Research Summary

Malware:

- Malware is commonly associated with an intentionally created program that has the potential of causing harm to a network system in case it infects computers, stealing data or controlling other applications on the device. These include computer viruses, worms, Trojans, spyware, and adware. Malware also steals data, messes with systems, and overall a slow running machine.
- Trojans: A Trojan Horse is a sort of malware that masquerades as legitimate software in order to deceive users into installing it. Once triggered, it can conduct a variety of nefarious acts, such as stealing sensitive data, granting illegal access to a system, or allowing attackers to operate the machine remotely.
- Viruses: Viruses are harmful programs that attach themselves to normal files or applications in order to proliferate and spread. They can corrupt, change, or delete data once launched, and in some situations, replicate over a network or system, inflicting significant damage.
- Spyware: Spyware is software that is placed on a device without the user's permission in order to collect information about the user's online activity, browsing patterns, or personal information. It frequently acts invisibly, sending acquired data to third parties without the user's knowledge.

Ransomware:

- Another kind of malware – ransomware that makes it impossible to use a PC, including the information stored on it, unless you will pay. In this case, it denies people’s right to access information through encryption of files and locking users’ accounts. Perpetrators most of the time instruct on paying for an encryption key and gaining back access to the system.
- WannaCry: WannaCry was a 2017 global ransomware attack that exploited a Windows vulnerability, encrypting data on infected computers and demanding Bitcoin ransom payments for decryption, affecting over 200,000 systems in 150 countries and causing widespread disruption in industries such as healthcare and telecommunications.
- Petya: Petya was a ransomware strain that first appeared in 2016 and has since resurfaced in various variants, encrypting the master boot record (MBR) of infected computers, rendering them inoperable, and demanding Bitcoin ransom payments for decryption, targeting both individual users and large organizations globally, causing significant disruptions to various sectors and industries.

Hospital Security:

- Healthcare professionals may have limited awareness of certain threats within a system. The rise of cyber violence has become more prominent and rampant in recent years, especially in high income countries such as the US, Norway and even some lower-middle income countries such as Kenya. Healthcare was among the top three sectors most affected by ransomware worldwide.

- Cyberattacks include a variety of threats: brute force and Denial-of-Service attacks to the use of phishing and malware or social engineering methods to compromise security.
- The US Department of Justice revealed that an average of 4000 ransomware attacks occurred daily across different sectors in 2016—a 300% increase since 2015.
- Healthcare staff IT training focused on ‘functional’ features of the software and applications. There is increased emphasis on ‘cyber hygiene’ and information governance issues through mandatory training which has raised the understanding of these risks.
- Around 2%–3% of the large volume of emails and internet traffic to an NHS Healthcare Organisation are considered suspicious, emphasizing the need for robust firewalls, cyber security infrastructure and IT policies and staff training.
- Phishing scams are one of the largest risks as they are usually targeted towards specific individuals. Many phishing emails are linked to malicious websites and their files, firewalls, act as one layer that can be used to block access to these sites and files.Phishing resulted in more breaches than malware and unpatched systems combined (48% vs 41%), especially true of staff who maybe using personal devices for remote working.
- People that work in healthcare must be careful with what they share online as things like uniforms or identification badges can be copied and used. More vulnerable users are less likely to practice cautious regarding links and attachments and are less able to distinguish phishing from legitimate emails.
- General approaches to reduce risk should include both technical and behavioral tactics. Employees should be encouraged to question the authenticity of any email that deviates from their standard work. They should carefully consider the sender and context and if in doubt do not open and seek the advice of the organizational security team.
- Healthcare cybersecurity focuses on preventing attacks by defending systems from unauthorized access, use, and disclosure of patient data. The primary aim is to ensure the availability, confidentiality, and integrity of critical patient data, which, if compromised, could put patient lives at risk.
- The healthcare sector, which was already stretched and stressed by the pandemic, continued to be heavily targeted in 2020 with at least 560 facilities being impacted in 80 separate incidents (an attack on a health system can impact multiple facilities).

Hospital Systems:

- Electronic patient record (ERP) systems are being more widely used as healthcare organizations are becoming more digitized. The move to widespread comprehensive ERP systems and digital storage of novel information types, such as genome screening and drug prescribing information, increased the potential value of health data and also increased the likelihood of sophisticated methods of gaining access. Hospitals are becoming increasingly dependent on their hospital systems for administrative, financial, and medical operations – with the use of connected medical devices. Cloud storage services, and network systems simultaneously rising.

- Digital technologies make it easier and more efficient to deliver patient care and provide better outcomes. But the rise of digital technologies and the growing interconnectedness between healthcare systems come with increasing healthcare cybersecurity threats.
- IT and digitization have also empowered patients to make better decisions about their care, as patients have greater access to information about their health through EHRs and patient portals.
- Healthcare systems include EHRs (electronic health records), health tracking devices, medical equipment, and software used for healthcare delivery and management. The systems focus on preventing attacks by defending systems from unauthorized access, use, and disclosure of patient data. Component of health informatics that focus largely on the administrative, financial, and clinical needs of hospitals.

