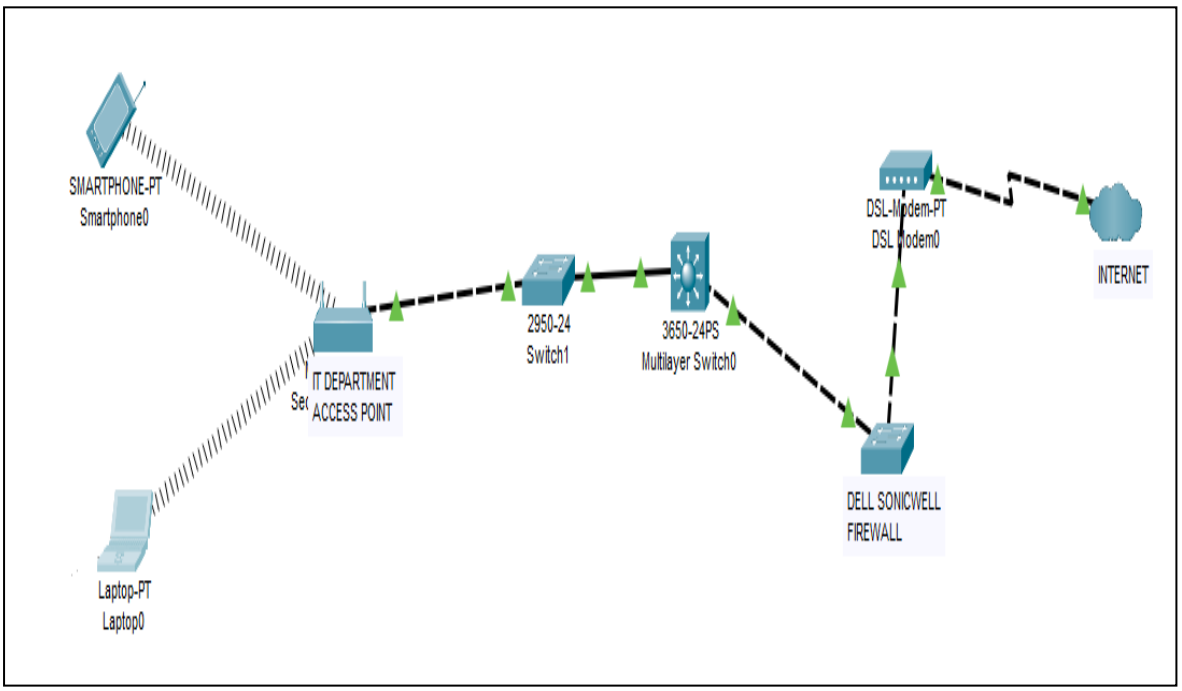


Figure 9: Scenario 1

The IT department protects its local network from wireless device security risks and attacks by putting them in a separate vlan that is not allowed to communicate with other vlans in the company's network, and this is done as follows:

- When the mobile devices connect to the access point, they send a DHCP request to get the IP address details.
- The access point is not configured as a DHCP server, but it forwards the DHCP request through the trunk line to the layer 3 core switch.
- The layer 3 core switch is also not configured as a DHCP server, but it is configured with a DHCP helper with the IP of a firewall to forward any DHCP request to the firewall, which is configured as a DHCP server for the wireless vlan.
- The firewall replies to the DHCP request with the IP address details that are required by the wireless devices to access the network and connect to the internet only, depending on the configured firewall policies to control the internet access.

