

**COMP1608Managing IT Security and Risk**



Student name:

student id:

**Contents**

[Executive Summary 3](#_Toc86497031)

[Introduction 5](#_Toc86497032)

[Scenario 6](#_Toc86497033)

[Organisation and Business Unit operations 7](#_Toc86497034)

[Assumptions 10](#_Toc86497035)

[Key Assets 11](#_Toc86497036)

[Threats and Exposure Research 13](#_Toc86497037)

[Risk Assessment and Risk Treatment Strategy 19](#_Toc86497038)

[New technology to the operations 20](#_Toc86497039)

[Conclusion 23](#_Toc86497040)

[References 24](#_Toc86497041)

**List of tables**

[Table 1: Risk assessment 19](#_Toc86497076)

[Table 2: Risk treatment strategy (Modified) 22](#_Toc86497077)

**List of figures**

[Figure 1: New architecture for healthcare organisation 20](#_Toc86497092)

# **Executive Summary**

Technological aspects have been completely integrated in the organisations who are participating in the digital transition. It has been analysed that the organisations are eager to integrate the advanced technology in the organisation for increasing their productivity and optimise their capabilities so that they can provide better services. When it comes to providing better services the industry which seeks the best options available in the Healthcare industry as these types of organisations have the responsibility of saving the life of a human being. There are a number of health organisations who operate around the country for the Welfare of the people. The identification of risk and threat among organisations is one of the most effective ways to prevent the organisation from being vulnerable to the attacks. In the Healthcare organisation the management deals with a large number of sensitive data that is required to be preserved in a way that integrity of data is maintained.  The Royal London hospital is a kind of healthcare organisation in London which deals with a large number of HealthCare facilities provided to the patients on a regular and on emergency basis. This Hospital is popular at the international level as it has various specialist services that attract the patient during their emergencies. This Hospital provides the best possible care to the patient so that they can live a healthy life while having all the standard facilities that are required for providing care to a Patient.  In order to identify the risk and threat there is a requirement of analysing each of the departments and their operational capabilities so that major aspects related to the functions carried out inside the organisation can be obtained. Nowadays it should be the foremost responsibility of the organisation to undergo the various safety measures so that they can provide optimised services and enhance their performance while providing best services.

# **Introduction**

Technological aspects have been completely integrated in the organisations who are participating in the digital transition. It has been analysed that the organisations are eager to integrate the advanced technology in the organisation for increasing their productivity and optimise their capabilities so that they can provide better services. When it comes to providing better services the industry which seeks the best options available in the Healthcare industry as these types of organisations have the responsibility of saving the life of a human being. There are a number of health organisations who operate around the country for the Welfare of the people. The identification of risk and threat among organisations is one of the most effective ways to prevent the organisation from being vulnerable to the attacks. In the Healthcare organisation the management deals with a large number of sensitive data that is required to be preserved in a way that integrity of data is maintained.  The Royal London hospital is a kind of healthcare organisation in London which deals with a large number of HealthCare facilities provided to the patients on a regular and on emergency basis. This Hospital is popular at the international level as it has various specialist services that attract the patient during their emergencies. This Hospital provides the best possible care to the patient so that they can live a healthy life while having all the standard facilities that are required for providing care to a Patient.  In order to identify the risk and threat there is a requirement of analysing each of the departments and their operational capabilities so that major aspects related to the functions carried out inside the organisation can be obtained. Nowadays it should be the foremost responsibility of the organisation to undergo the various safety measures so that they can provide optimised services and enhance their performance while providing best services.

# **Scenario**

The organisation has been referred to as a teaching hospital which is also a part of national Healthcare services trust. The hospital is majorly concerned with providing services to the city as well as to the patients from outside of London.  The hospital has a large number of facilities available because of which they have embedded wide services that can be accessed to a large number of people at the same time. The hospital is known for having the facilities related to the major disease which are treated and operated in the hospital in a wide range. As the hospital also deals with educating the students who have been assigned under their supervision, they have a different department for it.  The students also help the doctor by assisting them in their regular activities and simultaneously seeking experiences from the doctors. While the hospital was gaining popularity among the patient day continuously adding more services and expanding their operating capabilities so that they can provide services to more customers (Leblanc et al. 2021). The hospital now has emergency care services and paediatric facilities which have been located in different buildings of the hospital. It can be analysed that the hospital is currently giving a large number of patients by providing them wide health care services and facilities. The Major department that is working among the organisation are the Trauma centre and emergency department. Organisation has various services in several branches which are located in existing hospitals of London. The organisation is supported by various Healthcare trusts because of which they are capable of providing effective treatment to the patient. Hospital has various advanced services like an emergency ward (McCullagh et al. 2021). It can be specified that as the organisation is largely located in London and being popular has made them a centre of attraction for implementing attacks on their services so that their performances can be reduced. Also, the organisation is working remotely as well which can add a large number of security threats due to the utilisation of their personal networks while adding their personal details to the network of the hospitals.

