sciendo

Scientific Bulletin
Vol. XXVIII, No. 1(55), 2023

CYBERSECURITY IN HEALTHCARE THROUGH THE 7-S MODEL STRATEGY

Darrell Norman BURRELL
dburrell2@thechicagoschool.edu

MARYMOUNT UNIVERSITY, ARLINGTON, VIRGINIA, SUA

ABSTRACT:

According to the 2019 HIMSS Cybersecurity Survey, most healthcare organizations are aware of the importance of cybersecurity, with 96% of respondents indicating that cybersecurity was a priority for their organization. Despite this, the survey also found that healthcare organizations are not adequately prepared for cyberattacks, with only 39% reporting that they had a comprehensive cybersecurity plan. This paper uses the 7-S Model strategy as a foundation for strategy development for healthcare organizations in a post-COVID-19 world.

KEYWORDS:

Healthcare cybersecurity, Health IT, 7S Strategy, Organizational Development

1. Introduction

The COVID-19 pandemic has significantly impacted the healthcare system, both in terms of increasing the demand for healthcare services and the risk of cybersecurity breaches and cybercrime (Coventry & Branley, 2018; Alghamdi, 2022). Cybersecurity breaches and cybercrime pose significant cybersecurity risks to the healthcare sector, as they can cause financial losses, data breaches, and disruption of services (Coventry & Branley, 2018).

Since the beginning of the COVID-19 pandemic, there has been a discernible rise in the number of instances of cybercrime and breaches of cybersecurity that have occurred inside the healthcare industry. According to Southwick and 2023, in 2022, there were about 50 million Americans whose medical records were compromised due to data breaches. According to Southwick (2023), in 2020, 34.4 million people in the United States had their private information compromised. Compared to 2021, the number of global cyberattacks in 2022 was 38 percent higher. According to McKeon (2023), healthcare was one of the three industries that faced the most significant number of cyberattacks in 2022.

Healthcare organizations increasingly use electronic health records (EHRs) and other digital systems to manage patient health data. These digital systems are vulnerable to cybercrime and can be used

DOI: 10.2478/bsaft-2023-0003
© 2023 Darrell Norman Burrell. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

by cybercriminals to access sensitive health data (Coventry & Branley, 2018; Alghamdi, 2022). Cybercriminals can use this data to commit identity theft, financial fraud, and other malicious activities. Cybercrime in healthcare can lead to significant financial losses, data breaches, and reputational damage for healthcare organizations (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Healthcare organizations often lack the resources and expertise to defend themselves against cybercrime (Coventry & Branley, 2018; Alghamdi, 2022). This makes them an attractive target for cybercriminals. Cybercriminals are increasingly targeting healthcare organizations due to their high value and the potential for long-term financial gain (Coventry & Branley, 2018; Alghamdi, 2022). Cybercriminals are using the healthcare sector as a sustained business model. Cybercrime is no longer a one-time attack but rather a sustained business model. Cybercriminals are using a variety of tactics to make money from healthcare organizations. These tactics include ransomware, malware, data breaches, and identity theft (Coventry & Branley, 2018; Alghamdi, 2022).

Ransomware is malicious software that encrypts a victim's data and holds it for ransom (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Cybercriminals demand payment in exchange for the release of the data. Ransomware attacks can lead to significant financial losses for healthcare organizations (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Malware is malicious software designed to damage or disable computers and networks (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Malware can be used to steal sensitive data, delete data, or take control of computers and networks. Malware attacks can lead to data breaches, system outages, and financial losses for healthcare organizations (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Data breaches occur when sensitive data is accessed or stolen by unauthorized individuals. Data breaches can lead to significant financial losses and reputational damage for healthcare organizations (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Cybercriminals can also use stolen data to commit identity theft, financial fraud, and other malicious activities (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Identity theft involves the unauthorized use of an individual's identity. Cybercriminals can use stolen data to open fake accounts, make online purchases, or commit fraud. Identity theft can lead to significant financial losses and reputational damage for individuals and organizations.

