Cybersecurity Report on The Web-Based Appointment and Scheduling Management Information System (ASMIS)

Queens Medical Centre is an important component in the community. It plays a key role as the first point of call for all residents within the catchment area who feels unwell. Therefore, acquirement of a web-based Appointment and Scheduling Management Information System (ASMIS) will play an important role in ensuring that the ever-growing number of ill residents can schedule a consultation with a specialist online.

However, most of the cybercriminals continue to target healthcare sector due to healthcare systems having the most cybersecurity vulnerabilities. For instance, around 62% of all data breaches have occurred in healthcare sector from the past 15-year period, and this percentage increased to 77% in 2019 and 79% in 2020. (SafetyDetectives Cybersecurity Team, 2021).
Prioritization of Cybersecurity will be essential for this information system to be implemented successfully and with less risks of breaches and cyberattacks.

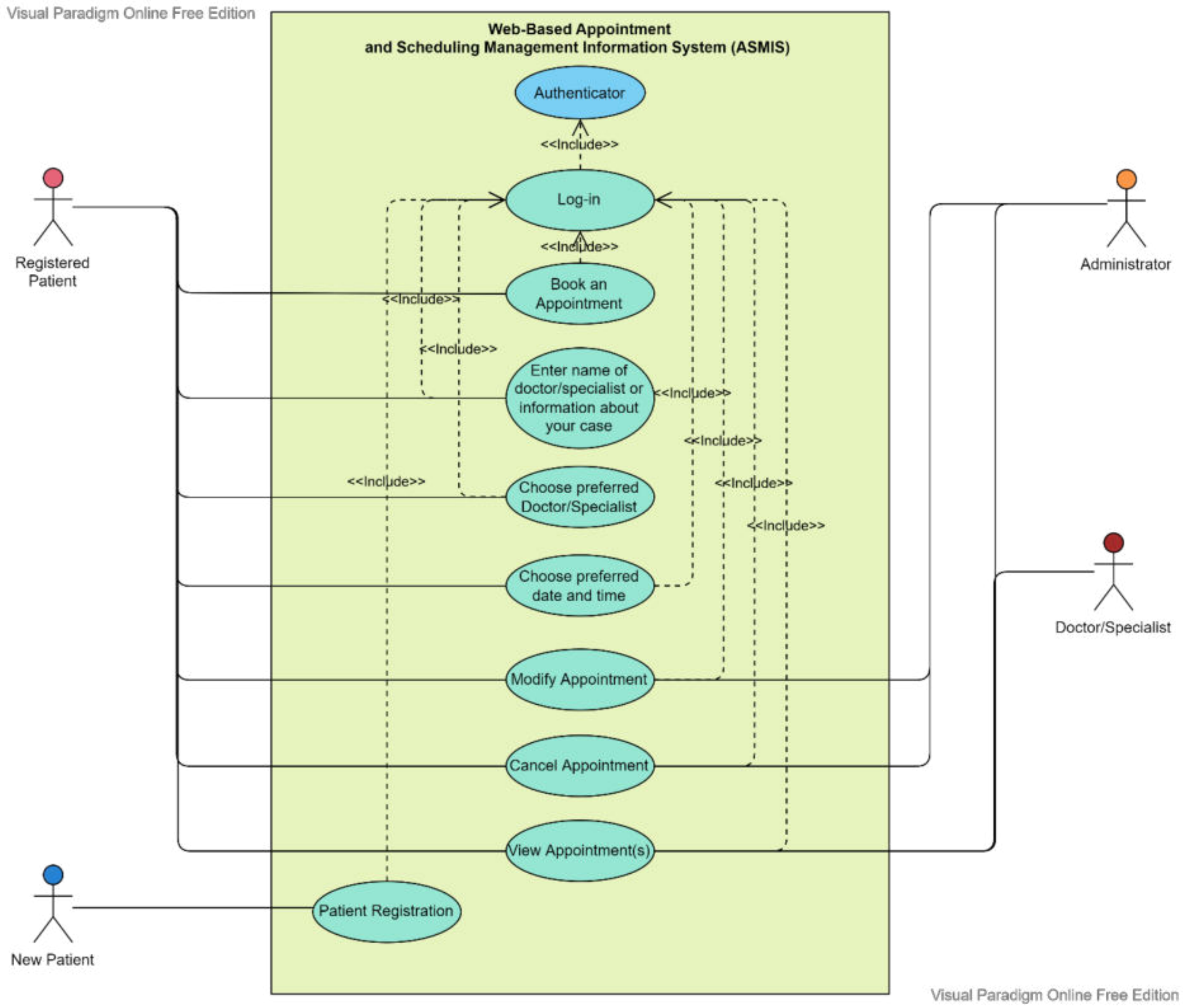
The pages that follow will explore the:

- Benefits of the ASMIS,
- Potential cyber threats problems to the system and how to mitigate them,
- Solutions and techniques on how to diminish these cyberthreats

The web-based Appointment and Scheduling Management Information System (ASMIS) aims to digitize the clinic's appointment method from the traditional way (which was by phone call) to a simplified, web-based appointment scheduling system.

Below are Unified Modelling Language (UML) diagrams that describes the functioning of the system.

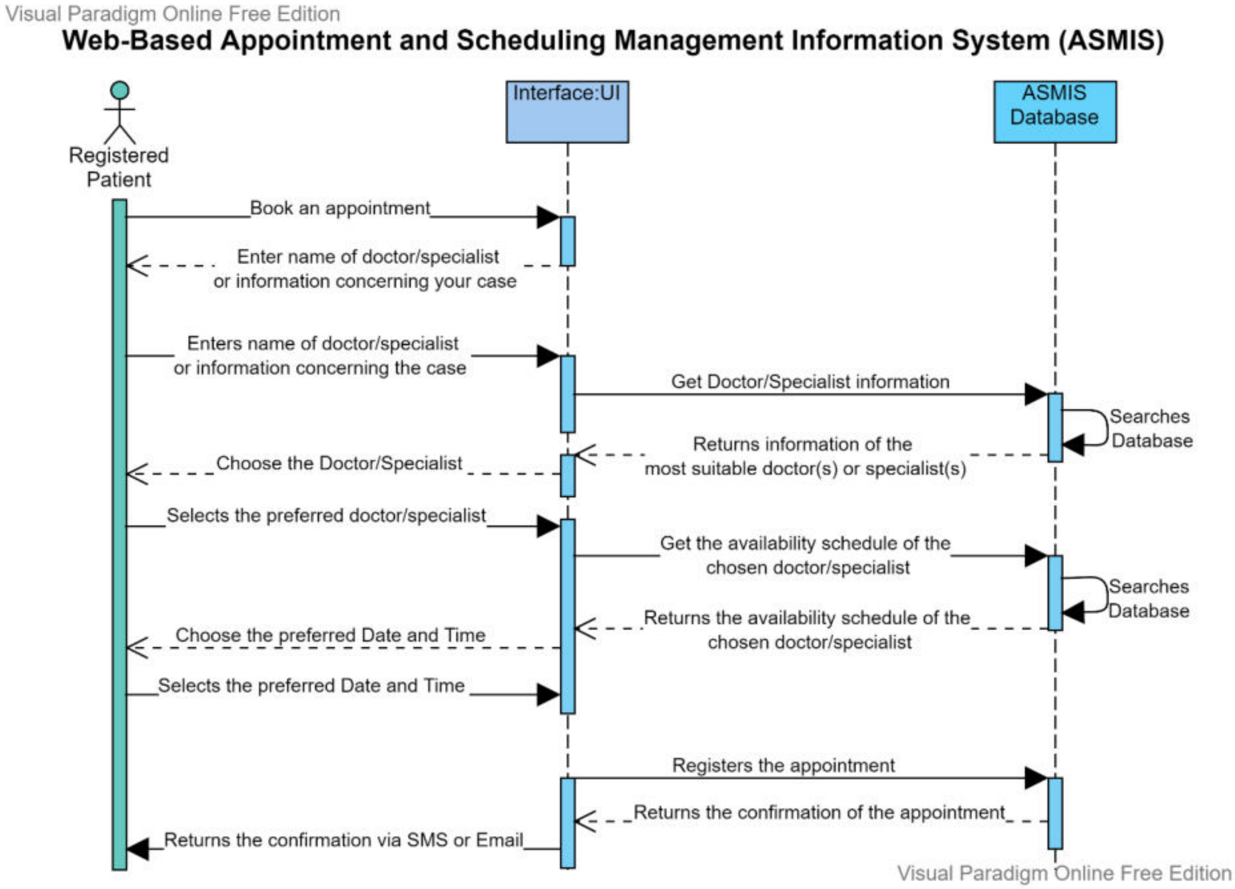
Figure 1: Use case Diagram



From the use case diagram above (Figure 1), new patients will able to register. The already registered patients, doctors/specialists and administrator will have to log-in to the system and must be authenticated first for them to be able to book, schedule, modify, view and cancel appointments respectively.

The diagram below (Figure 2) is a sequence diagram of an already registered and logged-in patient that is booking an appointment by interacting with the system's user interface and database.

Figure 2: Sequence Diagram


Visual Paradigm Online Free Edition
Web-Based Appointment and Scheduling Management Information System (ASMIS)
Registered Patient
Interface:UI
ASMIS Database
Book an appointment
Enter name of doctor/specialist or information concerning your case
Enters name of doctor/specialist or information concerning the case
Get Doctor/Specialist information
Searches Database
Returns information of the most suitable doctor(s) or specialist(s)
Choose the Doctor/Specialist
Selects the preferred doctor/specialist
Get the availability schedule of the chosen doctor/specialist
Searches Database
Returns the availability schedule of the chosen doctor/specialist
Choose the preferred Date and Time
Selects the preferred Date and Time
Registers the appointment
Returns the confirmation of the appointment
Returns the confirmation via SMS or Email
Visual Paradigm Online Free Edition

Implementation of this system will lead to efficiency, flexibility and time-saving for both the clinic's employees and the patients since the patients will be able to create and manage their own appointments.

Not only does digitalization of the appointment and scheduling system brings about positive benefits mentioned above, but it also brings cyberattack challenges. These challenges include:

- **Data Breaches and Theft: -** This is where unauthorised people gain access to sensitive data in a network or a system either by taking it physically (stealing storage disks, etc), hacking, social engineering, brute forcing, key logging, etc. This kind of attack happened to Georgia-based medical testing laboratory whereby a hacker targeted a network server that affected 312,000 individuals. The unauthorized intruder obtained files from its systems, including documents that may contain patient data. (McGee, 2022)
- **Ransomware and Malware Attacks: -** Both are malicious software that installs itself and runs so as to encrypt or steal data, or damage or destroy or even cause disruption to a system or a network. Headlines about ransomware attacks tend to be more common in healthcare than in other business sectors. Moreover, 65% of healthcare organizations attacked by ransomware agreed that cybercriminals succeeded in encrypting the data. 28% of them said they were able to stop the attack before encryption of the data, while the other 7% said they were still held ransom even though their data was not encrypted. The reason for this is that some attackers do not encrypt the data but steal it and then threaten to release the data if a ransom is not paid (extortion-style attacks). (SOPHOS, 2021).
- **SQL Injection Attack: -** In this attack, the hacker gains access to sensitive information by using a Structured Query Language (SQL) code to manipulate a

database. The target is usually any web application or website that uses an SQL-based database. (Anon, N.D.)

- **Distributed denial-of-service (DDoS): -** This happens when the victim's network or server is flooded with traffic and service requests to make it offline and unusable.

  In 2018, a hacker was convicted of targeting a Boston hospital by flooding 65,000 of the hospital's IP addresses. Over two weeks, the targeted hospital and several other hospitals in the area had their day-to-day operations, research capabilities and patient care internet services disrupted. The hospital spent more than $300,000 on the damages caused by the attack and also $300,000 more in donations since their fundraising website was offline too. (Smith, 2021)
- **Phishing Attack: -** This is when an attacker seeks to gain unauthorised access to data poses as a trusted entity to trick a victim into opening an email or message or a website.

