

**PROBLEM-SOLVING AND DECISION MAKING IN HEALTH
AND SOCIAL CARE**

STUDENT NAME: ZAINAB JALLOH

STUDENT ID: 2008337

MODULE ID: BMSW4004

Table of Contents

Introduction.....	3
Overview of the health care issues.....	3
Choosing a healthcare issue	4
Impact of a cyber security issue on the stakeholders.....	6
Analysis of decision making process	7
Alternative solution for controlling cyber security	9
Decision making techniques	10
Solution implementation and stakeholder's communication.....	11
Review and monitoring the implemented solution	12
Conclusion	13
Reference list	15

Introduction

The Healthcare centre (HCC) is a sensitive industry and connected to the people physically, emotionally, mentally and financially. Discussing the challenging issues would help to modify the activity level in the HCC. It becomes essential to give focus on the new technology and economy in the HCC. The introduction will give a general outline of this report. Different HCC issues will be discussed in the project. Controlling cyber security technology has a huge impact on the HCC. Taking an appropriate solution will help to eradicate the problematic situation in the HCC. Different tools and techniques would be used for solving challenging situations for managing HCC issues. A decision-making strategy will help to identify some solutions for controlling health care technology for developing cyber security. Implementation of the solution and stakeholders' communication will help in managing this issue. Review and monitoring will help to justify the implemented solution. A conclusion will be given to justify this project.

Overview of the health care issues

Nowadays, immense HCC is suffering from different challenging situations in the company. Focussing on the challenging issues would help to make suitable decisions for improving the management issues in the HCC.

Controlling advanced technology

During this current situation, it becomes essential to control hardware and software systems in the HCC. It becomes essential to increase the use of cyber security technology from 2017. According to the *Health Solution Report* in the UK, without cyber security, it becomes quite critical for managing all activities. According to Dos Santos (2020), nearly **48% of medical devices** are completely connected to the **IoT**. Using a cyber-security process would help to increase the efficiency level in the company. Lack of knowledge in the HCC's employees is responsible for the restriction of the economic stability in the medical sector. Clinicians, health care organiser and the entire managing department are suffering from different challenging issues in the company.

Lack of cyber security

Lack of cyber security in the HCC causes huge issues the HCC. It becomes essential to keep all records of important data for managing HCC performances. There are immense malicious hackers to hack different information. According to Kalabikhina (2020), *healthcare data breach statistics* are showing the upgrading issues in the HCC. Healthcare organisers are becoming more responsible for providing enough security to keep safe all necessary data in

the company. Technological advantages will give enough security for managing organisation's issues in the HCC.

Increasing healthcare cost

Cost crisis is becoming one of the huge issues in the HCC. Many employees in the HCC are responsible for increasing the cost of HCC's services and medical instruments. As per Martin Gaynor, a successful economist has said, ***"Health care spending is high, and it is ultimately unsustainable."*** A huge number of people are suffering from the economic crisis; increasing HCC is becoming difficult to take people. In the opening of Franklin *et al.* (2019), many clinicians recommend unnecessary tests to **42%** of patients.

Payment procedure in HCC

Inefficiency in the payment processing system is increasing the problematic situation in the HCC. As per the opinion of Surr *et al.* (2017), nearly **15% of people** faced many difficulties for completion of the payment procedure in the HCC. HCC needs to simplify the entire process for maintenance of the flexibility in the HCC. ***The Accountable Care Organisation*** takes responsibility for giving security to the employees for managing organisational activities.

Choosing a healthcare issue

HCC needs to keep all patients' records in a systematic way. According to the recent report, immense malicious hackers are responsible for hacking necessary records. According to McCann and Brown (2018), HCC's data breaches report is gradually increasing, from 2009 to 2018 HCC are suffering from huge problems with cyber security. A huge number of health records are exposed every year. ***Patient Administration System (PAS), Appointment Management System, Laboratory Information Management System*** needs to be more careful about the efficiency of HCC. As per the opinion of Jennings *et al.* (2017), 59% of the HCC who are suffering from a lack of cyber security is present in the US. A huge number of HCC has been attacked in 2014. Public and private HCC were bound to spend millions of costs for managing all these activities in the company.

