TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Vugar Gafarli 194478IVSB

Information Security Risk Assessment of dental clinic “Only Dent”

Bachelor’s Thesis

Supervisor: Tauseef Ahmed (PhD)

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Vugar Gafarli 194478IVSB

“Only Dent” infoturvariski hindamine

Bakalaureusetöö

Juhendaja: Tauseef Ahmed (PhD)

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Vugar Gafarli

16.05.2022

Abstract

With a growing number of dental clinics, the key priority is always to grow as soon as possible. Dental clinics most of the time find themselves in a fast-paced environment with limited amounts of time and financial resources to invest in cybersecurity.

As a part of healthcare industry, dental clinics need to store special category data about their patients in order to be able to operate the business. Thus, the importance of keeping this data confidential is essential for establishing trust between the patient and healthcare providers. Moreover, it is obligatory to ensure security of the data to comply with the law regulators.

While security is not prioritized as much as growth, the importance of it cannot be overlooked. New clinics, especially small dental offices are less likely to have sufficient security software or firewalls in place to satisfy standards, making them a valuable target for hackers. Failing to treat patient data securely according to cyber security standards can have catastrophic end results for the patient as well as the clinic.

Risk assessments relating to information technologies are vital in order to have a clear outlook and understanding of the vulnerabilities, threats and risk exposures of the company's technology assets.

Throughout this study, an in-depth mapping report about the risk assessment of a dental clinic is provided by evaluating the vulnerabilities as well as IT infrastructure issues present, by utilizing different methodologies of data gathering and analysis. This report aims to minimize security risks and provide an outlook for possible threats.

Furthermore, it can be a template for new small dental clinics to implement in their early stages to meet minimum required legal demand to store and process special category data in healthcare industry.

This thesis is written in English and is 47 pages long, including 5 chapters, 5 figures and 19 tables.

List of abbreviations and terms

AP	Access Point
CEO	Chief Executive Officer
DRP	Disaster Recovery Plan
FW	Firewall
HP	Hewlett-Packard
ID	Identification
IT	Information Technology
MMC	Məhdud Məsuliyyətli Cəmiyyəti
NIST	National Institute of Standards and Technology
PhD	Doctor of Philosophy
SSH	Secure Shell
VPN	Virtual Private Network
WEB	World Wide Web
Wi-Fi	Wireless Fidelity

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

Cyber security currently is becoming a vital part of the way society is to navigate and manage the complex and varied landscape of information systems with their massive amounts of data. As a result of this the need to securely contain, utilize, and communicate data and information throughout businesses and people is at an all-time high. The issues that can crop up due to having inadequate, faulty, or insufficient implementations of cyber security can be catastrophic, especially in the health care industry, and such it is necessary that proper care and time must be invested to prevent such situations from arising.

Healthcare organizations have been inundated with cyber-attacks, and they can expect more to come in 2022 [7]. Small businesses are attacked about four thousand times per day, making up 62% of all cyber-attacks according to IBM [6]. There are more than 70 private clinics in Azerbaijan since 2020 [5] which people around the visit for dental related issues. These people in order to be treated properly must provide a sizable amount of personal and sensitive information, where the storage, retrieval, sharing and use of it must be secure.

This information therefore must be stored confidentially in order to establish trust between patients and healthcare providers. The failure of cyber security can be disastrous to all parties involved, that being the case the protection of this data is at utmost importance by goodwill and law.

1.2 Problem Statement

Dental clinics most of the time themselves in fast-paced environment with limited amount of time to invest in cybersecurity, however this is a large concern that requires immediate attention, that left unaddressed could lead to a variety of issues.

“Only Dent” manages and stores personal and sensitive information of patients that cyber criminal’s desire. The secure storage and management of this data is a high priority for the safety of the clinic’s operations.

“Only Dent” has a visible online presence that can be used as an initial vector for exploitation as well a potential avenue for social engineering by malicious individuals.

“Only Dent” web system has been outsourced to third party.

1.3 Goal and objective

The main purpose of this research paper can be classified as:

- Evaluate a dental clinic and identify vulnerabilities that could potentially lead to data loss of confidential information of the patients.
- Perform cyber security risk analysis based on threats and vulnerabilities found concerning dental clinic.

While the objectives of this research paper are:

- To perform risk assessment on the clinic
- Analyse other IT infrastructure problems and come up with a friendly IT infrastructure layout for new dental clinics to implement in their early stages, in order to meet minimum required legal demand to store and process special category data in the healthcare industry.

1.4 Research questions

To clearly understand what is needed to be done for the research the following questions need to be answered:

- How susceptible and prepared is “Only Dent” against the current security vulnerabilities?
- What are the vulnerabilities and associated threats posed to the information systems of “Only Dent”?
- How the special category data of patients handled? Are they stored and processed securily?
- What are the risks that arise from the identified threats and vulnerabilities?

- What security controls can mitigate identified risks that can be implemented in small-medium companies without much effort?

2 Methodology

The purpose of this chapter of the thesis is to explain how the data was collected and analysed. This chapter includes research method, data collection and chosen risk assessment method.

2.1 Research methods

By the means of research, proof can be submitted to the solution of a problem by clearly putting out the data, and this is done by utilizing a variety of research methods. They can be classified accordingly to its purpose, scope, the data that is been used or the source of information. As this thesis is primarily focused on data, the research method that will be used is based according to the type of data used.

Qualitative method has been used to carry on with the research

- Qualitative research method uses tools such as interviews, surveys and records to gather the data compared to the numerical data of quantitative method. Good communication is a must and final decision is based on the judgement of conductor of the interviews, which results rather different outcomes with different assessors.

Additionally, the method used for the literature review was “forward snowball”. With locating the appropriate work and determining where it was cited to locate similar literature for this research.

Theoretical background was obtained from scientific articles as well as books matching the thesis topic. On the other hand, technical data was gathering by conducting questionnaires, participant observation and interviews with the dentists, IT specialist as well as the owner of “Only Dent”.

