MEDITOLOGY
SERVICES

TOP 10 HEALTHCARE CYBERSECURITY PREDICTIONS FOR 2023

Meditology supports hundreds of healthcare entities across the country. We have compiled the top cyber risk trends for 2023 to help you map out your defensive strategy heading into the new year.

TOP 10 HEALTHCARE CYBERSECURITY PREDICTIONS FOR 2023

1 **RANSOMWARE ATTACKS** increase and impact patient safety, operational disruption, and financial performance for healthcare entities

2 **HEALTHCARE VENDOR BREACHES** increase in frequency, cost, and severity as cyber criminals target healthcare and clinical delivery moves into patient homes via third-party solution providers

3 **CLOUD-HOSTED PLATFORMS** become the primary custodians of electronic patient information and cloud misconfigurations remain a top source of data breaches

4 **BOARDS INCREASE FOCUS AND INVESTMENT** on third-party cybersecurity risk management as awareness of the HCO's dependence on vendors for critical business operations grows and breach events escalate

5 **NEW INDUSTRY STANDARDS AND GUIDANCE** establish baseline expectations for healthcare cybersecurity programs and enforcement (e.g., OCR's Recognized Security Practices and CISA's Cybersecurity Performance Goals)

6 **FEDERAL AND STATE GOVERNMENTS TARGET HEALTHCARE CYBERSECURITY** with new laws and ramped-up enforcement that build off the newly established baseline expectations for healthcare and Critical Infrastructure cybersecurity

7 **REMOTE AND HYBRID WORKFORCE BECOMES PERMANENT** and as a result, cybersecurity programs adopt more restrictive "zero trust" models for remote work models

8 **ATTACKERS ACCELERATE TARGETING OF MEDICAL DEVICE, IOT, AND OT** security gaps, which introduces unprecedented risks to patient safety and business operations

9 **LEGAL ACCOUNTABILITY MOUNTS** as class action lawsuits increase in frequency and put financial pressure on healthcare organizations to bolster cybersecurity defenses

10 **CYBERSECURITY TALENT SHORTAGES** intensify as demand grows for specialized skills sets and more organizations turn to managed services to deliver security programs

HONORABLE MENTIONS

The following cybersecurity and risk trends in healthcare did not quite make the top ten list but are still worth keeping on your radar heading into the new year.

1 **The false perception of cyber liability insurance as a silver bullet wanes** as insurers raise premiums, limit coverage levels, and decline some claims. HCOs realize that insurance is an important line of defense in a mature security program, but not the only line of defense

2 **Cyber resilience capabilities** including incident response and disaster recovery become a focal point for investment for healthcare entities

3 **Fourth-party risks and vulnerabilities** escalate and drive maturity in vendor inventory tracking via Software Bill of Materials (SBOMs) and related models

4 **Cybersecurity certification adoption** increases as pressure mounts for healthcare organizations to demonstrate strong security programs

5 **Leading-edge cyberattacks** including deepfake technology, MFA bypass attacks, and quantum encryption attacks begin to emerge and set the stage for the next decade of cybersecurity risks

6 **Continual risk management and compliance** models emerge and replace many of the traditional annual or periodic security assessment and mitigation approaches

7 **Cyber risk analytics and reporting** elevate the cybersecurity conversation from one that is deeply technical and confusing to one that is more easily understood by business and clinical leaders

*Meditology Services is a top-ranked cybersecurity, privacy, and risk consulting firm dedicated to the healthcare industry. **Contact us** to learn more about how we can support you and your program in 2023.*

MEDITOLOGY
SERVICES

info@meditologyservices.com
MEDITOLOGYSERVICES.COM