While being a large organisation and having advanced services there is still the possibility that organisations are experiencing Cybercrimes ranging from the data breaches to the unauthorised access in their database as well as financial accounts.  When a renowned personality is involved with the organisation there are still chances of digital impersonation which can reduce the positive impact of the organisation when they initiate to provide various services (Schroeder et al. 2017).

**There are few assumptions that can be taken into consideration while analysing the possibility of threats among the organisation:**

* There are high chances of disruption among the organisation through which cybercriminals can easily distract the organisation which can cost money and time.  As the organisation has a large number of advanced technology services the distraction can occur from any network which can hamper the productivity of the organisation. It will be easier for the cyber criminals to get access to the information that is very much sensitive to the organisation (Qiu et al. 2020). Currently the trend of ransomware attacks has made this task easier for the attackers.
* The organisation might also face difficulties due to distortion of the data as well as the technology that can be utilised by the criminals for manipulating the data and make the employees vulnerable for compromising their security as well as sensitive information.
* There might be a scenario where attackers can take over the control of every business practice that is carried out among the hospital.  The possibility of Deterioration is very likely among the organisation as there can be unexpected outcomes that will be inviting cyber criminals to the organisation for the exposure of their vulnerabilities.

All these assumptions have been stated on the basis of general capabilities in a large-scale organisation which deals with simultaneous activity while including personal details of the patient and the hospitals. The assumptions are also highly dependent upon the aspect of working remotely that can affect the security of the organisation with the addition of personal detail.  It can be stated that the major threat of data leakage among the organisation is because of working remotely as there is the utilisation of public networks and giving information on the public networks.

# **Organisation and Business Unit operations**

It has specified that there are a number of activities at Royal London hospitals. The company has become internationally renowned for teaching and providing Healthcare services to the patients because of which they have found an effective position in the market. The organisation is concerned with treating the patients for chronic conditions and detecting early cancer stages.  While providing a large number of health care services the company has been distributed widely in London where they provide a number of facilities. They have a full range of specialist services as well as local services. It has also been considered as the largest hospital for children and has the busiest schedule for dealing with emergency departments and paediatric accidents. They also provide first class Oral and Dental Health Care and they have been recognised as a specialist for these services.  Apart from that the business units of this organisation have been listed below:

**Overnight accommodation-** The hospital provides overnight accommodation to the family of the patient who has been admitted to the hospital. The involvement of stakeholder in this business unit are ward staff and pre-admission staff who are responsible for checking the availability for the accommodation related to the patients and their relatives. Overnight accommodation is consistently required by the relatives of the patient being in a critical condition. The organisation has reflected this requirement by providing a wide range of services through which they can easily take care of the patient by staying at the hospital.

**Constraint:** There is a possibility that during the peak hours availability for every relative cannot be available in the hospital premises, which can be considered a major constraint in these services. Also, as there will be various options available for the accommodation the people belonging from high class might not be getting the required accommodation facilities in case of unavailability.

**Stakeholder:** The management of this facility can be provided with the administrative department of the hospital who has the record as well as previous history of the patient. It is the responsibility of the administration to take care of the accommodations related to the patient as well as their relatives so that they can take full advantage of this facility. Apart from this, ward staff is required to fulfil all the requirements related to the relatives as well as providing them all the necessary facilities which can help them in taking care of their patients. They are responsible for maintaining the records of the patients and time and hours they will be staying at the hospital.

**Telephone services:** The Hospital also provides telephone services that have been directly linked to the taxi companies so that it can be easier for the patients and their relatives to travel from one branch to another branch of the hospital if they have been advised to do so. It is one of the major requirements for the people coming from different locations. The relatives of the patient might also require continuous taxi services so that they can fulfil the requirements of the patient and make the medicines and other facilities available for their patients.

**Constraint:**  During the peak hours the relatives might be asked to wait for a longer period of time even if they are requiring the services in an emergency. This aspect cannot be ignored by the hospital staff.  Also, people might not be satisfied with the extra charges caused to them while taking the taxi services from the hospital.