2. Problem statement

The healthcare industry was targeted by an average of 1,410 weekly cyberattacks per organization. This number represents an increase of 86 percent over the data collected in 2021 (McKeon, 2023). Healthcare organizations are at a greater risk of cybercrime due to their use of electronic health records (EHRs) and other sensitive data (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). This paper will discuss the threat of cybercrime in healthcare organizations and use frameworks from the literature to find solutions that can influence the world of practice.

3. Reasons for the Increase in Attacks

The global pandemic of COVID-19 has had a tremendous impact on the healthcare industry. Hospitals, health centers, and medical group practices have been forced to change operations and adapt to the new reality of providing care amid a global health crisis. As healthcare organizations become more reliant on technology and digital systems, they become

increasingly vulnerable to cyber threats (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Several factors have contributed to the increase in the number of cybersecurity breaches and cybercrime attacks in the healthcare sector since the start of the pandemic. The first factor is the increased demand for healthcare services due to the pandemic, which has led to a strain on resources and reduced the amount of time and resources available to dedicate to cybersecurity measures. This has made healthcare organizations more vulnerable to cyberattacks, as they have been unable to protect themselves from cybercriminals adequately.

Furthermore, the shift to remote working due to the pandemic has also increased the risk of cybercrime attacks, as remote workers may need to be adequately trained in cybersecurity best practices and may be using insecure devices or networks vulnerable to attack. Additionally, the increase in the use of telemedicine due to the pandemic has created new opportunities for cybercriminals, as it has increased the amount of data being transmitted over the internet, which cybercriminals can intercept and exploit.

Finally, the economic impact of the pandemic has also increased the risk of cybercrime attacks, as cybercriminals have seen an opportunity to exploit the economic downturn and target vulnerable healthcare organizations with ransomware attacks. This is because healthcare organizations are often unable to recover from a ransomware attack due to the significant financial losses and disruption of services that can occur, making them an attractive target for ransom ware attackers.

4. Emerging result on the topic

The rise in cybercrime in healthcare has made it one of the most vulnerable sectors to digital threats. Cyber attackers often target healthcare institutions due to their access to sensitive patient data, making them attractive targets for those seeking financial gain, as well as those seeking to damage reputation (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). The sheer amount and sensitivity of patient data make healthcare organizations a lucrative target for cyber attackers (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Healthcare information systems provide valuable services to both patients and healthcare providers, allowing for efficient and accurate storage, management, and exchange of sensitive data (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Although these systems are valuable assets, they are also at risk from cyber attackers, who use malicious software such as 'ransomware' to gain access to sensitive data. Sometimes, this can lead to patient data being held for ransom in exchange for a financial payoff. The consequences of a healthcare data breach can be wide-ranging; financial damage, reputation damage, and degraded quality of care are all possible outcomes. The continued growth in cybercrimes such as identity theft, extortion, and data manipulation has made the healthcare industry a prime target for cyberattacks (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

An effective cybersecurity strategy is essential for protecting healthcare organizations from data breaches. Weaknesses in digital networks leave them vulnerable to cyber criminals seeking access to this valuable data. Malware attacks, data manipulation, identity theft, and extortion are all risks posed by cybercrime in healthcare. As the threat landscape evolves, healthcare organizations must be vigilant in protecting against these malicious activities (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

When cyber attackers gain access to healthcare data, they can use, sell, or

manipulate data in various ways. Identity theft is rampant in healthcare, and stolen patient information can be used for financial gain by taking out fraudulent loans or making unauthorized purchases. Data manipulation is another significant risk posed by cybercrime in healthcare; hackers can alter medical records or manipulate systems to obtain patients' treatments and medications without authorization. Finally, ransomware is a hazardous type of attack in which attackers essentially hold data hostage, demanding a ransom in exchange for relinquishing control (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

One major challenge to healthcare cybersecurity is the widespread use of outdated or insecure systems. Many healthcare organizations rely on legacy systems that are vulnerable to cyberattacks. These systems often lack the encryption and authentication protocols required for modern cybersecurity solutions (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). In addition, healthcare organizations are often hampered by limited budgets regarding security upgrades (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

5. 7-S Model as a framework

In the wake of the COVID-19 pandemic, organizations worldwide have had to rapidly adapt to a new way of working. One of the key challenges they have faced is becoming more security-aware and tech-savvy to protect themselves from cyberattacks and cybercrime. Organizations have had to change their organizational cultures and strategies to do this.