For the purpose of conducting the research the following criteria was set:

- Avoiding quantitative research method as it is not beneficial for individuals with limited amount of time and resource.
- All the documentation should be available in English or Azerbaijani.
- The cost of the resources used should be free of charge as the thesis is targeting the dental clinic with limited amount of income.

To make it more relevant, the resources chosen were publications with high number of citations. Permission to use the feedback was granted in order to protect people's privacy from all the personnel that were subject to the interviews.

2.2 Risk assessment method

For the purpose of this research paper, qualitative type of risk assessment has been chosen. The risk ratings will be defined as low, medium and high. The guideline used for this research paper is Risk Management Guide for Information Technology Systems by the National Institute of Standards and Technology [2].

The NIST Framework is truly applicable to small businesses as a jumping off point to establish their cybersecurity posture [6].

3 Background Information

3.1 Risk management

For the purpose of this research paper, risk assessment from the broader definition of the risk management process is used. This chapter is dedicated to the three main processes which are covered by risk management, to understand clearly how the processes works. Risk management revolves around three main processes, risk assessment, risk mitigation, and risk evaluation and assessment.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions [2]. In simple words it is the process of identifying and accessing potential security risks to implement preventor measures. It is essential for a business to have a solid foundational risk management plan in order to operate securely and successfully.

3.2 Risk assessment

Risk assessment is the initial stage where potential threats and the vulnerabilities are identified and evaluated.

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. [2]

Risk assessment compromises of few steps, these steps that are correlated with risk assessment which is shown in Figure 1.

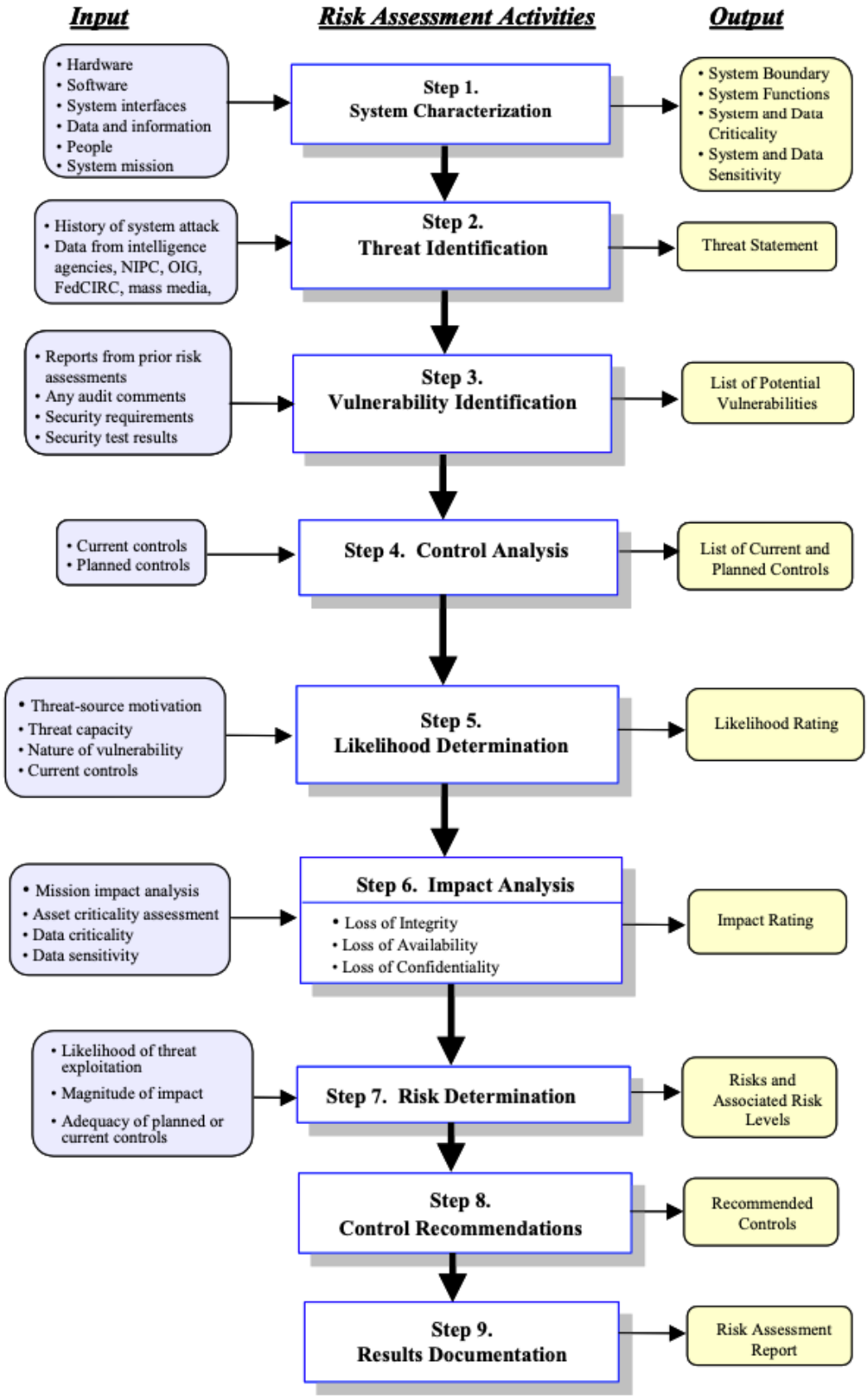

Figure 1 Components of Risk Assessment (Source: [2])

3.2.1 System characterization

This stage is required to define and list the resources, which include IT systems as well personnel, in order to identify where issues may occur. A few examples of these include:

- Hardware
- Data and information
- Network topology
- Organizational data
- System users
- Data sensitivity

Furthermore, anything that can be valuable for the IT system and organization can be classified in system characterization.

The data collected needs to be classified and prioritized depending on its sensitivity to have better understanding on what to focus on.

