

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

Healthcare Cyber Infrastructure Risk Assessment: A Use-Case Approach

¹Emmanuel Song Shombot (CA), ²Gilles Dusserre, ³Robert Bestak & ⁴Nasir Baba Ahmed

^{1&2}Laboratory for the Science of Risks (LSR), IMT Mines Ales, France

³Czech Technical University in Prague, Czech Republic

⁴IMT Mines Ales, France

E-mails: emmanuel.song@mines-ales.fr; gilles.dusserre@mines-ales.fr; robert.bestak@fel.cvut.cz;
nasir-baba.ahmed@mines-ales.fr

ABSTRACT

The healthcare sector and its cyber infrastructure are of great significance in modern healthcare administration as they allow for the fluid and efficient operations of health service delivery. In recent years, the sector has witnessed an expansion in the attack surface that can be exploited by cybercriminals. This is as a result of new and more sophisticated medical devices, IoT devices, and generally, more improved technology that are constantly introduced to the networks. This study considered the NIST and ISO 270001 frameworks as a point of reference and carried out an adapted risk assessment for a hospital use case. In our methods, we comprehensively took an inventory of the cyber assets that are currently used in the facility, then subsequently considered the known inherent vulnerabilities of those assets and external threats that could potentially exploit those assets. Lastly, quantification of those risks was carried out according to a matrix to help situate the threats that are deserving of the key risk control strategies of defence, transfer, mitigation, acceptance, and termination. Key findings of this paper include the identification of high, medium and low risk assets and the corresponding threats and vulnerabilities based on the National Vulnerability Database (NVD) and Mitre Common Vulnerabilities and Exposures (CVE). Finally, this work also shows that although the improvement in technology helps the hospital's cyber infrastructure enormously, it also adds vulnerability dimensions that should be anticipated using adaptive risk management measures.

Keywords: Healthcare, Cyber Infrastructure, Risk Assessment, Use-Case Approach

Proceedings Citation Format

Emmanuel, S. S., Gilles, D., Robert, Bestak & Nasir, B. A. (2024): Healthcare Cyber Infrastructure Risk Assessment: A Use-Case Approach. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 97-120. <https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P10>

1. INTRODUCTION

The growing number of healthcare-related incidents in the past few years indicates that the sector lags behind other industries in protecting both people and processes (Jalali & Kaiser, 2018). Healthcare is considered one of the most targeted sectors for cybersecurity breaches (*The Need for Cybersecurity Self-Evaluation in Healthcare | BMC Medical Informatics and Decision Making*, n.d.). The industry has experienced significant data breaches and privacy compromises, which, if left unaddressed, could jeopardise the quality of services they are required to provide (Frumento, 2019). For non-tech-savvy stakeholders or board members, enormous investment in IT infrastructure is a contentious subject as it is perceived to be unjustifiable, with no real tangible outcomes attached to the spending (Cartwright, 2023), so it remains an issue of constant debate (Jofre, 2020). Therefore, internal politics, complex organisational structures, and regulatory pressures will continue to be a bottleneck in realising safety and cybersecurity objectives in the healthcare domain (Jofre et al., 2021).

Cybersecurity refers to the combination of methods and technologies designed to secure computers, software, data and other related assets from cyber threats or unauthorised access. In today's world, many services and operations, such as healthcare, rely heavily on the Internet ((PDF) *CYBER SECURITY AND ITS IMPORTANCE*, n.d.) . Even with robust standards in place designed to mitigate the majority of risks, the healthcare sector remains exposed to a plethora of cyber threats. This makes cybersecurity a critical consideration for many firms, particularly healthcare institutions (M. A. Ahmed et al., 2022).

The exploration of cybersecurity paradigms in the healthcare domain is relatively in its infancy (Jalali & Kaiser, 2018). It generally involves all proactive and reactive measures that can be taken to safeguard and protect electronic devices as well as the data within them. Over the last two decades, the healthcare sector has improved rapidly, with increased usage of new technologies (Argaw et al., 2020). Currently, all patients' personal identifying information (PII) and personal health information (PHI) are stored on the systems of the institutions they visit. Even if growing technological use enhances healthcare services, it also raises the risk of cyberattacks. Even though the assimilation of technology in healthcare operations is a welcomed development for improved service delivery, there is, however, an underlying risk of increased susceptibility to cyberattacks (Bansal et al., 2023).

There are a lot of methods and techniques by which cybersecurity is administered to protect IT assets. Some are more technical and tailored to very specific cyber threats, i.e., using machine learning to detect spoofing, DoS, NMap port scans, and smurf attacks in Internet of Health Things (IoHT) environment (M. Ahmed et al., 2021), while others are more policy-driven towards people and processes (Coppolino et al., 2019). In most cases, the approaches used are stochastic and do not present a holistic perspective to address cybersecurity in healthcare. Risk is generally perceived as a function of threat, vulnerability, and impact (Ekstedt et al., 2023). Another definition of risk is given as the probability of an external cyber threat exploiting a vulnerability in an asset and the corresponding impact of that adverse incident on an organisation (Jofre et al., 2021). To assess the relative risk for each identified vulnerability, most experts adopt a method of risk assessment that entails assigning a risk rating or a score that communicates an idea of the relative exposure of that organisation (Whitman & Mattord, 2014).

Even though the risk rating or score in itself hardly means anything in scientific or absolute terms, it does provide a basis for comparative rating so therefore, caution should be applied when transposing the risk assessment method to a different context (Whitman & Mattord, 2014).

The contributions of this paper are

- 1 Propose a refined approach for conducting risk assessment based on established standards and frameworks (Baze University Hospital Cyber Risk Assessment Framework, “BUHCRAF”).
- 2 Implement a reproducible risk calculation technique that is fully customizable and adaptable to similar contexts.

2. USE-CASE OVERVIEW

The work presented in this research presents an adapted risk assessment solution for a defined healthcare facility. Baze University Hospital (BUH) is a 200-bed hospital associated with Baze University in the Federal Capital Territory of Abuja, Nigeria. BUH was established to provide advanced healthcare services. The facility is equipped with modern facilities for the sole purpose of providing quality health services. Additionally, the hospital engages in research activities leveraging technology that are functionally and aesthetically urbane (*BAZE FOCUS MAGAZINE (2022 CONVOCATION EDITION) by Baze University - Issuu, n.d.*).

Table 1. Department, Services and Description (No reference)

SN.	Services	Description
1.	Registration Kiosk	Registration portal with Data protection compliant efficient hospital management systems (HIMS).
2.	Emergency Services	Ambulance, Advanced point-of-care diagnostics, mobile X-Ray, mobile ultrasound scan, ABG machine, Monitors, Defibrillators and Mobile Ventilators.
3.	Family Medicine & General Outpatient Clinic	Routine medical checkups, health screening and wellness packages.
4.	Pharmacy Department	Counselling and drug information - high level pharmaceutical administration.
5.	Pediatric Unit	Emergency and Neonatal Intensive Care Unit.
6.	Ear, Nose & Throat (ENT) Department	Audiological examination, general ENT, head and neck surgery, ENT diagnosis and emergency management.
7.	Ophthalmology	Diagnosis and treatment of eye diseases, cataract surgeries and vision rehabilitation.
8.	Obstetrics and Gynecology	Assisted conception, general surgery,
9.	Laboratory Services	Microscopy, CSF, ESC, HVS, culture and sensitivity of clinical specimens.
SN.	Services	Description

10. Radiology Department	Magnetic Resonance Imaging, digital radiography, computed tomography (64 slice CT) with coronary and Angiographic study options.
11. Histopathology Department	Incisional, excisional, Exfoliative and aspiration cytology.
12. Blood Transfusion and Haematology Department	Diagnosis and treatment of haemato-oncology disease. Leukaemia and bleeding disorders.
13. Chemical Pathology Laboratory	Cardiac marker testing for cancer screening, endocrine diagnosis, metabolic disorders, infertility evaluation and cardiovascular risk assessment.
14. Physiotherapy and Rehabilitation Department	Hydrotherapy, laser therapy, reatherm diathermy and shockwave therapy
15. Utility Unit	Water supply, power system supply, firefighting equipment, gas plant and Air conditioning system.
16. Catering Services	Fully functional Catering and laundry services.

