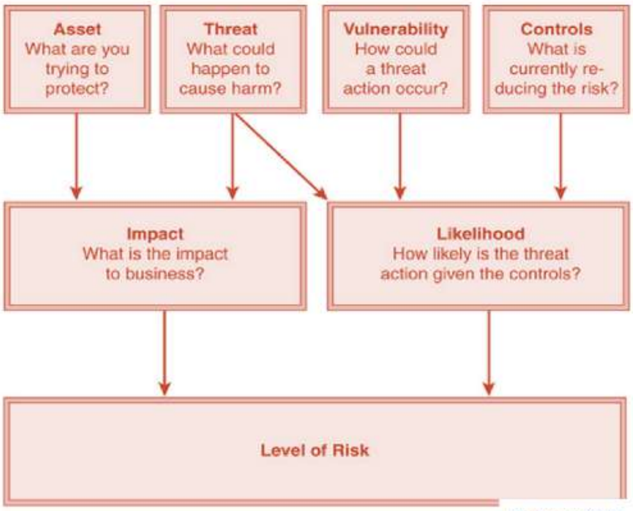
RISK ASSESSMENT OF MARY SEACOLE HOSPITAL

The main purpose of the risk assessment is to allow the hospital administration to evaluate a suitable budget for security and that budget should cover security controls to enhance the level of protection. This goal is reached by delivering an estimative of the assumed cost of security breaches joined with a valuation of the possibilities of those breaches.

NIST Cybersecurity Framework(CSF) highlights the first step of a risk assessment is the recognition of at risk assets. Vulnerability management methods can be used to determine the potential threats. The priority of responding to risks it is determined by the asset's value to the hospital and its exposure to risk. The findings, along with an evaluation of risks levels and benefits, consequences and financial implications will determine the incident's impact on the organisation. An assessment of risk impact on CIA (Confidentiality, Availability and Integrity of information) should be put in place using ISO 27005 or NIST CSF frameworks. (Stallings,2019)

