International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 4, Jul-Aug 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Healthcare Cybersecurity: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Healthcare cybersecurity is a strategic imperative for any organization in the medical industry such as from healthcare providers to insurers to pharmaceutical, biotechnology and medical device companies. This has to do with a lot of measures to protect organizations from external and internal cyber attacks and ensure the available of medical services, proper operation of medical systems and equipment, preservation of confidentiality and integrity of patient data and compliance with industry laws and regulations. The three goals of cybersecurity are: protecting the confidentiality, integrity and availability information, also known as the "CIA triad." The paper attempts to look at the benefits, challenges, and the future prospects of healthcare cybersecurity.

KEYWORDS: *Healthcare cybersecurity, cyber attacks, Internet of Medical Things (IoMT), phishing*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Healthcare Cybersecurity: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-4, August 2024, pp.1042-1051, URL: www.ijtsrd.com/papers/ijtsrd68277.pdf

IJTSRD68277

INTRODUCTION

The rapid and widespread adoption of digital technologies by the healthcare industry is transforming care delivery, which also creates a number of new and potentially damaging cyberthreats that threaten to impact organizations' activities and putting patients at risk. Therefore, cybersecurity is now a critical and integral part of the healthcare industry by safeguarding sensitive patient data, ensuring that all healthcare operations are resilient, protected, and available, as shown in Figure 1 [1]. The Internet of Medical Things (IoMT) security is the combined cybersecurity defense mechanisms and strategy that protect against cyberattacks targeting connected medical devices, sometimes referred to as medical IoT Security [2].

HISTORY OF CYBERATTACK / CYBERSECURITY

The first cyberattack technically occurred in France in 1834, when two thieves stole financial market information by hacking the French Telegraph System. Over the years, other "hackers" emerged who disrupted phone services and wireless telegraphy, but it wasn't until 1940 that thing got really interesting. In 1940, Rene Carmille became the first ethical hacker, who used his machine to hack information processed by the machines used by France's Vichy government to track down the Jews by the Nazis and disrupted their efforts.

In 1962, the first computer passwords set up by MIT to limit students' time on the computers and provide privacy for their computer use was infiltrated by Allan Scherr, an MIT student, through the use of a punch card that triggered the computer to print all the passwords in the system. He then used them to get more computer time and also gave them to his friends. They also hacked into their teacher's account and trolled them by leaving taunting messages.

In 1969 at the University of Washington Computer Center the first computer virus was said to be used by an unnamed person who installed a program that came to be known as "RABBITS Virus" on one of the computers. The program replicated itself until it overwhelmed the computer causing it to shut down.

Kevin Mitnick is often referred to as the first cybercriminal. From 1970 until 1995, Mitnick managed to access some of the most guarded and secure networks in the world, including Motorola and Nokia via use of complex social engineering schemes to trick key personnel to provide him with passwords and codes which he used to penetrate the internal computer systems. He was arrested by the FBI and faced a number of charges. After prison, Mitnick became a cybersecurity consultant and author.

The history of cybersecurity is said to have started in 1971 when Bob Thomas, a computer programmer with BBN, created and deployed a virus that served as a security test, which was not malicious but did highlight areas of vulnerability and security flaws in what would become "the internet." The virus, named after a Scooby Doo villain, "Creeper," was designed to move across ARPANET (Advanced Research Projects Agency Network) – the forerunner to what we now call the internet. ARPANET was established by the U. S. Department of Defense. However, Thomas created the computer worm to be a non-harmful self-replicating experimental program that was intended to illustrate how mobile applications work, but instead it corrupted the DEC PDP-10 mainframe computers at the Digital Equipment Corporation, and interfered with the teletype computer screens which were connected. Bob Thomas is the father of modern cybersecurity.