3. CYBERSECURITY FRAMEWORKS AND STANDARDS

In the domain of risk management, there are several standards and frameworks designed for cybersecurity risk assessment (Bolbot et al., 2020). Some of the widely known frameworks include the International Organisation for Standardisation (ISO 27000) series (Meriah & Arfa Rabai, 2019)The National Institute of Standards Cybersecurity Framework (NIST CSF) (Toussaint et al., 2024), and the European Union Agency for Cybersecurity (ENISA) (*Compendium of Risk Management Frameworks with Potential Interoperability*, n.d.). In the area of research, authors have proposed frameworks such as the “Yet Another Cybersecurity Risk Assessment Framework” (Yacraf) (Ekstedt et al., 2023), while other authors have leveraged the strengths of the Information Technology Infrastructure Library (ITIL) model tailored towards meeting specific security management objectives of a defined context (Lopes et al., 2024).

It is not an uncommon practice to decompose several cybersecurity frameworks and adapt them according to the unique needs of a firm (Alshar’e, 2023). In this work, we evaluated the similarities between the NIST and ISO 27000 series and used them as a reference to develop a risk assessment solution suited for our context.

3.1 ISO/IEC 27000 series

The ISO/IEC 27000 series, popularly referred to as the ISMS family of standards, provides the best practices and recommendations for information security management (*ISO - ISO/IEC 27000 Family – Information Security Management*, 2022). The scope of the series is very comprehensive in design and transcends beyond confidentiality, privacy, and cybersecurity issues.

For instance, the ISO/IEC 27001 standard generally stipulates the requirements for establishing, implementing, maintaining and continuous development of information security strategy (Kitsios et al., 2023). The ISO/IEC 27002 stipulates a universally accepted and acknowledged benchmark for restrictions tailored for specific information security risk circumstances (Kitsios et al., 2023). The ISO/IEC 27005 stipulates guidance for the management of information security risks (Alazzawi, 2021). Most of the ISO/IEC standards were implemented to varying degrees to achieve the objectives of this work.

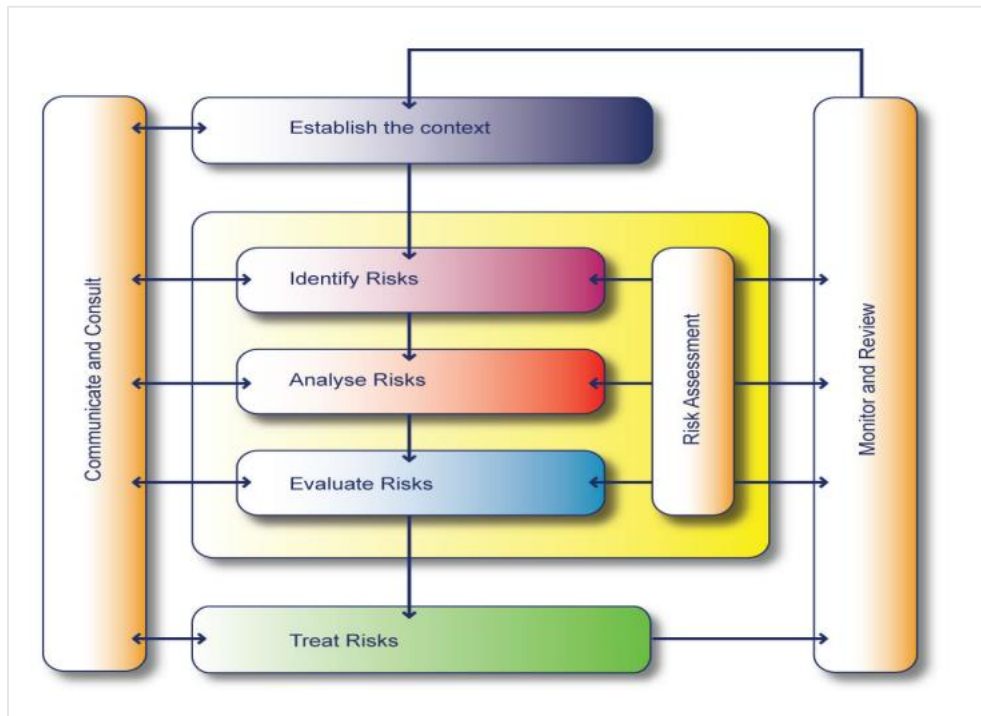


Fig. 1: ISO 27005 Risk Management Process

- Communicate and Consult:** This level of the risk management process opens the communication pathways of stakeholders that will be involved in the process. Ensuring there is a healthy feedback loop of information flow and decision making (Alazzawi, 2021).
- Establish the context:** This stage involves defining the scope, context and criteria in alignment with organisational objectives. Thoroughness should be exercised in this stage, as it should provide details for how risks are identified and how the impact and likelihood will be calculated (ISO 27005 | IT Governance UK, n.d., p. 27005).
- Risk Assessment (Identify Risks, Analyse Risks, Evaluate Risks):** The Risk assessment process, generally, as shown in Fig. 2, consists of three key steps of identifying risks, analysing risks and evaluating risks. To achieve this, the risk assessment analyst will comprehensively compile all the information assets and identify all existing threats and vulnerabilities applicable to the assets. Subsequently, the risk criteria are defined then followed by assigning impact and likelihood values. To complete this stage, each

identified risk is evaluated against predetermined levels of acceptance so that priorities can be established on which risks should be addressed.

- Risk treatment:** The risk treatment is also referred to as the risk control strategy (Whitman & Mattord, 2018). This stage stipulates the five key strategies that can be taken to treat the articulated risks. it could be defense, where measures are taken to stop the exploitation of vulnerabilities; transference, which moves the responsibility associated with the risks to other assets or organizations; mitigation, to reduce the impact of an incident; acceptance, where no action is taken to protect an asset especially when the cost of the asset is less than the safeguards employed to protect it; termination are conscientious measures taken to avoid introducing activities that expose the organization to uncontrollable risks.
- Monitor and Review:** cybersecurity risks are not stationary; the risk landscape can abruptly change as a consequence of changing threats; therefore, continuous monitoring is needed to identify such changing dynamics and include them in the risk management scope.

3.2 NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework (NIST NCF) is designed to help organisations improve their cybersecurity posture by identifying exploitable cybersecurity gaps (*An Introduction to Buildings Cybersecurity Framework | IEEE Conference Publication | IEEE Xplore, n.d.*). The framework facilitates understanding, managing and reducing risk associated with cybersecurity infrastructure in organisations of all sizes (Wang et al., 2024).



Fig. 2: NIST CSF

The NIST CSF framework is fully customizable to the precise needs of an organisation. This functional adaptability gives the organisation sufficient leverage to determine the specifics of the implementation framework (*Integrating Cost–Benefit Analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model | Journal of Cybersecurity | Oxford Academic, n.d.*). The framework is made up of three major components: core, implementation tiers and profiles (Alshar'e, 2023). The core consists of five activities designed to deliver specific cybersecurity outcomes. These activities, as shown in Fig. 3, are identify, protect, detect, respond and recover (National Institute of Standards and Technology, 2018),(Parmar & Miles, n.d.).

- **Govern:** In the governance layer, the organisational context is established and planning a programme that aligns with the mission, goals and stakeholders' expectations. Roles are also established and assigned to individuals to define hierarchy and responsibility.
- **Identify:** This stage constitutes the identification of assets owned by the organisation. These assets are typically data, hardware, software, systems, facilities and people. Additionally, the risks to these assets are also identified and classified. Another crucial activity carried out in this stage is Risk Analysis (RA), which involves attack surface management (ASM) and vulnerability analysis (VA).
- **Protect:** These are the measures or safeguards put in place to ensure the confidentiality, integrity and availability (CIA) of the assets already identified. Some of the measures used in protecting assets could also be cryptography, multifactor authentication, passkeys and backup or recovery systems.
- **Detect:** This layer of the framework ensures timely discovery of cyberattacks. Usually, this is achieved with specialized tools such as a monitoring dashboard, Network intrusion detection systems (NIDS) and anomaly detection systems.
- **Respond:** This level of the framework involves practical actions taken to contain the impact of the detected cybersecurity incidents. Dynamic playbooks are employed in this stage to outline a series of steps to be taken to resolve the incident.
- **Recover:** The recovery process supports the timely restoration to normalcy in operations in the event of a successful attack exploitation. The backup systems used for protection are commonly used in recovery. Also, communication dynamics must also to manage at this level to notify regulatory bodies of the incident.

