MEDITOLOGY SERVICES

THE SECRET SAUCE
FOR CYBERSECURITY INCIDENT RESPONSE

Cybersecurity incidents in healthcare can impact patient safety, system availability & uptime, revenue generation, and regulatory compliance.

Meditology reveals their recipe for the secret sauce required to cook up an effective incident response program for healthcare entities.

WHY YOU NEED A RECIPE

Healthcare entities must understand the targeted investments in incident response capabilities required to limit the damage from the onslaught of escalating attacks.

Ingredients	Instructions
$7.13M	the average cost of a breach for healthcare entities[1]
$20.8B	the cost of ransomware attacks on US healthcare organizations in 2020[2]
329 DAYS	the average time to identify and contain a breach for healthcare[1]
24%	of all cybersecurity breaches in 2020 were in healthcare (the highest of all industry segments)[3]
46%	of the breaches in healthcare were caused by ransomware attacks[3]

PREPARATION & PROGRAM DEVELOPMENT

DEVELOP
a comprehensive incident response Plan and make sure it is aligned with the latest threat scenarios, including ransomware

DEVELOP
and train your security incident response team

GET
your cyberliability insurance in place and understand what it does and does not cover

IDENTIFY AND DEVELOP
contacts with your local law enforcement entities and the FBI

MAINTAIN
a contact list for critical parties, including internal resources and third-party vendors

INVOLVE THE BUSINESS
Incident response is not just for security teams. Make sure all stakeholders know the plan and their associated roles

DEFINE
escalation points for when to involve the business in decision making

ENGAGE
a forensics and breach investigation firm on retainer

DEVELOP AND MAINTAIN
downtime procedures at the department level

INVEST
in risk assessments and remediation to understand potential gaps in security control effectiveness, particularly for backups and recovery & vulnerability management

TABLETOP EXERCISES

- Tabletop exercises are the most effective way for an organization to test their incident response capabilities
- Tabletops are also less traumatic for the team because they do not involve working on live productive systems
- Discuss the roles that each team member of the Security Information Response Team will have during an incident
- Review the incident response plan and available tools & capabilities in a safe and academic setting
- Practice routine downtime and continuity exercises in addition to administrative, IT, and security tabletops
- Involve third-party vendors in the exercise and have them on the phone/video for the exercise

INCIDENT RESPONSE SCENARIOS

- Ransomware events are the most critical scenarios right now
- Conduct scenarios for incidents deriving from or involving key third-party vendors and solution providers
- Consider separate sessions for senior leadership versus IT and Security Incident Response Teams
- Scale up or down the level of detail and decision points depending on the stakeholders involved
- Discuss business-level decisions including scenarios for operational impacts like diverting patients to other healthcare providers or shutting down key systems
- Consider scenarios where medical devices become impacted, unavailable, or malfunction
- Include scenarios where common communication platforms like email become unavailable

COMMON MISTAKES

- Don't assume that handling routine small scale incidents will prepare you for a large scale, complex incident
- Maintain offline copies of incident response plans in the event that computer systems may be unavailable
- Have a single source of incident response documentation; don't have everything spread out across dozens of disparate documents
- Don't assume that third-party vendors experiencing a breach will be responsive to your questions or transparent about incident details; develop a response plan that is independent of vendor dependencies
- An incident response policy is not the same as an incident response plan
- Involve your media and public relations teams in testing to be able to anticipate common breach scenarios and approaches for communicating with the public and the media
- Don't forget that HIPAA regulations require incident response planning and testing

WHAT OUR CLIENTS ARE SAYING

The two tabletop exercises were phenomenal, we had positive feedback, and we had conversations on lessons learned. And we continued to have conversations; it didn't just end at tabletop – people would see things in the news and reach out to me and that sparked a dialogue, that was very valuable.

– Chief Technology and Security Officer, Premier Pediatric Health System

★★★★★

Meditology's tabletop exercises were of exceptional value. I trusted Meditology based on my prior history with the Firm. The knowledge and communication the team brings is second to none. I wanted my C-levels to see the value Meditology brings and the interaction, and they all thought Meditology brought industry-specific knowledge and were appreciative of the multiple sessions to get the content of the tabletop exercises right. Those sessions were joined by Meditology leadership, which spoke volumes to our leadership.

– Senior Manager, Information Assurance, Ivy League Academic Medical Center

★★★★★

Learn more in our CyberPHIx interview with Meditology Services Partner Nadia Fahim-Koster: People Get Ready: Cyber Incidents are Coming

LISTEN IN

Contact our team at Meditology for more information and guidance to support your risk management and incident response program.

CONTACT US

Ranked #1 Best in KLAS for Cybersecurity Advisory Services in 2019 and 2020, Meditology Services and Meditology Assurance are leading providers of information risk management, cybersecurity, privacy, and regulatory compliance consulting services, exclusively for healthcare organizations.

[1]Cost of a Data Breach Report 2020
[2]Ransomware attacks on US healthcare organizations cost $20.8bn in 2020
[3]TLDR: The Tenable Research 2020 Threat Landscape Retrospective

MEDITOLOGY SERVICES
info@meditologyservices.com
MEDITOLOGYSERVICES.COM