3.2.2 Threat identification

It is vital to discern the difference between a threat, vulnerability and exploitation. Another crucial bit information to understand is that a threat itself does not possess a risk if there is no vulnerability associated with it. The purpose of this chapter is to clear what a threat is and how to list them.

Threats are generally identified as dangers to assets. Threat is defined as the potential for a threat-source to exercise specific vulnerability [2]. A Threat can be an object, or any source of danger to an asset.

Figure 1 below describes the threats to information security and their corresponding examples.

Threat	Example
Compromises to intellectual property	Piracy, copyright infringement
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail of information disclosure
Missing, inadequate, or incomplete controls	Software controls, physical security
Missing, inadequate, or incomplete organizational policy or planning	Training issues, privacy, lack of effective policy
Quality of service deviations from service providers	Power and WAN quality of service issues
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of property

Figure 2 Threats to IT [4]

There are multiple factors that can be associated with motivation, each of them being unique. The next Table 1 demonstrates a variety of threat sources, motivations, and threat actions that may occur.

Table 1 Threats and motivations [2]

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Curiosity	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g., cyber stalking) Fraudulent act (e.g., replay, impersonation, interception) Information bribery Spoofing System intrusion

Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/Terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on an employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

With all the gathered knowledge about threats, it is needed to determine the likelihood of it, which will be described in chapter 3.2.5.

3.2.3 Vulnerability identification

With having the knowledge of information assets as well as the threats, the next stage will be identifying and analysing them with possible vulnerabilities. Vulnerability is the weakness/flaws in our system or entity that can be exploited. It is only limited to the research done and today a safe feature might end being a vulnerability tomorrow.

With that said, a table needs to be created, to showcase the gathered threats and possible vulnerabilities associated with it. This information will show us a clear picture of how the puzzle pieces fit together.

Table 2 below is an example of possible vulnerabilities and threats listed in a table.

Table 2 Vulnerability and Threat examples [2]

Vulnerability	Threat-source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

3.2.4 Control analysis

Control analysis is the part where the organization determines and analysis the controls/methods and security controls to prevent or decrease the likelihood of a threat.

There security controls can be categorized as preventive and detective controls. An example of preventive control would be security policies, encryption and authentication. On the other hand, detective controls might be auditing and intrusion detection system.

3.2.5 Likelihood determination

With every work done there is a chance it might fail, due to internal or external factor, to better evaluate the scenario, likelihood is used.

Likelihood is associated with probability of an attacker's success on infiltrating our vulnerability. It gives us an estimate on how likely our system might get compromised.

The accuracy of likelihood cannot be full proof that is why it is probability. However, to have a solid rating for each the probability few key elements should be taken into consideration. Which include the threat source and its capabilities, what kind of vulnerability is dealt with and are there effective controls against it.

Table 3 below gives us an example of the likelihood levels.

Table 3 Definition of likelihood [2]

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

With such table identification of the level of likelihood of the given threat is easier.

3.2.6 Impact analysis

Not all the time the threat will be successfully immobilized, which will lead in failure of the security systems and attackers gain. In such cases the end results need to be analysed.

The impact can be seen in three main areas, which include loss of integrity, loss of availability and loss of confidentiality.

Similarly, to likelihood, after the analysis a rating of low, medium or high from the impact analysis is gathered, which later will be used to determine the risk with the use of risk matrix.

Table 4 below is an example to the magnitude of the impact on given condition.

Table 4 Impact analysis rating [2]

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

3.2.7 Risk determination

At this stage the gathered data from likelihood and impact will be used to determine the risk level. Risk matrix will be used for this purpose.

To get a result from the risk-level matrix, a table needs to be formed where the variables are likelihood and impact. The levels of each need to be cross referenced to give us an estimate of the risk level.

Risk rating matrix can be seen below on Table 5.

Table 5 Risk rating matrix [2]

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

This matrix can be enlarged with likelihood of very low or high, or with impact of very low or very high depending on needs.

With the results from the risk matrix, it is important to understand what the outcome is. For this purpose, risk scale is required, where the rating can be labelled with the corresponding explanation.

Below Table 6 displays an example of risk scale.

Table 6 Risk scale [2]

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.

Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

3.2.8 Control recommendations

The sole purpose of risk assessment is finding the risks and to have them in control. Each vulnerability needs to be controlled after carefully assessing the threats that are associated with it. It is important to understand that sometimes it is not possible to eliminate the risk completely, and at times can be deemed acceptable after being addressed to the best possible level.

There are different ways to have controls, which can be obtained by setting good policies. Such as security rules. Another way is through education and awareness programs. And finally, by using software and technologies such firewalls or intrusion detection systems.

3.2.9 Results documentation

With the conclusion of our assessment the next step is documenting them in a final report. This will help the organization to come up with decisions regarding the policies, budget and operational costs. Overall, this report should give us brief recommendations for control systems.

3.3 Risk mitigation

With the initial part of risk management plan completed, the next step is risk mitigation. The purpose of risk mitigation is, take in the result from risk assessment and implementing or minimizing the risks.

3.3.1 Options

There are several cases of risk mitigation which can be identified as:

- **Avoid**. Getting rid of the risk by eliminating the cause
- **Accept.** Accepting the risk and continue operating
- **Transfer.** Passing the risk to third party, such as getting insurance

- **Limit.** To decrease the probability of the risk

3.3.2 Strategy

It is necessary to come up with a solution that is to be implemented utilizing appropriate control mechanisms under different scenarios. A methodology is required to determine what should be implemented to minimise the risk and to address the issue in the organizations scope.

For the ease of these kind of scenario there are templates to follow such as the one shown in Figure 3.

