International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity in Hospitals: A Case Analysis of the University of Ghana Medical Centre

Richard Aggrey[1], Nana Adwoa Dsane[2], Karl Osei Afoduo[3], Bright Ansah Adjei[4]

[1]Dep. Director, Head of IT, University of Ghana Medical Centre
[2]Deputy Director of Medical and Scientific Research Centre, University of Ghana Medical Centre
[3,4]Senior Health Research Officer, University of Ghana Medical Centre

Abstract

The University of Ghana Medical Centre Ltd is a premier academic health facility that delivers tertiary/quaternary level health services, education and research in Ghana, Africa and the globe. It is Ghana's premier quasi health institution and is the only quaternary health centre in Ghana. It is a fully digitalised institution vulnerable to cyberattacks because of patient data, hospital systems, availability of health services and also data of prominent people in society. The paper analysed cybersecurity measures implemented at the health facility to reveal its advantages and disadvantages, and further outlook for its development. The research method comprised an assessment of cybersecurity-related activities, reports and documentation to explore cybersecurity measures and regulatory compliance in explaining timely employee awareness and responding to incidents to protect patients' details with cybersecurity specialists' cooperation. The study reports the proactive measures taken by the health facility to avert and mitigate potential cybersecurity threats. However, it also identifies the need for the facility to partner with cybersecurity experts in developing comprehensive response plans, and this comes in recognition of some weaknesses in the current implemented system which are institutional, bureaucratic and technology related.

1. Introduction

Challenges of cybersecurity have been widely reported. Hospitals are a focus as cyber attackers threaten patient data, hospital systems, and the availability of health services. The lack of accurate and country-specific datasets limits understanding of the prevalence and vulnerabilities of cybersecurity incidents within institutions such as hospitals (Nifakos. S et al., 2021). The UGMC has since its founding established an Information Security Policy and Procedures and its enforcement as a foundation for leadership's commitment to ensuring a cyber hygiene environment, assessing risks, implementing controls, and mitigating many associated risks. However, there are still some shortcomings. Attack vectors continue to increase daily due to digital transformation in healthcare. In over two decades in Healthcare IT, we have seen the growth of Cloud Computing, the Internet of Medical Things, Electronic Health Records, Biomedical Diagnostic equipment embedded with AI functionalities and Internet of Things, among others. By providing a case study for the UGMC, we illustrate the importance and context of these findings.

The University of Ghana Medical Centre LTD (UGMC) is a 1000-bed state-of-the-art facility providing world-class quaternary health services, training, and research in Ghana, West Africa, and beyond. The

Centre opened for partial operations in 2018. The Centre has been digitised since its inception, and all Patient's Health Information is generated and stored digitally on-site and in the cloud. The institution runs thirty-nine clinical services ably supported by sixteen non-clinical directorates and departments.

Health data is increasingly being digitalised due to the technologies mentioned above. As hospitals depend on digital systems, they face increasing threats to availability, patient care, confidentiality, and data integrity. This section explains the hazards associated with cyber-attacks to hospitals' cyber teams. It should also justify investment in mitigation strategies, legislation and cybersecurity improvements. In this context, the research questions are: what are the possible patient care and data security implications of cybersecurity influences in similar healthcare settings? How should hospitals minimise their susceptibility to cyber-attacks against their Health IT infrastructure? Research on available cybersecurity initiatives and premature observations in this hospital inform that answer (Cerchione et al., 2023).

1.1. Background and Rationale

Hospitals have rapidly transitioned from paper-based medical records to Electronic Health Records (EHR) over the past two decades. They now depend heavily on digital technologies for delivering telehealth services, booking appointments and consultations, preparing medical charts, drug prescriptions and history, creating and accessing medical images, remote scheduling of medical devices and services, and communicating with hospital staff and patients through their mobile apps. This digitisation wave in hospitals has brought higher efficiency, error reduction, faster coordination, timely decisions, convenience, and simplified medical data collection, curation, analytics, and reporting. Yet, this digitisation wave has opened new gates for cybercriminals to breach security and access Patient Health Information, violating patient privacy and confidentiality (Li, J. P. O., et al., 2021).