  In March 2019, there was an incident where a worker of the Montpellier University Medical Centre opened a virus infested email that ended up infecting over 600 computers. Fortunately, the virus was prevented from spreading to all 6,000 machines due to their networks been internally independent. (Genovese, 2019)
- **Human Error: -** Unintentional actions by employees or users makes up large portion of the causes of data breaches and cyberattacks. "This can be seen in a case where an employer accidentally uploaded a file containing members information to a publicly accessible website. This prompted a major insurer to

warn 17,000 members that their health information may have been compromised". (Sweeney, 2018)

The cyberattacks mentioned above can result to the patients and the clinic getting effects like:

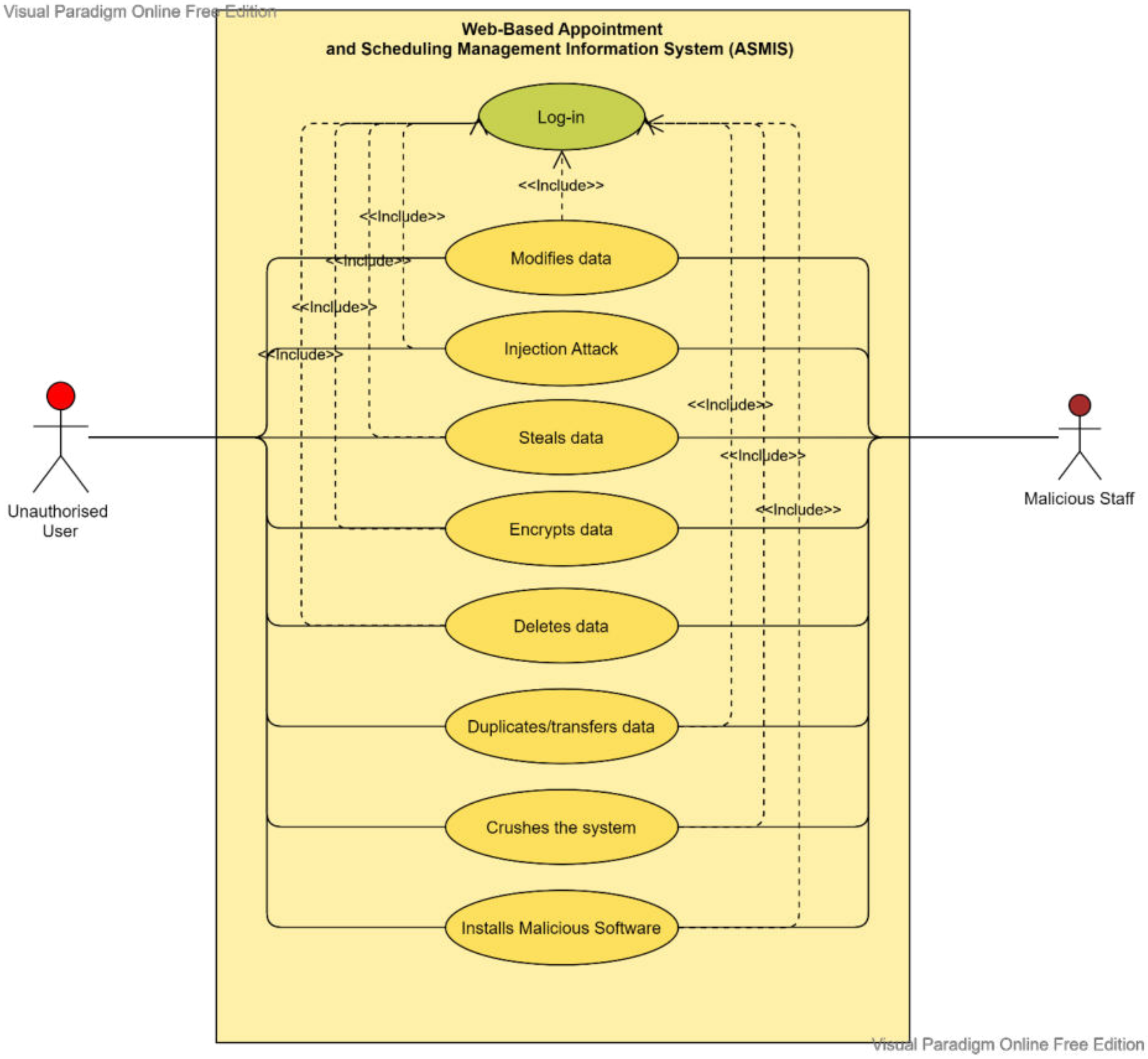
- Loss or leakage of important information like patient's personal information, medical history, etc, which can also lead to identity theft.
- Bad reputation and financial losses,
- Limitation of user's access or services getting delayed. This may result to patients seeking treatment elsewhere or their lives being put in jeopardy due to them not getting healthcare on time. (DocASAP , 2022). In the worst-case scenario, this can even lead to a patient's death.
- Inaccessibility of critical services such as bed capacity, scheduling and data exchange. (McKeon, 2021)