4.2.1Scenario two (2):

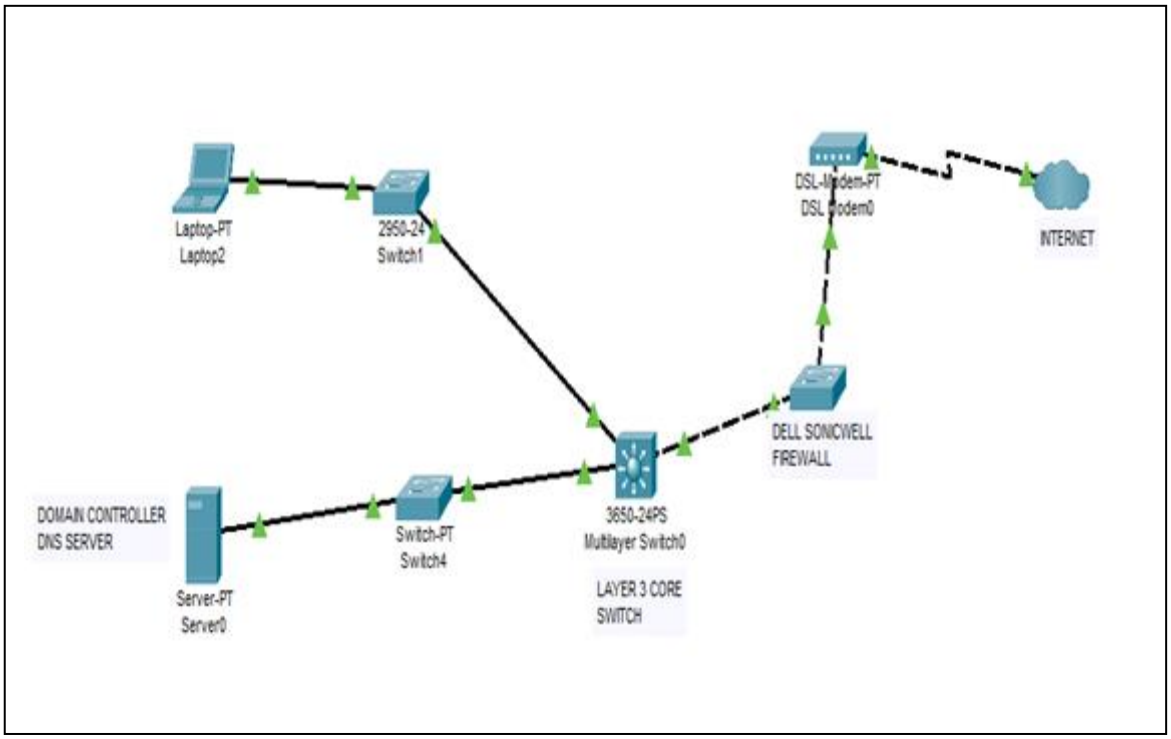


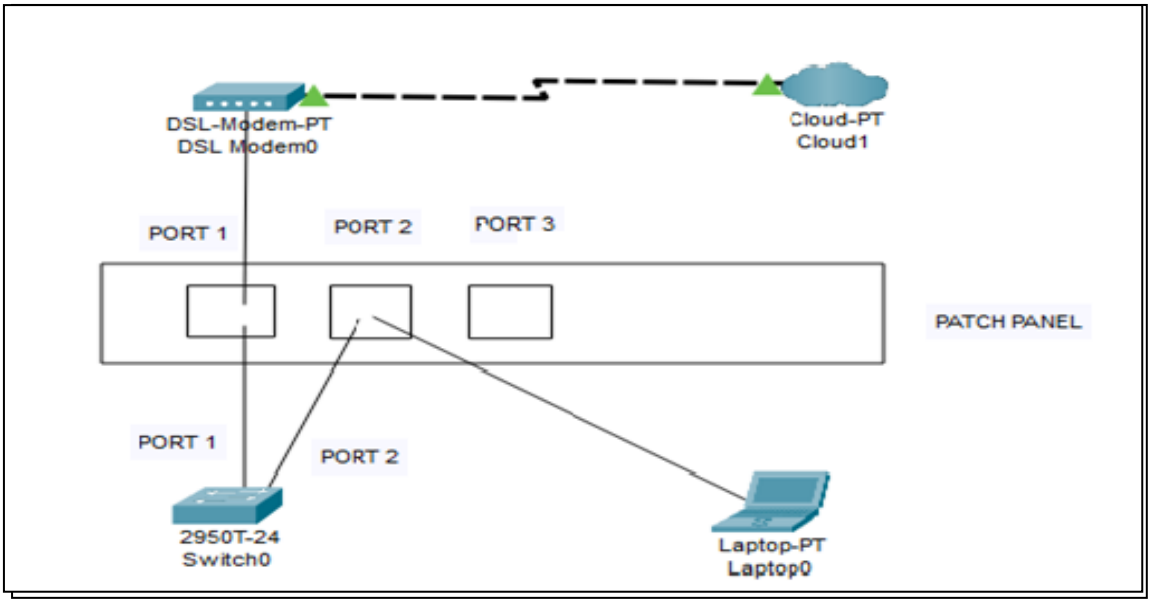
Figure 10: Scenario 2

Usually, all the workers at Aden Refinery Company (A.R.C.) use desktop computers to perform their duties, but sometimes some of them need to use laptop computers, especially in the IT department. To do this safely, the following steps must be taken:

- The antivirus program must be working and updating according to local standards.
- The network setting must be configured manually according to the location of the laptop on the local network.
- Rights and permissions must be granted according to the user category: regular user or administrator.
- The connected laptops cannot access the internet unless they are in the IT department vlan. How this is done is described in the following steps:
- When the user who works on the laptop opens a web browser to open a website, the website address is sent to the local DNS server for translation.
- The local DNS server does not translate the website address to an IP address, but it is configured with a public forwarder to send the request to a public DNS server that is located on the internet, such as Yemennet or Google DNS servers.
- When the layer 3 core switch receives the traffic and finds that the destination is not a local address, it forwards it to the default route, which leads to the firewall.

4.1.1. The firewall, in turn, checks the source IP address of the incoming traffic to see if it is allowed to access the internet or not, according to the configured firewall policies

4.1.2. 1.1.1. Scenario three (3A):