**Stakeholders:**

* The staff at the reception is responsible for making the tax arrangements for the hospitals. They are required to maintain the record of the available taxi and update it simultaneously so that no error can be faced by the patient and their relatives.
* The cab driver is also one of the major entities in this aspect as they are required to continuously provide information to the hospital while being available for their patients as well as for their relatives.
* The relatives are responsible for booking the taxi services in advance so that they can avoid the unavailability of taxi services.

**Restaurant and kiosk:**  The hospital provides the services for the visitors as well as the patients for the food services. This is provided by a specific sector of the hospital that has complete arrangements for the patients and their relatives for having their meals that are available in the hospital's restaurant. This is the foremost requirement that can be asked by the patient and their relatives because of which hospital has provided an easier facility for this.  It can be a challenge for the hospital to handle the large number of people coming to their food facilities as it is one of the essential requirements of the people.

**Constraints:** There is a possibility of unavailable seating arrangements for the patient during the peak hour which is required to be extended due to the crowded scenario.  In order to avoid the crowd, the hospital is required to make necessary arrangements by updating the number of people that will be coming to the restaurants.

**Stakeholders:** The restaurant manager is required to assess the facilities that are required to be provided by them. They are responsible for analysing each the number of people coming to the hospital in a single day so that they can manage all the arrangements for each of the patients and their relatives.

# **Assumptions**

While analysing the business units and operation carried out at the royal London hospital there are some assumptions that are required to be assessed properly in case it is witnessed in the future for the organisation is currently facing issues related to the security among the organisation. There can be a number of risks present in your organisation which can hamper the regular activities carried out by the management and administration of the hospital. Also, it has been analysed that with the presence of a number of stakeholders there is a possibility that stakeholder’s responsibility can lead to the invitation of cybercrime to the network of healthcare organisations.  There can be number of incidents which can lead to data loss which is very crucial for the patient and in this scenario the given below assumptions are required to be considered so that it can be mitigated beforehand with the prior solution for it:

* There is a possibility that branches of the hospital associated at the lower level of the organisation might share the data which can profit them in terms of monetary evaluation.  When Hospital staff maintain the record of patients there is a lot of data accumulation taking place regarding each and every relative aspect of the patient.  This can be misused by the staff member if they are not evaluating the data with the implementation of standard practices.
* Due to the aggregation of data in large amounts there is a requirement of advanced analytics methods that might not be present currently at the organisation because of which standardization of the data is not possible. This aspect led the organisation management to the improper management of data and not updating the data continuously which can result in uncertain record maintenance of the patient.
* The people coming from different locations at the prime location of the hospital might have difficulties in getting access to the various facilities which can lead to the unknown data of the patient as it is not possible for the hospital to have every detail of the patient during their visit to the hospital. There is a risk of admitting patients without sufficient details as they can misuse the resources available in the hospital.
* While implementing various policies in the organisation for protecting the data it is important for the organisation to consider the accessibility to the consumers as well as the reliable entities and stakeholders of the organisation.  However, most of the organisation does not think through the perspective of various relative entities which can lead to cyber threats as well as data breaches.
* As the organisation has a popular name in the Healthcare industry there are chances that the organisation is completely ensured that their data is completely secured and will not be attacked in the future.  The organisation is required to eliminate this perspective as while handling a large number of patients the attackers can benefit from maintaining a large number of patients at the same time. The large accumulation of patients will not be manageable by the organisation due to which they might end up losing their sensitive information to the attackers.
* The hospital is still extending their services at various locations that can lead to the possibility of data breaches by handling and controlling the environment loosely at the initial level. It is important for the organisation to assess the possibility of risk and threats in the organisation before implementing a new technology in their infrastructure.

The assumptions above described are related to the management and administration handled by the organisation. It is largely done for the management of data that are accumulated in the organisation on a regular basis. It is important to analyse each aspect so that the possibility of data breaches and other security theft can be reduced in the organisation and the hospital can efficiently manage the patient's record while providing enhanced and optimised services to their patients.

# **Key Assets**

An asset of an organisation is considered as a value to the organisation. As the chosen organisation belongs to the healthcare industry, there is a requirement of information security to focus upon the risk evaluation related to the assets which are highly dependent upon the information and responsible for storing the information. For the chosen organisation the important assets will be falling in the category of information system, People, services, and applications which are related to the organisation. These assets are highly related to the data which are generated in the hospital on a regular basis. In order to assess the critical assets related to the hospital there is a requirement of preventing the records being disclosed to the unauthorised people as well as it is important to save the data from getting lost and destroyed. The modification and authorisation should also be prohibited in the systems of hospitals that can be carried out by the cyber criminals.  The interruption during the data access should also be avoided so that organisations have the capability of fulfilling their purposes and continue with their regular activities. It is important for the organisation to analyse the critical acids properly so that they can prevent the regular activities in their systems and in their network.