Vulnerabilities:

- The healthcare sector is especially vulnerable to attacks because the nature of the work makes it extremely sensitive to any disruption in its services. A delay in hospital operations—much less a halt—can have devastating consequences on patient safety.
- Ransomware attack on Hollywood Presbyterian Medical Center in Los Angeles caused cancellations of procedures and redirection of in-coming ambulances over the span of 10 days.
- These risks heighten risks to patient safety as providers will lose access to virtual records of comorbidities, allergies, and existing prescriptions.
- Cybercriminals' goals can vary from terrorism, fraud, or selling data for financial or personal gain.
- Outsider theft: Hackers from outside that penetrate patient and medical systems to steal and collect data mainly for financial gain. Local actors tend to exploit vulnerabilities and remote actors will often
- target digital infrastructure
- Insider misuse: Often from curiosity and convenience. Unintentional actions include human error, including mistyping information into EHRs or clicking on a phishing email, make up the rest of insider misuse cases. Deliberate acts such as unauthorized access or accidental acts like unintentional data leaks, require an insider approach.

Prevention:

- Organizational IT departments can disable functionality that is not required in an employee's daily work, such as Office macros and Windows PowerShell, and run appropriate firewalls with blocked lists of known phishing sites with email spam filters using machine learning approaches.

Steps taken to prevent issues
-Personal:

- The weakest link in security are the people working there. They are the most likely the leak information or click on something that they should not have. Worst of all, most of them will want to stay quiet about any potential problems they fear they have caused.

The best way around this is to ensure that the general public is well informed and will have the ability to respond quickly and appropriately. After all, you do not want users reporting every little problem that is not an actual threat and causing issues on the technical side.

- Practice phishing emails do wonders in determining who is a potential risk. By playing the role of the villain, the cybersecurity team can focus on people who actually fall victim to scams. It eliminates those who are doing the right thing and ensures that they are able to spend more time and attention on those who are having issues.
- Authorizations are crucial. Having every account be an admin account and have full access to everything would enable chaos when one account gets breached. Segmentation is of the utmost importance in these organizations as it is easy to separate pulmonary from oncology and so on.
- Multi factor authorization is a simple but effective tool used in ensuring that everyone logging in is who they say they are. Its power lies in its simplicity. By verifying the phone or device that is used by a person and allowing that to be a second confirmation as well as a password makes it much harder for people to just brute force a password and get in.

Network:

- Multiple networks is another form of segmentation that strengthens the defenses of any network. Having computers, printers, and equipment all on the same network would be a security nightmare. Another situation where one going down or being compromised by malware would bring everything to a standstill. In a multiple network situation, even if no one can log into their computer their equipment can continue to capture data and work properly. This is crucial as these might be life saving machines keeping patients heart beating.
- Backups are also another massive part of the prevention of malware and ransomware. If the virus deletes any information or encrypts it to hold it hostage, the file is not lost and the infiltrators have no leverage.
- As threats grow more mischievous and clever, so do the measures used to prevent them. Hospitals are commonly targeted as they contain information that is valuable so there is always a need for their employees to be trained on the latest technology. Many antivirus companies work in partnership with hospitals as it allows them to test their products against the worst of the worst.

Hardware:

- Encryption means that if the files are copied over and someone with malicious intent wants to view them, they are unable to do so without the use of a future computer. This ensures that hospitals do not need to worry about potential lawsuits about patient information leaking or getting stolen which is also crucial.
- Windows updates may sound like a boring solution to a complex problem, however, they are usually filled with patches to exploits used by viruses to breach the computers. These are cost effective methods to reduce the likelihood of malware.
- Running daily scans of anti virus software ensures that if there is a threat on the computers it is quickly identified and dealt with. Many of these softwares are able to deal with the issue immediately but will also reach out to hospital staff to alert them of the

issue and if any action is needed on their end.

References:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7062337/
https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-018-0724-5
https://usa.kaspersky.com/resource-center/threats/ransomware-attacks-and-types
https://online.maryville.edu/blog/healthcare-cybersecurity/
https://www.emsisoft.com/en/blog/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/
https://www.talkinghealthtech.com/glossary/hospital-information-systems-his
https://www.digitalguardian.com/blog/20-information-security-tips-hospitals
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2655907/
https://www.ivanti.com/blog/securing-iomt-devices-best-practices-for-hospitals-to-prevent-cyberattacks
https://www.techtarget.com/searchsecurity/definition/malware
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
https://www.sailpoint.com/identity-library/malware-examples/