Fig 4 Determining Information Security Risk

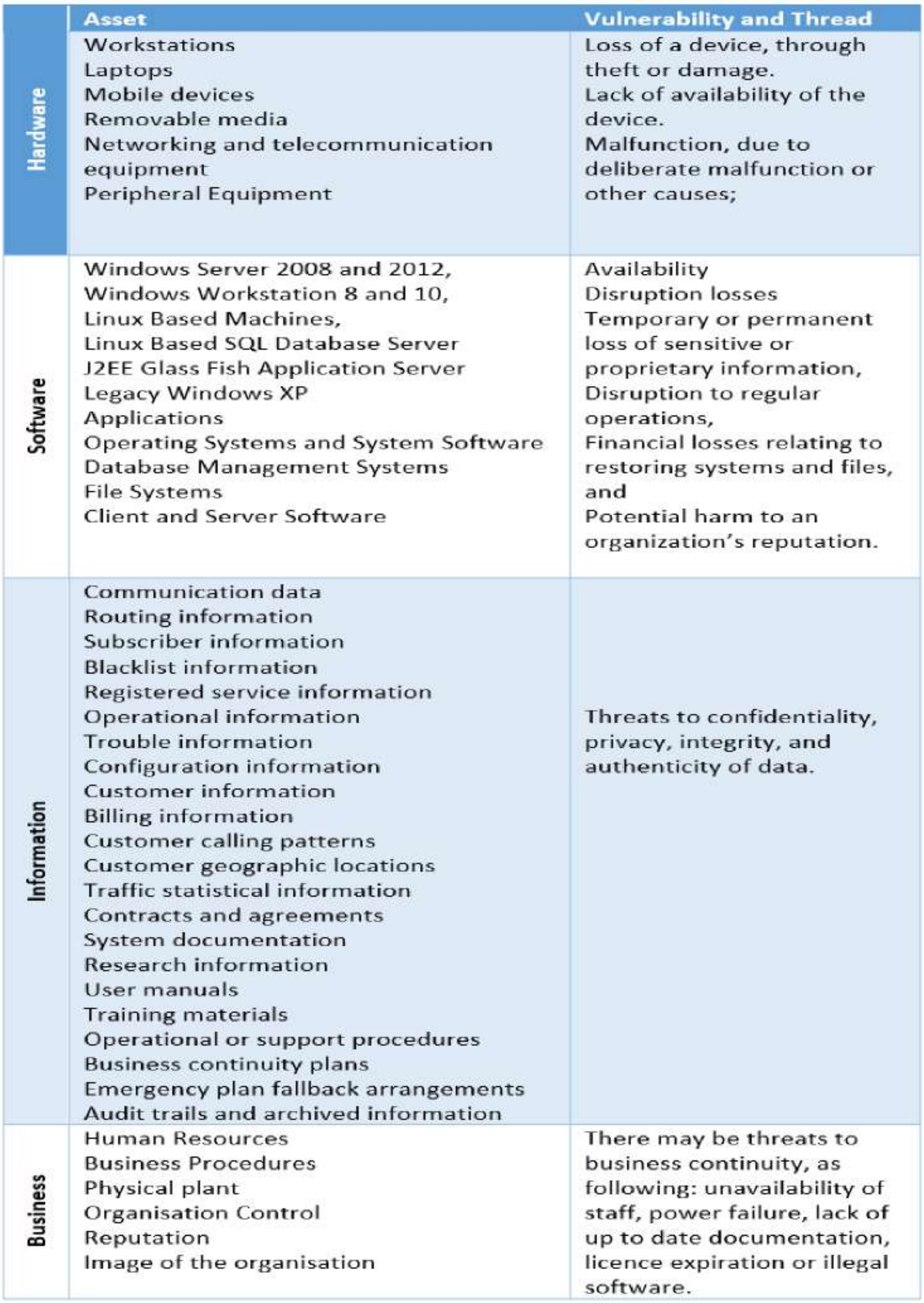

Asset
What are you trying to protect?
Threat
What could happen to cause harm?
Vulnerability
How could a threat action occur?
Controls
What is currently reducing the risk?
Impact
What is the impact to business?
Likelihood
How likely is the threat action given the controls?
Level of Risk