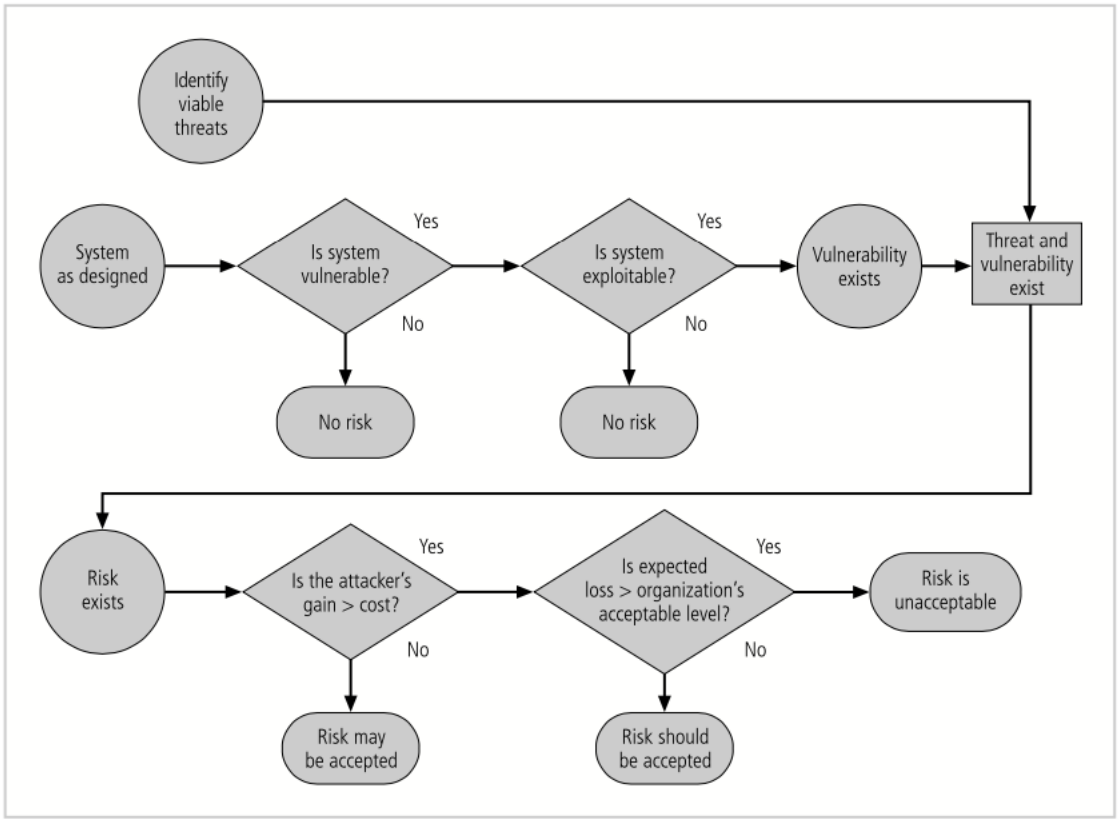

Figure 3 Risk Handling Template [4]

3.3.3 Cost-Benefit analysis

There are multiple ways of solving a problem. Once the risks are identified the organization must choose carefully and spend reasonable amount to minimize/remove the risks.

The decision process of making the wise decision if the amount spent by the organization to full proof its security is justified is called cost-benefit analysis.

3.4 Summary

To conclude this part of the research plan, briefly discussing about the importance of risk management and its importance to the organization is very important. It does not matter what sector of business is dealt with; the key fact here is that there will be always risk associated with it.

There are several advantages that come up with risk management, which include however not limited to,

- reducing unexpected results
- saving valuable time and resource
- making the working environment much safer
- accelerates the business/project success

With the given points, it's hard for an organisation to argue not to have a risk management plan. Good communication and mutual understanding withing the team will help achieve the goals much faster in this regard.

The special category data which is stored and processed by the healthcare industry needs to be always protected, which makes the risk management an undeniable process to have find and diminish the risks.

4 Analysis and result

4.1 Introduction to risk assessment

This section is the beginning of the analytical part of the research paper. Risk assessment was conducted on "Only Dent", with documenting results by evaluating threats and

vulnerabilities. Further in the paper risks are identified with their likelihood level, magnitude of impact as well as the overall risk score.

4.2 System characterization

4.2.1 Company overview

“Only Dent” is a small-medium dental clinic located in Baku, Azerbaijan. Its mission is to provide high quality dental care for adults as well as children. Established in 2014, the clinic is a small business with a compact rental office for their services.

The rental office is the first floor of a 16-floor residence building. The floor plan can be seen below in Figure 4.