4. METHODOLOGY

Given that there is considerable overlap between some components of NIST CSF and ISO 27000 series, this work streamlined commonalities between the two frameworks and customised it to fit the peculiarities of the use case. For example, the ISO 27000 series or family details comprehensive coverage of information security management, so this work leveraged the formalisation of the ISO/IEC 27001 standards addresses information security management requirements. Also, from the family of ISO/IEC 27000, this work specifically excerpts from the ISO/IEC 27005 standards that stipulate guidance for managing information security risks. Equally, the NIST CSF focuses on improving cybersecurity postures by identifying and mitigating risks. There is fine alignment of the CSF framework with the requirements of Baze University hospital in terms of Identify, Protect, Detect, Respond and Recover.

4.1 BUH Operations and Processes

To understand how to conduct the cyber risk management process for BUH, it is necessary to understand how the facility operates. Firstly, all internet traffic going in and out of the organisation is filtered through a firewall. However, it is worth mentioning that Baze University Hospital proceeds from Baze University, which started in 2011; therefore, there is the main site and the Baze University Hospital permanent site, as illustrated in Fig. 3. Currently, the main site houses electronic medical records (EMR), a staff/student portal, and a website server. From the main site, the traffic flows to the permanent site, where all medical devices, switches, management systems, etc., are situated.

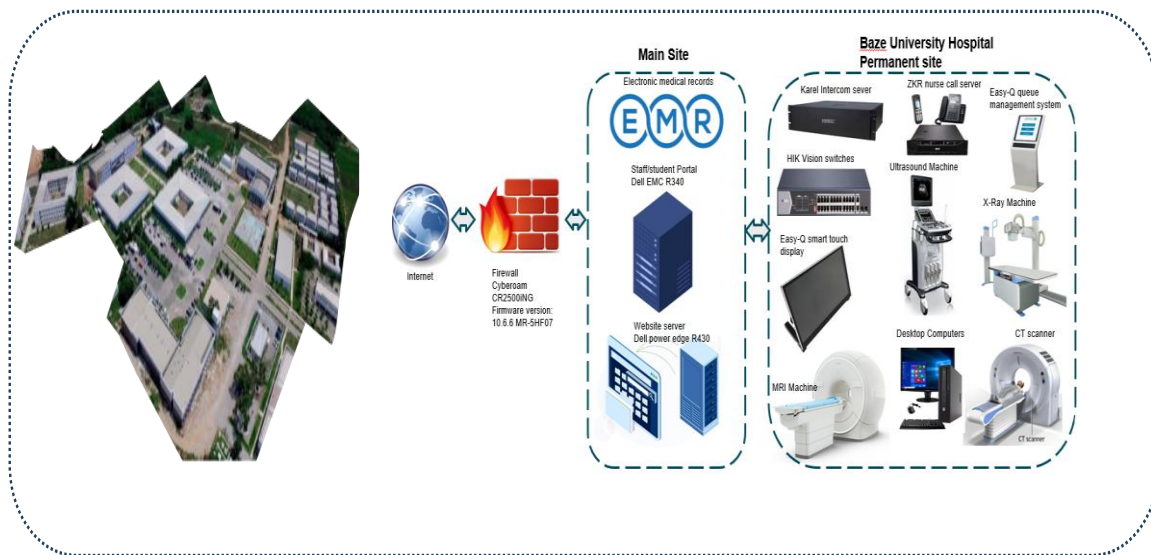


Fig. 3: BUH Cyber Operations and processes

4.2 Proposed BUHCRAF framework

The proposed Baze University Hospital Cyber Risk Assessment Framework (BUHCRAF) is a streamlined and fully adapted approach based on the iterations of the ISO27000 series and NIST CSF.

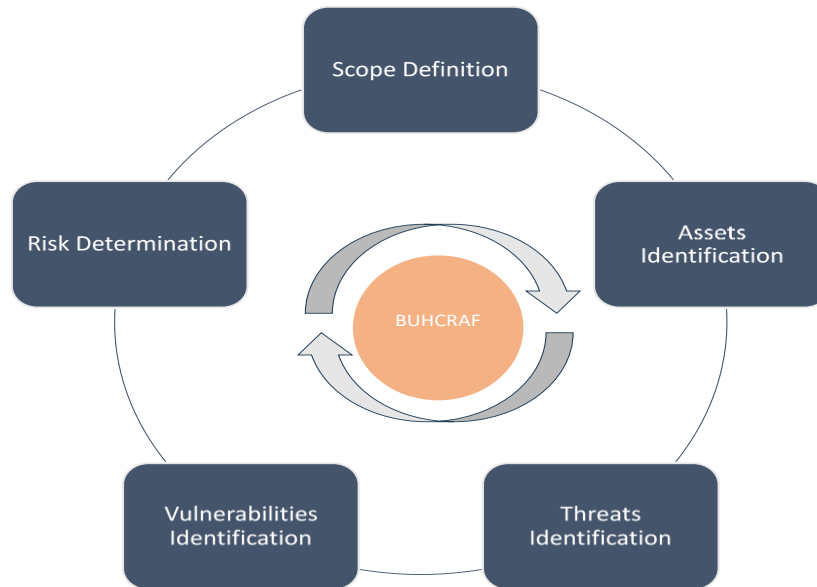


Fig. 4: Baze University Hospital Cyber Risk Assessment Framework (BUHCRAF)

Using the two frameworks provides flexibility in leveraging just the strong and applicable components from both in the proportion that applies to the defined context. Fig. 4 shows the five stages proposed in the BUHCRAF framework. In comparison to the existing frameworks, BUHCRAF is an improvement because of the contextual adaptation, flexibility and customisation, holistic risk management approach and practical implementation.

4.3 Scope Definition

In the scope definition stage, we articulated the boundaries of what the risk assessment would cover. Even though the mission and objectives of BUH are futuristic and very wide in scope, in this work, we confined the risk assessment to comprehensively cover the cyber infrastructure of the hospital. All other assets, such as buildings, automobiles, wheelchairs, and other physical assets, were excluded.

4.4 Assets Identification

Assets within the context and scope definition of this work, as articulated in Subsection 4.3, are defined as any hardware, software, networks, or substance of material value to Baze University Hospital. Should there be any compromise in the integrity of an asset, then it will result in some significant impact on the performance of the asset and negatively affect hospital operations.

4.4.1 Assets and Description

Hospitals generally have diverse assets. The European Union Agency for Cybersecurity (ENISA) has a loosely coupled methodology that helps categorise and group cyber resources in hospitals. We have adopted the categorisation technique to identify and group relevant assets that fall within the scope of our study. Fig. 5 shows the number of assets in BUH, while Fig. 6 shows the distribution of cyber assets based on the ENISA frameworks.

Table 2. Assets, Categories and Description

SN.	Asset	Type	Category	Description
1.	Switches	HIK Vision	Networking equipment	These switches are used for network distribution. There are two variations of the switches. (1) Power over Ethernet (POE) (2) non-power over Ethernet
2.	Ultra-sound machines	GE Logiq	Networked medical devices	Medical devices used for clinical imaging. There are two variations of the ultrasound machines. (1) GE Logic X (2) GE Logic Q
3.	MRI machines	GE Signa Creator	Networked medical devices	Magnetic resonance imaging (MRI) uses non-invasive imaging technology that produces detailed anatomical images in three dimensions
4.	CT-Scan	GE Revolution Maxima	Networked medical devices	A computed or computerised tomography (CT) scanner is a medical imaging technique used for obtaining detailed images of internal body parts.
5.	Advantage workstation	GE AW4.6	Networked medical devices	The advantage workstation is a networked medical imaging console dedicated to examination, review and diagnosis on film.
6.	Remote energy monitoring	Cerbo Gx	Buildings and facilities	The remote energy monitoring system helps in controlling, optimising and managing energy consumption from a central location in a building asset.
7.	Intercom server	Karel	Networking equipment	Karel is a modular and server-based IP communication platform that is designed for medium and large-scale organisations.
8.	Nurse call system	ZKR	Networking equipment	Communication system infused with a medical nurse calling and queue management system.
9.	Firewall	Cyberoam CR2500iNG	Networking equipment	A hardware device for plugging into the hospital network at the perimeter, serving as a gateway for traffic.
10.	Website server	Dell power edge R430	Networking equipment	Used for high-performance computing, web technology and infrastructure scale-out.
11.	Staff and student portal	Dell EMC R340	Data	Single socket 1U rack server designed for productivity and applications that are data-intensive and automation of daily tasks.
12.	Electronic medical record	EMR	Interconnected clinical information systems	The EMR is a digital patient health record for clinical care, billing, and reporting.
13.	Queue management system	Eazy-Q	Interconnected clinical information systems	A queue management solution that offers a unique way of handling customer inflow.
14.	Computers	Hp - Windows 11	Mobile client devices	Standard computers used by staff for technical and administrative tasks are all running Windows 11