In response to this, Ray Tomlinson, Thomas' colleague created the Reaper Program, similar to Creeper, which moves through the internet, replicating itself, and finds copies of the Creeper. As it locates the copies, it logs them out, rendering them impotent. The Reaper was the first attempt at cybersecurity – the first antivirus software program [3].

THE IMPORT OF CYBERSECURITY IN THE HEALTHCARE INDUSTRY

Cybersecurity is important in the healthcare industry because it protects patient confidentiality and reduces the risks of data breaches. Hackers breach network defenses so as to steal protected health information, as shown in Figure 2, hence the need for effective cybersecurity to detect these attacks before they lead to massive data exposure, thereby reducing the risk of regulatory fines, builds customer trust, and keeps operations running smoothly [4].

WHY HEALTHCARE INDUSTRY IS A PRIME TARGET FOR CYBERATTACKERS

The Office for Civil Rights (OCR) yearly handles over 800 data breach investigations in the healthcare sector – showing that the industry is under constant assault from external attackers as a result of new technology that has led to the acceleration in the digitalization of Electronic Health Records (EHRs), and with Internet of Things (IoT) devices generating more EHR every day. Because the electronically protected health information held by healthcare organizations are more detailed, containing more revealing records of patient, therefore their value rises for attackers, as shown in Figure 3.

With the rise in the use of third-party associates in the healthcare industry, App developers, security partners, cloud infrastructure providers, and IT vendors work closely with healthcare organizations. Their services are essential to delivering advanced health services, but the poor information security practices of the associates could allow attackers access to patient data.

As healthcare organizations struggle to keep pace with security developments, there may not be sufficient allocation of resources to security teams by covered entity. This will cause staff training to lag behind the activities of phishers, and coupled with the failure of the organization to update technology creating security vulnerabilities.

HEALTHCARE STAKEHOLDERS

Within the information ecosystem, the healthcare cybersecurity strategies consider the role of stakeholders. The stakeholders are the individuals that handle patient data or enable access to patient databases. Each person plays a vital role in protecting confidential data. These stakeholders are the [4]:

1. Patients – The aim of cybersecurity is to protect patient data, but patients themselves can sometimes put data at risk. Hence, providers need to inform patients about safeguarding confidential data in public and digital settings e.g. companies can use encrypted channels.
2. Clinical professionals – They are responsible for protecting patient confidentiality. Employees/workers should receive and understand corporate cybersecurity policies, know how to handle data safely, rules about disclosure limits, and the penalties for breaching security policies. They should be free to report cybersecurity concerns.
3. Executives: C-level officers have a critical supervisory role in the cybersecurity landscape. The Chief Information Security Officers (CISOs) are to manage and promote cybersecurity within the organization. Executive buy-in is vital to successful security strategies, and only proactive work by the CISO can make this happen.

   C-level employees have additional cybersecurity responsibilities. The individuals at the executive

level generally possess extensive privileges. Attackers obtaining executive-level credentials may gain wide-ranging network access. This makes extra phishing (or whaling) training for executives vital. Whaling is also referred to as "Business Email Compromise" (BEC) or CEO fraud [5]. Security teams should also minimize the allocation of administrative privileges where possible.

4. Business associates – The suppliers and vendors are also crucial stakeholders in healthcare organizations. Cybersecurity policies must consider all business associates that deal with the organization, including cleaning companies and even HVAC (i.e. heating, ventilation, and air conditioning) suppliers. The vendors store sensitive information about healthcare companies, attackers can leverage this information when mounting phishing attacks. It is therefore vital to assess every third party and choose suppliers with robust security records.

ARTIFICIAL INTELLIGENCE IN HEALTHCARE CYBERSECURITY

The frequency and sophistication in cyber threats globally now requires that healthcare organizations urgently upgrade their cyber defenses to be able to remain on top of the situation, hence the need for Artificial Intelligence (AI). AI has the potential to significantly enhance healthcare cybersecurity and help organizations detect and respond to threats in real time. It can automate the process of mapping out networks, identifying risk points, and detecting anomalous behavior that could indicate a cyber attack, as shown in Figure 4 [6].