4.2.3 Scenario three (3A):

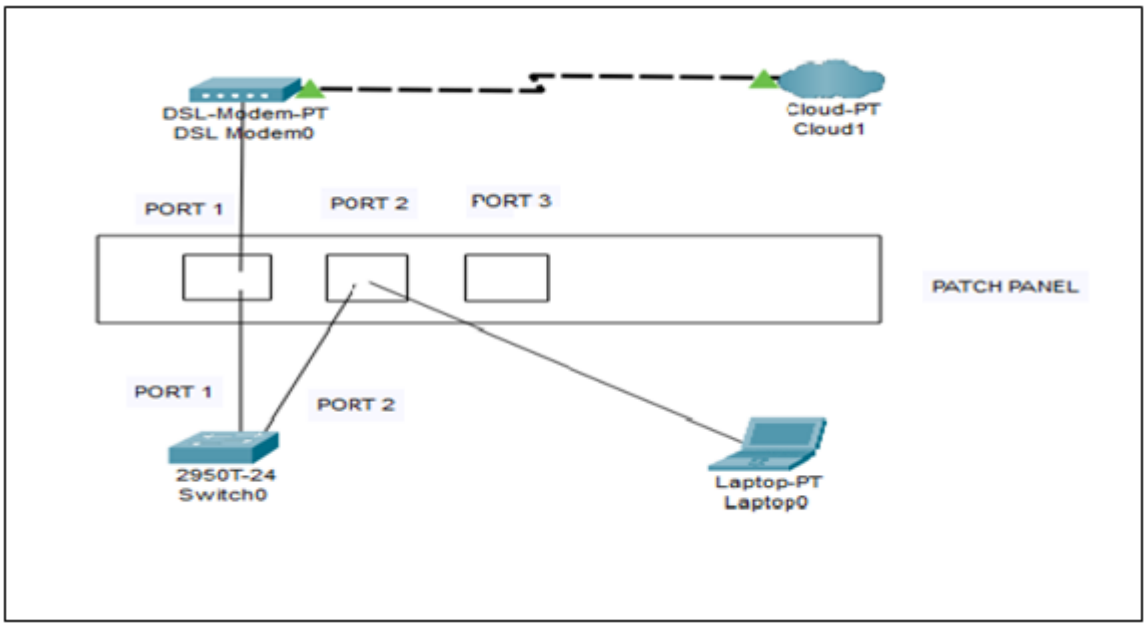


Figure 11: Scenario 3A

4.2.4 Scenario three (3B):

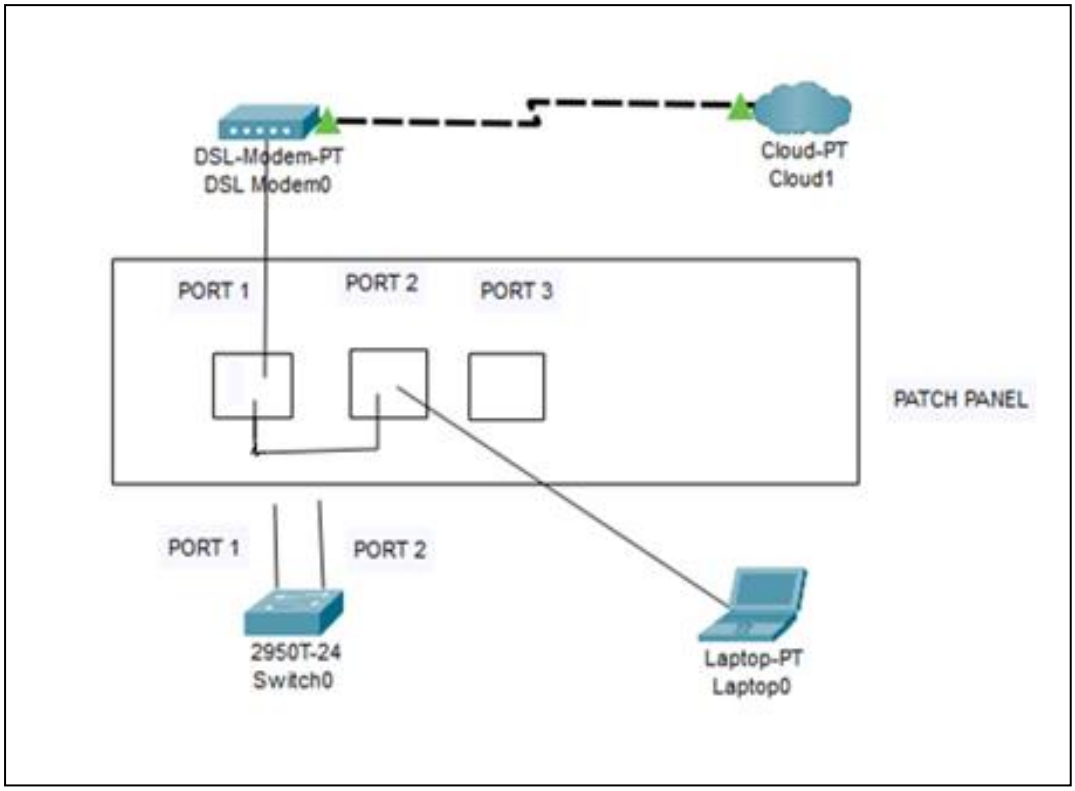


Figure 12: Scenario 3B

There is one socket prepared for guests who are not employed in the A.R.C. The socket is not connected to the IT department network; it is just connected to the internet, and this is done as follows:

- The ADSL modem connects to the nearest socket in the network.
- If this socket, for example, connects to port no. 1 in the patch panel, then it should connect to port no. 1 in the switch, as shown in Figure 11. Scenario 3A.
- The socket, which is especially for gust, connects, for example, to port two in the patch panel, and then it should connect to port two in the switch.
- To separate the gust socket from the network, port no one in the patch panel must be disconnected from port no one in the switch, and port no two in the patch panel must be disconnected from port no two in the switch.
- Port No. 1 in the patch panel must connect to Port No. 2 in the patch panel. So, the guest can use the internet, just as shown in Figure 12. Scenario 3B.