Stallings,2019

ASSET IDENTIFICATION

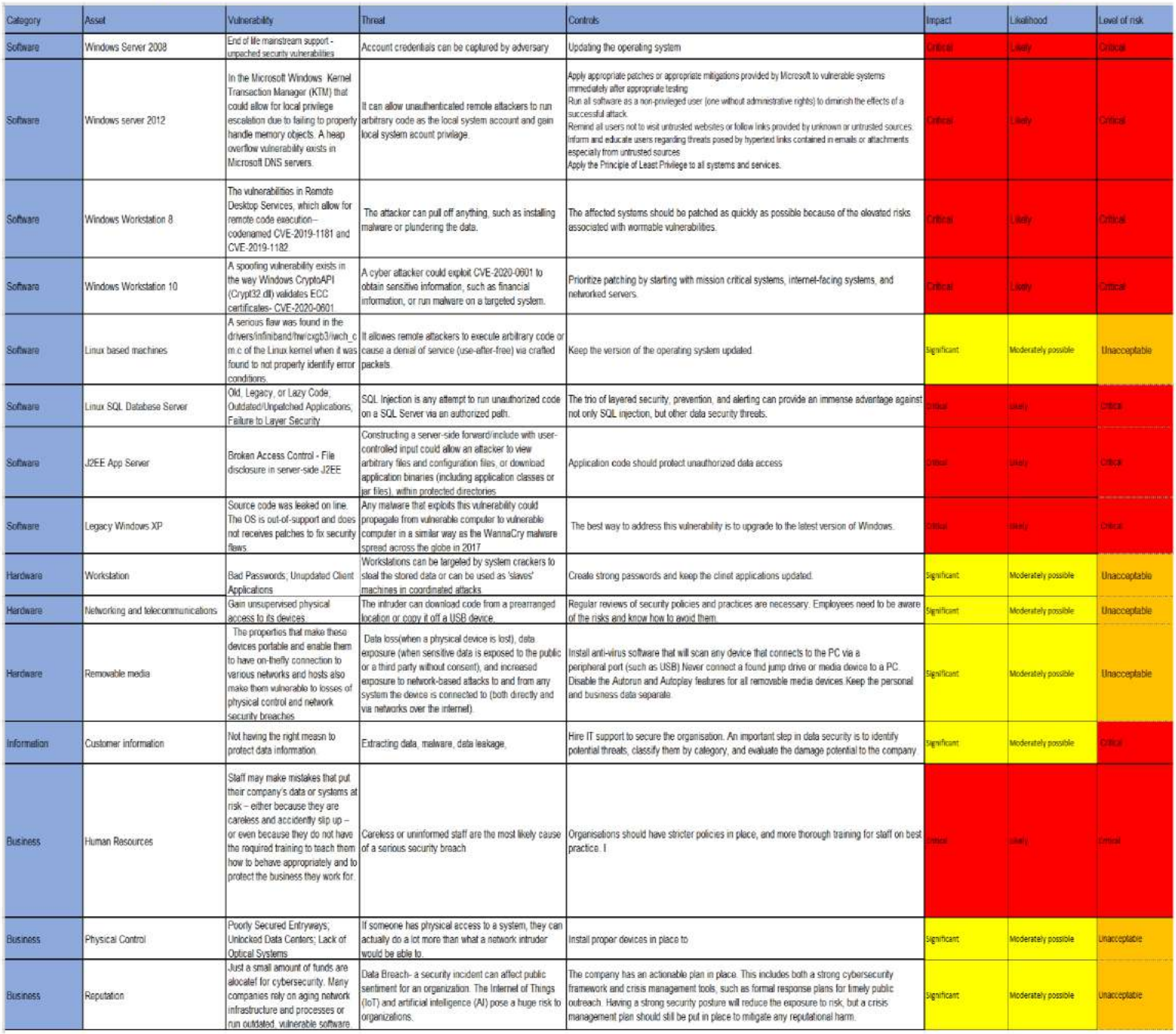
An organisation's assets are defined as anything of value to the organisation that needs to be safeguarded. Mary Seacole Hospital Assets include hardware, software, information and business assets.

Mary Seacole Hospital Assets in concordance with ITU-T X.1055(cited by Stallings, 2019)