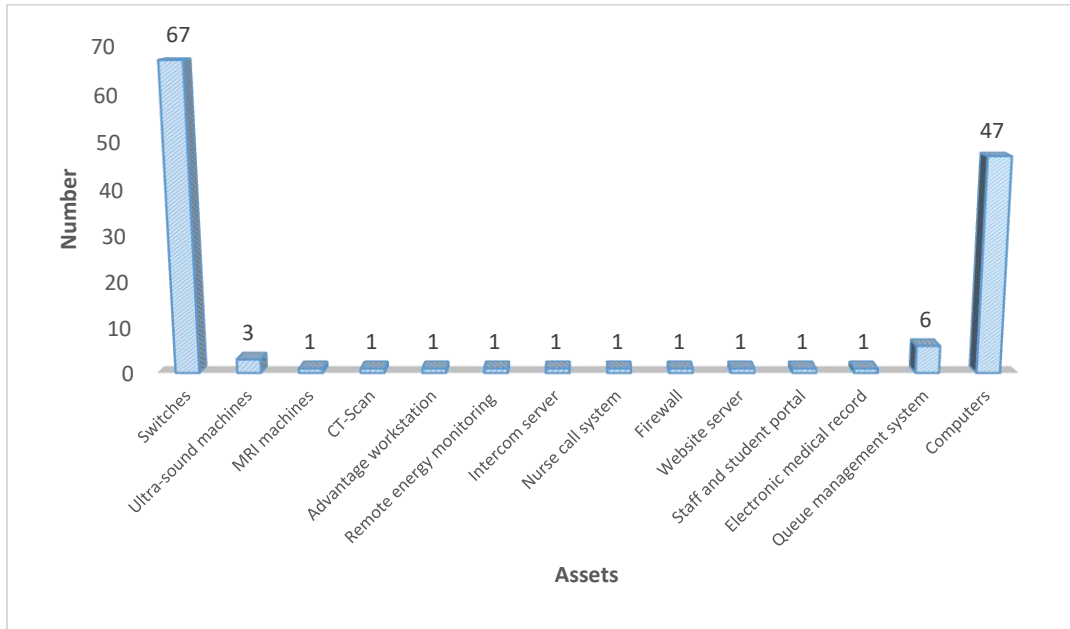


Fig. 5: Number of Assets in BUH

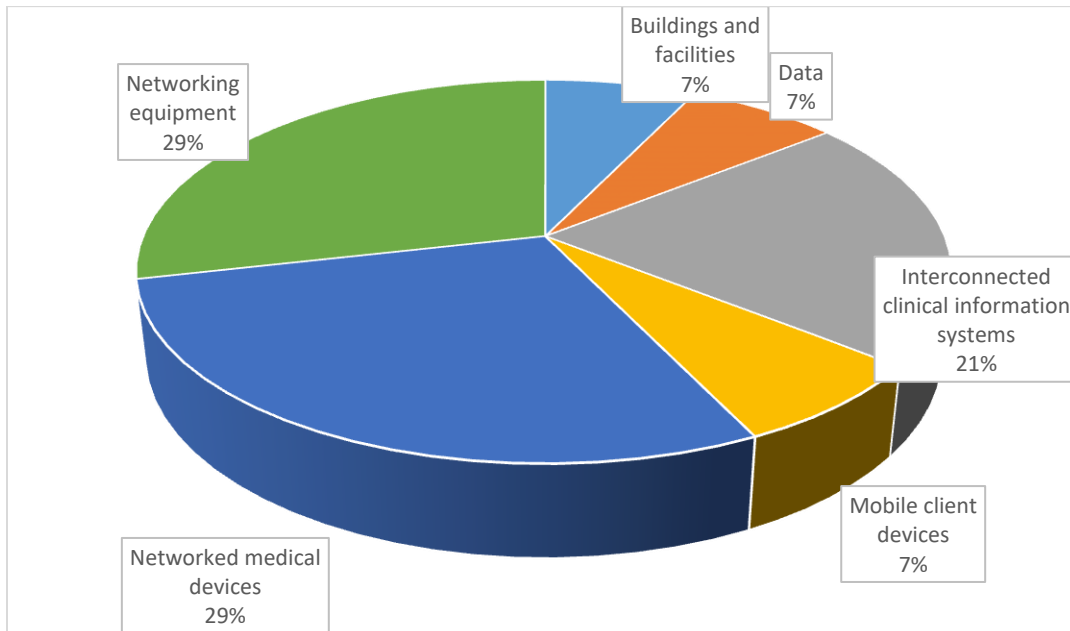


Fig. 6: Categorization of Assets

4.4.2 Asset Value

When determining the hierarchy of importance of each asset to the company, it is necessary to assign a relative value that indicates the order of priority. Factors that must be considered in this assessment include assets that are critical to the success of the organisation, assets that generate the highest revenue/profitability, assets with the highest replacement cost, and assets that, if compromised, cause the greatest embarrassment (Whitman & Mattord, 2014). Therefore, in this work, the matrix in Fig. 7 was used to assign relative values to each asset for the cyber assets in Baze University Hospital.

Value	Type of Effect Level of Effect	Company Embarrassment Level	Personal Safety Implication	Personal Privacy Infringement	Failure to Meet Legal Obligations	Financial Loss (£)	Disruption to Activities (£) (Time & Effort to Recover from Incident)
1	Insignificant	Contained within Work Area at worst	Minor injury to individual	Isolated personal detail revealed	Civil suit resulting in less than £10k damages	Up to 10k	Up to 10k
2	Minor	Contained within Company at worst	Minor injury to several people	Isolated personal detail compromised	Civil suit (above £10k). Small fine (up to £1k)	10k to 100k	10k to 100k
3	Significant	Local public or Press become aware	Major injury to individual	Several personal details revealed	Large fine (above £10k)	100k to 500k	100k - 500k
4	Major	National public or Press become aware	Major injury to several people or death of individual	Several personal details compromised	Custodial sentence imposed	500k - 1000k	500k - 1000k
5	Acute	Senior Staff forced to resign or Company fails	Death of several people	All personal details revealed and/or compromised	Multiple civil or criminal suits	Above 1000k	Above 1000k

Fig. 7: Asset Values and Impacts of Incident

4.5 Threats Identification

Threats are potential occurrences or externally acting agents that can damage or compromise assets. Threats can come from authorised and unauthorised users of assets; however, they cannot come from within the asset itself. Identifying all threats to a defined asset can be a tortuous and sometimes impractical endeavour, as threats are dynamic in nature. However, a good articulation of known threats is usually recommended to situate risks in their proper perspective.

4.5.1 MITRE ATT&CK®

MITRE ATT&CK® framework is a curated, globally accessible knowledge base drawn from adversarial tendencies and actions observed during cyberattacks (MITRE ATT&CK®, n.d.). ATT&CK®, which stands for Adversarial Tactics, Techniques, and Common Knowledge, primarily aims to model the behaviours with tactics, techniques, and procedures (TTP) to examine attack patterns (Lee & Choi, 2023).

The framework is primarily activated by most individuals/organisations to develop specific threat models; however, what is often overlooked with the ATT&CK® framework is the huge repository of articles that describe threats in detail and explain how attackers were able to carry out successful cyber-attacks and compromise certain cyber assets (Sun et al., 2024). Therefore, to efficiently identify potential threats to our assets, this research leveraged the ATT&CK® framework, articles and web sources to identify known threats to the assets in the BUHCRAF model.

4.5.2 Threat Rating

Different threats will have different severities or impacts; therefore, a consistent way of assessing these threats is necessary. Fig. 8 provides a rating system that captures several categories of threats, which include but is not limited to espionage, software attacks, theft, sabotage, technical hardware failures and information extortion (Whitman & Mattord, 2018).

