> **A study of healthcare cyberattacks in over 30 countries shows the scale of the rising threat**

- **A study of healthcare cyberattacks in over 30 countries shows the scale of the rising threat.**
- **Ransomware attacks dominate the broadening scope of threats to healthcare providers.**
- **More action is needed from actors in the sector, cybersecurity firms and governments to ensure access to healthcare.**

INFOCUS

by Stéphane Duguin

IF HEALTHCARE DOESN'T STRENGTHEN ITS CYBERSECURITY, IT COULD SOON BE IN CRITICAL CONDITION

It's hard to imagine anything more cynical than holding a hospital to ransom, but that is exactly what's happening with growing frequency. The healthcare sector is a popular target for cybercriminals. Unscrupulous attackers want data they can sell or use for blackmail, but their actions are putting lives at risk. A cyberattack on healthcare is more than an attack on computers. It is an attack on vulnerable people and the people who are involved in their care; this is well illustrated by the breadth of healthcare organizations, from hospitals to mental health facilities to pharmaceutical companies and diagnostic centres, targeted between June 2020 and September 2021.

Cyberattacks on healthcare have continued to plague the sector since the start of the COVID-19 pandemic. At the CyberPeace Institute, we have analyzed data on over 235 cyberattacks (excluding data breaches) against the healthcare sector across 33 countries. While this is a mere fraction of the full scale of such at-

Healthcare cybersecurity suffers from a general lack of human resources

tacks, it provides an important indicator of the rising negative trend and its implications for access to critical care.

Over 10 million records have been stolen, of every type, including social security numbers, patient medical records, financial data, HIV test results and private details of medical donors. On average, 155,000 records are breached during an attack on the sector, and the number can be far higher, with some incidents reporting the breach of over 3 million records.

Poor bill of health

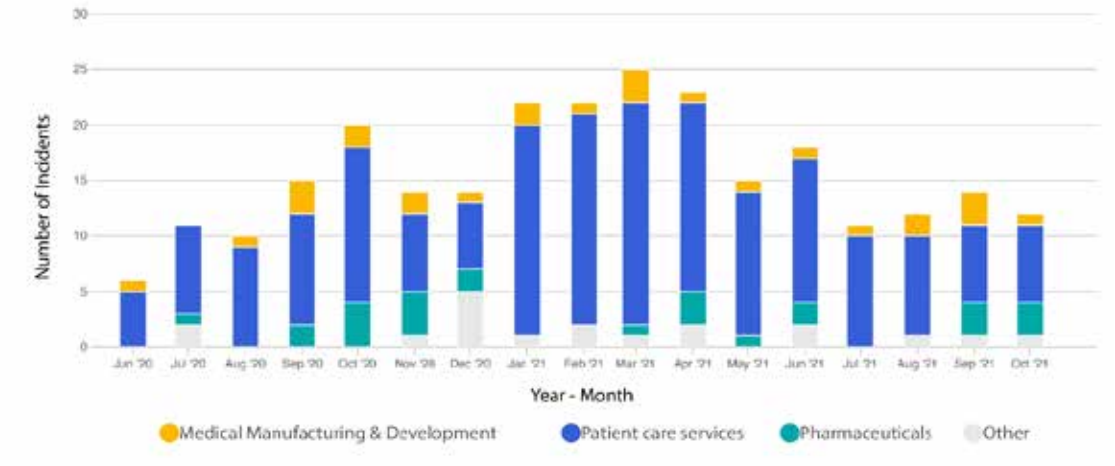
Ransomware attacks on the sector, where threat actors lock IT systems and demand payment to unlock them, have a direct impact on people. Patient care services are particularly vulnerable; their high dependence on technology combined with the critical nature of their daily operations means that ransomware attacks endanger lives. Imagine being in an ambulance that is diverted because a cyberattack has caused chaos at your local emergency department. This is not a hypothetical situation. We found that 15% of ransomware attacks led to patients being redirected to other facilities, 20% caused appointment cancellations, and some services were disrupted for nearly four months.

Ransomware attacks on the sector occurred at a rate of four incidents per week in the first half of 2021, and we know this is just the tip of the iceberg, as there is a significant absence of public reporting and available data in many regions. Threat actors are becoming more ruthless, often copying the data, and threatening to release it online unless they receive further payment.

Health records are low-risk, high reward targets for cybercriminals – each record can fetch a high value on the underground market, and there is little chance of those responsible being caught. Criminal groups operate across a wide range of jurisdictions and regularly update their methods, yet we continue to see that attackers act with impunity.

Securing the right to healthcare

We can, and should, be doing better. The first step is with cybersecurity itself. Healthcare cybersecurity suffers



■ *Incidents over time by healthcare sub-sectorImage: CyberPeace Institute*

from a general lack of human resources. More people need to be trained and deployed.

