LevelB/ue

CYBERSECURITY IN HEALTHCARE:

The Diagnosis and the Antidote

As Healthcare Data Breaches Increase, What Does It Take to Stay Ahead of Threats?

Healthcare Organizations Need Security Solutions to Stay Ahead of the Targeted Threats

40M

Nearly **40M health records** breached or stolen in 2022

US HHS OCR Breach Portal Data

Why?

- Expanded attack surface
- Lack of cybersecurity staff and budget
- Lack of data inventory (knowing what kind of data we have and where)
- Lack of data classification (e.g., PHI, PII, IP, etc.)

$10.93M

The average cost of a data breach in healthcare **continues to increase**.

2023 IBM & Ponemon Institute Report

13 Years

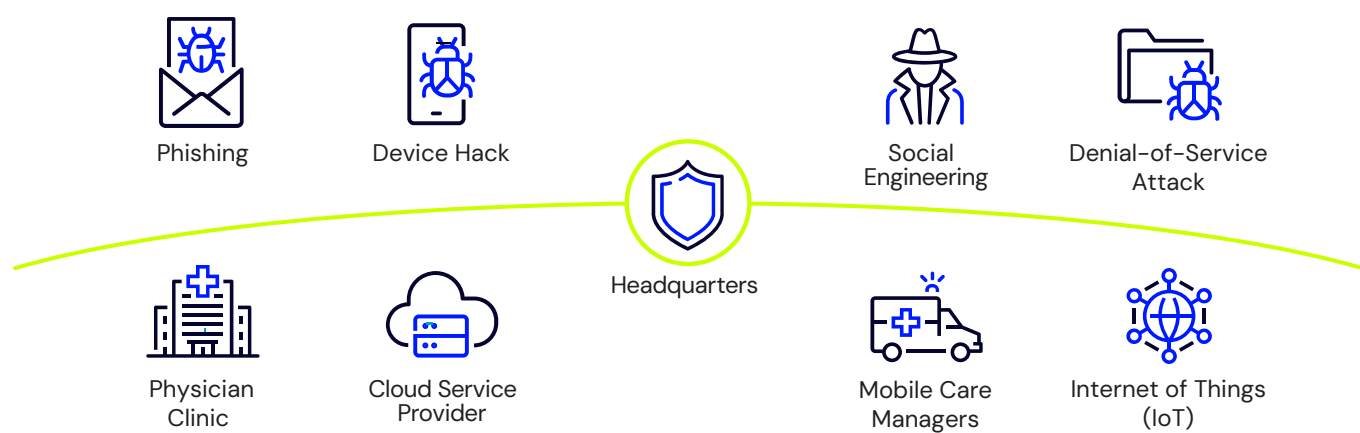Healthcare has had the highest industry cost of a breach for **13 consecutive years**.

2023 IBM & Ponemon Institute Report

53.3%

Since 2020, healthcare data **breach costs have increased 53.3%**.

2023 IBM & Ponemon Institute Report

These 4 Key Steps Can Help Your Healthcare Organization Reduce Cyber Risk with a More Business-Driven Approach:

1 Take a risk-based approach to security

2 Timely detection to help minimize the impact of data breaches

3 Effective vulnerability management

4 A well-formed incident response team and plan to help withstand a data breach

Secure Patient Data and Improve Patient Care

Phishing

Device Hack

Headquarters

Social Engineering

Denial-of-Service Attack

Physician Clinic

Cloud Service Provider

Mobile Care Managers

Internet of Things (IoT)

Secure Patient Data

CURRENT HEALTHCARE CHALLENGES	LEVELBLUE SECURITY SOLUTIONS
Adoption of healthcare industry–specific standard of HITRUST Common Security Framework (CSF)	• HITRUST CSF workshops, readiness, remediation, and validated assessments with certification
Security awareness training	• Security awareness training • Social engineering / phishing
Proactive incident response reporting processes	• Incident response tabletop exercise • Incident response retainer • Pre and Post Breach Services
Achieve and sustain compliance with HIPAA/HITECH regulations	• HIPAA/HITECH compliance assessment • Healthcare risk assessments • Compliance as a Service
Manage patient data in a highly secure manner	• SASE solutions • Zero Trust • Vulnerability, Threat and Fraud Management
Optimize security efforts for third-party vendors	• Third-party risk management
Protect healthcare operations	• MDR • Cyber SOC Design and Build • DDoS defense
Emerging technology and innovation	• Cloud security, OT Security • Emerging Technology Risk and Innovation Strategy

About LevelBlue

LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

To learn more about LevelBlue Cybersecurity Consulting, visit <u>LevelBlue.com</u>.