Forum: World Health Organization (WHO)

Issue: Safeguarding Critical Healthcare Infrastructure Against Cyberattacks

Chairs: Dana Daqa, Shahd ElBaz, & Kenzy ElFarrash

Introduction

Protection is key in health infrastructure and in cyberattacks. This paper seeks to discuss how such sustainable development can safely be elaborated on. Health organizations are particularly vulnerable due to the fact that they possess highly valuable information that is lucrative for cybercriminals and nation-state actors in terms of money and intelligence. WHO can help eradicate these cyberattacks and thefts by encouraging the backup of data, encryption of sensitive information, and providing patient safety without causing delays in care or putting patients' lives in danger. This will create conditions that improve security and well-being. Because the WHO has played an important role in ensuring that patients can be safe and secure in hospitals free from cyberattacks, safeguarding will be important to both the patients and hospitals.

Definition of Key Terms

Healthcare infrastructure

Services and facilities that support a population's health.

Safeguarding

The process of keeping individuals secure and ensuring that they live in a tranquil environment.

Cyber attacks

Any form of stealing or hacking through unauthorized access to the Internet in order to block or destroy computer systems.

Ransomware

A software designed to block access to a computer system until a sum of money is paid.

Background Information

WHO, an United Nation organization that was established in 1948, serves to connect countries, partners, and people to promote health, keeps the world safe, and protects the vulnerable to ensure that everyone, everywhere attains the highest possible level of health. The United Nations and the World Health Organization have one common goal: patient safety. Given the year 2024 has been a year of health care hacks, the task is not an easy one. For example, one ransomware attack involved the nonprofit donation service OneBlood; this interrupted the supply of blood for transfusions going to hundreds of hospitals throughout the Southeast. The world is becoming increasingly interconnected and relying on digital technologies; cybercrime is growing accordingly. The number of cyberattacks increased significantly in 2023, with over 343 million victims. Data breaches increased by 72% between 2021 and 2023, breaking the previous record.

Major Parties Involved

United States of America

- The United States was involved in ongoing talks and negotiations related to cybersecurity and cyber defense strategies. The U.S. The Department of Health and Human Services published voluntary cybersecurity performance goals that were developed for the healthcare industry on January 25, to assist health care organizations with prioritizing high-impact cybersecurity practices;
- The US actively participates in international sessions, including the UN, where it also plays a key role in the discussion of issues to do with cyber security. Though policies may change with each successive administration, it has continuously pressed for more international cooperation, especially in order to address life-sensitive sectors such as health that face serious cyber security problems. With continued dependence on AI and digital technologies in health care, the United States encourages the development of agreements and standards that assure responsible use and protection of private health information from online attacks;
- The benefits arising from cybersecurity are always fundamental to the basic functionality of the USA's economy, operation of its critical infrastructure, strength of democracy and democratic institutions, privacy of USA's data and communications, and USA's national defense;
- This represents the status and power of the United States in terms of security over the world, including patient safety. It is ranked as the country with the most cyberattacks, yet it still proposed multiple solutions to decrease its percentages.

Russia

-

- Russia has indeed been identified as one of the players in global cyber threats that involved attacks even on healthcare infrastructure. Such activities disrupt critical healthcare operations.
- Efforts to overcome this problem remain unclear, and little is known about Russia's weighty contributions to minimize these threats. Critical infrastructure protection requires international cooperation and an increase in cybersecurity against ongoing threats.

Brazil

- Brazil has provided much value to global cyber standards development, particularly through its involvement in crafting UN frameworks and norms. This is epitomized by endorsing the eleven non-binding, voluntary norms presented by the UN to promote responsible online behavior. These norms take up a range of cybersecurity-related themes: "protection of critical infrastructure, norm on the importance of international cooperation, norm on human rights online.";
- Brazil is actively involved in global cybersecurity campaigns and advocates for responsible AI, especially in medical applications. The country also adheres to voluntary guidelines that ensure moral state behavior in cyberspace and collaborates on programs to enhance cybersecurity capability. These efforts are hence aimed at enhancing global cybersecurity and the resilience of the digital infrastructure.

North Korea

- North Korea sees cyberattacks as the key to gaining an economic edge, political leverage, and military advantage. The regime is searching for ways to use AI in healthcare and the

military from technology and data in other countries. All these are part of a bigger strategy aimed at polishing its image before the international community;

- The Justice Department has levied charges in a string of hacking cases in North Korea but often points out that, unlike those from China and Russia, hackers there are more often motivated for financial gain. For example, in 2021, three North Korean computer programmers were indicted on a variety of hacking-related charges including a devastating attack on an American film studio and attempting to steal and extort more than $1.3 billion from banks and businesses around the world.

China

- There are accusations that it has engaged in cyber operations against critical infrastructures, governments, and corporations globally for economic progress, intellectual property theft, and national security.
- These activities often relate to espionage, industrial sabotage, and surveillance to acquire technological superiority and strategic leverage.
- Similar accusations have also taken place against China; its role in addressing the issue is mixed because it has proposed international rules through the UN and then formed cybersecurity pacts with China, but has shown limited cooperation with Western nations.

