CYBER INCIDENT TRACER (CIT) #HEALTH
Fact Sheet

Cyberattacks on healthcare are attacks on people. Understanding their true scale and impact is key to policy making and for redress for victims. The **Cyber Incident Tracer (CIT) #HEALTH** is a platform that aims to close the information gap related to cyberattacks on the healthcare sector on a global scale which disrupt the delivery of healthcare, compromise sensitive healthcare-related data, and have an impact on patients, healthcare professionals, facilities and organizations.

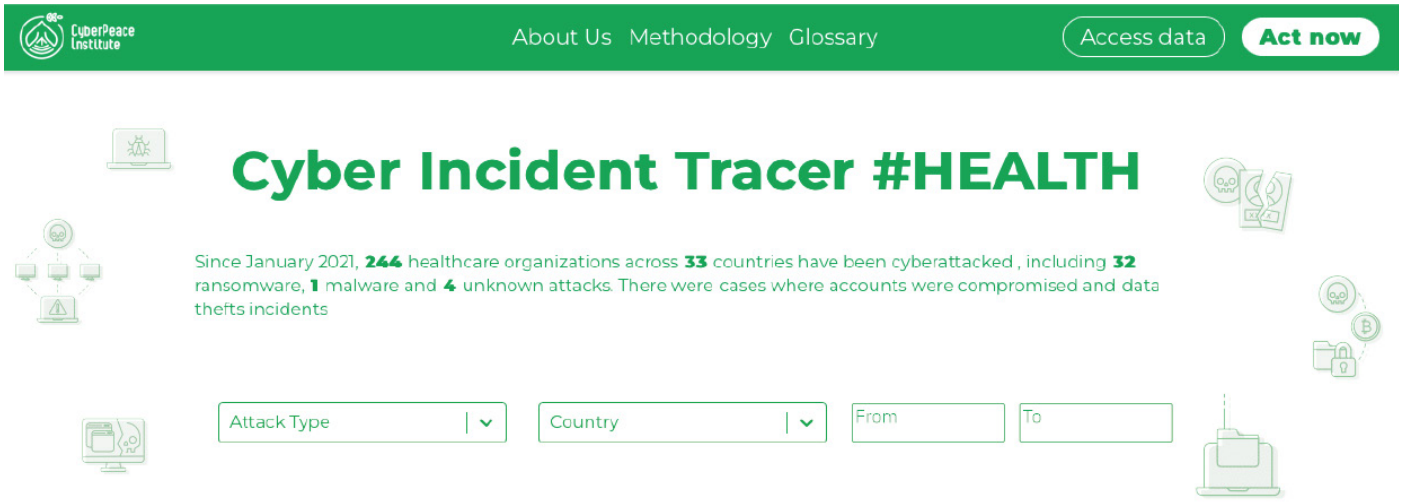
The platform provides evidence-based understanding of the impact of cyberattacks on healthcare. The aim is to bring greater visibility about such cyberattacks, and how they impact people and the provision of healthcare. Limited visibility and data on the impact of cyberattacks has complicated policy making. The inability to understand the human impact of cyberattacks has resulted in a failure to develop suitable policies to ensure a safe and secure cyberspace. This is essential to people benefiting from healthcare without concern for their privacy, security and safety.

Cyberattacks on healthcare impact people. Delays and interruptions to patient care endanger lives. Healthcare professionals suffer from their inability to save lives. Trust in healthcare is eroded. Threat actors pray on the fear and vulnerabilities of their targets.

The platform contains data about cyberattacks on healthcare from June 2020. Data on new attacks is updated on a weekly basis.

Access the Cyber Incident Tracer #HEALTH platform

The platform provides data driven understanding of the impact of cyberattacks on healthcare organizations, primarily: Patient care services, Medical Manufacturing & Development and Pharmaceuticals.



Analysis of the data shows in the first half of 2021:

122 attacks recorded in **6** months averaging in **20** attacks per month

102 healthcare organizations providing patient care services were targeted, of which **26** were hospitals

Ransomware attacks occured at a rate of **3.8** per week and result in an average of **21** days of operational disruptions but can range anywhere between several hours to **2.5** months.

75% resulted in systems going offline

25% led to appointments cancellations

22% led to patients being redirected

There is a disparity in reporting and availability of data on cyberattacks across the world.

Understanding the scale and societal impact of cyberattacks on healthcare can lead to change and help prevent such attacks. Join the CyberPeace Institute's Call for Action and Call for Support.

Call for Action to Governments:

Action must be taken to stop attacks on healthcare. Health is a fundamental right and it is the state's responsibility to protect this common good.

Meaningful action should be taken to enforce norms of behavior and international law in the healthcare sector. This is critical infrastructure and must be off-limits to attack.

Invest resources to ensure the healthcare sector is equipped to deal with cyber threats.

Contribute to initiatives that bring greater visibility to how attacks on healthcare really impact people and the provision of care.

Ensure accountability for cyberattacks on healthcare. Arrest perpetrators of attacks. Ensure a transparent and efficient judicial process to hold criminals to account.

Call for Action to the Healthcare Sector:

Be aware of current cyber threats and implement defences proportionate to them. Conduct vulnerability scanning, assessments and timely patching of systems.

Communicate about vulnerabilities to all relevant stakeholders. Secure potential attack vectors/endpoints. Report incidents and their impact on the ability to provide healthcare in a timely manner. Notify patients and/or customers when their data has been compromised.

Call for Action to Industry:

Implement security-by-design and security-by-default models for healthcare product development across the supply chain. Sponsor research in technical solutions such as zero-trust networks, behavioural authentication and monitoring to improve the protection of hospitals from vulnerabilities in their supply chain.

Adapt pricing models according to the diversity of resources in healthcare to prevent discrepancies for those who can afford cybersecurity and those that cannot.

Support initiatives that provide cybersecurity resources to those healthcare facilities without capacity, resources, or capability to protect themselves. Increase transparency and responsible disclosure of vulnerabilities.

Our Call for Support:

We are continuing to develop the CIT. We seek partners & contributions for collection of data, the technical development of the platform, and to develop an empirical methodology for measuring the human and societal impact of cyber incidents, and in defining a methodology for tracking attribution and accountability.

Mission Statement

The CyberPeace Institute is an independent and neutral non governmental organization whose mission is to ensure the rights of people to security, dignity and equity in cyberspace. The Institute works in close collaboration with relevant partners to reduce the harms from cyberattacks on people's lives worldwide, and provide assistance. By analyzing cyberattacks, the Institute exposes their societal impact, how international laws and norms are being violated, and advances responsible behaviour to enforce cyberpeace.

If you can support this please contact us at: **cit@cyberpeaceinstitute.org**

Our efforts focus on reducing the impact of cyberattacks on people's lives throughout the world. But we can't do it without you.

We welcome donations to support our mission. Donate at: **donate@cyberpeaceinstitute.org** or **cyberpeaceinstitute.org/donate/**

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15
1202 Geneva, Switzerland

cyberpeaceinstitute.org
@CyberPeace Institute
@CyberpeaceInst