At the centre of this study is the University of Ghana Medical Centre, which has been chosen as a case study into the cybersecurity mechanisms and threats to our hospitals. At the time of investigation, the hospital’s network was connected to thousands of devices and the Electronic Health Records (EHR). The EHR contains valuable patient data, including but not limited to patients' details (i.e., name, contact information, National Identification), and clinical data (i.e., diagnoses, drug history and dosage, laboratory test and imaging information, dental charts, surgery records, and specimen images). The 20% dip in patient satisfaction surveys since 2023 shows the need for security from the patients’ point of view (Wasserman, L., et al., 2022).

1.2. Research Objectives

The main aim of this study is to investigate cybersecurity issues at UGMC. This research focuses on a specific case and strives to achieve the following objectives. Firstly, it would assess the cybersecurity challenges faced. Secondly, it would investigate the effectiveness of the cybersecurity measures in place. Thirdly, it would outline the implications of cyber incidents occurring in healthcare from both patient care and operational stability perspectives. Moreover, the study would suggest strategic measures tailored to advance the existing cybersecurity capability. Through the results, this study attempts to identify measures and possibly improve the current state of cybersecurity in hospitals and other settings (Argaw, S. T., et al., 2020).

Even though cybersecurity has been identified as vital to safeguard the digital frontline in healthcare, existing studies remain largely theoretical. Moreover, appropriate studies can offer healthcare providers several best practices or directives to be considered for a proactive move regarding cybersecurity challenges. Leveraging empirical data, the results of this study should be valuable: Firstly, to operational healthcare experts for a detailed understanding of the applicable cybersecurity challenges, the

appropriateness of the existing cybersecurity measures, and the potential implications of a cyber incident. Secondly, to the IT experts for suggesting detailed guidelines, psychological traits of the workforce, and broader considerations for strengthening the existing cybersecurity framework. The academic literature would indeed benefit from such work and thus contribute to current holistically inclined researchers at the intersection between healthcare and cybersecurity. In the next section, we demonstrate the relevant literature in the domain along with the research questions (Moore, G., et al., 2023).

2. The Importance of Cybersecurity in Hospitals

It is mission-critical for healthcare institutions across the globe to adopt robust cybersecurity protocols that protect the organisation, patients, and staff. One contributing factor is that many hospitals store and manage large repositories of sensitive data belonging to patients. Breaches that compromise patient data can have profound implications for patient privacy. More importantly, excellent care delivery in hospitals depend, among other things, on operational reliability. Cyber threats aimed at hospitals could lead to severe disruption in service delivery, the consequences of which could affect the compromised organisation and patient trust to manage their health records securely. Public health infrastructure everywhere is becoming increasingly interrelated with information technology infrastructure. The strength of the lines between the physical and the cyber world is becoming increasingly blurred. In hospitals, cybersecurity needs to be a leading player in a proactive, rather than reactive, privacy and security culture worldwide (Bhuyan, S. S., 2020).

Data breaches often highlight failures in information technology or security oversight, implicitly accusing hospitals and healthcare institutions. Therefore, a data breach that involves private patient data may also lead to a loss of patient trust in the healthcare institution. There are increasing cybersecurity regulatory requirements and standards for healthcare institutions to comply with, associated fines, and enforcement mechanisms. Organisations can face significant penalties if they fail to meet these standards. Furthermore, guidelines for medical device are issued, and health institutions fail to meet such guidelines at their own risk of fines and brand trust, which implies that cybersecurity is shaped by literacy and compliance rather than general knowledge or curiosity about the domain (Aung, Y. Y., et al., 2021).

2.1. Patient Data Protection

The rising incidents of cyberattacks on organizations have called for the need to protect personal data, especially sensitive health information of patients also stored by these organizations. UGMC have various forms of personal data of individuals, including patients, healthcare workers, suppliers, and visitors. This personal data includes names, addresses, identification numbers, medical histories, financial data, etc. (Thapa, C., et al., 2021). For patients, the leakage, theft, or exposure of their health data could be dangerous since it could result in loss of employment, erode patients trust with their sensitive data, disrupt patient care and reduce access to innovative therapies, lack of patients' recruitment for clinical trials and emotional distress.