CYBERSECURITY CHALLENGES IN THE HEALTHCARE INDUSTRY

Some of the common cybersecurity challenges faced by healthcare organizations include:

1. Patient privacy protection – it is very challenging for healthcare providers to meet with the global requirements, cum the various legal frameworks and compliance rules, such as:
   - The Health Insurance Portability and Accountability Act (HIPAA).
   - In Europe, the General Data Protection Regulation (GDPR).
   - In Canada, companies must comply with the Electronic Documents Act (PIPEDA).
2. Avoiding reliance on vulnerable legacy systems: Legacy systems are older technologies that lack support from their original suppliers, they can become a cybersecurity nightmare. Due to unsupported apps not updated to reflect current security threats, codebase not evolving to prevent exploits, this will lead to web portals to gradually become more vulnerable to injection or scripting attacks. Some healthcare companies often rely on legacy systems in their everyday operations due to the good reason of high cost of transitioning to modern technology. Medical devices might rely on older firmware that IT teams cannot change. To save money, organizations can retain technology that once passed compliance tests.
3. Security teams need to make the case for change – The executives must be persuaded by the security teams to invest in new systems and upskill employees to use them safely, before cyberattacks occur.
4. Managing risks from emerging IT technologies – New IT products could also create cybersecurity risks. The use of telehealth systems [7], a video-based consultation by physicians to meet patients can open the door to attackers. It is suggested that interconnected IoT devices will soon become commonplace, and with its attendant benefits for patients, it will also create systemic risk.
5. Preventing data breaches – Security breaches can incur regulatory penalties, damage trust, and can even lead to criminal prosecutions under the Health Insurance Portability and Accounting Act (HIPAA) and its Security Rule, as shown in Figure 5. By posing as legitimate healthcare organizations, hackers can extract personal information from professionals and patients. Also network users can implant malware (such as computer viruses, worms, Trojan horses, ransomware, spyware, adware, rootkits, keyloggers, fileless malware, cryptojacking, and hybrid malmare) [8] by clicking a single malicious link, as shown in figures 6, 7, and 8. Insiders can use their credentials to steal and sell patient data. Cybersecurity teams must understand potential attack vectors and implement controls to keep data safe. There is the need by security teams to encrypt data and tightly control access, implement firewalls and filter unauthorized users. Security awareness training should enforce secure practices within the workforce. The cybersecurity teams must plan to document and report data exposure or incidents (i.e. incident report) [4, 9].

The HIPAA and its Privacy Rule defines Protected Health Information (PHI) as "individually identifiable information transmitted by electronic media, maintained in electronic media, or transmitted in any other form of media." Also is the HIPAA Security Rule to protect the confidentiality, integrity, and availability (known as the CIA triad) of ePHI [10].

CYBERSECURITY THREATS AND MITIGATION PRACTICES

The goal of the publication, Health Industry Cybersecurity Practices (HICP): for Managing Threats and Protecting Patients, is to foster awareness, provide practices, and move towards consistency within the HPH sector in mitigating the current most impactful cybersecurity threats. The five threats explored in this document are as follows [11]:

- Social engineering
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss
- Attacks against network connected medical devices that may affect patient safety.

The Technical Volumes detail ten Cybersecurity Practices (CSPs) to mitigate the above mentioned threats, which are:

CSP 1. Email Protection Systems

CSP 2. Endpoint Protection Systems

CSP 3. Access Management

CSP 4. Data Protection and Loss Prevention

CSP 5. Asset Management

CSP 6. Network Management

CSP 7. Vulnerability Management

CSP 8. Security Operation Centers and Incident Response

CSP 9. Network Connected Medical Devices

CSP 10. Cybersecurity Oversight and Governance

- Ransomware – Ransomware locks down IT systems and demands a financial ransom from victims.
- Phishing – In this case, administrators and physicians can fall victim to phishing emails that pretend to be from Federal agencies or associates. It is used to implant spyware that stays resident on healthcare network, passively collecting data for months or years. Phishers can as well persuade victims to provide their private information, which they use to gain network access.
- Insecure endpoints – Insecure endpoints can also allow access to malicious outsiders. This can occur when clinical organizations rely on medical devices linked to the Internet-of-Things (IoT). Remote sensors and communication tools become vectors for attackers if they lack cybersecurity protection.
- Web application attacks – Web applications such as health insurance portals and hospital inventory management systems pose security risk. If developers code applications incorrectly, attackers can use exploits [12] and code injection [13] to gain access to app backends [14].
- Credential theft – Attackers may steal credentials and use them to access patient databases. Remote workers may leak credentials when using WiFi networks. Employees may lose their devices or fall victim to theft, and while companies could send credentials to incorrect or wrong recipients.
- Insider threats – The most dangerous cybersecurity threat of all are the internal employees. Disgruntled workers can access databases and extract patient records, often without the risk of being detected. Former workers may also retain access and use their old credentials to sell patient data [4]

LEGAL FRAMEWORKS FOR HEALTHCARE CYBERSECURITY

Healthcare organizations have to use compliance frameworks to align cybersecurity systems with regulatory requirements. The U.S. Department of Health and Human Services (HHS) has created a series of framework documents to accompany HIPAA and related legislation, which are to guide companies as they mitigate cybersecurity risks and protect patients data, for example, the document prepared by HHS on: “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients” [11]/NIST framework documents for healthcare companies. Furthermore, it is important that companies attend industry events where they can learn about compliance strategies e.g. the HIMSS Global Health Conference.

HEALTHCARE CYBERSECURITY BEST PRACTICES

Healthcare companies are to refer to compliance frameworks when protecting patient data and neutralizing cybersecurity threats, as following these best practices will help you secure patient records, safeguard privacy, and minimize data breach risks. This can be carried out as follows [4]:

1. Conduct risk assessments for cybersecurity threats: Assess each potential threat based on the following:

- The probability of the risk
- The potential consequences of attacks
- The cost of mitigation
- Regulatory implications of taking action or not taking action.

Prioritize risks and focus attention on risks with the highest priority classification.

2. Put security controls in place: Mitigate critical risks with the appropriate security controls. The security teams should apply controls according to a defense-in-depth-strategy. If perimeter controls fail, fall-back systems should compensate and add an extra line of defense for critical data. Fundamental security controls for healthcare organizations include:

- Encryption of Protected Health Information (PHI) at rest and in transit
- Firewalls to protect sensitive data
- Access controls to enable legitimate access but block all other users
- Multi-factor authentication for all network users
- Threat detection tools, including anti-virus and anti-malware scanners
- Audit logs to record user activity and data integrity
- Patch management to update vulnerable apps and devices
- Virtual Private Network (VPN) coverage for remote connections
- Physical controls for data centers and other storage locations.

The security teams should audit security systems to ensure controls function as designed. They should carry out penetration testing at regular intervals, and record scan results and actions taken in response.

3. Create an incident response plan: Even with the best cybersecurity solutions, attackers can still strike, hence the need for incident response plans, which are:

- Identify and neutralize threats
- Assess data integrity and identify data exposure
- Report any regulatory breaches as soon as possible
- Restore system operations and use data backups to protect critical assets
- Learn from incidents and improve security practices in the future.

4. Cybersecurity training for employees – Employees are to undergo adequate training to be able to spot and avoid phishing emails, know the importance of strong passwords and security issues relating to accidental disclosure – these will ensure following secure practices, as shown in Figure 9. In addition, during training, the organization's data security and privacy policies, cum cybersecurity rules must be communicated to employees.
5. Carry out assessment of vendors and business associates: When engaging external services there is the need to assess the cybersecurity background of each vendor, ensure they have adequate safeguards for data security, and check HHS records for past penalties or disciplinary action. Healthcare regulations require organizations to sign Business Association Agreements with third parties.