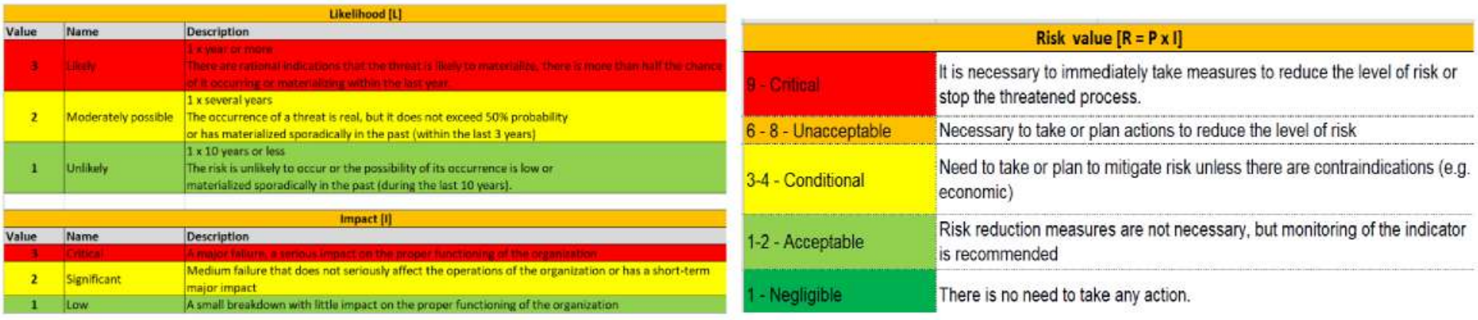


	Asset	Vulnerability and Thread
Hardware	Workstations Laptops Mobile devices Removable media Networking and telecommunication equipment Peripheral Equipment	Loss of a device, through theft or damage. Lack of availability of the device. Malfunction, due to deliberate malfunction or other causes;
Software	Windows Server 2008 and 2012, Windows Workstation 8 and 10, Linux Based Machines, Linux Based SQL Database Server J2EE Glass Fish Application Server Legacy Windows XP Applications Operating Systems and System Software Database Management Systems File Systems Client and Server Software	Availability Disruption losses Temporary or permanent loss of sensitive or proprietary information, Disruption to regular operations, Financial losses relating to restoring systems and files, and Potential harm to an organization's reputation.
Information	Communication data Routing information Subscriber information Blacklist information Registered service information Operational information Trouble information Configuration information Customer information Billing information Customer calling patterns Customer geographic locations Traffic statistical information Contracts and agreements System documentation Research information User manuals Training materials Operational or support procedures Business continuity plans Emergency plan fallback arrangements Audit trails and archived information	Threats to confidentiality, privacy, integrity, and authenticity of data.
Business	Human Resources Business Procedures Physical plant Organisation Control Reputation Image of the organisation	There may be threats to business continuity, as following: unavailability of staff, power failure, lack of up to date documentation, licence expiration or illegal software.

