WRITTEN BY

PAULA BABICOVÁ
Data Protection and Compliance Officer, Risk Manager
Dôvera

ROMAN VARGA
Cybersecurity Manager
Dôvera

DÔVERA

CYBER-SECURITY IN HEALTHCARE

AFFECTS EVERYONE

The saying that the riskiest link in cybersecurity is the human being holds true, whether it's an employee, contractor, or user. A single moment of inattention or ignorance can have a massive impact on an entire healthcare facility and its patients. This was recently evident in the experience of the Slovak Cadastre Authority and its clients.

Everyone—healthcare insurers, doctors, and patients—should take precautions to protect personal data, especially sensitive health information. In healthcare and cybersecurity, a patient's life is literally at stake. This makes it a critical, society-wide issue that deserves more attention, particularly in education.

HEALTHCARE AS A TREND

Global cybersecurity trends indicate that the healthcare industry is increasingly "under fire." The data targeted by attackers is highly valuable, as it is both sensitive and easy to sell. A well-executed attack on a healthcare facility can paralyze its operations and have devastating effects on patient health and safety.

The most common forms of attacks include so-called phishing attacks. Due to inattention or lack of education, the victim clicks on a link where they enter their login credentials, letting the attacker inside the systems. Alternatively, opening a malware-infected attachment can lead to data encryption. Add to that non-existent backup or the inability to restore the data, and the consequences, unlike in the case of the Cadastral Authority, can be tragic.

Imagine an attacker encrypting patient data, limiting medical professionals' access to vital records and affecting treatment. Worse yet, if data were altered, a patient might be given a drug they are allergic to or undergo surgery on the wrong part of their body. It doesn't matter whether it was an attack on a hospital or a practice. At the end of the day, the patient would suffer the most. Penalties for non-compliance with the appropriate security and technical measures set out in the GDPR would in turn "hurt" doctors and healthcare insurers.

> **Looking at the cyber literacy of doctors, there is no reason to cheer.**

EDUCATED PATIENT = EDUCATED PROVIDER

If we break down the responsibilities of the different actors into small pieces, and start with the patients, they should care about protecting their own data. Patients should approach doctors, specialists, and healthcare insurance companies if something feels off—like when their data is freely accessible in a practice—or push for updates if their health data is inaccurate. They should also stay informed, not just knowing but understanding the care they receive and the medications prescribed to them.

In the event of a successful attack and a missing data backup on the doctor's side, they will probably be the only ones to correctly reconstruct their own health data. They certainly should not freely distribute, publish, or send data about their health by unsecured email. Only secure (trusted) applications should be used.

Looking at the cyber literacy of doctors, there is no reason to cheer. In 2024, the health insurance company Dôvera in cooperation with the Slovak Medical Chamber (Lekar a.s.) and Eset spol. s r.o. conducted the first anonymous survey on the state of cybersecurity among physicians. Some of the responses were alarming, highlighting minimal interest in cybersecurity among practices. Hospitals, laboratories and maybe even pharmacy chains are a bit better off because they are obliged to comply with European regulations (NIS2 Directive) and the Cybersecurity Act, and have to have a cybersecurity manager and therefore invest in measures.

Cybersecurity is underestimated in practices and it is not perceived as a priority. Today, we already know that simply having antivirus software is not enough. An antimalware that covers all the necessary areas is also needed. Physical security must not be neglected either (securing paper documentation), all patient data must be adequately protected.

> **Key measures include the separation of a doctor's professional and private life.**

Key measures include the separation of a doctor's professional and private life. A doctor must not use the same email address for work and personal purposes. It is a mistake to share his/her access data (passwords) with staff. During cybersecurity webinars, we advise doctors to consult experts, just as they would rely on specialists in patient care. IT security should be managed by dedicated security professionals, not just outsourced to an IT company with no clear understanding of what systems are protected. We also recommend that doctors adopt the ten cybersecurity principles that we have developed and shared with them. Investment in relevant audits, finding out the real current situation and taking measures are also well-invested resources.

THE ROLE OF HEALTHCARE INSURERS

In the patient-doctor-healthcare insurer triangle, the position of the insurance company in the cybersecurity field is equally important. Healthcare insurers' obligations include being audited under the Cybersecurity Act and taking corrective action in a timely manner when there is partial compliance or non-compliance. The insurance company should continuously train its employees, including exercise (e.g. phishing) attacks. It should continuously improve its resilience and ideally build its own cyber 24/7 Security Operations Centre.

Other measures include investing in new technologies, so-called disaster recovery plans, regularly test them, and ensure adequate backups. Most importantly, cybersecurity must be a priority for health insurers, ingrained in the company's leadership and culture. Cybersecurity needs to be included in the priorities and budget of the health insurer and in the very DNA of the company's leadership. Management convinced of the importance of this topic is the driving force behind building the necessary resilience.