On the other hand, despite the previously discussed cyberthreats and there potential effects, there are Threat Methods and Techniques that are a proactive strategy to assess, identify and remediate potential cybersecurity threats to your software, data or Internet of Things (IoT). This includes understanding the attack's effects on the systems, classifying threats, taking appropriate countermeasures and developing tests or procedures to detect and respond to these threats. (Gonzalez, 2022).

An illustration of the methodologies to be applied are:

- **Abuse Case: -** Also known as misuse case, is an effective way of reinforcing a secure application by showing how user(s) can attack the software or system (Synopsys Editorial Team , 2015)

Figure 3: Abuse Case Diagram


Visual Paradigm Online Free Edition
Web-Based Appointment
and Scheduling Management Information System (ASMIS)
Log-in
<<Include>>
Modifies data
Injection Attack
Steals data
Encrypts data
Deletes data
Duplicates/transfers data
Crushes the system
Installs Malicious Software
Unauthorised User
Malicious Staff
Visual Paradigm Online Free Edition

The Abuse case above (Figure 3), shows damages that can be done by an unauthorised user or a malicious staff once they log-in to the system.

- **STRIDE: -** This is mainly used by Microsoft and is also known as the most mature threat modelling technique (SHEVCHENKO, 2018).

  This approach focuses on 6 core areas as viewed on the figure below:

Table 1: STRIDE table

	Threat	**Threat Definition**	**Property Violated**	**Potential Victims to be Attacked**
S	Spoofing	Faking identity	Authentication	Users, Processes, other entities like businesses, etc
T	Tampering	Modification of data on disk or database or network or memory	Integrity	Data banks like databases, data flows like emails, processes
R	Repudiation	A user denying performing action(s)	Non-repudiation	Processes
I	Information disclosure	Unauthorised access to information	Confidentiality	Data banks like databases, data flows, Processes
D	Denial of Service	Exhaustion of resources required to	Availability	Data banks like databases, data flows, Processes

		provide services		
E	Elevation of privilege	Unauthorized control of the system	Authorization	Processes

The 6 core areas from the table above (‘Threat’ column), helps software developers to recognise the cyberattack on the software (Shostack, 2014)

The key objective of cybersecurity is to protect the information’s Confidentiality (only authorised users can access data), Integrity (Information must remain uncorrupted and unmodified) and Availability (Information must be available to authorized persons whenever they need it) (threatmodeler1 , 2019).

In order to approach to this objective, below are security technologies and techniques that must be considered and applied to ensure security.

- **Multi-Factor Authentication (MFA) and Access Control: -** Since the use of usernames and passwords (single-factor authentication) is very common and vulnerable to attacks, implementation of multi-factor authentication is the most effective substitute.

  This is because for a hacker to gain access to data, they must submit a combination of factors, i.e., “something you are (iris, fingerprint, voice, biometric, etc.), something you have (a smartcard, mobile device, etc.) and something you know (security questions, username, password, etc)". For instance, “in 2014, Imprivata’s Confirm ID MFA solution (integrating a fingerprint reader into the electronic health records) was favourably accepted by NorthShore University Health System” (Wagenen, 2018).