Software and security tools need to be secure by design. This means putting security considerations at the centre of the product, from the very beginning. Too often security options are added as a final step, which means they paper over inherent weaknesses and loopholes.

Healthcare organizations should also do more, particularly increasing their investment in cybersecurity to secure infrastructure, patch vulnerabilities and update systems, as well as building and maintaining the required level of cybersecurity awareness-raising and training of staff. Healthcare organizations also need to commit to due diligence and standard rules of incident handling.

But these matters are ultimately too big for individual organizations to solve alone. Governments must take proactive steps to protect the healthcare sector. They must raise the capacity of their national law enforcement agencies and judiciary to act in the event of extraterritorial cases so that threat actors are held to account. This requires the political will and international

Governments must take proactive steps to protect the healthcare sector

cooperation of governments, including for investigation and prosecution of threat actors.

One point of real concern from our analysis is that information about cyberattacks, such as ransomware incidents, is inadequate due to under-reporting and lack of documentation of attacks. Thus it is impossible to have a global view of the extent of cyberattacks against the healthcare sector. To build even a partial picture of such attacks meant us accessing and aggregating the data that ransomware operators – the criminals – publish or leak online.

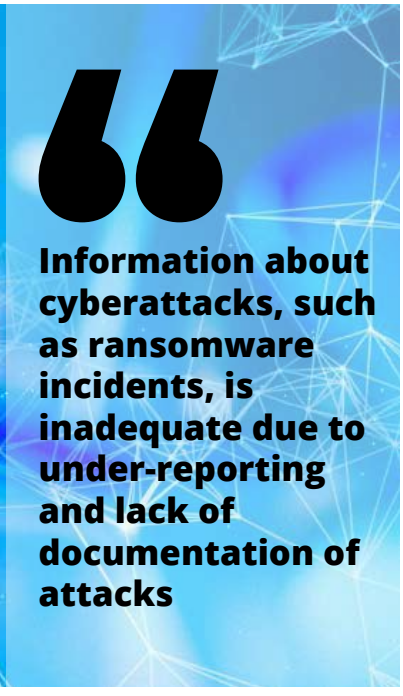
It is not acceptable that they are the significant source of information relating to cyber incidents and threats posed to the sector. We want to shift away from data published by or from malicious actors and encourage stronger reporting and transparency relating to cyberattacks by the healthcare sector to improve both the understanding of the threat and the ability to take appropriate action to reduce it.

Our analysis shows that 69% of countries for which we have recorded attacks have classified health as critical infrastructure. Healthcare must be recognized as critical infrastructure globally. Designation as critical infrastructure would ensure that the sector is part of national policies and plans to strengthen and maintain its functioning as critical to public health and safety.

Governments must enforce existing laws and norms of behaviour to crack down on threat actors. They should cooperate with each other to ensure that these laws are put into operation in order to tackle criminals that operate without borders. More should be done to technically attribute cyberattacks to identify which actors have carried out and/or enabled the attack.

Health is a fundamental human right. It is the responsibility of governments to lead the way in protecting healthcare. People need access to reliable, safe healthcare, and they should be able to access it without worrying about their privacy, safety and security.

We hope there is global recognition that the status quo is unacceptable and that we can all do more to prevent cyberattacks against healthcare, protect the victims of such attacks, and hold perpetrators to account.



THE AUTHOR

Stéphane Duguin is the Chief Executive Officer of the CyberPeace Institute. He has spent two decades analysing how technology is weaponized against vulnerable communities. In particular, he has investigated multiple instances of the use of disruptive technologies, such as AI, in the context of counter terrorism, cybercrime, cyberoperations, hybrid threats, and the online use of disinformation techniques. He leads the CyberPeace Institute with the aim of holding malicious actors to account for the harms they cause. His mission is to coordinate a collective response to decrease the frequency, impact, and scale of cyberattacks by sophisticated actors.

Prior to this position, Stéphane Duguin was a senior manager and innovation coordinator at Europol. He led key operational projects to counter both cybercrime and online terrorism, such as the European Cybercrime Centre (EC3), the Europol Innovation Lab, and the European Internet Referral Unit (EU IRU). He is a thought leader in digital transformation and convergence of disruptive technologies. With his work published in major media, his expertise is regularly sought in high-level panels where he focuses on the implementation of innovative responses to counter new criminal models and large-scale abuse of cyberspace.

This contribution, authored by Stéphane Duguin, Chief Executive Officer at CyberPeace Institute, was originally published by the World Economic Forum. The CyberPeace Institute is an independent non-governmental organization headquartered in Geneva.