The following will be the critical acids which has been identified for the chosen Hospital organisation:

* The Database used for maintaining the records in the organisation has been considered as one of the major critical assets for the hospital. It is a database which is used for storing the data related to the patient as well as the services provided by them. When a patient visits the hospital, it is the responsibility of the hospital to fetch the Record of the patient because of which has been considered as the most important asset in the organisation.
* Apart from using databases the hospital staff also maintains paper-based records which is considered as official documentation. Nowadays, these documents are scanned and uploaded to the database of the hospital because of which it is required to be preserved as it is going to be utilised for further formal activities that are going to be related to the patients coming to the hospital.
* It has been obtained that the hospital also provides emergency services because of which they have integrated a system called emergency data care system in their infrastructure. This system is responsible for maintaining as well as updating the records of patients and all the formal activities that are required to be carried out by the patients. This management system is also responsible for completing the building process in the case of Emergency due to which it is required to be given with high priority so that in the case of an emergency hospital can focus on the patient rather than completing the formalities.
* The hospital is continuously expanding and it has employed a large number of staff because of which the utilisation of personal computers takes place in a wide range. Each of the hospital staff is dependent upon their personal computer for accessing the system and fetching the information related to the patient for completing their roles in the organisation.  This is one of the highly critical assets to the organisation as the activities and the roles are relied upon the personal computers utilised by the staff members and the doctors. This asset is required to be secured with advanced tools so that each area can be covered specifically in terms of maintaining the data.
* The organisation is associated with health care services trust because of which it is the responsibility of the trust to maintain the computing infrastructure of the hospital so that they can maintain the network and communicate with each other on a regular basis for providing updates related to the patients and services which have been provided by the patients and their relatives.
* The administration of the hospital also comes under the critical assets as they are responsible for maintaining each of the records which are related to every activity that are carried out among the hospitals. The doctors as well as the patients are required to go through the administrative department that makes this asset more vulnerable as well as critical to the organisation. It can be stated that it is the key asset which is formulating each of these services that are carried out among the organisation.

These assets are required to be highly secured by fulfilling all the security requirements that determines a secured infrastructure of the organisation. It is the responsibility of the organisation to analyse the data which are highly beneficial for their organisation and that can help them in improving their performances. In terms of maintaining the security the major requirement of availability, confidentiality, and integrity of the data is required to be maintained so that they can reduce the possibility of attacks among the organisations.

# **Threats and Exposure Research**

The Royal London hospital has gained popularity internationally because of which they are required to have the advanced system in their organisation and make their services Easily available to their customers. After the advent of digital transition around the world it has been recognised that a large number of healthcare industries are completely relying upon Technology for carrying out their daily activities and maintaining sensitive records related to their business. On the basis of an organisation, the organisation is highly equipped with advanced technologies because of which they are capable of providing services to the patient in a large range by distributing their services to various locations in London.  It has been analysed that as the current digital changes has provided ease of usability among the organisation it has also welcomed large number of threads among the organisation as organisations are highly dependent upon computers and other information management systems due to which the organisation is becoming more vulnerable than the utilisation of traditional management system in their organisation (Svečnjak et al. 2021). It can be stated that as technology has made the organisation vulnerable but it also has a large number of solutions which are required to be recognised by the organisations so that they can make suitable implementation for reducing the impact of threats and vulnerabilities that are present in their organisations.  While analysing the working of healthcare industry the major threats which have been recognised for the royal London hospitals have been listed below:

* The **mobile devices utilised** for the hospital application which is providing the functionality of checking the availability in the hospital as well as updating their medical records and getting recommendation from the doctor.  This has been considered a major threat to the organisation because the patients use their personal network for fetching the information of the hospital and it is easier for cyber criminals to get into the system while hacking it and fetch the data related to health care services.  These devices are prone to the security breaches which can impact on the data available in the databases of the organisation related to the patients. This can be mitigated through advising the patient for using the application in high security and implementing a security tool which can restrict the utilisation of application without having complete information of the patient. In this manner authorisation of patients will be carried out and only the verified patient will be allowed for access in the application of the hospital.
* **Insider misuse** by the staff member of the organisation can make the system utilized in the infrastructure of the hospital more vulnerable. It has been analysed that major security breaches that have occurred in the past few years are due to insider misuse. This type of threat is committed by the employees of the organisation itself for the purpose of stealing the properties and committing related crimes for gaining more profit from the organisation. In most of the cases it has been realised that the sole purpose of getting employed in the organisation is stealing the data and accessing Healthcare records of the patient for misusing it (Ravi et al. 2019). It is the responsibility of the organisation to make a policy while hiring an employee in their organisation and check the back history of them so that they can reduce the threat of inside devices used in the organisation.
* The **unintentional actions** of the staff member can also lead to the security threat in the Healthcare organisations.  These often occurred due to the utilisation of outdated systems which have already been discarded and the information related to the patient is not removed. In such scenarios staff members tend to display the information of the patient by utilising the discarded system in the case of unavailability of current systems (Gwebu et al. 2020). Every time a system is outdated it is the responsibility of the hospital to update the system regularly and remove the system that have been discarded already by a staff member. During the time of discarding a system the employee can also remove the data that have been recorded in the system.
* **Supply chain** of the organisation is also required to be overlooked as the hospital consists of interacting with the Trustee members as well as patients on a regular basis. This activity has a wide potential of having data breaches in the organisation as it was transactions and sensitive Communications which is required to be secured. This threat can be mitigated through checking the security at every step of transaction and communication that are carried out among the organisations. Every transaction should go through security protocols so that the transactions can be authorised and the risk of supply chain threats can be reduced in the organisation. The hospital is responsible for authorising and authenticating each of the transactions that are carried out among the organisation while interacting with different stakeholders.
* **Ransomware:** Malware has been considered as one of the most serious problems around every kind of Industry. In the sector of healthcare malware infection can cost life and death to the patient. The industry of Health Care is required to deal with patients' lives which cannot be hampered by any cybercriminal attacker. However, with the utilisation of ransomware the attack is very much possible to the hospital. Majorly interlocking that works which is possible for communicating the information related to the health of patients are available to the attacks of ransomware. The most popular example of WannaCry attack at the at the various Health Care trust force to the hospital for closing doors to the new patient and the treatment of existing patient was interrupted as the accessibility to the records was restricted by the attackers.  This attack is one of the dangerous attacks to the Royal London hospital as well because it is associated with trust and it has expanded its organisation to various locations which are vulnerable to malware and ransomware attacks (Clauson et al. 2018). The mitigation of ransomware can be carried out with the utilisation of content filters and Virus scanner among the mail server of the organisation. This has been considered as a smart way for preventing the attack of ransomware. It helps in reducing the spam risks inside the computer system that is having malicious attachment as well as infected links that are inside the mailbox of the employer (Spence et al. 2018).  It is important to reduce the effect of ransomware so that the risk of providing access to Cyber criminals can be reduced and the data is preserved among the organisation.
* **Phishing:** The Healthcare sector is also at the risk of phishing attacks as there are about 66% malware are initiated with the utilisation of email attachments. In this type of attack the data related to the patient and other personal data becomes vulnerable to the cybercriminal as they implement huge threat to the login credentials of the patient and administration that are utilising the system of the organisation. It has been analysed that it is one of the easiest methods for accessing the data from the patients as most of them are curious about the email attachments which lead them to open the attachments containing malicious activities (Thomas et al. 2017). In order to reduce the impact of a phishing attack, organisations are required to utilise an SSL certificate so that they can be capable of securing all the traffic that is coming and going from the website of the organisation. This certificate is important for protecting information that has been sent among the web server and browser of the customers (Priestman et al. 2019). This can also help in reducing the threat of eavesdropping and ensure that computers are highly protected against the cyber criminals that are willing to implement phishing attacks on the system.
* Nowadays the utilisation of **cloud computing** is highly integrated with the Healthcare services as they are provided with improved access and cost efficiency related to the data. These systems are required to be correctly protected as they are vulnerable to cyber criminals as the resources for cloud computing are made available through third parties which cannot be secured without having suitable measures like encryption. Encryption is required to be imposed on every store data so that it can be appropriately handled in the organisation and risk related to losing the data to the third party can be reduced (Ahmed et al. 2018). There are various ways through which Cloud Computing can be protected that includes implementation of access and identity control.  Most importantly, the organisation is required to have multi-Factor authentication while having a strong password so that access cannot be provided to any outside of the system (Carre et al. 2018). It is very important for the organisation to monitor the behaviour of the user all the time so that identification of sensitive information can be carried out. A cloud computing environment can also be secured among the organisation through revoking excessive exercise for the sensitive information. the account which has not been currently and used is required to be removed with its credentials while applying the principle of least privileges.
* **Distributed denial of service attacks:** the hospital organisation is highly reliable on the iot devices for measuring the disease and other scales related to the analysis of disease among a patient. These devices are vulnerable to the ddos attack as they come with the potential threat of disrupting the treatment. This is one of the major attacks because it contains personal data of the patients that can lead to the issues of redundancy. In such scenarios denial of service attacks can easily be imposed on the organisation where data will not be possibly prevented from the cybercriminal which are highly critical to the organisation (Salemi et al. 2021). The distributed denial of service attack can be reduced by knowing the traffic of the network and creating a plan for the response. It is important for the hospital to make their network resilient and have better cyber hygiene so that they can always filter the unauthorised users in their network (Mantzana et al. 2020). Hospitals can also limit the router for preventing their web server from the outsider and add filters on the router for dropping packets for the attack sources that are obvious. The implementation of the DDOS protection can also be utilised for monitoring the traffic at the website so that illegitimate access is denied by the network itself.
* **Authentication issues** are always there among the organisation which makes it difficult for maintaining the computer interfaces while enjoying their usability and security. even if the users have their unique passwords, it is quite dangerous to use it without having any two factor methods.  It is important for the organisation to implement it correctly so that high degree mitigation techniques can help in reducing the effect of authentication issues. Two factor authentication provider facility through which users’ passwords are secured and it cannot be utilised by the cybercriminal which can lead to preserving the system while analysing all the security patterns that are required for accessing a particular system (Viswanathan et al. 2021). two factor authentication provides a security aspect which is required to be utilised in almost every system for reducing the threat of Cyber criminals inside the system. Authentication issues can be present in the hospital as there are a large number of staff having unique passwords but not having two factor authentication methods. It will be easier for anyone to get access to the system of the staff as they are not having two factor authentication methods Which will be easily providing access to the cybercriminals.
* Nowadays **Legacy applications** are highly utilised among the hospitals that are leaving gap holes for cybercriminals as they can easily take advantage of such applications. These applications enable cyber criminals to exploit the vulnerability of the system which cannot be retained. In this type of scenario, the recommendation can be made for using penetration testing so that vulnerabilities can be found among the infrastructure of the organisation (Alkinoon et al. 2021). Penetration testing helps the infrastructure for evaluating the exploitation made on the systems vulnerability. In this type of test the tester usually tests the service, application, networks, and other entry points for finding the weakness among the system which reduces the impact of Systems exploitation by the cyber criminals.