The combination of Multi-Factor Authentication (MFA) and Access Control (controlling the accessibility of data) will reinforce security on the networks, systems and Internet of Things (IoT) devices from unauthorised access.

Not only is it expensive to implement a Multi-Factor Authentication (MFA), but it can be frustrating for user(s) to have to validate through multiple layers of authentication every time they access a system or data.

- **Data Loss Prevention: -** Whether the data is in motion (email, network) or at rest (database, desktop, laptop) or in use (data in devices such as on removable storage media, in the cloud, printers, etc), it must all be protected from unauthorised deletion, modification and duplication. This is achieved by using a software to detect, monitor and block actions that put data at risk. (McAfee, N.D.)

  There are products like Tessian that use machine learning to combat data loss by analysing email data. (Rosenthal, 2021).

  The downside to this is that false positives can occur.

- **Firewalls: -** They monitor traffic into or out of a network thus securing data and Internet of Things (IoT) devices.

  It is categorised into: traditional firewalls like packet filtering firewalls (it is the easiest to configure and it filters packets in the network layer level of OSI model), and Cloud firewalls like Web Application Firewalls (WAF) (they filter, monitor and block HTTP traffic at the application layer and require advanced troubleshooting skills to avoid false positives); all of which have the purpose of combating cyberattacks. (Anwar, et al., 2021)

- **Data Privacy: -** These are rules and regulations that control the accessibility to sensitive information. The General Data Protection Regulation (GDPR) recognises data in the healthcare sector thus enforcing trust between healthcare providers and patients.

  Other than the General Data Protection Regulation (GDPR), there are several others that are meant for the healthcare sector. Some examples are:

  - Health Insurance Portability and Accountability Act (HIPAA) – a law from the United States of America that gives patients control over their medical information,
  - The Health Information Technology for Economic and Clinical Health (HITECH) Act United States of America, etc.

(BOX COMMUNICATIONS, 2021).

- **Cybersecurity Awareness Training: -** This is where users are trained on cybersecurity threats and good security practices i.e., how to prevent and recognize threats and how to respond to an incident. For example, companies like MetaCompliance offer cybersecurity awareness training that is tailored for the healthcare sector (Anon, N.D).

  This leads to a reduction in human error and therefore a reduction in the number of cyberattacks.

- **Endpoint Security: -** Also known as Endpoint Protection Software, is a centrally managed security solution that includes various security applications and tools such as Firewalls, Antivirus, Endpoint Detection and Response (EDR), Events Manager, Incident Response, etc.

  Together, they all serve to protect the entire network and its endpoints (including Internet of Things (IoT) devices that are connected to the network) from cybersecurity threats (Anon, N.D.).

  The advantage is that it is cost efficient, can be controlled remotely and can be deployed in the cloud or internally.

- **Cybersecurity Breach Insurance: -** Having a Cybersecurity coverage on the clinic is one of the necessary measures to protect the clinic in the event of a cyberattack.

  Without such insurance, a cybersecurity breach can result in the closure of the clinic if there is no enough money to fund for costs like penalties, fines, recovery costs, hiring of a specialist to respond to the incident and possible reputational damage and fines. (Johns, 2021)

In summary, this paper has provided insight into the web-based Appointment and Scheduling Management Information System (ASMIS) and contributed to our understanding of Cybersecurity in several ways providing a foundation for the implementation of a secure Appointment and Scheduling Management Information System (ASMIS).

References

Synopsys Editorial Team , 2015. *Abuse cases can drive security requirementts.* [Online]
Available at: https://www.synopsys.com/blogs/software-security/abuse-cases-can-drive-security-requirements/
[Accessed 9 May 2022].

Anon, N.D.. *What Is Endpoint Protection Software.* [Online]
Available at: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-protection-software.html
[Accessed 5 May 2022].

Anon, N.D.. *What is SQL Injection?.* [Online]
Available at: https://www.kaspersky.com/resource-center/definitions/sql-injection
[Accessed 5 20 2022].