Cybercrime is an increasingly pervasive threat to healthcare organizations, resulting in significant financial losses, reputational damage, and unauthorized access to confidential patient data. The 7-S Model is a framework developed by McKinsey & Company in the 1980s. The model is based on seven factors that can be used to analyze an organization's performance and strategy. The seven factors are Strategy, Structure, Systems, Skills, Style, Staff, and Shared Values (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Each factor is interdependent on the other, and the model provides insight into how a company is organized and how its strategies are executed (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008).

The model has been used in various industries, including healthcare, to analyze and improve organizational performance. For example, the 7-S Model has been used to identify areas of improvement in hospital management. The model can also be used to develop strategies to protect healthcare organizations from cyberattacks.

6. Why Use the 7-S Model

The 7-S Model is a valuable tool for cybersecurity managers to develop effective strategies to protect healthcare organizations from cyberattacks. As stated above, the model relies on seven interdependent factors that can be used to analyze an organization's performance and strategy (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). By examining each factor, a cybersecurity manager can gain insight into the organization’s current state and develop a plan to improve security.

First, the 7-S Model allows cybersecurity managers to analyze an organization's strategy. A cybersecurity manager must understand the organization's current strategies and objectives to develop a plan to protect it from cyberattacks. The 7-S Model can help managers identify what strategies are currently in place and what changes need to be made to improve security.

Second, the 7-S Model can be used to examine an organization’s structure

(Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). An organization's structure can affect its ability to protect itself from cyberattacks. The 7-S Model can be used to analyze an organization's structure to identify areas that need improvement. For example, the model can be used to identify whether an organization's IT department is adequately staffed and has the right personnel to handle cybersecurity issues.

Third, the 7-S Model can be used to examine an organization's systems (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Cybersecurity managers must understand an organization's systems to develop an effective strategy to protect it from cyberattacks. The 7-S Model can examine an organization's systems, such as its network architecture, to identify weaknesses that must be addressed.

Fourth, the 7-S Model can be used to analyze an organization's skills (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). A cybersecurity manager must understand the skills of an organization's personnel in order to develop an effective strategy to protect it from cyberattacks. The 7-S Model can analyze an organization's skills and identify improvement areas. For example, the model can be used to identify whether the organization's personnel have the necessary skills to detect and respond to cyberattacks.

Fifth, the 7-S Model can be used to analyze an organization's style (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Cybersecurity managers must understand an organization's culture to develop an effective strategy to protect it from cyberattacks. The 7-S Model can be used to analyze an organization's style to identify areas that need improvement (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). For example, the model can identify whether the organization has a security culture and whether its personnel are trained to recognize and report cyberattacks.

Sixth, the 7-S Model can be used to examine an organization's staff (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Cybersecurity managers must understand an organization's personnel to develop an effective strategy to protect it from cyberattacks. The 7-S Model can be used to examine an organization's staff to identify areas that need improvement (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). For example, the model can identify whether the organization has the right personnel to handle cybersecurity issues.

Finally, the 7-S Model can be used to analyze an organization's shared values (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Cybersecurity managers must understand an organization's values to develop an effective strategy to protect it from cyberattacks. The 7-S Model can be used to analyze an organization's shared values to identify areas that need improvement (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). For example, the model can be used to identify whether the organization's personnel are committed to protecting the organization from cyberattacks.