5. CONCLUSION

In the survey, the researcher asked the targeted population about ten security controls and which of them are used by the Aden Refinery Company to protect its information. The first control was antivirus/malware, which has been chosen by forty people and represents 100%. The second control was the backup, which has been chosen by forty people, which represents 100%. The third control was data loss prevention, and this has been chosen by twenty-eight people, which represents 70%. The other twelve people did not choose data loss prevention, which means that control is not used in the company, and this represents 30%. The fourth control was disabling administrator accounts / limiting user account privileges, and this has been chosen by thirty-six people, which represents 90%. The other four persons did not choose disabling administrator accounts / limiting user account privileges, which means that control is not used in the company, and this represents 10%. The fifth control was encryption, and this has been chosen by four persons which represents 10%. The other thirty-six people did not choose encryption, which means that control is not used in the company, and this represents 90%. The sixth control was the firewall, and this has been chosen by forty people, which represents 100%. The seventh control was identification/authentication, and this has been chosen by thirty-seven people, which represents 92.5%. The other three persons did not choose identification/authentication, which means that control is not used in the company, and this represents 7.5%. The eighth control was a secure Internet connection and Wi-Fi, and this has been chosen by thirty-two people, which represents 80%. The other eight people did not choose a secure Internet connection and Wi-Fi, which means that control is not used in the company, and this represents 20%. The ninth control was strong passwords, chosen by twenty-three people, which represents 57.5%. The other seventeen people did not choose NO, which means that

control is not used in the company, and this represents 42.5%. The tenth control was VPN, and this has been chosen by twenty-three people, which represents 57.5%. The other seventeen people did not choose VPN, which means that control is not used in the company, and this represents 42.5%. The participants in this survey have also asked which of these identification and authentication tools are used in the company. Strong passwords have been chosen by eighteen people, and this represents 45%. Multifactor authentication has been chosen by five people, and this represents 12.5%. Biometrics has been chosen by thirty-one people, and this represents 77.5%. Thirty-one people agreed with the phrase "Using antivirus / antimalware on their mobile devices is very important," and this represents 77.5%. Eight people slightly agreed, and this represents 20%. Only one person disagreed, and this represents 2.5%. The agreed persons have been asked which kind of antivirus they used, and the answers were: seven persons used Symantec, two persons used default protection, five persons used Avira, five persons used Avast, six persons used Kaspersky, three persons used Nod, only one person used AVGI, and also one person used Nova. Just one person from the agreed persons did not answer. Twenty-six people agreed to the phrase "You must update your application, operating system, and antivirus regularly," and this represents 65%. Fourteen people slightly agreed, and this represents 35%. No one disagreed. The participants were asked about the period that must update their application, operating system, and antivirus, and the answers were: two persons said weekly, sixteen persons said monthly, four persons said every two months, six persons said every three months, only one person said when prompted, and eleven persons did not answer. Thirty-seven people agreed to the phrase "You should use backups to ensure a minimum acceptable level of protection from mobile devices while working through a network," and this represents 92.5%. Two people slightly agreed, and this represents 5%. Only one person disagreed, and this represents 2.5%. Thirty-five people agreed to the phrase "You should implement policies (privileges, licenses) to ensure maximum acceptable protection from mobile devices while working through a network," and this represents 87.5%. Three people slightly agreed, and this represents 7.5%. Two people disagreed, and this represents 5%.

6. LIMITATION

This research has done in the IT department at Aden Refinery Company (A.R.C) and the participants in this study just only forty persons, so in the future if this research has done again to more petrochemical companies not only A.R.C such as oil and gas companies in Aden governorate or other companies. This would increase the numbers of the participants and maybe obtain new challenges and solutions. Another limitation should be considered that the research has comprehended just only the IT department employees not all the employees in the A.R.C. The number of the participants would increase and might gain new challenges and solutions.

