CSS | ISSUE BRIEF

INCREASING CYBERATTACKS ON HEALTHCARE SYSTEMS

***Khushi Baldota* ***

Over the past decade, healthcare sectors have emerged as one of the leading targets for conducting cyberattacks. The transition of healthcare from physical statistics and record-keeping to digital mediums for the same – which enhances convenience and efficiency – has come at the cost of sensitive data being exposed and compromised. Healthcare sectors stand at the risk of cyberattacks and the corruption of critical information due to the lack of sufficient measures taken and resources dedicated to mitigating the threat. This paper discusses the increasing cyberattacks in healthcare sectors, and it goes into the details of why these sectors are a lucrative option for conducting these attacks. Further, it also mentions the consequences faced upon being targeted by these attacks. By undertaking a brief and critical analysis, this paper also highlights the measures that can be undertaken and incorporated to thwart these cybersecurity threats and attacks. Additionally, it also aims to provide an insight into how these paradigms have been impacted by Covid-19 and the protection of their data emerges as a national concern.

Healthcare sectors are beginning to use digital technology to optimize data storage and transform the operating procedures for clinical outcomes and care delivery. Healthcare sectors have shifted to electronic health records, e-prescribing software, remote patient monitoring and laboratory information system[1]. However, this change is not accompanied by measures to protect personally identifiable information and sensitive health data from cyberattacks. The healthcare sectors have a weak security posture which makes them vulnerable to cyberattacks. This directs concern towards the valuable data stored in the medical record and its pertinent need for protection against malware attacks. Further, to carry out administrative, financial and tasks relating to medical information, hospitals use connected medical devices and cloud storage. In this uptake of utility and efficacy, privacy and security measures are compromised. The convenience and delivery of care, come at the cost of increased exposure to sensitive data. Cyberattacks in healthcare are most often carried out through *social engineering* or *human hacking*, where people are used as an entry point to carry out malicious activities[2]. In this domain, cyberattacks are made to adapt to and exploit human tendencies. Common ways are forging emails, providing a credible pretext, and deliberately appealing to people's emotions that allow them to surpass suspicion. Through this, users are persuaded to enter sensitive and

* ***The Author is a student at the Jindal School of International Affairs and Research Assistant at the Centre for Security Studies, JSIA.***

[1] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al.* "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks". *BMC Med Informatics and Decision Making.* 20, no.146 (2020).

[2] Wiggen, J. "The Impact of COVID-19 on Cybercrime and State Sponsored Cyber Activities". *Konrad Adenauer Stiftung*. (2020).

critical information in an authentic-looking portal which is then infected with malware[3]. Cybercriminals use such techniques to encrypt data stores in healthcare facilities and make a vague promise to decrypt them in return for a ransom payment.

Healthcare sectors have proven to be an attractive target due to their porous guard of protection, easy accessibility, and abundance of rich information. On account of this, healthcare has come to be known as one of the most targeted sectors, thereby causing the data of millions of patients to be compromised[4]. Statistics show that there has been a 300 percent increase in cyber attacks in the healthcare sector since 2015, highlighting the ascending frequency of ransomware cyber attacks[5]. Healthcare has become one of the top three affected sectors for ransom – across the world, proving that it is being targeted specifically and aggressively. Healthcare sectors are vulnerable and soft targets due to their relatively insecure codes that are created to enhance data interoperability and provide access to health records in case of emergencies[6]. Additionally, tracing the cyber attacks using digital forensics is a challenging task due to the absence of an entity that would be responsible for the same. The sensitive and valuable information contained in medical health records are personal identifiers, which can be widely used for medical fraud and identity theft. The selling of this data on the dark web is priced more than social security and credit card details[7]. Along with financial gain as a repeatedly surfacing motive for cyber attacks in healthcare sectors, terrorism, and retribution, making a political statement through '*hacktivism*', obtaining intellectual property and demographic information, access to drugs and performing insurance fraud are other factors. These cyberattacks are also known to be led by sophisticated criminal groups or state agencies that wish to access the interaction of health services with armed forces, for gaining a strategic edge.

In a heightened global, dynamic, and interconnected landscape, the greatest threat to civilians comes from unforeseen cyberattacks that target the information systems in healthcare sectors. This establishes that the virtual domain is just as formidable, if not more, as the physical domain. The National Health Sectors in the United Kingdom in 2017 and Los Angeles in 2016 have had debilitating effects on patient safety. The information technology systems of hospitals have been crippled, important procedures and outpatient appointments have been cancelled on account of cyberattacks. Furthermore, incoming ambulances have been redirected and blood product refrigeration has been destroyed. Threats to medical devices and critical infrastructure are of concern because of their potential effects on patient health and safety. Patients are especially at risk from attacks that could disrupt critical medical infrastructure, disrupt communications and services, interfere with medical devices, alter, and falsify critical data, or

[3] Wiggen, J. "The Impact of COVID-19 on Cybercrime and State Sponsored Cyber Activities". *Konrad Adenauer Stiftung*. (2020).

[4] Martin, G, Martin P, Hankin C, Darzi A, and Kinross J. "Cybersecurity and Healthcare: How Safe Are We?" *BMJ: British Medical Journal*. 358 (2017).

[5] Protecting Your Networks from Ransomware. Washington, D.C.: The United States Department of Justice. (2016). 2–8.

[6] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al.* "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks". *BMC Med Informatics and Decision Making.* 20, no.146 (2020).

[7] Humer C, Finkle J. "Your Medical Record is Worth More to Hackers Than Your Credit Card". *Reuters*. 2014.

make them unavailable [8] . Cyberattacks include threat, phishing, malware, and social engineering methods to compromise security. In healthcare sectors, they lead to a backlog in information integration and disrupts the workflow, healthcare provisions and hospital operations[9].