In order to protect this sensitive data from unauthorized disclosure, the UGMC has implemented several security controls, including security policies, physical and IT security measures. However, the increasing use of Electronic Health Records systems over standalone software applications requires a more stringent security control to protect patient information. One of the best security practices carried out by the Centre to protect patient socio-technical information assets is the implementation of user access controls, especially through data encryption technologies in the form of encrypting data at rest, data in transit, and data in use. Data protection compliance requirements have specific security rules embedded, which

involve user access data control, data encryption, secure analysis, and other related security measures that Critical Information Infrastructure (CII), including hospitals, are expected to comply with in order to prevent data breaches and minimise the occurrence of cyberattacks (Bani Issa, et al., 2020).

Organizations, including hospitals, that want to protect their patients' data usually involve their patients through awareness on how to protect their data since patients have responsibilities to protect their own data. However, the ultimate responsibility to safeguard sensitive data against unauthorized exposure primarily lies with the hospital management and other regulatory bodies. Some recommend that to create better and more effective systems for protecting data, technologists and healthcare professionals should cooperate more with each other to develop systems that are adequate, appropriate, and sustainable (Keshta, I., et al., 2021).

2.2. Operational Continuity

In a hospital, situations that lead to operational downtime can have severe consequences for patient health and even lead to the loss of life. With modern-day technology, there are reported cases of hospitals going down due to cyber incidents. These could range from a brute force knock-out of a hospital network, data loss, malicious threats, and data breaches. Furthermore, some hospitals have been known to operate off non-digital systems while the digital system is being worked on. Fast and pragmatic remediation of these incidents is required to restore the system to operation. Any lasting catastrophic effect is to be considered abnormal while providing care to patients. Maintaining essential hospital functions and services in the wake of such threats to cyber resilience and operational reliability requires a range of proactive protective measures and resilience-building strategies to ascertain operational continuity when a cybersecurity breach occurs (Larsen, E. P., et al., 2020).

While it is necessary to invest in anti-forensic and pre-emptive protection methods, UGMC is committed to hardening of the network, incident handling, offering readiness reactions and continuous upkeep of critical safeguard components as part of the system defence of the Centre. A continuity of operations and incident plan presents the foundational proof of the hospital (Jovanović, A., et al., 2020). Incidents involving important healthcare systems are planned and managed with the assistance of well-documented processes in order to contain, repair, and restore healthcare services. This is done to offset the downtime of networking activities and systems after an incident, financial losses and disruption of critical healthcare services, as these impacts the essential budgetary allocations. It is also necessary to educate and provide awareness to all hospital staff about the threats to information and communications technologies, as this could potentially impact the hospital's resilience and continuity of operations to perform its services (Papastergiou, S., 2021). Technological advances present new vulnerabilities to the operational infrastructure of the hospital and as such necessitate adaptive security precautions woven into the organisational culture to establish operational risks and managed within the realm of operational resilience. It is common to collaborate with industry-respected cybersecurity researchers for joint partnerships to advise on detection, monitoring, and prevention steps to secure the operational integrity of the Centres services, ensuring an up-to-date security posture is maintained.

3. Cybersecurity Threats in Healthcare

It has been highlighted that the health sector is prone to high cybersecurity threats. The most common cybersecurity threat in the healthcare industry is ransomware. Ransomware is a form of malware that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid. When it

comes to hospitals and healthcare facilities, the consequences of a ransomware attack can be catastrophic. People may die because treatment is delayed due to affected operations (Abbas, H. S. M., et al., 2022).

Another common cybersecurity threat in healthcare is a phishing attack that leads to a data breach. Phishing is a process of fraudulently attempting to obtain sensitive information like usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in a digital communication. In the healthcare industry, attackers usually target employees who work in the organisation to gain unauthorized access to patient data or the hospital's operational data. Given that most healthcare systems rely on outdated systems and software, which are no longer updated by the vendors, the chance of being hit with ransomware becomes more likely as attackers exploit weaknesses in these outdated systems (Seh, A. H., et al., 2022). Another reason hospitals are vulnerable to cyberattacks is related to employees. Most healthcare employees are not trained on cybersecurity, making them prone to cyber-attackers. The attacks on UK National Health Service (NHS), US healthcare-associated systems and non-affiliated organisations rose significantly, with numerous cases of large-scale breaches having occurred. The cost of these breaches has been estimated to be in billions of US dollars. In times like this, identifying and responding to abnormal activity on hospital networks is vital. Unfortunately, this is far-fetched due to the peculiar challenges identified with the current state of digital healthcare systems. It is, therefore, imperative to invest in a comprehensive monitoring system designed to identify abnormal activities in UGMC's operation early enough (Al Kinoon, et al., 2024).

