Cybersecurity Essentials for Healthcare and Financial Systems

GM sectec | DataPreserve powered by Metallic®

What is your cybersecurity program missing?

The healthcare industry is a profitable target for malicious actors.

What proven practices and ransomware strategies can strengthen cyber defenses to minimize impact to patient health, revenue streams and institutional reputation?

Ensure operational resiliency with tested rapid data and file recovery

- Information backup and recovery for restoring operations must be continual, programmed, rapid, complete (100%), tested/retested, and institutional-wide.
- Cybersecurity hygiene demands continually 1) knowing all information assets, 2) what is on those assets, and 3) sensitive and confidential data is classified, protected, and backed up.
- Business continuity requires simulating how to maintain essential operations without IT, manually sustaining processes in disconnected ways to minimize impact to patient healthcare services.

Protect patient and institutional data backup integrity

- Secure backup data and files should employ a non-porous defense with air gapping, data isolation, anomaly detection and immutability (meaning a process, user or service account cannot delete, change, move backups).
- Backup systems should have 24x7 security monitoring, detection, and response with attack simulations to confirm defenses are operational and attacks being detected and blocked.
- Backed-up data and files should follow the 3-2-1 Rule - 3: Create one primary backup and two copies of your data. 2: Save your backups to two different types of media. 1: Keep at least one backup file offsite.

Commit to stringent information security policies and metrics

- Establishing measurable metrics is a Top 3 Essential Practice
- Tested Recovery Point & Time Objectives for backups
- Continual Asset and Data Inventory (99%) and Discovery
- Evaluating internal resource capabilities and limitations and measuring internal operational utility.
- Enforcing strict policy and review of SLAs, SOWs, metrics, and reporting for internal and external resources and services.
- Metrics matter for State Privacy, HIPAA Security Rule, GDPR which have consequences, along with HIPAA, HiTrust, FDA, ISO, SOC, and PCI compliance.

Looking to improve your backup and recovery capabilities?

GM Sectec's MSSP program offers Data Preserve—data protection as a Service, powered by Metallic. This managed security service deploys enterprise-wide backup and recovery services, establishes and tests recovery objectives and priorities, and monitors operational health and cybersecurity.

In 2021:

- 50 million patient records compromised
- 900+ annual reported security incidents[1]

- Attack surfaces focus on maximum impact and disruption, prioritizing payment and CRM systems, medical devices, and business associates.
- Attack vectors are well-researched spearfishing and highly engineered DDoS attacks.
- Attack techniques include sophisticated, dynamic ransomware variants with multiple extortion levels.

Source:

[1] Protenus, "2022 Protenus Breach Barometer," 2022 https://www.protenus.com/breach-barometer-report