Risk Likelihood	Description	Interpretation
1	Negligible	Once every 1000 years or less
2	Extremely unlikely	Once every 200 years
3	Very unlikely	Once every 50 years
4	Unlikely	Once every 20 years
5	Feasible	Once every 5 years
6	Probable	Annually
7	Very probable	Quarterly
8	Expected	Monthly
9	Confidently expected	Weekly
10	Certain	Daily

Fig. 8: Likelihood of Threat

4.6 Vulnerability Identification

Vulnerabilities are inherent flaws or weaknesses in the assets where threats can exploit to compromise the confidentiality, availability, and integrity of an asset (Whitman & Mattord, 2014). The process of vulnerability identification usually overlaps with the threat identification stage because all known vulnerabilities associated with an asset are mapped precisely to the known potential threats that can likely exploit them. Third-party catalogues are critical to finding a great number of documented vulnerabilities.

Alongside the MITRE ATT&CK® framework, this work greatly utilised the Common Vulnerability and Exposure (CVE) database (CVE Website, n.d.) and other sources to identify known vulnerabilities to the assets in the scope of the BUHCRAF model.

4.6.1 CVE

The Common Vulnerabilities and Exposures (CVE) database is a standardised system for identifying, tracking and cataloguing known vulnerabilities (A et al., 2024). The CVE keeps a unique identification number, a brief description and references for publicly known cybersecurity vulnerabilities (*Predicting Vulnerability Type in Common Vulnerabilities and Exposures (CVE) Database with Machine Learning Classifiers | IEEE Conference Publication | IEEE Xplore*, n.d.). Using the same rating system in Fig. 9, we assigned a corresponding vulnerability rating to the threats and assets.

4.7 Risks Determination

In determining the overall risks, a systematic approach is utilised in the form of a Threats-vulnerability-Assets (TVA) worksheet that logically presents the list of assets, their threats and corresponding vulnerabilities (Whitman & Mattord, 2018), (Mejias et al., n.d.).

5. Risk Ranking

The Risk register is a repository for all anticipated risks ranked according to their priorities (Patterson & Neailey, 2002), (Willams, 1994). The risk register may also include other associated information that guides the risk management process (Kendrick & ebrary, 2003), (Leva et al., 2017). Within the scope of this research, the relevant controls as identified by the NIST framework and other relevant scholarly sources capable of mitigating the impact of the risk are also included. As shown in Table 3, all identified risks that could potentially put assets at risk are assigned a value and ranked in descending order. This means that the higher the number, the more senior managers should prioritise these risks. The formula used to determine risk score is Risk = Asset x Threat Score x Vulnerability Score.

Table 3. Risk register

Asset	Value	Threat	Rating	Vulnerability	Rating	Risks value	Control
Website server	5	Phishing attacks	9	Outdated Vulnerable web application components	9	405	Regular patch updates
Electronic medical record	5	Phishing attacks	9	Email compromise	9	405	Build strong social engineering training and culture
Electronic medical record	5	Phishing attacks	9	Web features are susceptible to phishing attacks	9	405	Introduce technical sophistication and AI detection techniques
Electronic medical record	5	Phishing attacks	9	Redirect vulnerability	8	360	Strong usage policies and redirect checks
Website server	5	DDoS Attacks	8	Loophole in Apache server	8	320	Regular patch updates
Website server	5	DDoS Attacks	8	Server resource insufficiency	7	280	Implement technical DDoS attack techniques
Electronic medical record	5	Ransomware attacks	8	Inadequate monitoring and regulation system	7	280	Strong usage policies and training
Asset	Value	Threat	Rating	Vulnerability	Rating	Risks value	Control

Proceedings of the Cyber Secure Nigeria Conference – 2024

Electronic medical record	5	Data breach	9	Weak authentication	6	270	Secure user authentication profiles
Electronic medical record	5	Malware	6	Outdated anti-virus scans	9	270	Use the most recent anti-virus software
Computers	3	Virus	10	Indiscriminate flash drives on computers	9	270	Regulate flash drive usage for systems on networks
Firewall	4	DoS Attacks	8	Use of a custom signature-based IPS	8	256	Implement robust AI prevention techniques
Website server	5	Data breach	8	Insufficient security and access control	6	240	Deploy an efficient traffic monitoring routine
Website server	5	DDoS Attacks	8	UDP overflow	6	240	Socket monitoring
Electronic medical record	5	Malware	6	Inadequate monitoring and regulation system	8	240	Strong usage policies and training
Website server	5	Sabotage	6	SMM communication buffer verification vulnerability	7	210	Secured component verification (SCV), Intrusion detection
MRI machines	4	MDHRex	7	Vulnerability in FTP (port 21), SSH (port 22), Telnet (port 23), REXEC (port 512)	7	196	Restrict and monitor ports, use port control mechanisms
CT-Scan	4	MDHRex	7	Vulnerability in FTP (port 21), SSH (port 22), Telnet (port 23), REXEC (port 512)	7	196	Restrict and monitor ports, use port control mechanisms
Electronic medical record	5	Cross-site scripting	6	Insufficient sanitation of user-supplied data	6	180	Systems to check user-supplied data
Electronic medical record	5	SQL injection	7	Unvalidated input fields	5	175	Validated form checks
Electronic medical record	5	Cross-site scripting	6	Loophole in client-side script	5	150	Regular patch update
Ultra-sound machines	3	Insider threats	6	Protection mechanism failure	8	144	Strengthen the physical access protocol
CT-Scan	4	Hacking	7	Unprotected Transport of Credentials	5	140	credential update, patch update
Website server	5	Missing function-level access control	5	Insufficient server authentication and authorisation checks	5	125	Strong culture of verification and validation checks
Electronic medical record	5	Cross-site request forgery	5	Exploitation of session cookie vulnerability	5	125	Session variable management control
MRI machines	4	Unauthorized access	6	Insufficiently protected credentials	5	120	Protect credentials LDAP, keystore
Firewall	4	Privilege escalation	6	Exposure of Sensitive Information to an Unauthorised Actor	5	120	Strong organisational policy on asset usage
Website server	5	Missing function-level access control	4	Misconfigured function-level protection	6	120	Due care is given to configuring level access control
Switches	2	DoS Attacks	8	Not utilising virtual local area networks (VLANS)	7	112	Proportionately deploy VLANS
Asset	Value	Threat	Rating	Vulnerability	Rating	Risks value	Control

Proceedings of the Cyber Secure Nigeria Conference – 2024

CT-Scan	4	Hacking	7	Flaws in the Unix operating system	4	112	Ensure Unix is patched with the current OS
Ultra-sound machines	3	Insider threats	6	Incorrect User Management	6	108	Restrict access to kiosk mode functionality
Staff and student portal	3	Sabotage	6	SMM communication buffer verification vulnerability	6	108	Secured component verification (SCV), Intrusion detection
Ultra-sound machines	3	Elevation of privileges	5	Misconfigured access control list	7	105	Strengthen the physical access protocol
Computers	3	Escalation of privilege	5	Improper input validation	7	105	Continuous monitoring of access privileges
Firewall	4	Cross-site scripting (XSS)	5	Improper sanitation of login credentials	5	100	Strong credentials for assignment and monitoring
Switches	2	DoS Attacks	8	Not disabling unused ports	6	96	Close unused ports
Switches	2	DoS Attacks	8	Lack of Network monitoring tools	6	96	Deploy Network monitoring tools, i.e. Nagios XI
Switches	2	DoS Attacks	8	Lack of regular updates	6	96	Regular patch update
MRI machines	4	Hacking	6	GE (remote) service user privileges	4	96	Change default login credentials
MRI machines	4	Hacking	6	Unprotected Transport of Credentials	4	96	Implement cryptographic mechanisms
MRI machines	4	Hacking	6	Exposure of Sensitive System Information to an Unauthorised Control Sphere	4	96	Implement cryptographic mechanisms
Firewall	4	Privilege escalation	6	Incorrect Permission Assignment for Critical Resource	4	96	Vetted ACLS and proper coordination of access privileges
Ultra-sound machines	3	Insider threats	6	Improper input validation	5	90	Enable the "system lock" password in the Administration GUI menu if possible
Staff and student portal	3	Malware Injection	7	Firmware vulnerability	4	84	Silicon-based Root of Trust
Firewall	4	SQL injection threats	5	pre-authentication SQL injection vulnerability	4	80	Update "hotfix" patch
Ultra-sound machines	3	Command injection	5	Bug in the operating system	5	75	Restrict physical access
Firewall	4	Shell injection	3	Web admin portal vulnerability	6	72	Patch update
Firewall	4	Privilege escalation	6	Component access restriction	3	72	Patch update
Firewall	4	Privilege escalation	6	Improper access control	3	72	Vetted ACLS and proper coordination of access privileges
Firewall	4	Privilege escalation	6	Improper input validation	3	72	Vetted ACLS and proper coordination of access privileges
Firewall	4	Privilege escalation	6	Improper privilege management	3	72	Vetted ACLS and proper coordination of access privileges
Firewall	4	Privilege escalation	6	Exposure of Resource to the Wrong Sphere	3	72	Patch update
Asset	Value	Threat	Rating	Vulnerability	Rating	Risks value	Control
Queue management system	2	ARP poisoning	6	Misconfigured IP to MAC address table	6	72	Deploy secure traffic management systems