# **Risk Assessment and Risk Treatment Strategy**

Table 1: Risk assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serial no.** | **Risk scenario** | **Potential damage** | **Risk likelihood** | **Impact** | **Mitigation** |
| **1.** | The patient and the hospital staff are highly utilising mobile devices in the organisation which includes a large number of risks with the utilisation of their personal networks. | A huge data loss and error in data management can occur among the organisation due to which the organisation might suffer a lot in managing data related to the patient in presenting the correct record of the patient. | High | High | There is a requirement of using more validated access control in the mobile devices used for hospital application. |
| **2.** | Insider misuse can be witnessed among the organisation for making the infrastructure vulnerable to the cyber-attack. Their employees hired to the hospital might have the sole purpose of getting into the hospital for accessing the data that can provide them personal benefits apart from the hospital. | These threats can lead to the data sharing of the patient which is very sensitive to the hospital and can be misused in a number of ways for example gaining access to the higher authority computers and fetching the data related to the upcoming transactions (Cagnazzo et al. 2018). | Medium | High | Insider misuse can be prevented through reducing the usability of the system by newly hired staffs. It would be better if hospital will first monitor the activities and record performances. |
| **3.** | Unintentional actions of staff members and a large number of security threats among the organisation.  This threat can be present among the organisation due to the availability of discarded and outdated systems. | The utilisation of outdated systems can make the infrastructure vulnerable to the cyber criminals which can provide them access to the actual records of patients that have been previously stored in the discarded systems (Siow et al. 2020). | Low | Medium | It can be advised to keep the system up-to-date so that the system will not be required to discarded. |
| **4.** | Ransomware attacks are very likely in the hospital as there are a large number of staff members who rely upon computer systems for keeping the information and updating each other about the upcoming task that has been allocated to them. | Cyber criminals can get all the information related to the staff members as well as they can interrupt the communication carried out among them and provide them wrong information to do some malicious activities. | High | High | The utilisation of virus scanner as well as content filtering and reduce the likelihood of ransomware attacks. |
| **5.** | The hospital is widely using Cloud Computing services for their database management which can add large number of threats to the organisation that can lead to the hospital losing their data as well as having the data manipulated. | The organisation will no longer be capable of managing the data related to the patient efficiently and they will require a lot of time to recover from the data loss which can also lead to giving wrong information to the patient. | High | High | Multi-factor implementation at the system utilised in the hospital is necessary to secure the cloud environment. |

