MEDITOLOGY SERVICES

NAVIGATING CYBERSECURITY LANDMINES IN HEALTHCARE

WARNING MINES

There are many cybersecurity landmines that health systems must navigate in 2021.

- **46% of the breaches** in healthcare were caused by ransomware attacks[1]
- **Supply chain attacks** like SolarWinds and Blackbaud breaches have unprecedented scale
- **Regulators are moving the goal posts** including HIPAA, HITECH, CMS, OCR, and state regulations
- **Class action lawsuits** have become the norm
- **Cybersecurity incidents** are now being linked to patient safety adverse outcomes
- **Cloud attacks and hacking** have become the dominant source of breaches
- **Global cybercriminals** are reaping major profits from exploiting healthcare entities
- **IoT and medical devices remain frail** and vulnerable to attack
- **Remote workforce and telehealth** are extending the healthcare attack surface
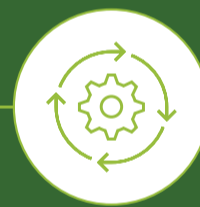
TAKE THE FOLLOWING MEASURES TO REDUCE THE POTENTIAL FOR CYBER BLOW UPS THIS YEAR:

ASSESS

Perform annual enterprise-wide security risk assessments

Adopt frameworks like NIST and HITRUST

Perform routine penetration tests

MANAGE THIRD-PARTY RISK

Mature your vendor risk management program

Assess supply chain risks across your entire vendor portfolio

Invest in outsourced support and automation from solutions like CORL Technologies

MAINTAIN COMPLIANCE

Document your risk analysis

Implement controls aligned with HIPAA

Maintain a risk register

Pay attention to major regulatory shifts underway for HIPAA, HITECH, CMS, OCR, and state regulations

Adopt new HIPAA safe harbor protections

PREPARE

Update incident response plans and test them often

Focus on ransomware simulations, phishing, and cloud hacking attacks

Expect and prepare for class action lawsuits

Invest in automation of security controls that can help you scale to respond to attacks yet to come

[1] Tenable Research 2020 Threat Landscape Retrospective

MEDITOLOGY SERVICES

info@meditologyservices.com
MEDITOLOGYSERVICES.COM