Playing with Lives: Cyberattacks on Healthcare are Attacks on People

CyberPeace Institute

Executive Summary

Online or offline, cyberattacks on healthcare are attacks on people. As a critical service provider, healthcare should be off-limits to any malicious intent or action, safeguarded for and by all.

The Strategic Analysis Report focuses for the first time on the impacts of attacks on people and society. From ransomware to COVID-19 related disinformation operations, as incidents are underreported, attacks seldomly attributed and threat actors act with impunity, the Report shows how accountability is critical to any systemic solution.

A series of recommendations are addressed to governments, industry, the healthcare sector, academia and civil society aiming to secure long-lasting impact by reducing attacks on healthcare, and increasing resilience.

Recommendations:

1. **Document attacks and analyse their human and societal impact.**
2. **Improve the healthcare sector's preparedness and resilience by:**
   - Reinforcing the cybersecurity of healthcare infrastructure,
   - Enhancing healthcare capacity and capabilities,
   - Galvanizing healthcare preparedness to attacks;
3. **Activate technical and legal instruments to protect healthcare to:**
   - Reinforce the legal and normative ecosystem,
   - Improve information-sharing and reporting standards;
4. **Hold threat actors to account.**

Why is the healthcare sector under attack?

The healthcare sector has long been a target of attacks. The COVID-19 pandemic has further exacerbated the sector's threat landscape, exposing it to a convergence of threats that can be attributed to three key factors:

1. Healthcare has become a target of choice for disruptive digital extortion attacks due to its **responsibility** to maintain critical systems to ensure public health.
2. Healthcare organizations are **custodians of valuable data**. Medical records are among the most profitable data on underground markets.
3. The healthcare sector's **strategic importance** during the COVID-19 pandemic has placed it at the center of nation-state interest for cyberattacks. States have sought to undermine global pandemic response by targeting healthcare and the trust that people place in it.

These threats are facilitated by the sector's **fragile digital infrastructure** and its pervasive **underinvestment in cybersecurity**.

What is the real impact of attacks on healthcare?

Attacks on healthcare are causing direct harm to people and are a threat to health and life, globally.

The convergence of attacks on the sector's digital infrastructure, on its pandemic response, and on the trust in the sector's ability to function as needed is creating a **global threat to health and human life**. While the targets of attacks are most often portrayed as the healthcare organizations or service providers whose data or infrastructure was compromised, the actual direct victims of attacks are healthcare professionals, patients and society as whole, who suffer in the long term.

Whether through the breach of confidential medical records, the disruption of medical services, or the dissemination of COVID-19 disinformation, attacks against the healthcare sector generate a **climate of fear**, confusion and distrust.

The business and economic impact of attacks on healthcare has lasting effects for several years after the attack itself. Following an attack, healthcare organizations suffer from a time-consuming recovery process, requiring funding to recover and improve its systems, cover regulatory penalties, re-train staff, and manage reputational damage. Such costs may include a ransom payment which is strongly discouraged for its likelihood to incite similar extortive demands in the future, with no guarantee that the ransom payment will yield the outcome sought.

Who are the prevalent threat actors?

Attacks on healthcare are low-risk, high-reward crimes. Acting with near impunity, criminals and state actors are joining forces against healthcare with varying motives and agendas.

Two types of threat actors pose the greatest danger to the healthcare sector: cybercriminals and state actors. The line is increasingly blurred between the two as **state-sponsored / funded proxies** who act on behalf of states have emerged in recent years,further complicating the attribution of attacks.

All types of perpetrators attacking healthcare have been able to operate with near impunity. The enforcement and prosecution rate for perpetrators of attacks on healthcare is extremely low. This stems notably from the underreporting of attacks, from the lack of resources in law enforcement and the judiciary, and from shortfalls in attribution.

What instruments are available to protect healthcare from attacks?

States are not availing of the full extent of norms and laws available to protect healthcare.

Many instruments and opportunities – ranging from domestic law to international law to voluntary non-binding norms – are available to hold threat actors accountable for their actions, to protect critical infrastructure and better secure digital products.

Regrettably, these opportunities also come with corresponding challenges such as international agreements on thresholds for applying international law principles, and questions of territoriality. These challenges ultimately inhibit a nation state's ability to conduct and complete cyber investigations, thus perpetuating impunity in cyberspace.

The CyberPeace Institute has identified that closing the accountability gap is a prerequisite to establishing cyberpeace and securing the protection of vulnerable communities. Closing the accountability gap implies more than attribution alone.

The CyberPeace Institute commits to supporting the recommendations through: 1. the continuous monitoring, documentation and dissemination of information on attacks on healthcare and the application and violation of laws, norms and regulations; 2. supporting and developing information-sharing initiatives, and 3. the holding to account of threat actors.

Mission Statement

The CyberPeace Institute is a non governmental organization whose mission is to reduce the harms from cyberattacks on people's lives worldwide, provide assistance to vulnerable communities, and call for responsible cyber behaviour, accountability and, ultimately, cyberpeace.