3.1. Ransomware Attacks

Ransomware is a type of malware that cybercriminals use to access a healthcare organisation's critical data and systems, without which the hospital can no longer operate efficiently. It encrypts important files, databases, and records so that personnel cannot access them, leaving hospital administrators with two undesirable options: either pay the cost of ransom or struggle until backups become viable. The global healthcare industry has become a popular target for ransomware attacks that disrupt hospital operations and, in some cases, even put patients in life-threatening situations. One of the key characteristics of such attacks is the systematically disguised hacking methods, which delay the detection of these attacks. An example occurred in 2016 during an incident at a medical centre which had to relocate patients and send ambulances elsewhere after a ransomware infection severely disrupted operation for several days. Luckily, no one was hurt during this incident (Humayun, M., et al., 2021).

There are ways to prevent ransomware attacks from affecting hospital operations or to recover quickly after attacks. First, hospitals should encrypt and regularly back up their critical databases and assets so that they can be restored if they are attacked by ransomware. Maintaining controlled access at all times, maintaining security awareness for hospital staff and the information system are also crucial for preventing these attacks. These are essential to guarantee that hospital services are minimally affected, and to quickly recover databases in ransomware attacks, we recommend an immediate action plan (Kumar, S., et al., 2021).

3.2. Phishing Schemes

Phishing is a scam that targets people by tricking them into providing sensitive information, ranging from personal login credentials to banking and credit card information. Phishing is a major threat from cybercriminals. Attackers of this nature utilize various tactics that involve tricking employees into opening emails or clicking on links that contain malware in order to steal credentials and personal information. Interestingly, healthcare has become more susceptible to cyberattacks, especially phishing, due to their large, readily available treasure of medical data (Abdelhamid, M., 2020). Phishing is a low-level scheme

that relies on hiding the previous identity and skill behind a fraudulent enterprise and, thus, is a cybercrime technique that requires no technical skills. In healthcare organisations, training and ongoing awareness against phishing schemes can save organisations significant money. It would be beneficial for individuals to contact the IT department immediately should they feel, they may have been the victim of a phishing attack (Jampen, D., et al., 2020). Additionally, cybercriminals will research target organisations prior to attack, craft realistic-looking emails, and engage patients via social media in order to learn about medical treatments.

As a healthcare provider, UGMC has taken steps to protect patient information in several ways, one of which is filtering emails to reduce phishing test emails. Additionally, the use of multi-factor authentication to help protect against stolen credentials can be adopted. Organisations can further protect themselves against external phishing attacks by adopting a mailbox feature that allows cybersecurity teams to recover the deleted emails that the attackers wanted to hide. There should be real-world scenarios that provide full-time experience of the impact of phishing. For example, a phishing email sent to a hospital presents a "real-life" scenario described as the consequences of staff falling victim to phishing schemes (Vokamer, et al., 2020). Additionally, training must be continuous, not just a one-time session. Employees must constantly receive cybersecurity awareness and training on the potential consequences of each phishing attempt to achieve a proactive approach to a pervasive culture of cybersecurity. To address phishing, information workshops or campaigns can easily be conducted to provide employees a better understanding of these techniques and the potential hazards of engagement.

4. Cybersecurity Measures and Best Practices

Several measures and best practices are necessary to protect healthcare organisations from cybersecurity threats. The measures undertaken by the UGMC include deterring technologies, policies and procedures, user training and manual actions, user password management, software updates and security patch installation, and incident response strategies. The IT team has implemented a multi-layered approach to cloud services such as corporate emails to prevent intrusion or outbreaks in the case of cybersecurity threats (Landoll, D., 2021).

To begin with, firewalls have been implemented to block unwanted traffic. These appliances have the capability of an Intrusion Detection System and Intrusion Prevention System as part of its intrinsic design. Next, antivirus software has been deployed to protect against the intrusion of malware or any other files using the Internet. Additionally, updating software and security patches is an essential procedure to control system integrity. Often times, the updates and patches are implemented in a test environment to forestall any eventuality that might be detrimental to the network. Also, regular updates of firewalls are carried out to prevent unwanted traffic from reaching intended recipients within the healthcare organisation.