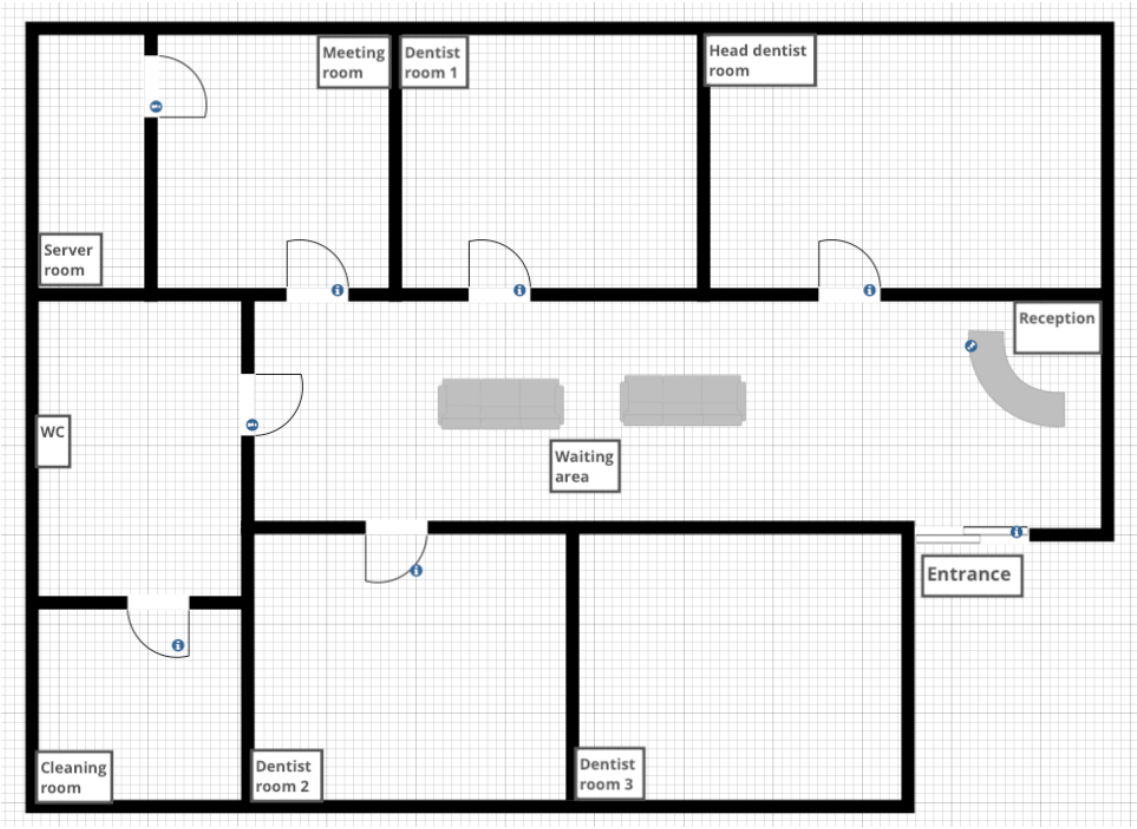

Figure 4 "Only Dent" Floor Plan

It consists of 5 rooms, a waiting area and WC and cleaning room. Four rooms are dedicated for the doctors as their service area, one room is dedicated to store the server and other IT equipment and last one is used as meeting room.

The staff includes four dentists, four nurses, one receptionist, one IT specialist and one cleaning lady.

The CEO who is also the head dentist is responsible for general management, which includes acquiring the necessary technical dentist equipment and medicine as well keeping track of their maintenance, acquiring and training proper staff as necessary. The receptionist oversees utilizing the electronic health record, practice management and billing systems the clinic utilizes. The IT specialist manages computer systems and network. The clinic outsources a variety of operations including digital marketing, law, and legality related services.

4.2.2 Infrastructure characterization

The knowledge was acquired by the conducting interview with IT specialist and onsite investigation at "Only Dent". The knowledge was acquired by the conducting interview with IT specialist and onsite investigation at "Only Dent".

Below Table 7 shows the ownership and information about IT system of "Only Dent".

Table 7 IT System Identification and Ownership

IT System Ownership	
IT System Name	ODSystem
Company Owned By	Only Dent MMC
Data Owned By	CEO
System Owned By	CEO
System Administrator	IT Specialist
Physical Location	Mirali Seyidov, 31/18, Baku, Yasamal, AZ1100
Business Function	Dental care services

Below Table 8 describes the users who have access to the network, their roles and security level corresponding to it.

Table 8 IT System Users

Position	Employee	Role Description	Clearance Level
CEO (Head Dentist)	Yes	managing operations, equipment and dental duties	High
IT Specialist	Yes	reviewing the functionality and efficiency of computer systems	High
Dentist no 1	Yes	examining patient's and giving proper treatment for dental problems	Medium
Dentist no 2	Yes	examining patient's and giving proper treatment for dental problems	Medium
Dentist no 3	Yes	examining patient's and giving proper treatment for dental problems	Medium
Receptionist	Yes	handling oncoming patients, emails and phone calls, office management	Medium
Web developer	No	Managing and updating website, email server and database	High

Below Figure 4 shows the network topology in "Only Dent" office.

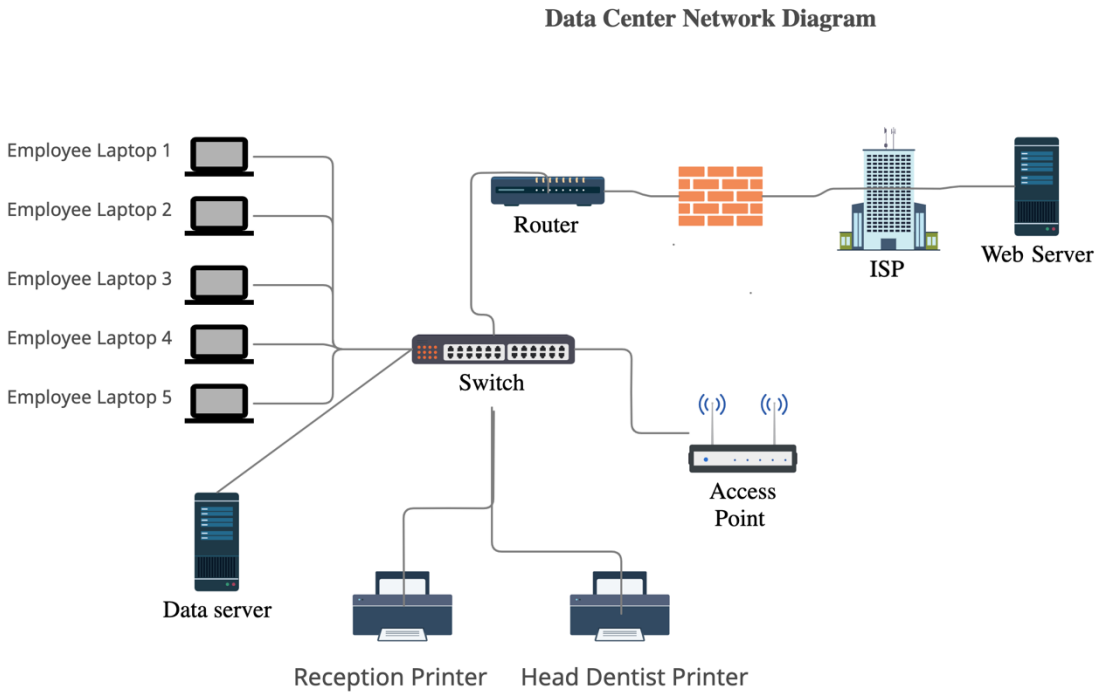

Figure 5 "Only Dent" Network Topology

Below Table 9 shows the data stored and its sensitivity.