7. Application of the 7-S Model

The 7-S Model can be applied to healthcare organizations to address cybercrime as a sustained business. Cybercrime is an increasingly pervasive threat to healthcare organizations, resulting in significant financial losses, reputational damage, and unauthorized access to confidential patient data. Healthcare organizations must adopt a holistic cybersecurity approach to protect their data

and networks (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

8. Structural changes

The first element of the 7-S Model is structure (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Healthcare organizations must ensure that their formal hierarchies are well-defined and that roles and responsibilities are clearly delineated. This will help to ensure that the appropriate personnel are in place to manage cybersecurity efforts. Additionally, healthcare organizations should implement organizational changes that ensure cybersecurity is given the appropriate priority and resources. For example, organizations could create a dedicated cybersecurity team or appoint a Chief Information Security Officer (CISO).

In order to become more security-aware and tech-savvy, an organization needs to make sure that it has a structure that is conducive to achieving its security objectives (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova & Iliev, 2021). This can involve the creation of a dedicated cybersecurity department or team responsible for managing and monitoring the organization's cybersecurity posture.

9. Strategic changes

The second element of the 7-S Model is strategy. Healthcare organizations must develop a comprehensive cybersecurity strategy that is aligned with the organization's mission, objectives, and goals. This strategy should outline the organization's approach to preventing, detecting, and responding to cyber threats. It should also include a risk assessment process to identify potential threats and vulnerabilities and a plan for mitigating them (Khan, 2018). Furthermore, the strategy should emphasize the importance of education and training in order to ensure that all personnel are aware of the organization's cybersecurity policies and procedures.

In order to become more security-aware and tech-savvy, an organization needs to make sure that its strategy is focused on investing in cybersecurity and technology. This should involve investing in the necessary personnel and resources to ensure that the organization is up to date with the latest cybersecurity trends and technologies.

10. Systems changes

The third element of the 7-S Model is systems (Gökdeniz, Kartal & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Healthcare organizations must develop effective processes and procedures for managing cybersecurity. This includes implementing technical measures such as firewalls, encryption, and intrusion detection systems. Additionally, organizations should ensure that their systems are regularly updated and that personnel have access only to the data and systems necessary for their job functions. Furthermore, organizations should plan to respond to cyber incidents and recover data during a breach (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

In order to become more security-aware and tech-savvy, an organization needs to invest in the necessary technology and processes to ensure that its systems are secure (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). This could involve implementing tools such as firewalls, antivirus software, and intrusion detection systems to protect the organization from cyberattacks and cybercrime.

11. Shared values changes

The fourth element of the 7-S Model is shared values (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana & Kanchanasuntorn, 2008). Healthcare organizations must adopt a culture of

cybersecurity in order to ensure that all personnel are aware of the importance of protecting the organization's data and networks. This can be accomplished by establishing policies and procedures that are designed to protect patient data, as well as by providing education and training on cybersecurity best practices (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Additionally, healthcare organizations should incentivize personnel to adhere to cybersecurity guidelines and reward those who demonstrate responsible behavior.

In order to become more security-aware and tech-savvy, an organization needs to ensure that its staff are all on the same page regarding cybersecurity and that they share the same values when it comes to protecting the organization from cyberattacks and cybercrime. This could involve creating a culture of security awareness and emphasizing the importance of cybersecurity in all aspects of the organization (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

12. Skills changes

The fifth element of the 7-S Model is skills (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Healthcare organizations must ensure that personnel have the appropriate knowledge and abilities to protect the organization's data and networks. This can be accomplished through training and certification programs that emphasize cybersecurity best practices. Additionally, organizations should consider hiring personnel with specialized skills in cybersecurity, such as certified ethical hackers and information security analysts.

In order to become more security-aware and tech-savvy, an organization needs to ensure that its staff has the necessary skills to be able to protect the organization from cyberattacks and cybercrime (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). This could involve training programs to help staff understand the basics of cybersecurity and specialized training for more experienced staff.