Employee training and manual actions form an essential aspect of the multi-layered approach to creating a well-established culture of security in the workplace. System and network administrators have been trained to monitor, maintain and interpret network traffic, firewall logs and pieces of technical information, to efficiently administer infrastructure. Furthermore, as much as possible, annual risk assessments must be performed in order to detect vulnerabilities to protect the network from cybersecurity threats (Aslan, Ö., et al., 2023). Unfortunately, financial constraints at the organizational level hinders the implementation of such measures.

In addition, a dedicated team or staff is assigned the responsibility for cybersecurity issues by taking proactive steps to help the organisation to address and prevent threats from entering or infiltrating other

systems. On the other hand, packets that are leaving the network are also monitored as well. As part of the responsibilities, regular security awareness trainings are organised for staff to bring them to speed on the evolving threat landscape and many more. What's more, users are sensitised on the most appropriate way to report threats or vulnerabilities encountered effectively. Through these trainings, an incident response strategy guide is developed to help the organisation define the steps and actions required to prevent, respond to, and detect cyber threats and vulnerabilities. This may include the implementation of a disaster recovery and confidential plan. The Domain Name Server (DNS) is monitored by implementing security measures such as cryptographic implementation or setting up DNS responses with a minimal amount of normal resolvable records constructed to poison the DNS or respond insecurely to users (Oniagbi, O., et al., 2024).

Additionally, host-based intrusion prevention systems are also implemented to help protect user computers by using fault detection approaches, especially when a certain application is triggered by the user or by other events such as network activity. Also, the configured interfaces on the routers are delineated according to the ingress or egress while the available and unused ports are deactivated. This is a precautionary measure against any physical access to the router. A Security Information and Event Management (SIEM) is also deployed within the same subnet as the router to analyse security alerts from external-to-internal and internal-to-external to prompt the team responsible for data security. The notification from the SIEM takes advantage of other existing security systems already in existence and complements the existing systems report as part of the vulnerability and threat risk registry.

Finally, the organisation's storage and management of large volumes of data is automated twice in a day to minimise the Restoration Point Objective (RPO), should there ever be an unforeseen circumstance. This is actualised by managing, backing up and replicating data to two different remote sites and in the cloud. After completion, a report on the analysis logs and events are sent by email to the assigned team. The business continuity and disaster recovery plan provide policies and procedures already disseminated and agreed upon to continue providing services during times of disaster.

4.1. Firewalls and Antivirus Software

Strong foundational elements of security include a personal firewall and antivirus software. Firewalls act as a barrier between a trusted internal network and an untrusted external network. They perform this role by examining all Internet Protocol packets to determine whether to allow them through the firewall to the trusted network or block their passage altogether. The firewall software feature is enabled on end-user computers to complement the parameter security provided by the firewall and the Endpoint Detection Response (EDR) on end-user computers.

There are two basic types of firewalls: network layer firewalls and application layer firewalls. Both types of firewalls can be configured to completely block incoming or outgoing traffic that does not meet set security criteria, to filter traffic based on location carefully, or to filter traffic based on user identity. Hardware firewalls work either through a router-like setup between two or more networks or as a stand-alone appliance and are sold by companies specialising in network security. A software firewall is specifically developed for the computer's operating system and can be a pricey add-on to a computer operating system. A firmware firewall is a software, however, that is pre-installed onto a more permanent memory location than essential software, such as read-only memory, which cannot be altered by regular updates or installed software. In addition, in order to be effective, firewalls require regular updates and ongoing maintenance to keep up with the evolving threats from computer hackers. Ideally, a series of security measures should be in place outside of the firewall for further defence (George, A. S., 2023).

Antivirus software detects and eliminates malicious software that looks for specific target viruses. They use a range of techniques, such as checking for patterns in the files or examining them at the time of execution. The antivirus software gives extra security to the endpoint while investigating the files to establish a pattern in the Operating System. In the event that an unusual file extension is captured after a scan, it is either quarantined or deleted based on the configuration by the IT personnel. Some antivirus software uses heuristics in its effort to identify viruses. Heuristic scans test a potentially infected file to see whether the file has attributes of a virus or if it should be investigated further (Arogundade, O. R. 2023).