Proceedings of the Cyber Secure Nigeria Conference – 2024

Computers	3	Spoofing	6	Windows certificate vulnerability	4	72	Continuous monitoring of access privileges
Computers	3	Spoofing	6	Secure server handler compromise	4	72	Access privilege segmentation
Computers	3	DoS attack	7	Information disclosure via adjacent access	3	63	System resource management systems
Ultra-sound machines	3	Path Traversal	4	Bug in the operating system	5	60	Restrict physical access
CT-Scan	4	Arbitrary code execution	5	Unix OS vulnerability	3	60	Ensure end-to-end encryption of PHI
Remote energy monitoring	3	DoS attack	5	Missing Authentication for Critical Function	4	60	Use a firewall
Remote energy monitoring	3	DoS attack	5	Unsafe Reflection	4	60	Block access from untrusted networks and hosts
Firewall	4	Cross-site scripting (XSS)	5	Vulnerability in "LiveConnectionDetail.jsp" application	3	60	Patch update
Firewall	4	Command injection	3	Improper Neutralisation of Special Elements used in a Command	5	60	Check externally influencing input from upstream components
Staff and student portal	3	Component tampering	5	Physical server vulnerability	4	60	Secured component verification (SCV), Intrusion detection
Staff and student portal	3	Unauthorised open-port attacks	5	Server management vulnerability	4	60	Implement remote attestation control
Computers	3	Buffer overflow	4	Arbitrary code execution	5	60	Regular patch updates
Computers	3	Insider threats	4	Windows Security Centre API Remote Code Execution Vulnerability	5	60	Patch update of Windows Security Centre API
Computers	3	Spoofing	6	read/write/execute capabilities vulnerability	3	54	Personnel vetting for computer usage
Computers	3	Remote code execution	3	Poorly defined access control list	6	54	Regulated usage of VPNs
Firewall	4	Privilege escalation	6	Unknown function of "Licenseinformation.jsp" vulnerability	2	48	Patch the "Licenseinformation.jsp" vulnerability
Computers	3	Buffer overflow	4	Overwriting function pointers	4	48	Regular patch updates
Computers	3	Control list DoS	4	Misconfiguration of the access control list	4	48	IP reputation protection
Advantage workstation	3	Hacking	3	Stack-based Buffer Overflow	5	45	Upgrade to DICOM Viewer version 2024
Advantage workstation	3	Insider threat	3	Improper Authorisation in Handler for Custom URL Scheme	5	45	Minimise network exposure
Staff and student portal	3	Malware Injection	3	Software vulnerability	5	45	Patch as required
Computers	3	preimage attack	3	MD5 thumbprint certificate vulnerability	5	45	Regular patch updates
Nurse call system	2	sabotage	4	Insecure access protocol	5	40	Access granted to authorised personnel
Asset	Value	Threat	Rating	Vulnerability	Rating	Risks value	Control
Remote energy monitoring	3	Unauthorized access	3	Remote function calling	3	27	Use a virtual private network (VPN), restrict physical access

Switches	2	MAC Address Flooding	3	Inadequate segregation of network traffic	4	24	Coordinated segregation of the network
Switches	2	MAC Address Flooding	3	Outdated firmware	4	24	Regular patch update
Switches	2	MAC Address Flooding	3	Unimplemented port security control	4	24	Close unused ports
Switches	2	Insider threats	4	Incorrect access control list (ACLs)	3	24	Vetted ACLS and proper coordination of access privileges
Switches	2	Insider threats	4	Unchanged default passwords	3	24	Always change default passwords
Switches	2	Insider threats	4	Lack of a log review system	3	24	Proper coordination of access privileges
Firewall	4	Shell injection	3	Susceptibility to SSL VPN console manipulation	2	24	Patch update
Computers	3	Buffer overflow	4	System bugs leading to an infinite loop	2	24	Code vetting
Switches	2	MAC Address Flooding	3	Use of the HTTP protocol	3	18	Use the HTTPS protocol
Switches	2	VLAN Hopping	3	Not utilising virtual local area networks (VLANS)	3	18	Proportionately deploy VLANS
Switches	2	MAC Address Flooding	3	Use of the Telnet protocol	2	12	Use Secure Shell Protocol (SSH)
Switches	2	VLAN Hopping	3	Network segmentation deficiencies	2	12	Coordinated segregation of the network
Intercom server	1	Packet sniffing	3	Unencrypted packets in transit	3	9	End-to-end network encryption
Intercom server	1	SIP (Session Initiation Protocol) spoofing	2	Lack of call session monitoring state	3	6	Implement safeguards such as Session Border Controllers
Intercom server	1	Black Storm Attacks	2	Susceptibility to IP manipulation	3	6	Strict session monitoring standards
Intercom server	1	DDoS Attacks	3	Poor network segmentation and multi-tenant service provision	2	6	Implement services such as content delivery networks
Intercom server	1	Jamming attacks	2	Poorly implemented anti-jamming algorithm	2	4	Implement signal strength monitoring systems, practice good password and encryption hygiene.
Intercom server	1	Vishing attacks	2	Untrained operator staff are susceptible to social engineering manipulation	2	4	Good policy practice and staff training

6. OBSERVATIONS AND DISCUSSIONS

The risk assessment analysis of critical assets using the BUHCRAF model, based on the combination of asset value, threat likelihood, and vulnerability rating, revealed several low to high-risk areas within the Baze University Hospital’s IT infrastructure. Many studies have been conducted in the healthcare sector that expose the susceptibility of the sector to cyberattacks as a whole (Abbou et al., 2024), (Argaw et al., 2019).

However, the knowledge distilled from these studies seems to be fragmented and non-holistic, leading to a sporadic approach to addressing the issues (Ghayoomi et al., 2021), (Guinet, 2017). Therefore, contextualising specific areas of vulnerabilities in BUH cyberinfrastructure will certainly minimise prioritising the wrong risks because they are overrepresented in the literature (Chahid et al., 2021) and tackling cybersecurity problems that may not be necessarily applicable to the BUH facility.

From our risk register, we considered risk values above 250 to be high risks, and electronic medical records (EMR) emerged as some of the most critical assets with the most consistent high-risk scores across multiple threats and vulnerability scenarios. This is also corroborated in the literature, as several works give credence to these findings (McGlade & Scott-Hayward, 2019), (Bhosale et al., 2021), (Shah & Khan, 2020), (Sandhane et al., 2024), (Alhammad et al., 2022), (Yeo & Banfield, 2022).

Notably, ransomware attacks also have a high risk ranking in our risk register with a value of 280. The healthcare sector has been plagued in the past with several iterations of the ransomware attack; therefore, the high-risk placement in our study appears justifiable. Ostensibly, one of the most renowned ransomware attacks that plagued the healthcare sector is the WannaCry ransomware attack that cost the NHS over £92m and is presumed to be one of the most devastating breaches in recent years (Askarifar et al., n.d.), (Mattei, 2017), (“WannaCry Ransomware Attacks Cost the NHS £92m,” 2018).