Business associates of large healthcare organizations are often the targets of some attackers. Partner organizations sometimes fail to audit third parties to verify their security processes, and if allowed access to the networks of their partners, attackers can steal their credentials as they can pose as legitimate associates.

THE USE OF THE PUBLICATION: HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)

With regards to the Cybersecurity Act of 2015 (CSA), this publication (i.e. The Publication: Health Industry Cybersecurity Practices) sets forth a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to achieve these three core goals [11]:

1. Cost-effectively reduce cybersecurity risks for the HPH sector,
2. Support the voluntary adoption and implementation of its recommendations, and
3. Ensure that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level on an ongoing basis.

CONCLUSION

Cyber attacks facing the healthcare sector is causing increasing disruption to the care continuum globally and as evidenced in the United States Healthcare and Public Health (HPH) sector. These attacks by hostile nations that are responsible for launching highly visible, crippling ransomware attacks against the health sector, are now growing both in numbers and severity. These attacks are responsible for the disruption and the delay of care delivery at healthcare facilities leading to an increasing risk to patient care and safety. The increasing adoption of digital tools is enhancing the ability for clinical, revenue cycle, and business workflow enhancements through technologies such as electronic medical records (EMR), digital billing, scheduling services, Human Resource (HR) information systems, and customer relationship management software [15]. As technology has improved significantly since the past, emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) promise a renaissance in healthcare. Through the use of

computing, even the most minute and most negligible parts of any operation can be simplified to near perfection. ML is already present in healthcare and offers much potential for future implementation [16], to improve the quality of automation and intelligent decision-making in primary/tertiary patient care and public healthcare systems – which could be the most significant impact of ML tools, as it can improve the quality of life for billions of people worldwide [17, 18].

More information on the impact of AI and machine learning in healthcare/ways to prevent cyber attacks can be found in the journals [19-21].

REFERENCES

[1] "What is Healthcare Cybersecurity," https://www.paloaltonetworks.com/what-is-healthcare-cybersecurity

[2] "What is Internet of Medical Things (IoMT) Security?" https://www.paloaltonetworks.com/what-is-internet-of-medical-things

[3] "Cybersecurity History: Hacking & Data Breaches," https://www.monroecollege.edu/cybersecurity-history-hacking-and-data-breaches

[4] "Healthcare cybersecurity: protect PHI and ensure data integrity," https://nordlayer.com/healthcare-cybersecurity-protect-phi

[5] Leila Sharma, (September 27, 2023), "Phishing, spear phishing, and whaling - NYU," https://www.nyu.edu/phishing-spear-phishing

[6] "The role of AI in healthcare cybersecurity: Enhancing threat detection," February 20, 2024, https://www.oldnational.com/the-role-of-ai-in-healthcare-cybersecurity

[7] Shaw D. K., (June 2009), "Overview of telehealth and its application to cardiopulmonary physical therapy." Cardiopulmonary Physical Therapy Journal, vol. 20, no. 2, pp. 13-18.

[8] "The comprehensive guide to 11 types of malware in 2023," https://www.titanfile.com/the-comprehensive-guide-to-11-types-of-malware

[9] "8 types of workplace incidents + how to file and incident report," (March 16, 2023), https://www.doforms.com/8-types-of-workplace-incidents

[10] "What is Protected Health Information (PHI)," https://www.paloaltonetworks.com/what-is-protected-health-information

[11] "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," 17 April, 2023, https://aha.org/2023-04-17-health-industry...

[12] "What is an exploit?"https://www.fortinet.com/what-is-an-exploit

[13] "Code injection attacks: identification and prevention," https://www.contrastsecurity.com/code-injection-attacks

[14] "Understanding the importance and value of backend security," https://teskalabs.com/understanding-the-importance-and-value

[15] "Hospital cyber resiliency landscape analysis," PDF.