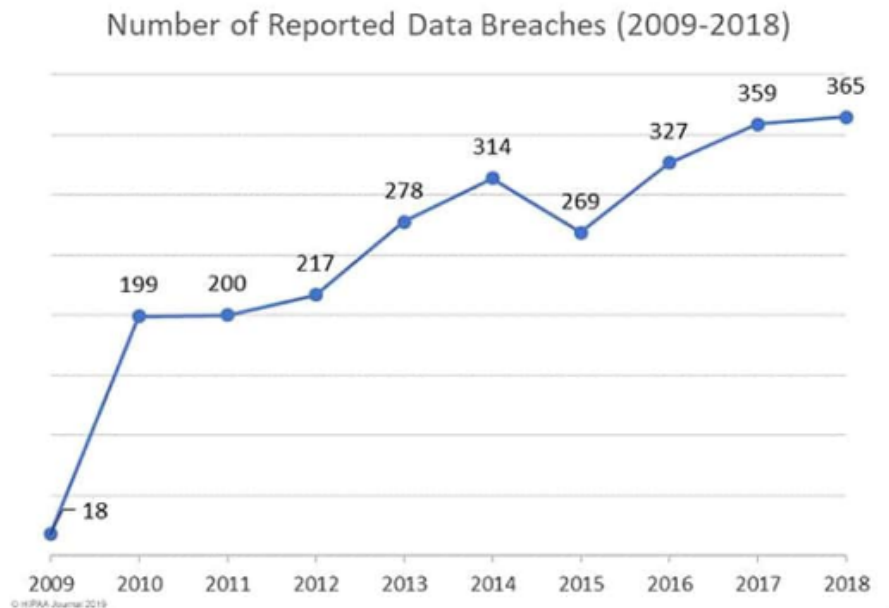


Figure 1: Data breachment report

(Source: Jennings *et al.* 2017)

As per above-mentioned picture, the data beached record was significantly low in 2009. Day by day, the number of breached cases is increasing. In 2018, it has reached the highest place in the data breachment cases. A huge number of the HCC was attacked in 1014.

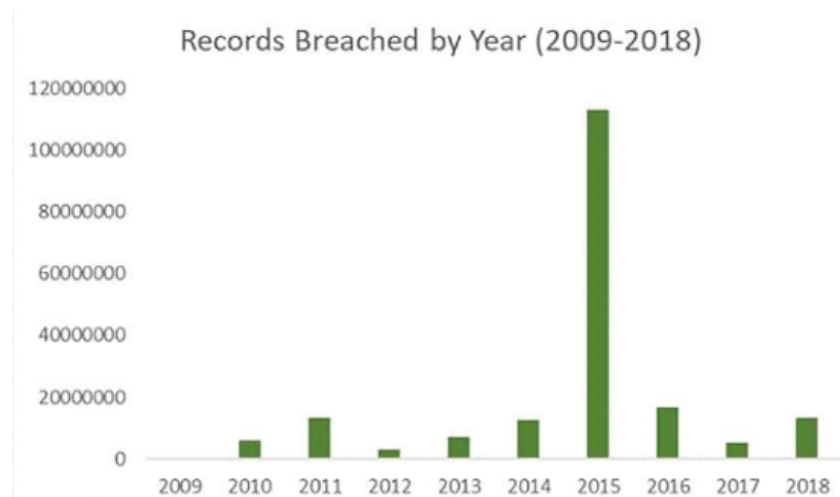


Figure 2: Yearly record breach

(Source: Carr and Luth 2017)

Healthcare administration has taken the responsibility to increase the technological advantages for developing business performances. It is necessary to be more conscious about the importance of advanced technology for maintenance of the security in the HCC. It is important to keep all data safe in the HCC. Healthcare administrators have taken several strategies to reduce the chances of data breachment in health care.

- Constructing a centralized system will give security to the HCC to keep all data safe.
- Implementation of the security protocol would be used for managing different activities in the company.
- Making a suitable structure of the proprietary network would give security to keep safe all data in the company.