RISK REGISTER



Category	Asset	Vulnerability	Threat	Controls	Impact	Likelihood	Level of risk
Software	Windows Server 2008	End of life mainstream support - unpached security vulnerabilities	Account credentials can be captured by adversary	Updating the operating system	Critical	Likely	Critical
Software	Windows server 2012	In the Microsoft Windows Kernel Transaction Manager (KTM) that could allow for local privilege escalation due to failing to properly handle memory objects. A heap overflow vulnerability exists in Microsoft DNS servers.	It can allow unauthenticated remote attackers to run arbitrary code as the local system account and gain local system acount privilage.	Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources Apply the Principle of Least Privilege to all systems and services.	Critical	Likely	Critical
Software	Windows Workstation 8	The vulnerabilities in Remote Desktop Services, which allow for remote code execution–codenamed CVE-2019-1181 and CVE-2019-1182	The attacker can pull off anything, such as installing malware or plundering the data.	The affected systems should be patched as quickly as possible because of the elevated risks associated with wormable vulnerabilities.	Critical	Likely	Critical
Software	Windows Workstation 10	A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates ECC certificates- CVE-2020-0601	A cyber attacker could exploit CVE-2020-0601 to obtain sensitive information, such as financial information, or run malware on a targeted system.	Prioritize patching by starting with mission critical systems, internet-facing systems, and networked servers.	Critical	Likely	Critical
Software	Linux based machines	A serious flaw was found in the drivers/infiniband/hw/cxgb3/iwch_cm.c of the Linux kernel when it was found to not properly identify error conditions.	It allowes remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted packets.	Keep the version of the operating system updated.	Significant	Moderately possible	Unacceptable
Software	Linux SQL Database Server	Old, Legacy, or Lazy Code; Outdated/Unpatched Applications; Failure to Layer Security	SQL Injection is any attempt to run unauthorized code on a SQL Server via an authorized path.	The trio of layered security, prevention, and alerting can provide an immense advantage against not only SQL injection, but other data security threats.	Critical	Likely	Critical
Software	J2EE App Server	Broken Access Control - File disclosure in server-side J2EE	Constructing a server-side forward/include with user-controlled input could allow an attacker to view arbitrary files and configuration files, or download application binaries (including application classes or jar files), within protected directories	Application code should protect unauthorized data access	Critical	Likely	Critical
Software	Legacy Windows XP	Source code was leaked on line. The OS is out-of-support and does not receives patches to fix security flaws.	Any malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017	The best way to address this vulnerability is to upgrade to the latest version of Windows.	Critical	Likely	Critical
Hardware	Workstation	Bad Passwords; Unupdated Client Applications	Workstations can be targeted by system crackers to steal the stored data or can be used as 'slaves' machines in coordinated attacks	Create strong passwords and keep the clinet applications updated.	Significant	Moderately possible	Unacceptable
Hardware	Networking and telecommunications	Gain unsupervised physical access to its devices.	The intruder can download code from a prearranged location or copy it off a USB device.	Regular reviews of security policies and practices are necessary. Employees need to be aware of the risks and know how to avoid them.	Significant	Moderately possible	Unacceptable
Hardware	Removable media	The properties that make these devices portable and enable them to have on-thefly connection to various networks and hosts also make them vulnerable to losses of physical control and network security breaches	Data loss(when a physical device is lost), data exposure (when sensitive data is exposed to the public or a third party without consent), and increased exposure to network-based attacks to and from any system the device is connected to (both directly and via networks over the internet).	Install anti-virus software that will scan any device that connects to the PC via a peripheral port (such as USB) Never connect a found jump drive or media device to a PC. Disable the Autorun and Autoplay features for all removable media devices Keep the personal and business data separate.	Significant	Moderately possible	Unacceptable
Information	Customer information	Not having the right measn to protect data information.	Extracting data, malware, data leakage,	Hire IT support to secure the organisation. An important step in data security is to identify potential threats, classify them by category, and evaluate the damage potential to the company.	Significant	Moderately possible	Critical
Business	Human Resources	Staff may make mistakes that put their company's data or systems at risk – either because they are careless and accidently slip up – or even because they do not have the required training to teach them how to behave appropriately and to protect the business they work for.	Careless or uninformed staff are the most likely cause of a serious security breach	Organisations should have stricter policies in place, and more thorough training for staff on best practice. I	Critical	Likely	Critical
Business	Physical Control	Poorly Secured Entryways; Unlocked Data Centers; Lack of Optical Systems	If someone has physical access to a system, they can actually do a lot more than what a network intruder would be able to.	Install proper devices in place to	Significant	Moderately possible	Unacceptable
Business	Reputation	Just a small amount of funds are alocatef for cybersecurity. Many companies rely on aging network infrastructure and processes or run outdated, vulnerable software.	Data Breach- a security incident can affect public sentiment for an organization. The Internet of Things (IoT) and artificial intelligence (AI) pose a huge risk to organizations.	The company has an actionable plan in place. This includes both a strong cybersecurity framework and crisis management tools, such as formal response plans for timely public outreach. Having a strong security posture will reduce the exposure to risk, but a crisis management plan should still be put in place to mitigate any reputational harm.	Significant	Moderately possible	Unacceptable



Likelihood [L]		
Value	Name	Description
3	Likely	1 x year or more There are rational indications that the threat is likely to materialize, there is more than half the chance of it occurring or materializing within the last year.
2	Moderately possible	1 x several years The occurrence of a threat is real, but it does not exceed 50% probability or has materialized sporadically in the past (within the last 3 years)
1	Unlikely	1 x 10 years or less The risk is unlikely to occur or the possibility of its occurrence is low or materialized sporadically in the past (during the last 10 years).

Impact [I]		
Value	Name	Description
3	Critical	A major failure, a serious impact on the proper functioning of the organization
2	Significant	Medium failure that does not seriously affect the operations of the organization or has a short-term major impact
1	Low	A small breakdown with little impact on the proper functioning of the organization

Risk value [R = P x I]	
9 - Critical	It is necessary to immediately take measures to reduce the level of risk or stop the threatened process.
6 - 8 - Unacceptable	Necessary to take or plan actions to reduce the level of risk
3-4 - Conditional	Need to take or plan to mitigate risk unless there are contraindications (e.g. economic)
1-2 - Acceptable	Risk reduction measures are not necessary, but monitoring of the indicator is recommended
1 - Negligible	There is no need to take any action.