[16] P. Kaur, M. Sharma, M. Mittal, (2018), "Big data and machine learning based secure healthcare framework, *Procedia Compt. Sci.*, vol. 132, pp. 1049-1059.

[17] A. Gupta, R. Katarya, (2020), "Social media based surveillance systems for healthcare using machine learning: A systematic review, J. Biomed. Info., 103500

[18] Chinmay Chakraborty (ed.) "Digital Health Transformation with Blockchain and Artificial Intellignce," Boca Raton, FL: CRC Press, 2022.

[19] Mohd Javaid et al., "Significance of machine learning in healthcare: Features, pillars and applications." *International Journal of Intelligent Networks*, vol. 3, no. 11, pp.58-73, June 2022.

[20] Andy Greenberg, (June 12, 2024), "Medical-Targeted Ransomware is Breaking Records after Change Healthcare's $22m Payout," https://www.wired.com/medical-targeted-ransomware

[21] "30 Best Cyber Security Search Engines In 2024," https://cybersecuritynews.com/30-best-cyber-security-search...

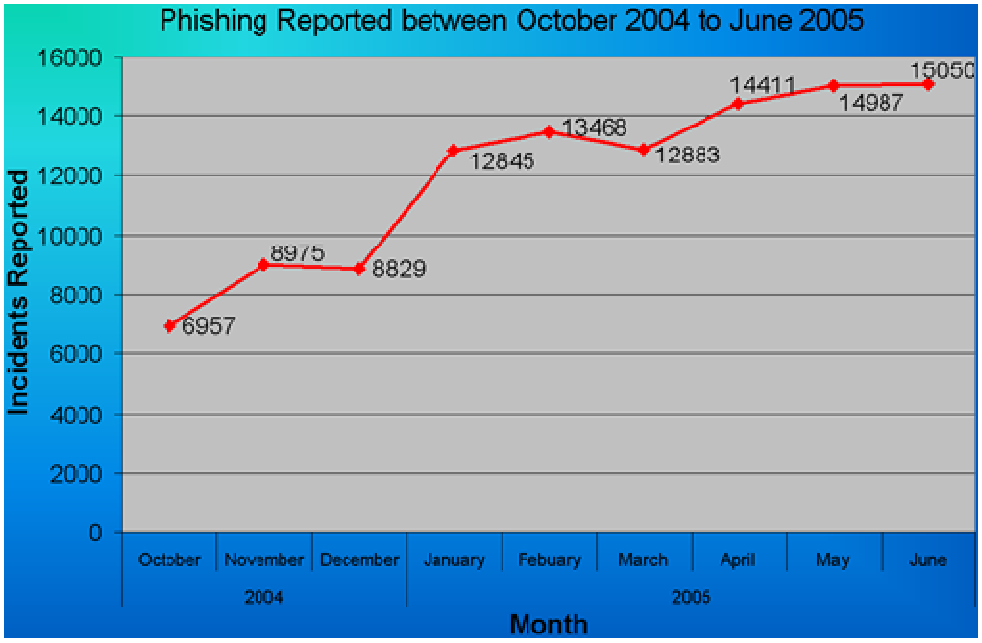

Figure 1. Phishing chart.png

Source:https://www.google.com/search?sca_esv=60fec118eeb925b4&sxsrf=ADLYWIJ6oLU_hPgNaM8yGJp_fqftYkmF5g:1720177928335&q=images+on+phishing+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7Fp0IjgBlPsjyPVyhjQuVydiDtulbHO4W4Gaas-BHqDbxIDWX-cpn0K0xlli2tt1haKSJT2JvyCW3mrE7BRGdJaPODB925oKmt6G5dPsm2WmDXOsa&sa=X&ved=2ahUKEwjgnvmS4oHAxXMU6QEHb_oAGcQ0pQJegQIDhAB&biw=1034&bih=539&dpr=1#imgrc=SPTjGN1HH5JoOM