13. Staff changes

The sixth element of the 7-S Model is staff (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Healthcare organizations must ensure that personnel are adequately trained and equipped to handle cybersecurity tasks. This includes providing personnel with the appropriate tools, such as antivirus software and password management systems, and ensuring they know the organization's policies and procedures. Additionally, organizations should consider hiring personnel with specialized skills in cybersecurity, such as certified ethical hackers and information security analysts (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). In order to become more security-aware and tech-savvy, an organization needs to invest in the necessary personnel to ensure that its staff are appropriately trained and knowledgeable about cybersecurity.

14. Style changes

The seventh element of the 7-S Model is style (Gökdeniz, Kartal, & Kömürcü, 2017; Weber, 2008; Adsavakulchai, Sopajitwattana, & Kanchanasuntorn, 2008). Healthcare organizations must ensure that their cybersecurity efforts are carried out in a manner that is consistent with the organization's values and goals. This includes adhering to regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA), and following cybersecurity best practices. Additionally, organizations should ensure that their personnel is adequately trained and equipped to handle cybersecurity tasks (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

In order to become more security-aware and tech-savvy, an organization needs to ensure that it has a style conducive to achieving its security objectives. This could involve a culture of openness and transparency regarding cybersecurity issues and implementing policies and procedures to ensure that everyone follows the same security protocols.

15. Challenges and recommendations

In conclusion, the COVID-19 pandemic has significantly impacted the healthcare sector, with a significant increase in the number of cybersecurity breaches and cybercrime attacks since the start of the pandemic. The increase in the number of attacks is due to several factors, such as the increased demand for healthcare services, the shift to remote working, the increase in telemedicine use, and the pandemic's economic impact. Therefore, healthcare organizations must protect themselves from cybercrime attacks by ensuring their staff is adequately trained in cybersecurity best practices, using secure networks and devices, and implementing robust cybersecurity measures.

The literature review has revealed that healthcare organizations are increasingly vulnerable to cyberattacks and cybercrime. In order to protect themselves, organizations should take steps to ensure that their systems are secure and that their data is protected and use a framework like the 7-S model to lead organizational strategy concerning cybersecurity.

Healthcare organizations should ensure their systems are secure and updated with the latest security patches (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Organizations should also ensure that firewalls, antivirus software, and other security measures protect their systems. Additionally, organizations should regularly monitor their systems for any potential security threats and take steps to address them quickly.

Organizations should also ensure their data is protected with encryption and other security measures. Data should be encrypted both at rest and in transit, and organizations should also ensure that their data is backed up regularly in case of data loss (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Additionally, organizations should ensure that they regularly monitor their systems for any unauthorized access or activity and take steps to address any potential security threats quickly.

Organizations should also ensure that their employees are familiar with security best practices. Employees should be trained to recognize and respond to potential security threats, such as phishing emails and malicious links (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Additionally, organizations should ensure that their employees are aware of the importance of following security protocols, such as using strong passwords and not sharing confidential information (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Organizations should also ensure a response plan during security breaches (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). The plan should include steps for responding to the breach, such as notifying affected parties and mitigating any potential damage. Additionally, the plan should include steps for ensuring that the organization's systems are secure and that any security vulnerabilities are addressed (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Organizations should develop and implement a comprehensive cybersecurity plan that covers employee training and awareness, organizational culture, and the physical environment (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021). Healthcare organizations should provide employees with regular security updates and training on the latest cyber

threats and how to protect against them (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Organizations should promote a culture of security within the organization, focusing on the importance of data security. This culture could be driven through rewards, recognition, and other employee engagement activities. This culture should stress that cybersecurity is everyone's responsibility, not just those in information technology (Coventry & Branley, 2018; Alghamdi, 2022; Bhosale, Nenova, & Iliev, 2021).

Healthcare organizations should implement innovative physical security measures like access control, CCTV, and key cards. Healthcare organizations should ensure that IT systems are secure using firewalls, antivirus software, and other security measures.Healthcare organizations should implement policies for the secure disposal of documents and data.