Table 9 Data and Information Sensitivity

Data	Confidentiality	Integrity	Availability
Patient Data	High	High	High
Personnel Data	Low	Medium	Low
Referrer Data	High	High	Medium
Company Financial Data	High	Medium	Medium
Email Data	High	High	High

Below Table 10 describes the hardware information in “Only Dents” clinic corresponding to the location and additional information. The room information can be seen from Figure 4.

Table 10 Hardware characteristics

Hardware	Producer	Location	User
Employee Laptop 1	Lenovo	Room No 1	Head Dentist
Employee Laptop 2	HP	Room No 2	Dentist
Employee Laptop 3	HP	Room No 3	Dentist
Employee Laptop 4	HP	Room No 4	Dentist
Employee Laptop 5	HP	Reception	Receptionist
Switch	Cisco	Server room	IT Specialist
Router	Cisco	Server room	IT Specialist
Firewall	Cisco	Server room	IT Specialist
Printer 1	Canon	Room No 1	Head Dentist
Printer 2	HP	Reception	Receptionist
Wireless Access Point	Cisco	Reception	IT Specialist
Data Server	Dell	Server room	IT Specialist

4.3 Identification of risks

4.3.1 Threat identification

The purpose of this section of thesis is to identify threats, following the guideline mentioned in **Error! Reference source not found.**.

The below Table 11 show the threats identified.

Table 11 Identified Threats

Threat-Source	Motivation	Threat Actions
Hacker	Challenge, ego, curiosity	Record destruction, social engineering

Insider	Curiosity, monetary gain, revenge	Falsification of records
Computer criminal	Destruction of information, data alteration	Social engineering, information bribery
Disaster (natural)	Nature	Nature

4.3.2 Vulnerability identification

The purpose of this section of thesis is to identify vulnerabilities, following the guideline mentioned in **Error! Reference source not found.Error! Reference source not found.**.

The knowledge was acquired by the conducting interview with IT specialist and onsite investigation at "Only Dent".

Below Table 12 shows the vulnerabilities identified.

Table 12 Identified Vulnerabilities

Vulnerability	Threat-Source	Threat Action
Inadequate training and cyber awareness of employees using IT system	Hacker, computer criminal, insiders	Social engineering, unauthorized system access, malicious use
VPN access	Hacker, computer criminal	Unauthorized system access, system intrusion
Unprotected public network connection	Hacker, computer criminal	Unauthorized system access, system intrusion
Weak passwords	Hacker, computer criminal	Social engineering, unauthorized system, information bribery, impersonation, interception
Hardware maintenance	Insiders	System bugs
Secure door entry to server room	Insiders,	Falsified or corrupted data, fraud and theft, system bugs
Email/Web server	Hacker, computer criminal	Unauthorized system access, data theft

Dicastery recovery plan	Disaster (Natural)	IT system failure
Unrestricted access to all platforms	Computer criminal, hacker	Malicious code, data theft
User passwords not hashed	Hacker	Unauthorized system access, data theft

4.4 Control analysis

The purpose of this section of thesis is to list possible control methods to prevent the threats for “Only Dent”.

The below Table 13 lists the control methods.

Table 13 Security Controls

No	Area of Control	Planned Control
1	Encryption	Hashing the passwords in the database, using secure algorithms
2	Password policy	Setting up password complexity rules in order to avoid weak passwords
3	Security awareness training	Setting up trainings to educate the employees about cyber security and latest trends
4	Physical access security	Minimal standards to be met securing important rooms with IT assets
5	Remote network access	Securing remote access with the use of VPN
6	IT facility maintenance	Regular maintenance of IT assets
7	Web access control	Restricting access to potentially dangerous/malicious websites from work laptops
8	Web data update	Receiving regular reports from IT outsource party
9	Disaster recovery plan	Preparing disaster recovery plan for the continuity of services in case of natural disaster
10	Control of IT inventory	Restring unauthorized access to internal network

The below Table 14 matches the threat with relevant control method. The assigned method is based on authors judgement.

Table 14 Control Method by Relevance

Risk	Relevant Control Method
The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure.	Relevant control is no 3, having cyber awareness trainings will drastically reduce the risk of employees being scammed and fall into phishing attacks.
The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access.	Relevant control is no 5, setting up VPN for the company adds an additional layer of protection to allow users to establish secure connection from distance.
Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre.	Relevant control is no 10, the access point would be better connected to the router rather than the same switch as the data server, to avoid the risk of hacking from unauthorized device.
Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft.	Relevant controls are no 1 and no 2, having policy for secure patterns for setting up the employee device password and updating it every 3 months will add more security to the device.
The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Relevant control is no 6, maintain the server room and the servers will reduce the risk of bugs and the failure of the server.
No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage.	Relevant control is no 4, having a secure door with key-card access system will drastically reduce the risk of unauthorized user entering the server room.

Email/Web server is outsourced, not receiving regular updates about the status at all.	Relevant control is no 8, regularly receiving updates from the outsource party including information about the logs and break in attempts will provide the information for better protection.
Absence of disaster recovery plan, in case of any disaster there is continuity in the services.	Relevant control is no 9, disaster recovery plan should be implemented for the service to restore as quickly as possible
Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks.	Relevant control is no 7, restricting access to potentially dangerous/malicious websites from work laptops by the system administrator using the desired tool.
The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss.	Relevant control is no 1, before storing the passwords of the users they should be stored as salted and hashed passwords using secure algorithm.

4.5 Risk likelihood determination

The purpose of this section of thesis is to assign likelihood level to the identified threats and the risks that they bring with it, keeping in mind the controls if there are any from the previous chapter.

The levels are assigned as low, medium and high, based on authors judgement following the guideline mentioned in **Error! Reference source not found.**.

The below Table 15 describes the level of likelihood.