4.2. Employee Training

The importance of adequate employee training in cybersecurity measures cannot be overstated. One of the common ways through which confidential information can be leaked is through human error, which has been confirmed to be the most significant cause of data breaches in hospitals. Regular cybersecurity training is fulfilled to foster security awareness and vigilance. Several methods exist to provide training, such as the mass training programs organised by the IT Department. The use of newsletters, emails, alerts, screen savers, management memos, and posters has been found to be an effective method of promoting and raising awareness of cybersecurity in the Centre. Additionally, refresher programs are especially important as healthcare providers work with technological tools in their day-to-day operations (A Pollini, et al., 2022).

Trainings are role-based and tailored to various employees' specific needs and challenges, including IT staff, clinical and non-clinical staff, vendors, and contractors. There are three levels of employee training: employers provide information security training, Information System Security Officer (ISSO), and Integrated Security System (ISS) participation training. Invariably, not every employee can respond to security incidents, so security awareness training complements education by training an organisation's personnel to avoid accidents or incidents. Hospitals can also create a response service to educate employees about security incidents and how to respond. This could be used to provide, among other things, cybersecurity requirements, procedures, and information to hospital employees, where responsibilities are identified as members of the cybersecurity incident response team. Providing information to employees can also prevent potential attackers from detracting interest. Equipping employees with the necessary tools and skills to help them defend against cyber attackers will enable an organisation to anticipate and prepare for such an attack (Marquis, Y. A., 2024).

5. Case Study: University of Ghana Medical Centre

The University of Ghana Medical Centre, a quasi-institution, is located in the precinct of the University of Ghana, Accra. This section will analyse the hospital's IT infrastructure, security methodology, and IT personnel. In addition, we will examine past occurrences to determine the hospital's strengths and weaknesses in dealing with potential cybersecurity incidents. This research will also gather other pertinent information, including the makeup of the patient population, the specific cybersecurity needs of the hospital, and how healthcare strategies can be applied to cybersecurity incidents in Ghana.

The hospital's analysis for this case study has several advantages over most healthcare facilities in Ghana. The report of the Head of IT, who is responsible for setting up and maintaining the hospital's network, indicates that there have been myriads of attacks such as Cross-Site Request Forgery (CSRF), SQL Injection, Brute force and Phishing. Several hospital employees were also interviewed to gather data on past incidents. Our primary focus was to examine three issues: the kind and frequency of incidents

encountered at the hospital, the primary causes, and how the hospital addressed and solved these incidents. During the hospital study, we learned about a phishing security breach that robbed a staff member of a research grant amounting to $80,000. This experience occurred at a sister-organisation of which we share the same domain, despite our numerous security and awareness training. This incident necessitated the implementation of Multifactor Authentication (MFA) of staff email access. Meanwhile, our observation over the past five years suggests that the hospital has a strong security profile, even though there are areas particular to the hospital that require attention.

5.1. Overview of the Hospital's IT Infrastructure

The University of Ghana Medical Centre has a three-tiered IT architecture that provides healthcare delivery services. This IT infrastructure contains integrated networks, system, databases, applications, and data to support administrative and clinical services. Essentially, the infrastructure comprises hardware resources, software, and networks. The hospital's key electronic services include Electronic Health Records, laboratory databases, mobile money transactions, appointment system, Picture Archiving and Communication Systems, Human Resource Information Systems, and financial software. A suite of research and e-library applications also resides on four virtualised servers.

Spectrum Internet Services, Comsys Ghana Limited and Telecel Ghana are our Internet Service Providers. Aside from the outsourced UPS maintenance and storage support services, all the other services are managed by the UGMC IT team. This diverse technology ecosystem is mainly used by clinical application support to resolve complex issues that may arise. The Centre also leverages cloud services that host the institution's website and intranet website and on-prem web servers that host the EHR application. These web servers are halted and restarted during the influx of overwhelming requests while the Machine Learning ability of the virtualised environment optimises to accommodate the load during peak hours. An electronic surveillance system consists of Closed-Circuit Television Cameras with a Network Video Recorder connected to an internet protocol address accessible anywhere. The hospital uses and allows staff to use intranet resources and other third-party applications as external communication tools. In summary, the IT infrastructure requires modernisation and resilience to thwart the growing cybersecurity challenges, hopefully to a Hyperconverged Infrastructure (HCI) where a private cloud would be built over it.