Implementing the 7-S Model in healthcare organizations can be a challenging endeavor. Organizations must ensure that all of the model's elements are aligned to ensure effectiveness and efficiency regarding cybersecurity risks, protection, and response. Additionally, organizations must ensure that all personnel are adequately trained and equipped to handle cybersecurity tasks. Furthermore, organizations must have the resources and personnel necessary to implement the model.

In order to overcome these challenges, healthcare organizations should consider implementing a comprehensive cybersecurity strategy aligned with the organization's mission, objectives, and goals. Additionally, organizations should ensure that their personnel are adequately trained and equipped to handle cybersecurity tasks. Furthermore, organizations should invest in the necessary resources and personnel to ensure that the 7-S Model is implemented effectively.

In order to protect themselves, organizations should take steps to ensure that their systems are secure and that their data is protected. For hospitals, health centers, and medical group practices to protect themselves from cyberattacks and cybercrime since COVID-19, they must ensure that systems are secure and up to date with the latest security patches, protect data with encryption and other security measures, train employees in security best practices, and having a response plan in place in the event of a security breach.

In conclusion, the 7-S Model is a powerful tool for helping healthcare organizations assess their strengths and weaknesses to identify improvement areas concerning cybersecurity risks and protection. The model can be used to address cybercrime as a sustained business by ensuring that the seven elements of the model are aligned. This includes ensuring that the organization's structure, strategy, systems, shared values, skills, staff, and style align with the organization's cybersecurity goals. Additionally, organizations must ensure that personnel are adequately trained and equipped to handle cybersecurity tasks. Although implementing the 7-S Model can be challenging, organizations can overcome these challenges by developing a comprehensive cybersecurity strategy, ensuring that personnel is adequately trained, and investing in the necessary resources and personnel.

REFERENCES

Adsavakulchai, S., Sopajitwattana, P., & Kanchanasuntorn, K. (2008). *Using the McKinsey 7-S Model for the Strategy Formulation and Implementation: Case Study in Ceramic Industry in Thailand.*

Alghamdi, A. (2022). Cybersecurity Threats to Healthcare Sectors during COVID-19. *2nd International Conference on Computing and Information Technology (ICCIT)*, Tabuk, Saudi Arabia, 87–92, DOI: 10.1109/ICCIT52419.2022.9711659.

Bhosale, K., Nenova, M., & Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. *6th Junior Conference on Lighting (Lighting)*, Gabrovo, Bulgaria, 1-6, DOI: 10.1109/Lighting49406.2021.9598947.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52.

Gökdeniz, I., Kartal, C., & Kömürcü, K. (2017). Strategic assessment based on the 7S McKinsey model for a business by using analytic network process (ANP). *International Journal of Academic Research in Business and Social Sciences, Vol. 7, Issue 6*, 342-353.

McKeon, J. (2023). Global Cyberattacks Increased By 38% Last Year, Healthcare Hit Hard. Health IT Security. Available at: https://healthitsecurity.com/news/global-cyberattacks-increased-by-38-last-year-healthcare-hit-hard

NIST. (2020). *NIST Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework

Southwick, R. (2023). *Nearly 50 million Americans impacted by health data breaches in 2022*. Chief Healthcare Executive. Available at: https://www.chiefhealthcareexecutive.com/view/nearly-50-million-americans-impacted-by-health-data-breaches-in-2022

Verizon. (2023). *Verizon 2023 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/?cmp=knc:ggl:ac:ent:ea:na:8888855284&utm_term=data%20breach%20investigations%20report%202022%20verizon&utm_medium=cpc&utm_source=google&utm_campaign=GGL_BND_Security_Phrase&utm_content=DBIR2022&ds_cid=71700000082349844&ds_cid=71700000082349844&ds_cid=&gclid=EAIaIQobChMInJbznJ6O_wIVIQKzAB0swgehEAAYASAAEgLUJvD_BwE&gclsrc=aw.ds

Weber, J. (2008). A Leader's Guide to Understanding Complex Organizations: An Expanded "7-S" Perspective. *Darden Case: Business Communications (Topic)*.