Another asset categorised as high risk is the website server, which is highly susceptible to threats such as phishing (risk score of 405) and DDoS attacks (risk scores ranging from 240 to 320). This asset is tied to vulnerabilities such as outdated web application components in the case of phishing and server resource insufficiencies in the case of DDoS attacks. The results of this risk ranking are not far-fetched, as there are a plethora of studies that investigated why the healthcare sector is vulnerable to these attacks and measures to take in mitigating this risk category (Priestman et al., 2019), (Wright et al., 2016), (Zhou et al., 2024).

Furthermore, most medical devices (CT scans, ultrasound, and MRI) and firewalls appear to be represented as assets with moderate risks, with values between 100 and 249. A key concern from a practical point of view is where the firewall is situated in the BUH cyber infrastructure. As seen in Fig. 3, a single firewall is used to cater for both the Baze University main site and the BUH permanent site. This should not be encouraged as an ideal practice, given that the Cyberoam CR2500iNG firewall uses a signature-based IDS/IPS with its known limitations. Therefore, configuring the firewall to accommodate both peculiarities of traffic filtering for a modern university and a hospital will be a challenge that will be difficult to overcome without making compromises that will translate into potential exploitable vulnerabilities.

A more ideal implementation of a firewall system in a hospital setting with adequate network segmentation to enhance security is provided in the literature (Liu et al., 2012). This deployment architecture is in stark contrast with what is obtainable in BUH. Many studies have reasonably established that firewalls are important for protecting multiple assets in healthcare organisations (Anwar et al., 2021), (Al-Shaher et al., 2017), (Tyler & Viana, 2021), (Zaki et al., 2021), (Ip et al., 2012) however, implementation nuances should be closely considered according to the context.

We anticipate that when the firewall repositioning is implemented, it will greatly minimise cyber threats to the firewall system and other medical assets that are exposed as a result of the firewall system's positioning. Finally, assets with scores typically below 100, such as switches and the intercom server, were categorised as low-risk. The possible risks of packet sniffing, MAC address flooding, and insufficient network traffic segregation are still worthy of concern, even with their lower risk scores.

The security and operational efficacy of these assets depend on the proper implementation of VLANs, firmware updates, and secure communication protocols. Despite the lower risks involved, research indicates that in a highly interconnected setting like a hospital, neglecting even low-risk vulnerabilities can result in compounded threats.

7. CONCLUSION AND FUTURE PERSPECTIVES

The risk assessment of Baze University Hospital's IT infrastructure using the BUHCRAF model has illuminated several critical areas where cybersecurity measures must be strengthened. The findings underscore the unique vulnerabilities present in healthcare settings, where assets like electronic medical records (EMRs) and website servers are particularly susceptible to high-risk threats such as phishing, ransomware, and DDoS attacks. These risks are not only theoretically significant but are corroborated by numerous studies and real-world incidents, such as the infamous WannaCry ransomware attack, which devastated healthcare systems globally.

This analysis highlights the necessity of adopting a holistic and contextualised approach to cybersecurity in healthcare, moving beyond generalised recommendations to address the specific risks inherent in the hospital's infrastructure. The results emphasise the importance of regular updates, robust access control mechanisms, and the implementation of advanced technical controls like AI-driven threat detection to mitigate the highest risks identified. Furthermore, even assets deemed to be of moderate or low risk should not be neglected, as their vulnerabilities, if left unchecked, can potentially lead to significant security breaches.

In conclusion, by prioritising and addressing the most critical risks, Baze University Hospital can enhance its defences against cyberattacks, safeguarding not only sensitive patient data but also ensuring the continuous and secure operation of its healthcare services. This targeted approach to cybersecurity is crucial in the increasingly digital landscape of modern healthcare, where the stakes of cyber threats continue to rise. Moving forward, future studies will be necessary to validate the framework in other studies/real-world applications and implement it in multiple healthcare settings with similar cyber particulars. Also, an approach such as the BUHCRAF model can benefit from longitudinal studies, which in most instances take a lot of time to monitor and evaluate to articulate the extent of the effectiveness of the solution in concrete terms. Therefore, Baze University Hospital must continue to refine its cybersecurity strategies using regularly updated risk assessment methods alongside other coordinated cybersecurity techniques to ensure the safety of patients in the facility.

REFERENCES

- A, M., Kota, K., Babu, A. S., & S, S. V. (2024). CVE Severity Prediction From Vulnerability Description—A Deep Learning Approach. *Procedia Computer Science*, 235, 3105–3117. <https://doi.org/10.1016/j.procs.2024.04.294>
- Abbou, B., Kessel, B., Ben Natan, M., Gabbay-Benziv, R., Dahan Shriki, D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A., & Dudkiewicz, M. (2024). When all computers shut down: The clinical impact of a major cyber-attack on a general hospital. *Frontiers in Digital Health*, 6. <https://doi.org/10.3389/fdgth.2024.1321485>

- Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy*, 2(4), Article 4. <https://doi.org/10.3390/jcp2040043>
- Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., & Haskell-Dowland, P. (2021). ECU-IoHT: A dataset for analysing cyberattacks in Internet of Health Things. *Ad Hoc Networks*, 122, 102621. <https://doi.org/10.1016/j.adhoc.2021.102621>
- Alazzawi, F. (2021). Assessment of Information Security Risk Management System based on ISOIEC27005 in the Independent High Electoral Commission. *Review of International Geographical Education Online*, 11, 4633–4656. <https://doi.org/10.48047/rigeo.11.05.339>
- Alhammad, A., Yusof, M. Mohd., & Jambari, D. I. (2022). A Review of Cyber Threats to Medical Devices Integration with Electronic Medical Records. *2022 International Conference on Cyber Resilience (ICCR)*, 1–6. <https://doi.org/10.1109/ICCR56254.2022.9995984>
- Al-Shaher, M. A., Hameed, R. T., & Țăpuș, N. (2017). Protect healthcare system based on intelligent techniques. *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*, 0421–0426. <https://doi.org/10.1109/CoDIT.2017.8102628>
- Alshar'e, M. (2023). CYBER SECURITY FRAMEWORK SELECTION: COMPARISON OF NIST AND ISO27001. *Applied Computing Journal*, 245–255. <https://doi.org/10.52098/acj.202364>
- An introduction to buildings cybersecurity framework | IEEE Conference Publication | IEEE Xplore.* (n.d.). Retrieved July 12, 2024, from <https://ieeexplore.ieee.org/abstract/document/8285228>
- Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences*, 11(19), Article 19. <https://doi.org/10.3390/app11199183>
- Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Medical Informatics and Decision Making*, 19(1), 10. <https://doi.org/10.1186/s12911-018-0724-5>
- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1), 146. <https://doi.org/10.1186/s12911-020-01161-7>
- Askarifar, S., Rahman, N. A. A., & Osman, H. (n.d.). *A REVIEW OF LATEST WANNACRY RANSOMWARE: ACTIONS AND PREVENTIONS*. 7.
- Bansal, M., Sirpal, V., Jain, T., Ujjwal, & Nangia, U. (2023). *Cybersecurity challenges in the healthcare domain and the road ahead*. 2796(1). Scopus. <https://doi.org/10.1063/5.0149167>
- BAZE FOCUS MAGAZINE (2022 CONVOCATION EDITION) by Baze University—Issuu.* (n.d.). Retrieved July 9, 2024, from https://issuu.com/bazeuniversity/docs/baze_focus_magazine_2022-_merged/44
- Bhosale, K. S., Nenova, M., & Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. *2021 Sixth Junior Conference on Lighting (Lighting)*, 1–6. <https://doi.org/10.1109/Lighting49406.2021.9598947>
- Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, 131, 104908. <https://doi.org/10.1016/j.ssci.2020.104908>
- Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, 37(5), 1123–1132. <https://doi.org/10.1007/s10877-023-01013-5>