5.2. Previous Cybersecurity Incidents

The University of Ghana Medical Centre commenced operations in 2018, and has not encountered any incident. However, the Business Continuity Plan outlines steps for the restoration of service with the Security team's involvement. In order to mitigate the effect caused by an incident, the UGMC devised a strategy to communicate with its stakeholders. The strategy included extensive collaboration with the Cyber Security Authority (CSA), a government agency under the Ministry of Communication and Digitalisation, developing a 24/7 rotating hospital command line, and a stationed senior IT team member on site. In order to collaborate with employees in responsive activities and identify issues related to attack. We have sourced funding for capacity building to invest in protecting equipment that is sorely needed in the wake of the ever-changing cybercrime world. Even more, we are building a culture of patriotism and incentivise staff to ward of external temptation in the event of a compromised system.

6. Cybersecurity Strengths and Weaknesses

UGMC's cybersecurity posture emphasises the importance of cybersecurity and the implementation of an Information Security Policy and Procedures, demonstrating a forward-thinking strategy to protect

infrastructure and patient information. Moreover, the hospital utilises digital technologies to improve efficiency and patient care, which can be enhanced by implementing robust cybersecurity measures. Data encryption has been put in place as a crucial protective strategy, being aware of the enormity of the ransomware and other facets of cyber-attacks.

Conversely, the organisation showcases some weaknesses in healthcare systems, including outdated or End-of-Life systems, limited staff training, potential phishing attacks, potential response gaps and evolving threats. Similarly, there's the need for a dedicated Cybersecurity Response Team and ongoing training to prevent data breaches.

6.1. Recommendations for Improvement

Regular risk assessments must be carried out to discover the vulnerabilities in the UGMC infrastructure and address the weaknesses. This practice will ensure that the identified risks that impact the organisation and people are mitigated. Additionally, to reduce human errors that could result in data breaches, it is expedient that continuous cybersecurity training is provided for all staff members, including the IT team, clinical, and non-clinical personnel. According to Stanford and Tessian, cited in Hancock (2022), 88% of data breaches are caused by human errors. Therefore, regular security and awareness training will minimise the impact of social engineering attacks and inform employees about current cyber threats and optimum measures for protecting patient information.

The IT team must perform routine penetration tests to mimic cyberattacks that might occur. This presents the opportunity to uncover weaknesses in the system before a hacker exploits them; by so doing, whatever needs to be patched or upgraded would have been implemented. As a best practice, the IT team will need to double-check software, patches, and perform upgrade regularly to avoid any risk exposures. Based on experience, the best approach to implementing the patches is in a test environment and not automatically rolling them out to prevent a semblance of the ***Crowd Strike*** encounter.

Furthermore, there's the need to utilise Two-Factor Authentication (2FA) or Multifactor Authentication (MFA) to provide an additional layer of security beyond login credentials before access is granted to critical systems like the Electronic Health Records which hold patient information. Also, recent ransomware attacks have conscientized users into encrypting sensitive data. It is to establish that in the event an attack is actualised, the data is kept safe. Therefore, deploying a blockchain backup will ascertain that the data is immutable. Finally, the institution must work with industry specialists and cybersecurity researchers to remain informed about the newest threats and effective strategies. This is because the threat landscape is constantly evolving, and industry specialists have more profound knowledge of the various aspects of cybersecurity. Their depth of knowledge is achieved through experience of real-world cyberattacks and many more.

7. Conclusion

In summary, our study provides strong evidence of the importance of cybersecurity in the healthcare industry. UGMC's strength ultimately lies in the awareness of the problem and the progressive steps to address it. The organisation has taken crucial steps to invest in data encryption, a fundamental measure to add an extra layer of security to protect data. Some weaknesses identified include the need for enhanced cybersecurity awareness training for staff and the potential shortcomings in the Incident Response Plan. The observed phenomenon can be attributed to a need for more testing personnel. The IT Department has not had the needed replacement since five of our staff moved on. The paper highlights the essence of strengthening partnerships with cybersecurity experts, considering that industry experts have first-hand

experience dealing with potential threats. Through this collaboration, the best practice of developing a comprehensive Incident Response Plan will be adopted. While our study also offers valuable insights, it is essential to note that the limited threshold of the Spending Officer, organisational bureaucracy and intricate external approvals at the Public Procurement Authority causes delays in the acquisition and implementation of technology projects which have a direct bearing on cybersecurity.