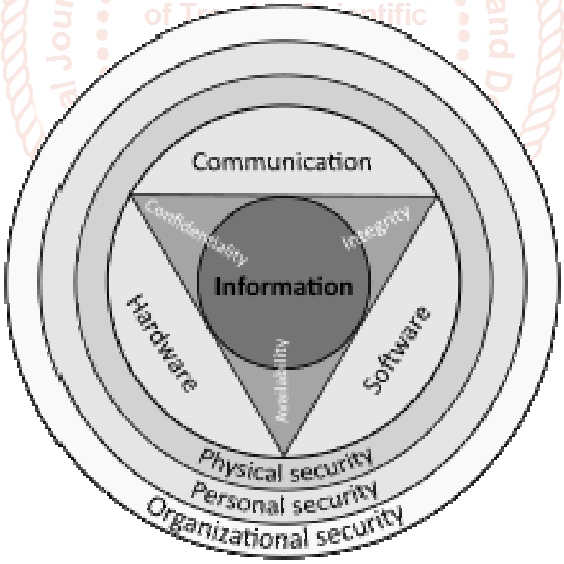

Figure 2. Information security

Source: https://www.google.com/search?sca_esv=0d90bbeb9060b7a6&sxsrf=ADLYWIJex-pf_oKljnji-ubF-Krn1uMrXw:1719109296973&q=images+on+healthcare+cybersecurity+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2s H3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwiepeeX1fCGAxUHRqQEHTvaDw8Q0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=bUNZePUfN5D3tM

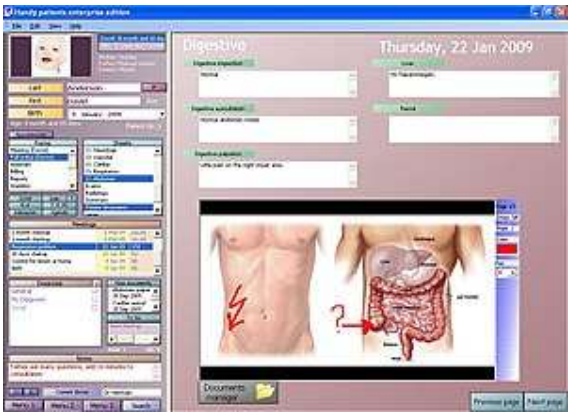

Figure 3. Medical privacy

Source: https://www.google.com/search?sca_esv=0d90bbeb9060b7a6&sxsrf=ADLYWIJex-pf_oKljnji-ubF-Krn1uMrXw:1719109296973&q=images+on+healthcare+cybersecurity+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7Y-vAPWsSmEmd7CANB-Ivwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwiepeeX1fCGAxUHRqQEHTvaDw8Q0pQJegQIDRAB&biw=1034&bih=539&dpr=1#imgrc=KHhrrgYlylmOqM

Figure 4. Artificial intelligence in healthcare

Source: https://www.google.com/search?q=images+on+AI+healthcare+by+wikipedia&tbm=isch&ved=2ahUKEwj30oiX3_CGAxVJVqQEHfsoDSsQ2cCegQIABAA&oq=images+on+AI+healthcare+by+wikipedia&gs_lp=EgNpbWciJGltYWdlcyBvbiBBSSBoZWFsdGhjYXJlIGJ5IHdpa2lwZWRpYUi_VlDcDFjALXAAeACQAQCYAdYCoAGlF6oBCDAuMTIuMi4xuAEMyAEAAEBigILZ3dzLXdpei1pbWfCAgQQIxgniAYB&sclient=img&ei=K5F3ZreRL8mskdUP-9G02AI&bih=539&biw=1034#imgrc=gKgkA4WHaJFIvM

Figure 5. Petya (malware family)