The healthcare sectors are facing a failure in protecting their main stakeholders, and in order to meet this lag, hospitals must invest considerable effort and capital in protecting their systems. Healthcare sectors are facing difficulty due to the lack of human resources, financial capital, and a history of underinvestment in hospital information security[10]. Public officials continue to deliberate on additional cybersecurity due to the finances involved. This cost-utility approach has proved to be precarious for information security in the healthcare sector. Data breaches in the healthcare sector occur due to the absence of sufficient resources dedicated to combating this threat. The increasing challenges validate that cybersecurity must be designed as a functional prerequisite rather than an afterthought. Additionally, the gaping hole of information security in the healthcare sectors is accentuated by the lack of credible tools for evaluating the degree of damage upon a security breach or estimating associated risks. Thus, healthcare sectors are required to strengthen their information technology infrastructure and work with policies that raise the target level of cybersecurity capabilities to deliver promised benefits safely. The healthcare sectors must begin by actively identifying vulnerable information through a threat monitoring process. Early detection through a pattern of risk assessment, mitigation and re-evaluation must be followed to reduce exposure. The administrative privileges must be regulated, and users must be vetted[11]. Further, the healthcare sectors are required to develop a comprehensive employee training program to raise awareness about the issue and adequately equip them to mitigate the threat, as they are the prime targets for social engineering tactics. As a preventative measure, personal work should not be carried out on critical devices to safeguard entry points and limit data to the confines of security parameters. Healthcare sectors should design a cybersecurity team that would spearhead the aforementioned initiatives.

COVID AND CYBERCRIME

As the globe was plagued with the Covid-19 pandemic, businesses, hospitals, and government agencies were forced to shift their operations and work processes on a digital platform in an ad-hoc fashion. This did not give them sufficient time to develop a strong cybersecurity infrastructure. Employees began working from home, observing government guidelines, where private IT devices were being used for conducting official business. Upon the short work-from-

[8] Harkins, Malcolm, and Freed A. "The Ransomware Assault on the Healthcare Sector." *Journal of Law & Cyber Warfare* 6, no. 2 (2018): 148-64.

[9] Ghafur, S., Kristensen, S., Honeyford, K. *et al.* "A retrospective Impact Analysis of The WannaCry Cyberattack on the NHS". *npj Digital Medicine.* 2, no. 98 (2019).

[10] Liveri D, Sarri A, Skouloudi C. *Security and Resilience in eHealth: Security Challenges and Risks*. (2015).

[11] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al.* "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks". *BMC Med Informatics and Decision Making.* 20, no.146 (2020).

home notice, remote access to internal networks was granted, making it increasingly harder to track the unauthorized users accessing internal networks and sensitive data[12]. The devices being used by employees lacked adequate security checks. Thus, Covid-19 has marked the increased usage of unencrypted or poorly protected digital applications whose data is prone to security risks. The lack of sufficient security creates a conducive environment for cybercrime attacks on critical infrastructure and espionage activities sponsored by states to obtain information about vaccine production, national plans for containing the virus and treatment plans in the healthcare sectors of other countries. Cyberattacks have been directed towards institutions that conduct research on the corona vaccine to probe into their intellectual property as well as public health concerns that is pertaining to their vaccine tests and treatment. It is believed that hackers sponsored by Russia, China and North Korea are using personalized emails containing references to the pandemic in order to infect their targets with malware. Two groups that are also believed to be connected to China are suspected to have sent emails with attached documents containing genuine health information to targets in Vietnam, Mongolia, and the Philippines to infect them with spyware. A Russian group operating against Ukrainian targets is believed to be using similar methods[13].

The advance of digitalization prompts the increase in cybercrime and as long as the virus dominates the headlines, Covid related scams will continue to persist. In order to combat this, in-service training should be expanded, cybercrime investigations should be undertaken, existing safeguards must be evaluated, and IT structure must be strengthened. Along with this, secure communication channels for confidential information exchange, digital literacy and education campaigns, and law enforcement resources must be made available. On a national, political, and strategic level, governments could resort to the imposition of sanctions or legal charges through cyber diplomacy, upon cyberattacks being launched by other states. The security, confidentiality and privacy of healthcare information have been classified as an ethical and moral concern. However, after experiencing the virtual calamities due to a poorly protected healthcare system, it should be relegated as a national security priority.

CONCLUSION

Cybercrime has been on the rise in healthcare sectors which has opened up avenues for compromising critical patient data and other sensitive information. The lack of adequate security measures taken in this sector coupled with its excess availability of valuable information has projected the healthcare sector to be a vulnerable target for cyberattacks. Some research in this regard highlights that cyberattacks are conducted for financial gains and strategic motives, predominantly. The healthcare sector has faced severe consequences and learning from these repercussions, it is imperative for them to strengthen their security posture, invest in cybersecurity resources and undertake education campaigns to sensitize the

[12] Wiggen, J. "The Impact of COVID-19 on Cybercrime and State Sponsored Cyber Activities". *Konrad Adenauer Stiftung*. (2020).

[13] Wiggen, J. "The Impact of COVID-19 on Cybercrime and State Sponsored Cyber Activities". *Konrad Adenauer Stiftung*. (2020).

employees to the potentially destructive efforts of social engineering and human hacking. Additionally, in the context of Covid-19, data about vaccination, research updates and treatment plans need to be protected from cyberattacks initiated by other countries. With the recent turn of events, the matter of cybersecurity in the healthcare sector has shored up as a matter of national concern and needs to be tackled with vigilance.