CyberProof®
A UST Company

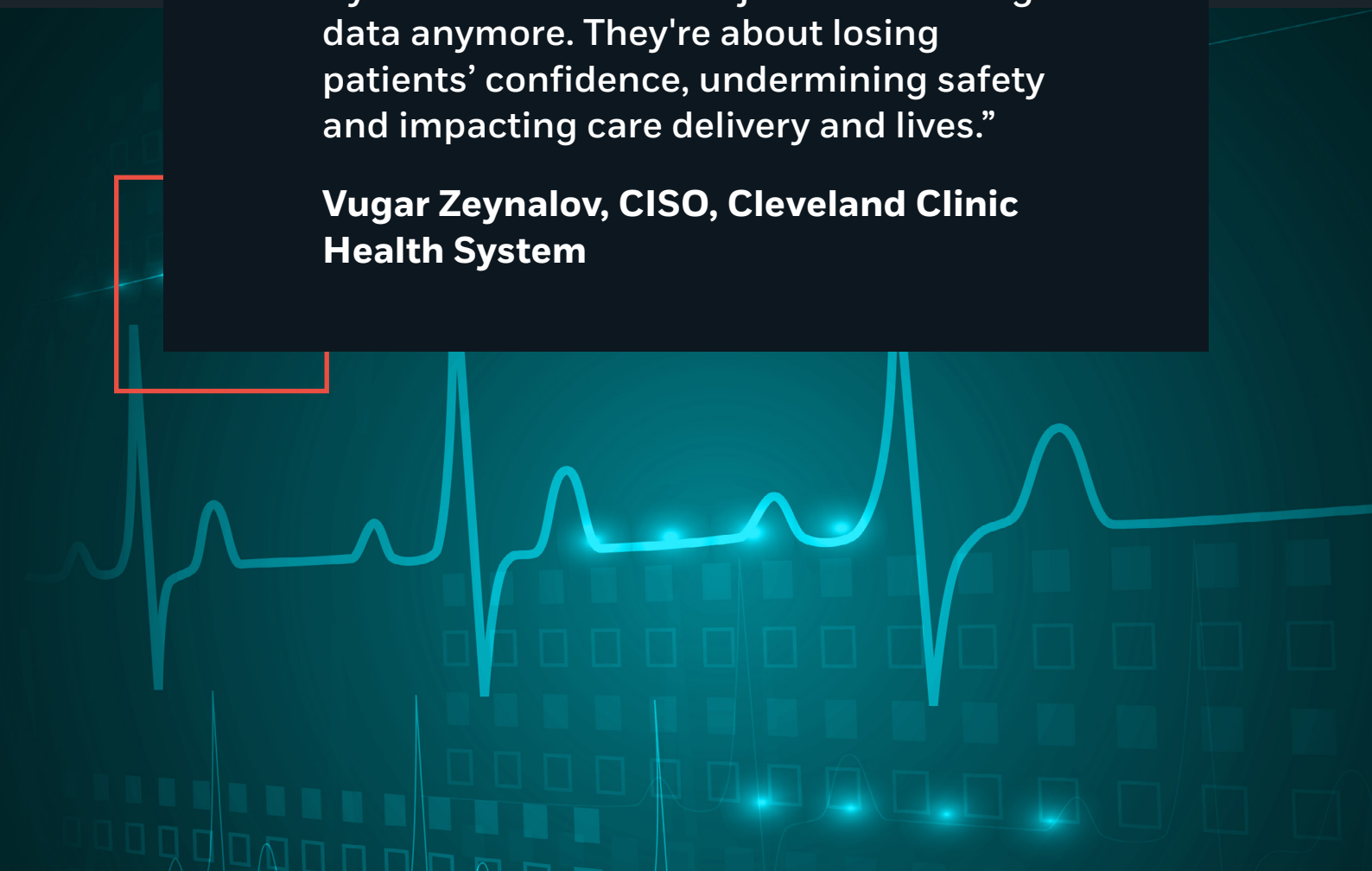
Better Security, Together.

The State of Healthcare Cyberattacks in 2024

6 devastating examples of the growing cybersecurity threat against Healthcare organizations

> Cyber incidents are not just about losing data anymore. They're about losing patients' confidence, undermining safety and impacting care delivery and lives."

Vugar Zeynalov, CISO, Cleveland Clinic Health System



1 Cost of the Change Healthcare Attack Due to Exceed $1.6B in 2024

Dubbed the most significant Healthcare cyber attack in history, Change Healthcare has attributed the attack to a failure to implement MFA on one of its systems.

What was the impact?

4TB of data stolen, with severe disruption to claims processing, e-payments, and invoicing systems that cost some healthcare providers $100M per day. 100 of United Health's services were taken offline entirely.

2 HCA Healthcare Breach Impacts 11M Individuals

In July 2023, the largest hospital system in the United States, HCA Healthcare, disclosed a breach that impacted 11 million individuals, a record breaking breach at the time.

What was the scope?

HCA includes 180 hospitals and 2,300 ambulatory sites nationwide. 11 million patients in 12 states were impacted. Approximately 27M rows of data was stolen, including patient names, addresses, DOB, and appointment details.

3 Over 100 Healthcare Systems in Romania Hit by a Cyberattack

In February 2024, Romania experienced one of the largest national Healthcare disruptions levied against a European Healthcare system.

What was the scope?

Cybercriminals encrypted data for ransom, and 25 hospitals and 79 healthcare organizations were taken offline due to the attack. Booking systems, access to patient records, and even the use of MRI machines were impacted.

4 3TB of NHS Scotland Data Stolen in a Targeted Attack

Over the course of 2024, the National Health Service in the UK has been the target of a number of cyberattacks, including a focused attack against NHS Dumfries and Galloway, a district with 150,000 patients.

How much data was exposed?

After initial access in March 2024, in May, a "proof pack" of data was leaked online. The group claims to have 3TB of data which includes sensitive information pertaining to thousands of patients.

5 Ascension's Ransomware Attack Impacts Senior Care

In May 2024, one of the largest private healthcare non-profits in the United States, Ascension, disclosed a ransomware attack. Ascension Health includes 140 hospitals and 40 senior living facilities across 19 states.

What was the impact?

Clinical operations were disrupted, including access to EHR systems, patient portals, phone systems, and the ordering of tests, procedures and medications.

6 More than 200 Cancer Surgeries Postponed Because of Synnovis' Ransomware Attack

In June 2024, pathology system provider Synnovis was hit by a ransomware attack by Russian hackers, Qilin.

What was the impact?

Within 48 hours, hundreds of life-saving and emergency surgeries were cancelled across six boroughs in the UK. GP services had to resort to pen and paper, as systems went offline. Just 10% of affected services were said to be working as usual.

Looking to protect your patients and their data, and prepare a ransomware readiness plan ahead of time? **Speak to one of our cybersecurity experts.**