Impact of a cyber-security issue on the stakeholders

The entire stakeholder has taken the responsibility to show efficiency for management of the organisation's risk factors. IT and non IT leaders and business administrators have taken many responsibilities for managing cyber issues. Stakeholders are responsible to know about the “*culture of cyber security*” and “*culture of care*” in the HCC. Most of the HCC has developed a “*culture of care*” and “*culture of cybersecurity*”. According to Bilsker *et al.* (2018), higher authorities and the healthcare leader have recognised the importance of technical advantages to keep a patient's record safe, death record, and financial record and so on.

- The higher authority has implemented a safety culture in the HCC for maintenance of cyber security. It becomes a practice for giving a higher quality of the management services in the HCC.
- The managing director has recognised the importance of cyber security to eradicate enterprise risk. It becomes quite critical to the non-IT stakeholders or non IT leader for managing organisational activities.
- Stakeholders in the IT sector have decided to get trained for being efficient in the technology sector.
- CEOs, BOD, CxOs, and CISOs have different responsibilities in the HCC. It becomes quite difficult to be engaged in multi activities.
- Lack Of knowledge in the technical department increases the risk factors for improving business performances. All non-IT stakeholders are continuously struggling to get accustomed about the lack of cyber security in the HCC.
- Stakeholders in the HCC have decided to implement ***Legacy risk management approaches*** for reduction of the cyber threats. This approach is used for increasing awareness among the people about modern cyber threats.

In the opinion of Karami *et al.* (2018), nearly **28%** of executives suffer from lack of confidence to get engaged in technical activities. According to a recent report, from 2017 to 2019 cyber threats have increased due to inefficiency in accessibility and lack of confidence.

Due to lack of knowledge and inefficiency, there are huge chances for making inappropriate designs for developing cyber security. Due to these reasons, data breaches have increased from **9% to 18%** in the HCC.

Along with these, it has been recognised that some stakeholders are involved in the data breached for personal profitability. In the words of Hilty *et al.* (2019), nearly **70%** of the US HCC has decided to give security to HCC by eliminating dishonest employees. It becomes quite difficult to trust employees for keeping all necessary data safe in the HCC. These cyber breaches have made a huge impact on the employees (Pinkney and Walker, 2020). The higher authority has decided to train all employees by giving technical knowledge for restricting data breached in the HCC.

Analysis of decision making process

There are seven steps for completion of the decision-making process in the HCC. These steps would be discussed in the following section

- **Decision identification**

Before taking any decision, it is necessary to identify the risk factor of data brachmentin the HCC. Development of the security culture could be effective for solving different problematic situations in the HCC. Detecting the risk factors would help to utilise appropriate strategies for better performance in the HCC.



Figure 3: Decision making process

(Source: Hua and Shaw 2020)

- **Gathering information**

Gathering information about the efficiency of the cyber security process would help to adopt some strategies. Knowing about the government cooperation would help to rectify all problematic areas in the HCC.

- **Alternative solutions**

Apart from developing security culture, there are many other strategies like using **firewalls**, **protecting computers and mobile devices** could be appropriate for managing several issues in the company.

- **Evidence weighing**

After choosing an alternative solution, it becomes important to know about the positive and negative impacts of the chosen solution. In the words of Hilty *et al.* (2019), it is also necessary to know about the impact on the HCC. Before adopting an alternative situation, it becomes essential to discuss with the higher authority and

- **Choosing alternative situation**

Choosing an appropriate solution is important in the decision-making process. Stakeholders are responsible to discuss with the higher authority to choose firewall or other techniques for data protection in the HCC.

- **Taking action**

The next step is to conduct a plan for the identification of any types of obstacles in the decision making process. The higher authority is responsible to develop a suitable plan for managing different activities in the HCC. Involvement of the **PDCA cycle** would help to complete the activities in a systematic process.

- **Review**

Reviewing the entire decision making process will help to manage all activities in a systematic process. It is important to execute the whole process for eradication of the data breached.