REFERENCES

1. Gerald Nyamaiko Mutoro Wangutusi, "An exploration of how BYOD (Bring Your Own Device) user behavior impacts on an," UNIVERSITY OF NAIROBI, 2013.
2. Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," IEEE 11th Consum. Commun. Netw. Conf, p. 80–85, 2014.
3. Z. Hallock, J. Johnston, F. Macias, R. Saville, and S. Tenneti, "Cisco Bring Your Own Device," Cisco, no 5, p. 1–338, 2013.
4. Ali RAH, "DEVICE MANAGEMENT IN THE SECURITY OF "BRING YOUR," University of Fairfax, March , 2023.
5. Tshimangadzo Brenda Sikhala, "An Evaluation of Information Technology Risks from the Use of Personal Mobile Devices for Work Purposes," UNIVERSITY OF JOHANNESBURG, 2019.
6. Dhingra, M., "BYOD SECURITY AND ITS POSSIBLE SOLUTIONS," International Journal of Engineering Technologies and Management Research, pp. 5(2), 101-106, 2018.
7. Ali, M. I., & Kaur, S., "BYOD Cyber Threat Detection and Protection Model.," International Conference on Computing, Communication, and Intelligent Systems, pp. pp. 211-218, 2021.
8. Phyllis Y. Moore, "FACTORS INFLUENCING THE ADOPTION OF BRING YOUR OWN DEVICE," Capella University, October 2018.
9. Shahbazi, M., "System and method for enforcing a security policy on mobile devices using dynamically generated security profiles.," 2014.
10. Griffin, J., "biggest risks of Data Leaks from personal devices.," January 2022, . [Online]. Available: https://www.fleksy.com/blog/5-biggest-risks-of-data-leaks-frompersonal-.
11. M. French, C. Guo and J. P. Shim,, "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," Communications of the Association for Information Systems, 2014.
12. G. Bello , . D. Murray and . J. Armarego, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments,," Information and Computer Security, 2017.
13. David Njuguna , Wambui Kanyi, "An evaluation of BYOD integration cybersecurity concerns: A case study," International Journal of Recent Research in Mathematics Computer Science and Information Technology, p. 80, March 2023.
14. M. Ratchford, P. Wang and R. O. Sbeit, "BYOD

Security Risks and Mitigations," New Generations. Advances in Intelligent Systems and Computing, 2017.

15. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," International Conference on Computer Applications & Information Security (ICCAIS), 2018.
16. Nima Zahadat, "Mobile Security: A Systems Engineering Framework for Implementing Bring Your Own Device (BYOD) Security Through the Combination of Policy Management and Technology," George Washington University, January 31, 2016.
17. M. Eslahi , M. V. Naseri, H. Hashim, N. M. Tahir and E. H. M. Saad, "BYOD: Current state and security challenges," IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014.
18. J. . M. Chang, P.-C. Ho and T.-C. Chang, "Securing BYOD,," IT professionals, 2014.
19. Hijji, M., & Alam, G., "multivocal literature review on growing social," Ieee Access,, pp. 9, 7152-7169, 2021.
20. Leipold, S., "Cybersecurity Policies in The Age of Remote Work," 2021, March 15. [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/15/cybersecuritypolicies-.
21. Guidotti, A., "Authentication and identification, essentials for secure," 17 April 2020. [Online]. Available: https://www.vintegris.com/blog/authenticationidentification-.
22. Amper, R., "Leveraging identity verification to secure assets in the postpandemic,," 08 June 2022, . [Online]. Available: https://www.securityinfowatch.com/access-identity/article/21270432/leveragingidentity-.
23. Engle, M., "Why Passwordless Authentication Has an Identity Crisis.," 21 January 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/01/21/whypasswordless-.
24. Abhijith, M., & Senthilvadivu, K., "Impact Of VPN Technology On IT Industry," 2020. [Online]. Available: https://www.ijeast.com/papers/152-157,Tesma505,IJEAST.pdf.
25. Zscaler., "Zscaler's 2022 VPN Report: As VPN Exploits Grow, 80 Percent of Organizations Shift Towards Zero Trust Security.," 2022, September 26. [Online]. Available: https://www.zscaler.com/press/zscalers-2022-vpn-report-vpn-exploits-grow-80-.
26. Venkat, A., "97% of enterprises say VPNs are prone to," 2022, September 26. [Online]. Available: https://www.csoonline.com/article/3674793/97-of-enterprises-say-vpns-areprone-.