(Source: CULondon,2021)

VULNERABILITIES AND THREATS IDENTIFICATION

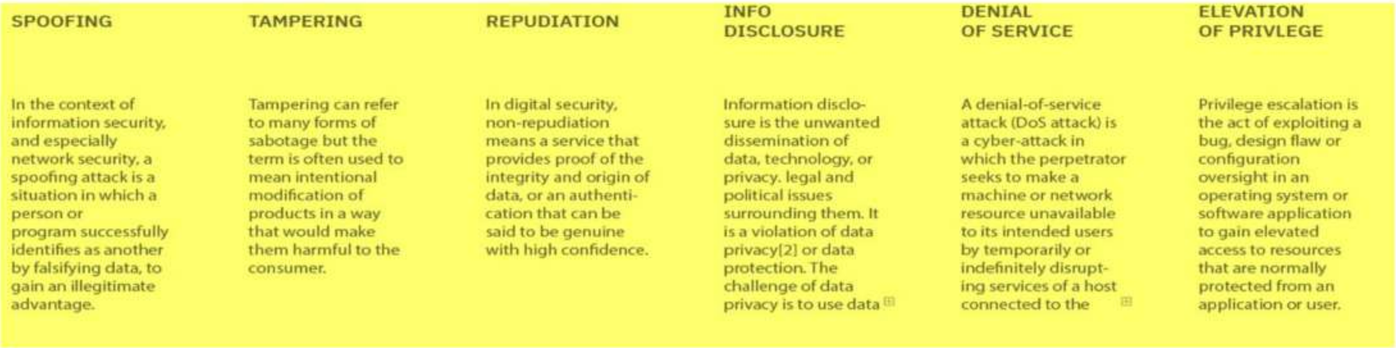
Anything that can damage an organisations asset are categorized as threats. Mary Seacole Hospital Administration has to deal with three types of threats: environmental (natural disasters or power failures), business resources (equipment breakdown, supply chain interruption or accidentally harm produced by employees) and hostile actors (hackers, insider-threats, villains or nation state actors).(Stellings,2019)

Mary Seacole Hospital deals with patient sensitive data as personal information, health information and financial information. IBM Report (2016) states that the cybersecurity attacks and data breaches in the health care system are escalating since 2010, making health care system one of the most targeted system by cyber-attacks. (Martin &all,2017). The privacy of the patients cannot be restored or undo the psychological harm when private data is breached. Cyberattacks can be responsible not only for stealing patient's identity and financial information, but also can obstruct Mary Seacom Hospital's Operations and be a danger for the health of patients.

Mary Seacole Hospital handles both PII (Personally identifiable information) and PHI (Protected Health Information). Both PII and PHI must use regulatory frameworks in concordance with GDPR (General Data Protection Regulation) and ISO 27001.

To handle threats Mary Seacole Hospital can use a threat classification system, STRIDE Threat Model to classify attacks that occur on purpose. (Hernan &all, cited by stallings,2019)

Fig 5. STRIDE Threat Model



SPOOFING	TAMPERING	REPUDIATION	INFO DISCLOSURE	DENIAL OF SERVICE	ELEVATION OF PRIVLEGE
In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.	Tampering can refer to many forms of sabotage but the term is often used to mean intentional modification of products in a way that would make them harmful to the consumer.	In digital security, non-repudiation means a service that provides proof of the integrity and origin of data, or an authentication that can be said to be genuine with high confidence.	Information disclosure is the unwanted dissemination of data, technology, or privacy. legal and political issues surrounding them. It is a violation of data privacy[2] or data protection. The challenge of data privacy is to use data	A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the	Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

(Source: McConville,2020)

Threat types classification and controls are discussed in *Appendix 1* and *Appendix 2.*

Thread identification and surveys are available to inform as following: Verizon Data Breach Investigations Report, annual Threat Horizon Report from ISF, ENISA Threat Landscape Report, Trustwave Global Security Report, CISCO Annual Security Report, Fortinet Threat Landscape Report.