Table 15 Risk Likelihood Levels

Risk	Risk Likelihood Definition	Risk Likelihood Level
The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure.	There are no safeguards in place to prevent the vulnerability from being exploited.	Medium
The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access.	The threat source is motivated and capable and there are no safeguards in place to prevent the exploit of the vulnerability.	High
Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre.	There are no safeguards in place to prevent the vulnerability from being exploited.	Medium
Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft.	The threat source is motivated and capable and there are no safeguards in place to prevent the exploit of the vulnerability.	High
The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Even though there is not regular maintenance, the likelihood of the risk low	Low

No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage	There are no safeguards in place to prevent the vulnerability from being exploited	Medium
Email/Web server is outsourced, not receiving regular updates about the status at all.	There are no safeguards in place to prevent the vulnerability from being exploited	Medium
Absence of disaster recovery plan, in case of any disaster there is continuity in the services	Even though the disaster recovery plan is missing, the likelihood of the natural disaster occurrence is low	Low
Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks	There are no safeguards in place to prevent the vulnerability from being exploited	Medium
The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss	The threat source is motivated and capable and there are no safeguards in place to prevent the exploit of the vulnerability	High

4.6 Impact analysis

The purpose of this section of thesis is determine the impact level if any identified threats have been successful.

The levels are assigned as low, medium and high, based on authors judgement following the guideline mentioned in **Error! Reference source not found.**

The below Table 16 describes the magnitude of impact to the given successful threats.

Table 16 Impact Ratings

Risk	Impact Definition	Impact Area	Magnitude of Impact
The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure	As a result, minor tangible goods and reputation will be damaged	Confidentiality	Low
The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Confidentiality Integrity	High
Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Confidentiality Integrity	High
Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Confidentiality Integrity	High
The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Availability	High

No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Confidentiality Integrity Availability	High
Email/Web server is outsourced, not receiving regular updates about the status at all.	Reputational damage and loss of resources	Confidentiality Availability	Medium
Absence of disaster recovery plan, in case of any disaster there is continuity in the services	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Availability	High
Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks	As a result, minor tangible goods and reputation will be damaged	Confidentiality	Low
The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss	Resulting in the loss of significant tangible assets or resources at a considerable cost also harming organization mission and reputation	Confidentiality Integrity	High

4.7 Risk determination

The purpose of this section of thesis is determine the risk level of the threat by using the risk rating matrix following the **Error! Reference source not found.**. The gathered data from previous chapters of likelihood levels and impact ratings will be used to determine the overall risk level.

The below Table 17 shows the risk level by multiplying likelihood level to impact rating.

Table 17 Risk Level Ratings

Risk	Likelihood Level	Impact Rating	Risk Level
The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure	Medium	Low	Low
The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access	High	High	High
Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre	Medium	High	Medium
Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft	High	High	High
The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Low	High	Low
No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage	Medium	High	Medium
Email/Web server is outsourced, not receiving regular updates about the status at all.	Medium	Medium	Medium
Absence of disaster recovery plan, in case of any disaster there is continuity in the services	Low	High	Low

Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks	Medium	Low	Low
The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss	High	High	High

The results of the risk level are judged in parallel with **Error! Reference source not found.** to better understand the situation and take necessary actions.

4.8 Control recommendations

The purpose of this section of thesis is to give out recommendations based on the results we got from previous chapters. As mentioned in before in chapter 3.2.8, sometimes it is not possible to eliminate the risk completely, therefore the recommendations should be given to minimize the residual risk to its best possible content.

The below Table 18 shows the recommendations given by the author for the given risk.

Table 18 Control recommendations

Risk	Control Recommendation	Risk Level
The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure	Company needs to organize cyber awareness trainings and seminars for its employees	Low
The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access	Company needs to set up internal VPN to secure the connection by adding additional protective layer for remote connection	High

Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre	Relevant control is no 10, it is recommended to separate internal and guest network in to two separate VLANs	Medium
Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft	Company needs to have policy for setting up the employee device with secure standards of password and updating it every 3 months preferably	High
The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Company needs to have regular inspection of the server room and hardware, for its cleanliness and maintain running efficiency of the hardware	Low
No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage	Company needs to install key-card access system to the door of the server room	Medium
Email/Web server is outsourced, not receiving regular updates about the status at all.	Company needs to sign agreement with the outsourcing company to receive regular feedback about the logs of email/web server	Medium
Absence of disaster recovery plan, in case of any disaster there is continuity in the services	Company needs to prepare disaster recovery plan	Low

Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks	Company needs to restrict potentially malicious websites including social platforms. The tools used can be chosen by the system administrator	Low
The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss	Company needs to store the passwords of the users salted and hashed with secure algorithm	High

4.9 Documentation of results

The purpose of this section of thesis is create risk assessment report with all the collected information from previous chapters, which include identified threat-sources, vulnerabilities, associated risks, control methods, risk likelihood levels, impact ratings, overall risk levels and control recommendations. Below Table 19 shows the risk assessment report with all the information filled in.

Table 19 Risk Assessment Report

Threat-Source	Vulnerability	Risk	Relevant Control Method	Likelihood Level	Impact Rating	Risk Level	Control Recommendation
Hacker, computer criminal, insiders	Inadequate training and cyber awareness of employees using IT system	The personnel of the company never had cyber awareness training and lack the minimal knowledge. Phishing scam, unintentional data disclosure	Relevant control is no 3, having cyber awareness trainings will drastically reduce the risk of employees being scammed and fall into phishing attacks	Medium	Low	Low	Company needs to organize cyber awareness trainings and seminars for its employees
Hacker, computer criminal	VPN access	The personnel can access internal network remotely without any VPN protection which can lead to data theft and unauthorized access	Relevant control is no 5, setting up VPN for the company adds an additional layer of protection to allow users to establish secure connection from distance	High	High	High	Company needs to set up internal VPN to secure the connection by adding additional protective layer for remote connection
Hacker, computer criminal	Unprotected public network connection	Access point as well as the data centre is directly connected to the switch, that may lead to unauthorized access to the data centre	Relevant control is no 10, it is recommended to separate internal and guest network.	Medium	High	Medium	Relevant control is no 10, it is recommended to separate internal and guest network, this can be achieved by creating new guest VLAN.