Developer	Admin	Officer
The developer has the	CA and PKI support is	Implementing encryption

capability to encrypt all data	important	policies
Secret manager	LUKS setup	Needs to implement policies
Shared keys and discard	Using network policies are important to develop the business plan.	Knowledge sharing and cryptographic training is important

Table 1: Organisation's responsibility

Government legislation

The Federal Bureau of Investigation (FBI) is taking most of the responsibilities for searching any types of cyber risk factors in the HCC. *The Department of Homeland Security* is also involved to manage cybercrimes; it is also responsible to give protection to the HCC for better practices in the HCC. **DHS** and **FBI** have made collaboration with many military agencies for providing security to the HCC. It is important to understand the kind of cyber threats in the HCC. FBI and DHS are taking full responsibility to alert HCC for eradication of the risk factors. In the words of Hua and Shaw (2020) cyber bulletins have the capabilities to give information about adversary tactics, malware signature and current cyber threats.

In the opening of Carr and Luth (2017), *Computer Misuse Act 1990* has provided some ethics and regulations for maintenance of cyber security in the company. In case of fraud representation in the HCC, the UK government has launched *Under the Fraud Act 2006*, as per this act, the suspected people get ten years of imprisonment. Along with these, the UK government has introduced the *Data Protection Act 2018*, *Communication Act 2003* and *Privacy and Electronic Communication Regulations 2003* for providing security to the people for managing cyber issues in the company.

Alternative solution for controlling cyber security

There are many important strategies for the maintenance of security in the HCC. This section will discuss the importance of the alternative securities for eradication of the data breachment in the company.

- **Giving importance to the insider threat**

Giving focus on the insider threat would help to modify different activities in a systematic process. Stakeholders in the HCC need to hire efficient trustworthy IT experts in the HCC. In the words of Petrini *et al.* (2019), it is quite difficult to detect the insider threats in the HCC.

There are chances to send viruses through email. It is important to give focus on the application before accessing any data, link or software applications.

- **Encryption of devices**

In the opinion of Hanley *et al.* (2019), data encryption is highly recommended in the HCC for solving different cyber issues. In this modern age, people prefer to use personal systems in the workplace also. Encryption of all data will help to provide security to the HCC.

- **Making strong password**

Many employees in the HCC have a tendency to use relaxed passwords, which increases the risk of cyber security in the company. According to Hillson (2020), implementation of strong passwords decreases the chances of cyber hacking. Using one special character would be appropriate for decreasing risk factors in the HCC.

- **Upgrading programs**

According to Brouwers (2020), regular or periodic upgrading apps will help to eradicate the risk factors for solving data breached in the HCC. Installing security updating applications in the system or mobile will help to secure all important data.

- **Data backup**

In the opening of Silove *et al.* (2017), it is required to implement IT security strategy for managing all issues in the company. Securing all data backup would help to restore it in the HCC.

- **Limitation in-network access**

Many stakeholders in the HCC have the tendencies to install different software or accessing links. It may impact cyber security. In the words of Yüksel *et al.* (2017), there are immense malicious hackers trying to hack important data from the HCC. Discussing with IT professional before accessing link or installing any unsecured software applications.

Decision making techniques

HCC needs to adopt a decision-making strategy for management of all activities in the company. These approaches would be discussed in the following section. Before taking any decision, it is essential to know the objectives and goals of the HCC. Structure, budget, tie period are all included in the decision making process.

- **Problem awareness**

This is the first stage of the decision making process, in this stage BOD, CEO and other administrators become aware of the risk factors of data breachment in the HCC. As per decision makers, there are possibilities of hacking many important data.

- **Diagnosis cyber issue**

Decision-maker analyzes all problematic situation or challenges. As per Hua and Shaw (2020), cyber insecurities have the possibility of having all necessary data, cost reduction, hacking organisation's internal data in the company. Decision-makers are responsible to collect necessary sources about the risk factors of the company. Eventually, it will help to adopt important strategies. As per collective sources, there are **21% of the data breached cases, the threat of compliance fine and 27%** in the UK. Survey methods would help to collect information about these factors.

- **Developing alternative situation**

The next stage is to develop an alternative situation for solving the risk factors in the company. Eradication of the risk factors would help to rectify cyber issues in the company. Developing strong password, data backup, upgrading programs would help to manage different activities in the HCC.

- **Evaluation of alternative process**

Identification of the HCC's performance activities, employee's efficiency would help to implement a specific alternative problem solving the issue in the HCC.