- Chahid, Y., Benabdellah, M., & Kannouf, N. (2021). Smart Hospitals and Cyber Security Attacks. In S. Motahhir & B. Bossoufi (Eds.), *Digital Technologies and Applications* (pp. 291–300). Springer International Publishing. https://doi.org/10.1007/978-3-030-73882-2_27
- Compendium of Risk Management Frameworks with Potential Interoperability. (n.d.). [Report/Study]. ENISA. Retrieved July 11, 2024, from <https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>
- Coppolino, L., D'Antonio, S., Romano, L., Sgaglione, L., Magliulo, M., & Pacelli, R. (2019). Protecting Critical Business Processes of Smart Hospitals from Cyber Attacks. *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, 363–367. <https://doi.org/10.1109/SITIS.2019.00065>
- CVE Website. (n.d.). Retrieved July 26, 2024, from <https://www.cve.org/>
- Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security*, 22(6), 1713–1729. <https://doi.org/10.1007/s10207-023-00713-y>
- Frumento, E. (2019). Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. In G. Andreoni, P. Perego, & E. Frumento (Eds.), *m_Health Current and Future Applications* (pp. 35–69). Springer International Publishing. https://doi.org/10.1007/978-3-030-02182-5_4
- Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *DIGITAL HEALTH*, 7, 20552076211059366. <https://doi.org/10.1177/20552076211059366>
- Guinet, A. (2017). How to Protect a Hospital Against Cyber Attacks. In P. Cappanera, J. Li, A. Matta, E. Sahin, N. J. Vandaele, & F. Visintin (Eds.), *Health Care Systems Engineering* (pp. 3–16). Springer International Publishing. https://doi.org/10.1007/978-3-319-66146-9_1
- Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model | *Journal of Cybersecurity* | Oxford Academic. (n.d.). Retrieved July 12, 2024, from <https://academic.oup.com/cybersecurity/article/6/1/tyaa005/5813544>
- Ip, C. H., Pun, S. H., Vai, M. I., & Mak, P. U. (2012). The Network Security Regime for the Hybrid Connection of Healthcare Entities. *2012 International Conference on Biomedical Engineering and Biotechnology*, 1832–1834. <https://doi.org/10.1109/iCBEB.2012.431>
- ISO - ISO/IEC 27000 family—Information security management. (2022, October 25). ISO. <https://www.iso.org/standard/iso-iec-27000-family>
- ISO 27005 | IT Governance UK. (n.d.). Retrieved July 12, 2024, from <https://itgovernance.co.uk/iso27005>
- Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5), e10059. <https://doi.org/10.2196/10059>
- Jofre, M. (2020). *Holistic View Of Healthcare Cybersecurity Ecosystem*. <https://doi.org/10.5281/zenodo.7999970>
- Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences*, 11(15), Article 15. <https://doi.org/10.3390/app11156699>
- Kendrick, T., & ebrary, I. (with Internet Archive). (2003). *Identifying and managing project risk [electronic resource]: Essential tools for failure-proofing your project*. New York : AMACOM. <http://archive.org/details/identifyingmanag00tomk>
- Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15(7), Article 7. <https://doi.org/10.3390/su15075828>

- Lee, I., & Choi, C. (2023). Camp2Vec: Embedding cyber campaign with ATT&CK framework for attack group analysis. *ICT Express*, 9(6), 1065–1070. <https://doi.org/10.1016/j.icte.2023.05.008>
- Leva, M. C., Balfe, N., McAleer, B., & Rocke, M. (2017). Risk registers: Structuring data collection to develop risk intelligence. *Safety Science*, 100, 143–156. <https://doi.org/10.1016/j.ssci.2017.05.009>
- Liu, C.-H., Chung, Y.-F., Chen, T.-S., & Wang, S.-D. (2012). The Enhancement of Security in Healthcare Information Systems. *Journal of Medical Systems*, 36(3), 1673–1688. <https://doi.org/10.1007/s10916-010-9628-3>
- Lopes, S., Leite, P., Carvalho, S., & Teixeira, P. (2024). Using ITIL as part of the NIST Cybersecurity Framework. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. <https://doi.org/10.1109/ISDFS60797.2024.10527256>
- Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World Neurosurgery*, 104, 972–974. <https://doi.org/10.1016/j.wneu.2017.06.104>
- McGlade, D., & Scott-Hayward, S. (2019). ML-based cyber incident detection for Electronic Medical Record (EMR) systems. *Smart Health*, 12, 3–23. <https://doi.org/10.1016/j.smhl.2018.05.001>
- Mejias, R. J., Shepherd, M. A., Fronmueller, M., & Huff, R. A. (n.d.). *Using Threat Vulnerability Asset (TVA) Methodology to Identify Cyber Threats and System Vulnerabilities: A Student Field Project Case Study*.
- Meriah, I., & Arfa Rabai, L. B. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, 160, 85–92. <https://doi.org/10.1016/j.procs.2019.09.447>
- MITRE ATT&CK®. (n.d.). Retrieved June 23, 2023, from <https://attack.mitre.org/>
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.04162018>
- Parmar, M., & Miles, D. A. (n.d.). *Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2.0 and EU Standards*.
- Patterson, F. D., & Neailey, K. (2002). A Risk Register Database System to aid the management of project risk. *International Journal of Project Management*, 20(5), 365–374. [https://doi.org/10.1016/S0263-7863\(01\)00040-0](https://doi.org/10.1016/S0263-7863(01)00040-0)
- (PDF) CYBER SECURITY AND ITS IMPORTANCE. (n.d.). Retrieved July 4, 2024, from https://www.researchgate.net/publication/347439655_CYBER_SECURITY_AND_ITS_IMPORTANCE
- Predicting Vulnerability Type in Common Vulnerabilities and Exposures (CVE) Database with Machine Learning Classifiers | IEEE Conference Publication | IEEE Xplore*. (n.d.). Retrieved July 26, 2024, from <https://ieeexplore.ieee.org/abstract/document/9513723>
- Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, 26(1), e100031. <https://doi.org/10.1136/bmjhci-2019-100031>
- Sandhane, R., Patil, K., & Sharma, A. R. (2024). Cyber Security Risk Assessment for Electronic Medical Records (EMRs). *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 1–6. <https://doi.org/10.1109/ICIPTM59628.2024.10563486>

- Shah, S. M., & Khan, R. A. (2020). Secondary Use of Electronic Health Record: Opportunities and Challenges. *IEEE Access*, 8, 136947–136965. IEEE Access. <https://doi.org/10.1109/ACCESS.2020.3011099>
- Sun, H., Shu, H., Kang, F., Zhao, Y., & Huang, Y. (2024). Malware2ATT&CK: A sophisticated model for mapping malware to ATT&CK techniques. *Computers & Security*, 140, 103772. <https://doi.org/10.1016/j.cose.2024.103772>
- The need for cybersecurity self-evaluation in healthcare | BMC Medical Informatics and Decision Making.* (n.d.). Retrieved July 12, 2024, from <https://link.springer.com/article/10.1186/s12911-024-02551-x>
- Toussaint, M., Krifa, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 39, 100604. <https://doi.org/10.1016/j.jii.2024.100604>
- Tyler, D., & Viana, T. (2021). Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture. *Applied Sciences*, 11(16), Article 16. <https://doi.org/10.3390/app11167499>
- Wang, W., Sadjadi, S. M., & Rische, N. (2024). A Survey of Major Cybersecurity Compliance Frameworks. *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)*, 23–34. <https://doi.org/10.1109/BigDataSecurity62737.2024.00013>
- WannaCry ransomware attacks cost the NHS £92m. (2018). *Computer Fraud & Security*, 2018(11), 1–3. [https://doi.org/10.1016/S1361-3723\(18\)30102-7](https://doi.org/10.1016/S1361-3723(18)30102-7)
- Whitman, M. E., & Mattord, H. J. (2014). *Management of information security* (Fourth edition). Cengage Learning.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (Sixth Edition). Cengage Learning.
- Williams, T. M. (1994). Using a risk register to integrate risk management in project definition. *International Journal of Project Management*, 12(1), 17–22. [https://doi.org/10.1016/0263-7863\(94\)90005-1](https://doi.org/10.1016/0263-7863(94)90005-1)
- Wright, A., Aaron, S., & Bates, D. W. (2016). The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *Journal of General Internal Medicine*, 31(10), 1115–1118. <https://doi.org/10.1007/s11606-016-3741-z>
- Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, 19(Spring), 1i.
- Zaki, M., Sivakumar, V., Shrivastava, S., & Gaurav, K. (2021). Cybersecurity Framework For Healthcare Industry Using NGFW. *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 196–200. <https://doi.org/10.1109/ICICV50876.2021.9388455>
- Zhou, Z., Gaurav, A., Gupta, B. B., Hamdi, H., & Nedjah, N. (2024). A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic. *Neural Computing and Applications*, 36(1), 1–14. <https://doi.org/10.1007/s00521-021-06389-6>