# **New technology to the operations**

With the advancement of technological aspects, the Healthcare industry is already known to the next level due to which they are now capable of providing vast services to large numbers of patients at the same time. In this manner the major transition that has been witnessed is booking appointments and consulting doctors in the utilisation of mobile devices (Hewitt et al. 2017). There are a number of applications and websites present related to the hospital through which patients can gain instant advice from their doctors while booking the appointments (Sultana et al. 2020).

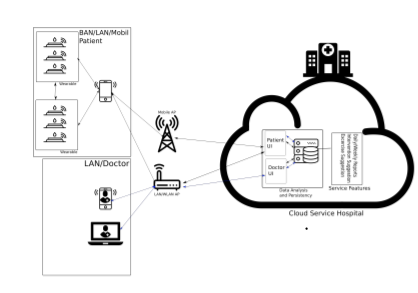


Figure 1: New architecture for healthcare organisation

(Source: Cagnazzo et al. 2018)

However, with the increase of these systems, the organisations are also facing a large number of security issues as the communications are carried out on a large scale and they are also involving financial transactions for booking the appointments and consulting to the doctors. This has made the complete system vulnerable for the hospital. Also, it has been analysed that the policy of bringing your own device in the hospital has added more risk in the healthcare industry as the workers are allowed to utilise their own devices while having the access to the organisational network (Senthilkumar et al. 2017). The major aim of BYOD policies was to increase productivity and reduce the complications that are faced by employees in learning a new computer system. Although it has provided a flexible environment for working to the hospital as well as for the employees and obtained increased effectiveness while having all the comfort and speed.

Apart from having a number of advantages added risk with the utilisation of personal computers and connecting to the organisation network. The major disadvantages that have been witnessed due to the utilisation of mobile devices is the data breaches among the personal data of the patient as well as the company as it is easier for the cybercriminal to steal the personal data of the employee as well as the patient (Rizvi et al. 2020).  Other than these risks there is a risk of lacking in Firewall and antivirus software which are required for supporting the personal devices.

Table 2: Risk treatment strategy (Modified)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serial no.** | **Risk scenario** | **Potential damage** | **Risk likelihood** | **Impact** | **Mitigation** |
| **1.** | Lack of firewall | The network will not be filtered to prevent the unauthorised access. Cybercriminals will easily be get into the system. | High | High | Install firewall at all the gateways of the network. |
| **2.** | Poor BYOD policies | It will be easier to get into the personal devices of the staff members and the data stored in the computer will be lost. | Medium | High | Add various authentication protocols to the BYOD policies (Dasgupta et al. 2017). |

# **Conclusion**

The report is based upon identifying the risk and thread availability in the royal London hospital. It has been analysed as a multi-speciality hospital which provides a large number of services to the patients. As it has been recognised internationally, they are using advanced technological advancement due to which there are a large number of threats present in their organisation. Some major threats which have been analysed in the organisation are because of using the mobile devices and cloud computing databases.  The services have provided flexibility of working and maintaining records of the patient but poor management and poor policies can lead to the inviting the cyber criminals to the networks.  The report has added a risk treatment strategy on the basis of which it has been analysed that it is important to validate each access among hospital networks and monitor the activities that are carried out by the attacker so that malicious activity can easily be obtained.  Apart from this, the changing need of working remotely is equal to the facility of BYOD in the organisation.  In this scenario your organisation is required to make strict policies Regarding the utilisation of personal devices and ensure that it has all the capabilities that are matching to the security requirement of the hospital. It can be stated that even if a large number of threats are present an effective management of activities that are carried out among the organisation can reduce the risk of losing data and having the risk of data breaches in the organisation.