- **Selecting an appropriate strategy**

Decision-makers adopt a suitable alternative strategy for managing data breachment issues in the company. Using enough resources would help to implement a new updated version of the application in the company.

- **Verification of strategy**

Next step is to verify the implemented strategy in the company for managing as per employee's efficiency in the workplace. It will give the opportunity to identify the limitations and the positive impact of the adopted strategy in the HCC.

Solution implementation and stakeholder's communication

According to Mulé (2020), nearly **43%** of businesses are suffering from cyber attacks in 2018. Implementation of the data encryption strategy would provide enough security for managing business performances. This process is effective to save all confidential data in the HCC.

- **Identify the requirement of data security**

Before implementing an encryption process, it is necessary to identify the causes of the data encryption process. There are many encryption schemes, need to be implemented in the HCC.

- **Choosing a proper encryption tools**

Choosing a proper encryption tool is important for maintenance of data security in the company. There are *multi data encryption schemes* for securing the entire process in the HCC. Implementation of the *Secure Socket Layers (SSL)* protocol will help to secure data. Another important factor is to make conjunction with *Advanced Encryption Standard (AES)* for securing all necessary data in the HCC. This system is also useful for creating data back up in the HCC. Apart from these, there are many important strategies to encrypt data, using *Encrypted email services, specific encrypted applications* would help to secure all data for improving the authenticity in the HCC.

- **Implementing encryption strategy**

Before implementing this strategy, it is required to know about the authenticity of the data encryption strategy. Involvement of the legacy system will help to manage the activity level in the company. Making contacts with the IT experts will help to simplify the whole process for improving the data encryption process in the company.

- **Implementation of the security alert process**

The higher authority of the HCC needs to give training to the employees to develop a good encryption process in the company. Human error is responsible for 84% of data breachment in the HCC. Using **robust firewalls** and **secure hardware** will provide security for managing business performances.

Data encryption is one of the authentic processes for securing all data in the company. Making communication with the employees will help to know their capacity of implementing encrypted strategy in the company. Another important factor is to give training to the employees for increasing their efficiency. Making communication with the employees would help to know about their complications in the company. Higher authority is responsible for managing all activities for developing authenticity in the HCC.CEO, BOD and managing director news to take the responsibility to hire efficient and honest IT specialists in the company.

Review and monitoring the implemented solution

Periodic monitoring and review is important for knowing the authenticity of the data encryption process in the HSS. The Higher Authority and *Information Security Office (ISO)* have taken the responsibility to develop a secured data encryption process. Periodic review will help to find out the limitations.

- IT experts need to gather information about the maintenance and installation of the encryption control process

- Identification of the security monitoring and performance assessment process would provide securities for managing health care activities.
- Reviewing and monitoring processes would help to identify the management process in the HCC. Giving enough support to the staff members is also important to know the authenticity of the data encryption program. Using CA encryption and master key would help to provide securities for improving business performances. Dual control system, duty separation processes are all required for managing all activities in the company.

Monitoring user's responsibility would help to rectify several challenging situations in the HCC. This section will discuss three important monitoring processes, to know the authenticity of the data encryption in the HCC.

Non TLS encryption

TLS or SSL process is used to identify the authenticity of the data encryption in the HCC. Using *secure shell, Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA)* is required for managing data encryption processes in the HCC. There are many rules and regulations in the data encryption process. Implementing these rule will help in periodic checking of the encryption process. All necessary strategies would be implemented in the risk management process.

Knowing about the personal information and technological information will help to solve different issues in the HCC. Regular monitoring will help to protect all authentic data for maintenance of authenticity in the HCC.

Conclusion

Nowadays a huge number of HCC are suffering from data treatment or lack of cyber security. This project has discussed detailed knowledge about the eradication of data breached. The introduction has discussed the general outline of this project. Lack of cyber security decreased the level of authenticity in HCC. All HCC is suffering from different management issues; an overview of the general issues has been discussed in this project. Detailed information about lack of cyber security has been discussed in this project. Impact of the cyber securities on the employees is also mentioned in this project. Analysis of the decision-making process has implemented all necessary steps in this project. There are several alternative solutions like strong passwords, data encryption, upgrading programs, data backup are all successfully described in this project. Proper decision-making techniques have been discussed in this project. Implementation of the data encryption process has been successfully

described in this project. Proper monitoring and review are recommended to complete this project. All these factors have successfully described this project.