United kingdom

- Due to the recent use of AI technologies in medical systems, awareness has increased in the UK of how targeted attacks can be mounted through cyber-attacks in healthcare. Some targeted threats, by threat actors like state-sponsored organizations, would aim at health data and infrastructure. They could also use AI to increase their measures of attack;

- Safeguarding health services from these types of threats is an integral part of the UK Cyber Security Strategy, given recent pandemic-related incidents. The NCSC uses technological innovation, together with advice to individuals and organizations, to protect the UK's critical services against cyberattacks, respond to major incidents, and improve the underlying security of the UK Internet.

Timeline of Key Events

Date	Description of Event
1960s-1980s	It has turned into an ecosystem much like any other legitimate business, with numerous groups offering services such as ransomware-as-a-service and even advertising their products. While it had recently exploded, its roots go back to 1834 when attackers used the French telegraph. Nowadays, cybercrime is seen using many different tactics, and it is very dangerous for every organization across the globe. There have been attacks and attackers who have become well-known to law enforcement and the hacking community.

1990s	The 1990s were revolutionary in communication technologies-the internet connected people all over the world. In its wake, this development facilitated the rise of cybercrime. Trust and safety were largely absent from the equation, serving as little deterrent to those who would seek to exploit emerging computer viruses for personal gain. There was no use of the term "cybersecurity" then, so an underground economy began to balloon along with emerging computer viruses. Major service providers, such as America Online (AOL), were being targeted with credential thefts and phishing attacks, touting a new breed of cybercriminals exploiting new technologies.

2000s	During the first decade of the 2000s, the number of complex threats increased-many because of the Advanced Persistent Threat (APTs) supported by nation-states. The next wave of development included new types of viruses and worms that inflicted serious blows on the global digital economy's critical infrastructure. By the end of the decade, cybersecurity had grown into a major problem for users, especially those with a high-risk profile-such as government agencies and large corporations.
2010s	Between 2010 and 2020, cybercrime went from a criminal activity to an enormous worldwide business; attackers released new, sophisticated malicious code and attack techniques, which caused the number of daily attacks to explode while losses reached trillions. Ransomware began spreading because of digital money, such as Bitcoin. This meant that more cybersecurity professionals were hired by organizations in

	response, hence giving rise to practice of probing computer systems, networks, or applications to identify and fix security vulnerabilities in the identification of vulnerabilities. These are some of the cyber threats that have constantly been evolving and hence pose a significant challenge to organizational defenses.
2020s	While the 2010s was definitely the time of establishment for cybercrime, the 2020s have seen the cybercrime ecosystem evolve. The decade is shaped by two major forces: on one hand, the surge in cybercrime driven by technological changes and socioeconomic problems, particularly in Eastern Europe and Asia, along with rapid digitization of organizations; on the other hand, while companies rapidly move to cloud solutions and expand globally, too often they leave their cybersecurity behind, hence making themselves increasingly vulnerable.

Previous Attempts to Resolve this Issue

1. **Legislation**

   Passed legislation, such as that on computer fraud and abuse, made laws prosecute cybercrime, thus bringing about some element of accountability.

2. **International Cooperation**

   Europol and INTERPOL programs have helped make international cooperation against cybercrime much easier, especially because shared intelligence and coordinated operations have been facilitated.

3. **Public Awareness Campaigns**

   Public awareness drives through education have proved quite successful in making people aware of the threats to cybersecurity and hence helped adopt safer online behaviors by individuals and organizations.

4. **Cybersecurity Frameworks**

   With the help of these frameworks, such as the NIST Cybersecurity Framework, structured guidelines were given to organizations on how to improve their security posture.

Possible solutions to resolve this issue

1. **Universal Standards for Cybersecurity**

   Universal cybersecurity standards would give the world a standard baseline on security procedures for all industries, all countries. This increases the bar for cybercriminals to exploit the gaps.

2. **Public-Private Partnerships**

   Much closer collaboration between public and private sector entities on information sharing and responding to cyberthreats would be possible.

3. **Cyber Insurance for Small Businesses**

   Encouraging small businesses to invest in cyber insurance would avail them of much-needed capital to develop better security measures that would help them prevent and recover from cyberattacks.

4. **Invest in Cybersecurity Education**

   Awareness in the cybersecurity workforce will be built by introducing the subject of cybersecurity right from elementary schooling to university courses, helping narrow the gap in managing cyber threats.

Bibliography

"Healthcare and Public Health Cybersecurity | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cybersecurity-best-practices/healthcare.

Ingram, Nick, et al. "North Korean Charged in Cyberattacks on US Hospitals, NASA and Military Bases | AP News." *AP News*, 26 July 2024, apnews.com/article/north-korea-hacker-military-intelligence-hospitals-b3153dc0ad16652a80a9263856d63444.

Redirecting. www.google.com/url?q=https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible?lang%3Den&sa=D&source=docs&ust=1731357815122692&usg=AOvVaw2MAVVK71GsP147K8w9wuCr.

"The Importance of Cybersecurity in Protecting Patient Safety | Cybersecurity | Center | AHA." *American Hospital Association*, www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-p

rotecting-patient-safety#:~:text=Health%20care%20organizations%20are%20particularly,thieves%20and%20nation%2Dstate%20actors.

Wolf, Arctic, and Arctic Wolf. “A Brief History of Cybercrime.” *Arctic Wolf*, 19 Apr. 2024, arcticwolf.com/resources/blog/decade-of-cybercrime.