Source: https://www.google.com/search?sca_esv=b95dd397e8ded20a&sxsrf=ADLYWIKeJQ8bismHLh0yoVMxkDekme5SCw:1719668412942&q=images+on+healthcare+cyber+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1a

B4gvrdKmvT1VKZKA7YvAPWsSmEmd7CANBIvwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3b nThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ah UKEwie7YiHICHAxXgTKQEHeFhCxQQ0pQJegQIDBAB&cshid=1719668470057034&biw=1034&bih= 539&dpr=1#imgrc=ZEj_A4_TddVgTM

Figure 6. WannaCry ransomware attack

Source: https://www.google.com/search?sca_esv=b95dd397e8ded20a&sxsrf=ADLYWIKeJQ8bismHLh0yo VMxkDekme5SCw:1719668412942&q=images+on+healthcare+cyber+security+by+wikipedia&tbm=isch& source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1a B4gvrdKmvT1VKZKA7YvAPWsSmEmd7CANBIvwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3b nThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ah UKEwie7YiHICHAxXgTKQEHeFhCxQQ0pQJegQIDBAB&cshid=1719668470057034&biw=1034&bih= 539&dpr=1#imgrc=hNaFSHpCEI5qUM

Figure 7. Vastaamo data breach

Source: https://www.google.com/search?sca_esv=b95dd397e8ded20a&sxsrf=ADLYWIKeJQ8bismHLh0yo VMxkDekme5SCw:1719668412942&q=images+on+healthcare+cyber+security+by+wikipedia&tbm=isch& source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1a B4gvrdKmvT1VKZKA7YvAPWsSmEmd7CANBIvwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3b nThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ah UKEwie7YiHICHAxXgTKQEHeFhCxQQ0pQJegQIDBAB&cshid=1719668470057034&biw=1034&bih= 539&dpr=1#imgrc=bgqb9YfJd5MEpM

Figure 8. HIPAA Compliance software – Updated for 2024.

Source: https://www.google.com/search?sca_esv=b95dd397e8ded20a&sxsrf=ADLYWIKeJQ8bismHLh0yoVMxkDekme5SCw:1719668412942&q=images+on+healthcare+cyber+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkW9NAzhPVmkAfB2zK1tnQfJ7YXLTPLGowL1aB4gvrdKmvT1VKZKA7YvAPWsSmEmd7CANBIvwj74YTa4EcvLAEU7kPaPmp2sH3bGLokZWpx8jf3bnThEzDTbSHZkAfWwnN3KW0kbQY2JlD62aLpzwzj3jXk7ajEAK8MMDRRy5e1Oj0C&sa=X&ved=2ahUKEwie7YiHICHAxXgTKQEHeFhCxQQ0pQJegQIDBAB&cshid=1719668470057034&biw=1034&bih=539&dpr=1#imgrc=1rhKacEmBLJYRM

Figure 9. Internet Training.jpg

Source: https://www.google.com/search?q=images+on+internet+security+training+by+wikipedia&tbm=isch&ved=2ahUKEwjsz2V4oHAxUFcqQEHSMPDNsQ2cCegQIABAA&oq=images+on+internet+security+training+by+wikipedia&gs_lp=EgNpbWciMWltYWdlcyBvbiBpbnRlcm5ldCBzZWN1cml0eSB0cmFpbmluZyBieSB3aWtpcGVkaWFIj88DULEWWNqsA3ABeACQAQCYAdsHoAHMogGqAQozLTEuMzkuNS4xuAEMyAEAAEBigILZ3dzLXdpei1pbWfCAgQQIxgnwgIFEAAYgATCAgYQABgIGB7CAgcQABiABBgYwgIGEAAYBRgewgIEEAAYHogGAQ&sclient=img&ei=DtWHZuyQGoXkkdUPo56w2A0&bih=539&biw=1034#imgrc=IBqpU8Kxdcw_NM