Reference list

Bilsker, D., Fogarty, A.S. and Wakefield, M.A., 2018. Critical issues in men's mental health. *The Canadian Journal of Psychiatry*, 63(9), pp.590-596.

Brouwers, E.P., 2020. Social stigma is an underestimated contributing factor to unemployment in people with mental illness or mental health issues: position paper and future directions. *BMC psychology*, 8, pp.1-7.

Carr, D. and Luth, E.A., 2017. Advance care planning: contemporary issues and future directions. *Innovation in Aging*, 1(1).

Dos Santos, L.M., 2020. The challenges of public health, social work, and psychological counselling services in South Korea: The issues of limited support and resource. *International journal of environmental research and public health*, 17(8), p.2771.

Franklin, P., Arber, A., Reed, L. and Ream, E., 2019. Health and social care professionals' experiences of supporting parents and their dependent children during, and following, the death of a parent: a qualitative review and thematic synthesis. *Palliative medicine*, 33(1), pp.49-65.

Hanley, T., Prescott, J. and Gomez, K.U., 2019. A systematic review exploring how young people use online forums for support around mental health issues. *Journal of mental health*, 28(5), pp.566-576.

Hillson, R., 2020. COVID-19: psychological issues for people with diabetes and health care staff. *Practical Diabetes*, 37(3), pp.101-104.

Hilty, D.M., Chan, S., Torous, J., Luo, J. and Bolland, R.J., 2019. Mobile health, smartphone/device, and apps for psychiatry and medicine: competencies, training, and faculty development issues. *Psychiatric Clinics*, 42(3), pp.513-534.

Hilty, D.M., Chan, S., Torous, J., Luo, J. and Bolland, R.J., 2019. Mobile health, smartphone/device, and apps for psychiatry and medicine: competencies, training, and faculty development issues. *Psychiatric Clinics*, 42(3), pp.513-534.

Hua, J. and Shaw, R., 2020. Corona virus (Covid-19)“infodemic” and emerging issues through a data lens: The case of china. *International journal of environmental research and public health*, 17(7), p.2309.

Jennings, V., Floyd, M.F., Shanahan, D., Coutts, C. and Sinykin, A., 2017. Emerging issues in urban ecology: Implications for research, social justice, human health, and well-being. *Population and Environment*, 39(1), pp.69-86.

Kalabikhina, I.E., 2020. Demographic and social issues of the pandemic. *Population and Economics*, 4, p.103.

Karami, A., Webb, F. and Kitzie, V.L., 2018. Characterizing transgender health issues in Twitter. *Proceedings of the Association for Information Science and Technology*, 55(1), pp.207-215.

McCann, E. and Brown, M., 2018. The inclusion of LGBT+ health issues within undergraduate healthcare education and professional training programmes: A systematic review. *Nurse education today*, 64, pp.204-214.

Mulé, N.J., 2020. State involvement in LGBT+ health and social support issues in Canada. *International Journal of Environmental Research and Public Health*, 17(19), p.7314.

Petrini, M., Cirulli, F., D’Amore, A., Masella, R., Venerosi, A. and Venerosi, A., 2019. Health issues and informal caregiving in Europe and Italy. *Annali dell'Istituto superiore di sanita*, 55(1), pp.41-50.

Pinkney, S. and Walker, G., 2020. ‘It was me, but it was them that helped me’: Exploring the issues for care experienced young people within higher education. *Children and Youth Services Review*, 108, p.104576.

Silove, D., Ventevogel, P. and Rees, S., 2017. The contemporary refugee crisis: an overview of mental health challenges. *World psychiatry*, 16(2), pp.130-139.

Surr, C.A., Gates, C., Irving, D., Oyeboode, J., Smith, S.J., Parveen, S., Drury, M. and Dennison, A., 2017. Effective dementia education and training for the health and social care workforce: a systematic review of the literature. *Review of educational research*, 87(5), pp.966-1002.

Yüksel, B., Küpçü, A. and Özkasap, Ö., 2017. Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, pp.1-13.