JAN 27

Lisa Phillips

Healthcare cybersecurity in 2023: Hive's shutdown is good news but cyberattacks are only getting worse

Article

First, the good news: The notorious **Hive ransomware group** has been shut down following a months-long operation by the Federal Bureau of Investigation. The Hive network targeted more than 1,500 entities in 80 countries, including hospitals, school districts, and financial firms.

The bad news: Cyberattacks on healthcare organizations worldwide are getting worse, and they're not going away.

- Healthcare organizations across the world **averaged 1,463** cyberattacks ***per week*** in 2022, **up 74%** compared with 2021, according to Check Point Research.
- US healthcare entities suffered an average of **1,410 weekly cyberattacks** per organization, **up 86%** vs. 2021.

It's not your imagination: US healthcare organizations continue to be the most compromised by data breaches for the third year in a row, with 344 breaches in 2022, per the Identity Theft Resource Center (ITRC) 2022 Data Breach Report.

- Patients' medical history, condition, treatment, and diagnosis information were the most compromised data in those attacks.
- Medical insurance account numbers and medical provider accounts were also high on the list.
- Phishing and related ploys remain the top cyberattack vectors, followed by ransomware, per the ITRC.

Batten down the hatches in 2023: Russia's war in Ukraine distracted some Russia-based ransomware operators in the first half of 2022, the ITRC reported, but they got back to business in the second half of the year.

Even with the Hive network shut down, healthcare providers have **three major vulnerabilities to protect in 2023**, per Security Magazine.

1. Third-party vendors

Cybercriminals can exploit weaknesses more easily than within a health system. Hundreds of healthcare organizations were affected by a ransomware attack on PFC Financial Company, an account receivable management firm, in February 2022, per ITRC.

2. Cloud breaches

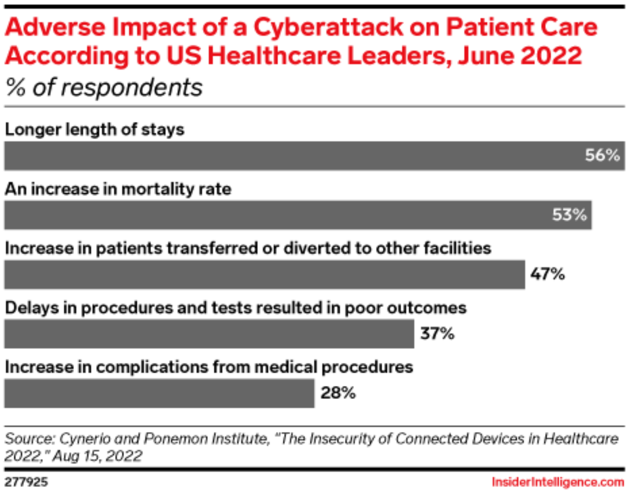
Cloud breaches are becoming more common, as 73% of healthcare companies store data in the cloud, per Netwirx Cloud Data Security Report.

- **61% of healthcare respondents experienced an attack on their cloud infrastructure** in 2022 via phishing, ransomware, or other malware attack.
- Most attacks were detected within minutes or hours, not days or weeks.

3. Internet of Things (IoT) attacks

53% of connected devices are at risk of a cybersecurity attack, per Cynerio's State of Healthcare IoT Device Security 2022 report.

- Most vulnerable are **IV pumps (38% of a hospital's IoT footprint)** and **VoIP systems (50%).**
- Weak or insecure passwords present the easiest opportunities for compromise.



Adverse Impact of a Cyberattack on Patient Care According to US Healthcare Leaders, June 2022

% of respondents

Source: Cynerio and Ponemon Institute, "The Insecurity of Connected Devices in Healthcare 2022," Aug 15, 2022

277925 InsiderIntelligence.com

This article originally appeared in Insider Intelligence's Digital Health Briefing—a daily recap of top stories reshaping the healthcare industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*