Anon, N.D. *Security Awareness Training Healthcare Sector.* [Online]
Available at: https://www.metacompliance.com/security-awareness-training-healthcare-sector/
[Accessed 6 May 2022].

Anwar, R. W., Abdullah, T. & Pastore, F., 2021. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences,* 11(9).

BOX COMMUNICATIONS, 2021. *What is data privacy in healthcare?.* [Online]
Available at: https://blog.box.com/what-is-data-privacy-healthcare
[Accessed 6 May 2022].

DocASAP , 2022. *How Cyber Attacks Disrupt the Patient Access Journey.* [Online]
Available at: https://martech.health/articles/how-cyber-attacks-disrupt-the-patient-access-journey
[Accessed 5 May 2022].

Genovese, M., 2019. *Top 5 Cyberattacks Against the Health Care Industry.* [Online]
Available at: https://www.stormshield.com/news/top-5-cyberattacks-against-the-health-care-industry/
[Accessed 5 May 2022].

Gonzalez, C., 2022. *Top 8 Threat Modeling Methodologies and Techniques.* [Online]
Available at: https://www.exabeam.com/information-security/threat-modeling/#:~:text=A%20typical%20threat%20modeling%20process,visibility%20into%20your%20security%20posture.
[Accessed 8 May 2022].

Johns, E., 2021. *Cyber Security Breaches Survey 2021.* [Online]
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf
[Accessed 5 May 2022].

McAfee, N.D.. *Data Loss Prevention Best Practices for Healthcare.* [Online]
Available at: https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dlp-best-practices-healthcare.pdf
[Accessed 6 May 2022].

McGee, M. K., 2022. *Big Hacks: 5 Health Data Breaches Affect 1.2 Million.* [Online]

Available at: https://www.govinfosecurity.com/big-hacks-5-health-data-breaches-affect-12-million-a-18873

[Accessed 4 January 2022].

McKeon, J., 2021. *The Threat of Distributed Denial-Of-Service Attacks in Healthcare.* [Online]

Available at: https://healthitsecurity.com/features/the-threat-of-distributed-denial-of-service-attacks-in-healthcare

[Accessed 5 May 2022].

Rosenthal, M., 2021. *At a Glance: Data Loss Prevention in Healthcare.* [Online]

Available at: https://www.tessian.com/blog/data-loss-prevention-in-healthcare/#:~:text=Data%20Loss%20Prevention%20(DLP)%20is,laws%20like%20HIPAA%20and%20HITECH.

[Accessed 6 May 2022].

SafetyDetectives Cybersecurity Team, 2021. *Healthcare Cybersecurity: The Biggest Stats & Trends in 2022.* [Online]

Available at: https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics/

[Accessed 04 May 2022].

SHEVCHENKO, N., 2018. *Threat Modeling: 12 Available Methods.* [Online]

Available at: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

[Accessed 9 May 2022].

Shostack, A., 2014. *Threat Modeling: Designing for Security.* Indiana: John Wiley & Sons, Inc..

Smith, R., 2021. *5 Things to Know About DDoS Attacks in Healthcare.* [Online]
Available at: https://healthtechmagazine.net/article/2021/09/5-things-know-about-ddos-attacks-healthcare
[Accessed 5 May 2022].

SOPHOS, 2021. *The State of Ransomware in Healthcare 2021,* England: SOPHOS.

Sweeney, E., 2018. *Independence Blue Cross reports data breach affecting 17,000 members.* [Online]
Available at: https://www.fiercehealthcare.com/payer/independence-blue-cross-data-breach-cybersecurity-privacy
[Accessed 5 May 2022].

threatmodeler1 , 2019. *Identifying security bjectives.* [Online]
Available at: https://threatmodeler.com/identifying-security-objectives/
[Accessed 9 May 2022].

Wagenen, J. V., 2018. *The Benefits of Multifactor Authentication in Healthcare.* [Online]
Available at: https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon#:~:text=As%20data%20breaches%20in%20healthcare,other%20cyber%20security%20best%20practices.
[Accessed 6 May 2022].