8. References

1. A Pollini, TC Callari, A Tedeschi, D Ruscio… - Cognition, Technology & …, 2022 - Springer. Leveraging human factors in cybersecurity: an integrated methodological approach. https://doi.org/10.1007/s10111-021-00683-y
2. Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. Plos one, 17(11), e0274550. https://doi.org/10.1371/journal.pone.0274550
3. Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. Journal of medical Internet research, 22(5), e18394. doi: 10.2196/18394
4. Al Kinoon, M. (2024). A Comprehensive and Comparative Examination of Healthcare Data Breaches: Assessing Security, Privacy, and Performance. https://purls.library.ucf.edu/go/DP0028279
5. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10. https://doi.org/10.1186/s12911-020-01161-7
6. Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems, 14(2). DOI: 10.7176/CEIS/14-2-03
7. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
8. Aung, Y. Y., Wong, D. C., & Ting, D. S. (2021). The promise of artificial intelligence: a review of the opportunities and challenges of artificial intelligence in healthcare. British medical bulletin, 139(1), 4-15. https://doi.org/10.1093/bmb/ldab016
9. Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. International nursing review, 67(2), 218-230. https://doi.org/10.1111/inr.12585
10. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of medical systems, 44, 1-9. https://doi.org/10.1007/s10916-019-1507-y
11. Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. Technovation, 120, 102480. https://doi.org/10.1016/j.technovation.2022.102480
12. George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172. https://doi.org/10.5281/zenodo.8274514
13. Hancock, J. (2022). Understand The Mistakes That Compromise Your Company's Cybersecurity.

14. Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal, 22(1), 105-117. https://doi.org/10.1016/j.eij.2020.05.003
15. Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10(1), 33. https://doi.org/10.1186/s13673-020-00237-7
16. Jovanović, A., Klimek, P., Renn, O., Schneider, R., Øien, K., Brown, J., ... & Chhantyal, P. (2020). Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. Environment Systems and Decisions, 40, 252-286. https://doi.org/10.1007/s10669-020-09779-8
17. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183. https://doi.org/10.1016/j.eij.2020.07.003
18. Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. Security and Privacy, 4(5), e162. https://doi.org/10.1002/spy2.162
19. Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press. https://doi.org/10.1201/9781003090441
20. Larsen, E. P., Rao, A. H., & Sasangohar, F. (2020). Understanding the scope of downtime threats: a scoping review of downtime-focused literature and news media. Health Informatics Journal, 26(4), 2660-2672. https://doi.org/10.1177/1460458220918539
21. Li, J. P. O., Liu, H., Ting, D. S., Jeon, S., Chan, R. P., Kim, J. E., ... & Ting, D. S. (2021). Digital technology, tele-medicine and artificial intelligence in ophthalmology: A global perspective. Progress in retinal and eye research, 82, 100900. https://doi.org/10.1016/j.preteyeres.2020.100900
22. Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts. Journal of Engineering Research and Reports, 26(5), 138-154. https://doi.org/10.9734/jerr/2024/v26i51141
23. Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research, 23(1), 1112. https://doi.org/10.1186/s12913-023-10076-8
24. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119
25. Oniagbi, O., Hakkala, A., & Hasanov, I. (2024). Evaluation of LLM Agents for the SOC Tier 1 Analyst Triage Process.
26. Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2021). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evolving Systems, 12(1), 91-108. https://doi.org/10.1007/s12530-020-09335-4
27. Seh, A. H., Al-Amri, J. F., Subahi, A. F., Agrawal, A., Pathak, N., Kumar, R., & Khan, R. A. (2022). An analysis of integrating machine learning in healthcare for ensuring confidentiality of the electronic records. Computer Modeling in Engineering & Sciences, 130(3), 1387-1422. DOI: 10.32604/cmes.2022.018163
28. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 129, 104130.

https://doi.org/10.1016/j.compbiomed.2020.104130. https://doi.org/10.1016/j.compbiomed.2020.104130

29. Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing simulated phishing campaigns for staff. In Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25 (pp. 312-328). Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3_19
30. Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, 862221. https://doi.org/10.3389/fdgth.2022.862221