# **References**

* Leblanc, R., 2021. The birth of experimental neurosurgery: Wilder Penfield at Montreal’s Royal Victoria Hospital, 1928–1934. *Journal of Neurosurgery*, *1*(aop), pp.1-8.
* McCullagh, J., Proudlove, N., Tucker, H., Davies, J., Edmondson, D., Lancut, J., Maddison, A., Weaver, A., Davenport, R. and Green, L., 2021. Making every drop count: reducing wastage of a novel blood component for transfusion of trauma patients. *BMJ open quality*, *10*(3), p.e001396.
* Schroeder, L., Patel, N., Keeler, M., Rocca-Ihenacho, L. and Macfarlane, A.J., 2017. The economic costs of intrapartum care in Tower Hamlets: A comparison between the cost of birth in a freestanding midwifery unit and hospital for women at low risk of obstetric complications. *Midwifery*, *45*, pp.28-35.
* Qiu, H., Qiu, M., Liu, M. and Memmi, G., 2020. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics*, *24*(9), pp.2499-2505.
* Svečnjak, L., Nunes, F.M., Matas, R.G., Cravedi, J.P., Christodoulidou, A., Rortais, A. and Saegerman, C., 2021. Validation of analytical methods for the detection of beeswax adulteration with a focus on paraffin. *Food Control*, *120*, p.107503.
* Gwebu, K. and Barrows, C.W., 2020. Data breaches in hospitality: is the industry different?. *Journal of Hospitality and Tourism Technology*.
* Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A. and Margolis, D., 2017, October. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434).
* Carre, J.R., Curtis, S.R. and Jones, D.N., 2018. Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*.
* Mantzana, V., Darra, E. and Gkotsis, I., 2020. Cyber-Physical Security in Healthcare. In *Safety and Security Issues in Technical Infrastructures* (pp. 63-87). IGI Global.
* Siow, W.T., Liew, M.F., Shrestha, B.R., Muchtar, F. and See, K.C., 2020. Managing COVID-19 in resource-limited settings: critical care considerations.
* Sultana, A. and Sobhan, A., 2020. RFID in Healthcare Systems.
* Hewitt, B., Dolezel, D. and McLeod Jr, A., 2017. Mobile device security: Perspectives of future healthcare workers. *Perspectives in health information management*, *14*(Winter).
* Rizvi, S., Pipetti, R., McIntyre, N., Todd, J. and Williams, I., 2020. Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*, p.100240.
* Viswanathan, G. and Jayagopal, P., 2021. A Threat Categorization of Risk-Based approach for analyzing Security Threats early phase in SDLC. *Arabian Journal for Science and Engineering*, pp.1-13.
* Alkinoon, M., Choi, S.J. and Mohaisen, D., 2021, August. Measuring Healthcare Data Breaches. In *International Conference on Information Security Applications* (pp. 265-277). Springer, Cham.
* Clauson, K.A., Breeden, E.A., Davidson, C. and Mackey, T.K., 2018. Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An exploration of challenges and opportunities in the health supply chain. *Blockchain in healthcare today*.
* Spence, N., Niharika Bhardwaj, M.B.B.S. and Paul III, D.P., 2018. Ransomware in healthcare facilities: A harbinger of the future?. *Perspectives in Health Information Management*, pp.1-22.
* Priestman, W., Anstis, T., Sebire, I.G., Sridharan, S. and Sebire, N.J., 2019. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics*, *26*(1).
* Ahmed, A., Latif, R., Latif, S., Abbas, H. and Khan, F.A., 2018. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: A systematic literature review. *Multimedia Tools and Applications*, *77*(17), pp.21947-21965.
* Salemi, H., Rostami, H., Talatian-Azad, S. and Khosravi, M.R., 2021. LEAESN: Predicting DDoS attack in healthcare systems based on Lyapunov Exponent Analysis and Echo State Neural Networks. *Multimedia Tools and Applications*, pp.1-22.
* Ravi, A.R. and Nair, R.R., 2019. Cybersecurity threats and solutions in the current e-healthcare environment: A situational analysis. *Medico Legal Update*, *19*(2), pp.141-144.
* Cagnazzo, M., Hertlein, M., Holz, T. and Pohlmann, N., 2018, April. Threat modeling for mobile health systems. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (pp. 314-319). IEEE.
* Dasgupta, D., Roy, A. and Nag, A., 2017. Multi-factor authentication. In *Advances in User Authentication* (pp. 185-233). Springer, Cham.
* Senthilkumar, K. and Easwaramoorthy, S., 2017, November. A Survey on Cyber Security awareness among college students in Tamil Nadu. In *IOP Conference Series: Materials Science and Engineering* (Vol. 263, No. 4, p. 042043). IOP Publishing.