Mary Seacole Hospital should follow ISO 27005 to categorize current and scheduled security controls.

Vulnerability identification is the procedure of acknowledging vulnerabilities that can be manipulated by threats to produce damage to assets. Vulnerability is defined as a fault or a limitation in a system security design, procedures, implementation or internal controls that that could be manipulated intentionally or not, when a threat is present. Vulnerabilities can be documented from NIST National Vulnerability Database (Stallings,2019). *Appendix 3* presents a list of vulnerabilities found in an organisation.

CYBERSECURITY RECOMMENDATIONS FOR MARY SEACOLE HOSPITAL

The hospital can offer high health care services if it's IT Infrastructure (any resource or service employed to carry and support IT services) is in a good state. ISO 27002 requirement for the IT infrastructure are as following:

- Configuration management- keep update inventory of assets
- Change management- holds the changings in a regulated method
- Logging and monitoring in place- responsible with quick recognition of an attack and obtaining details about it. (CIS,2016)

Mary Seacole Hospital should use a preventive approach to cyberattacks by allocating resources and budget to ensure a good maintenance of IT infrastructure and value cybersecurity as an indispensable asset. (Tanev &all , 2015)

Risk to an organisation will always persist. Mary Seacole Hospital should be aware of the presence of risk even with owning proper IT infrastructure and practices, on top of information security measures. The organisation should also adopt a risk based approach through a well known framework recognised by National Institute of Standards and Technology (NIST) or European Union Agency for Network and Information Security (ENISA).

Mary Seacole Hospital should take in consideration the ENISA's Security and Resilience in eHealth (2015) to provide cybersecurity training among all systems users (CIS,2016). End users should be aware of the risk they can trigger through involuntary actions. They should be conscious that loading data on personal devices can present a privacy and information integrity risk, while the usage of removable storage devices can growth the risk of malware execution. System users should be informed of the actual threats in online environment(ISO 27005 definitions presented in Appendix 4), how the threats can impact the system and how an attack can began. Social engineering attack focus on system users, so they should be trained on how to deal with unrecognized emails and phishing tactics, setting strong passwords and not accessing unknown links. (CIS, 2016)

In dealing with vulnerabilities Mary Seacole Hospital should use Endpoint Detection and Response(EDR) solution. Vulnerability management is composed of identification, evaluation and mitigation of systems vulnerabilities. An important step in dealing with vulnerabilities management is patch management and Mary Seacole hospital should be aware of the implications: the sensitivity of data stored on serves, the indispensable functions of the hospital that needs to run continuously. To reduce exposure the hospital should run penetration testing on their system.

Mary Seacole hospital should grant third party provider privilege accounts in a supervised and limiting way in order to decrease the risk of attack. These accounts should be recorded and checked for abnormal use. Their log entries should be also evaluated. Malicious insider threat can be prevented by applying local password policy end re-examine the criteria for privileged access. CIS(2016) advise the usage of multi factorial verification for administrative and privileged users with smart cards, one time passwords, or biometrics.

Marry Seacole hospital should have a cyber security leader and a nominated team where the roles and responsibilities are well known within the team. An incident response plan should be in place including post incident steps (password resetting, factory resetting or substitute affected hardware or software)

Mary Seacole Hospital shares information with other institutions and should be aware of the implication. The hospital should be part of National Health Information Sharing and Analysis Centre (NH-ISAC) , a globally non profit organisation which facilitate cooperation and information exchange between health care providers. (NIS,2016). The issues of data-sharing and data-processing can be approached through the application of advanced cryptographic methods (homomorphic encryption) , trusted hardware and SMPC(secure multiparty computation). (Kokoris,2019)

The information security department of Mary Seacole Hospital should prevent social engineering methods by checking and emails of suspicious URL, White-listing reliable applications and web-sites and block suspicious JAVA code.