Hacker, computer criminal	Weak passwords	Employees do not use strong passwords, nor is there a policy stating the standards of passwords to be chosen, this may lead to unauthorized access to the system and data theft	Relevant controls are no 1 and no 2, having policy for secure patterns for setting up the employee device password and updating it every 3 months will add more security to the device	High	High	High	Company needs to have policy for setting up the employee device with secure standards of password and updating it every 3 months preferably
Insiders	Hardware maintenance	The server and the server room are not maintained properly, the server room and equipment are covered in dust, may lead to high temperature or bugs in the system.	Relevant control is no 6, maintain the server room and the servers will reduce the risk of bugs and the failure of the server	Low	High	Low	Company needs to have regular inspection of the server room and hardware, for its cleanliness and maintain running efficiency of the hardware
Insiders	Secure door entry to server room	No proper security lock on the server room, is only protected by a door, rather simple to break in. May lead to data theft, system sabotage	Relevant control is no 4, having a secure door with key-card access system will drastically reduce the risk of unauthorized user entering the server room	Medium	High	Medium	Company needs to install key-card access system to the door of the server room
Hacker, computer criminal	Email/Web server	Email/Web server is outsourced, not receiving regular updates about the status at all.	Relevant control is no 8, regularly receiving updates from the outsource party including information about the logs and break in attempts will provide the information for better protection	Medium	Medium	Medium	Company needs to sign agreement with the outsourcing company to receive regular feedback about the logs of email/web server
Disaster (Natural)	Dicastery recovery plan	Absence of disaster recovery plan, in case of any disaster there is continuity in the services	Relevant control is no 9, disaster recovery plan should be implemented for the service to restore as quickly as possible	Low	High	Low	Company needs to prepare disaster recovery plan
Computer criminal, hacker	Unrestricted access to all platforms	Unrestricted access to all platforms from work on laptops, scamming and phishing are among the risks	Relevant control is no 7, restricting access to potentially dangerous/malicious websites from work laptops by the system administrator using the desired tool	Medium	Low	Low	Company needs to restrict potentially malicious websites including social platforms. The tools used can be chosen by the system administrator

Hacker	User passwords not hashed	The passwords of users stored in the database are not hashed, may lead to unauthorized access, data theft and loss	Relevant control is no 1, before storing the passwords of the users they should be stored as salted and hashed passwords using secure algorithm	High	High	High	Company needs to store the passwords of the users salted and hashed with secure algorithm

4.10 Summary

The summary of this research paper includes all the steps taken and the final documentation of the results.

Company IT assets have been gathered and categorized. The categories include System users and their clearance level, hardware and corresponding user and the data stored and processed with respect to their sensitivity. Furthermore, the physical location of the hardware has been documented.

Next stage, threats and vulnerabilities were identified and documented with detail of their motivation and possible actions. Possible control methods were listed to prevent the threats which “Only Dent” might face. Furthermore, with the gathered data from threats, vulnerabilities and control methods, several risks were identified and matched accordingly with the relevant control method.

With the risks identified, their likelihood level and the magnitude of impact were calculated and documented. With the determination of the likelihood levels and impact levels, overall risk levels were calculated.

At the end, following the overall risk levels and risks, detailed control recommendations were provided to mitigate the risks. All the process was documented in one final risk assessment report.

5 Conclusion

The core aim of this research paper was to analyse and assess the IT security of the small dental clinic as the resources might not be enough to implement or can be overlooked for the security related issues.

Being one of the small-mid sized business, “Only Dent” has limited number of resources to allocate to IT security. During the research conducted several vulnerabilities and threats were identified and it with conclusion that “Only Dent’ in some extents is not well prepared against current security vulnerabilities.

With the evaluation of the threats and vulnerabilities through the help of risk assessment, the possible risks were identified which answers the research question posed at the beginning of this paper.

Security controls have been recommended to implement which takes into consideration of the resources, the level of ease and speed in which it can be processed. This was one of the research questions and it has been fulfilled.

With the given recommendation the overall risk levels are bound to decrease and furthermore secure “Only Dent”. This research paper can be used by other small clinics as starting point to better understand the risk assessment process and implement it on their own business.

The application security has not been out of the scope of this research paper and can be considered for future work.

References

[1] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu 04.06.2010, accessed on 12.02.2022, https://www.e-gov.az/home/getfile/428.

[2] Stoneburner, G. , Goguen, A. and Feringa, A. (2002), Risk Management Guide for Information Technology Systems, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/nist.sp.800-30 (Accessed March 22, 2022)

[3] Ross, R. (2012), Guide for Conducting Risk Assessments, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-30r1 (Accessed March 22, 2022)

[4] 2012. Principles of Information Security. 4th ed. Boston: Michael E. Whitman, Herbert J. Mattord.

[5] State Statistical Committee of the Republic of Azerbaijan. Statistical Publication: Health Care in Azerbaijan. Baku, Azerbaijan: State Statistical Committee, https://www.stat.gov.az/source/healthcare/en/001_3_5en.xls

[6] A. Furneaux, "Small to Mid Sized Businesses: How to Consider the NIST Framework", *Cybersaint.io*, 2022. [Online]. Available: https://www.cybersaint.io/blog/small-business-nist. [Accessed: 13- May- 2022].

[7] R. Southwick, "Cyberattacks in healthcare surged last year, and 2022 could be even worse", *Chief Healthcare Executive*, 2022. [Online]. Available: https://www.chiefhealthcareexecutive.com/view/cyberattacks-in-healthcare-surged-last-year-and-2022-could-be-even-worse. [Accessed: 13- May- 2022].

[8] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital healthcare - cyberattacks in asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations. *IEEE Access, 10*, 12345-12364.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Vugar Gafarli

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Information Security Risk Assessment of dental clinic “Only Dent” supervised by Tauseef Ahmed
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

16.05.2022

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.