RSA

A 4-STEP APPROACH TO

MITIGATING CYBER ATTACK RISK IN HEALTHCARE

CYBER RISK AFFECTS PATIENTS AND MEDICAL PROFESSIONALS ALIKE

Connecting Security, Risk and Healthcare Teams to Mitigate Cyber Attack Risk

Cyber threats, particularly ransomware, are the number-one digital risk for healthcare entities and their third-party business associates. Cybercriminals are attracted by high-value protected health information (PHI); ease of access through a plethora of unsecured IoMT (internet of medical things) devices; and the rapid growth of information in complex, interconnected medical ecosystems. To provide some context, the volume of healthcare data has grown by an astounding 878% over the last two years[1]—a period in which a startling 90% of healthcare organizations suffered some sort of cyber attack.[2]

To prevent such attacks, healthcare organizations continue to invest in security technology. Yet the reality is that, no matter how hard we try, not every cyber attack can be prevented. However, healthcare organizations should still strive to improve their processes to manage cyber attack risk, because it's not just information but actual lives at stake.

THERE'S MORE TO RESPONSE THAN JUST CONTAINING THE ATTACK

When it comes to detecting cyber attacks and containing or neutralizing threats, your security team is on the front lines. And while a technical response is essential to protecting the organization and its assets, at many healthcare organizations, this is where the response stops.

While an incident may show up in an executive briefing, the rest of the organization may not have visibility into:

To mitigate the risk of cyber threats and reduce the real impact on people, healthcare organizations need to become more proactive, improving their risk management capabilities. They must also become more transparent about both attacks and plans for mitigating future events. Due to regulations such as the HIPAA breach notification, cross-functional teams have greater responsibility for notifying individual victims, media, and regulators about security incidents.

This dynamic requires security, risk management, healthcare teams and their business associates to work together to prepare for attacks, reduce their impact on patients and the larger healthcare ecosystem, and ensure the organization can be resilient and continue to deliver on its mission.

A 4-STEP APPROACH TO MITIGATE RISK

Even with the best preventative measures, it's impossible to eliminate cyber attacks entirely. And when they do happen, you need to be ready. To coordinate response by your organization's security, IT, and risk management teams, along with your business associates, follow these four steps:

STEP 1: PLAN FOR ATTACKS

STEP 2: DETECT SECURITY THREATS

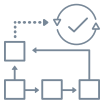
STEP 3: ASSESS THE IMPACT

STEP 4: RESPOND TO THE RISK

STEP 1:
PLAN FOR ATTACKS

HIPAA requires covered entities to have policies related to breach response and notification. But policies should go beyond that, including cyber incident response plans with steps for investigation, remediation, and response. Plans should consider factors including the organization's capabilities, established risk tolerance, and complexity of the healthcare delivery model—which includes reliance on business partners. Together, these policies and rehearsed plans make up a repeatable, cross-functional process that can improve communication, coordination and consistency.

TO PLAN FOR ATTACKS:



Create workflows to manage investigations, and correlate indicators of compromise (IOCs) across the organization.

Establish a central IT asset catalog and common taxonomy, so all critical IT assets are accounted for and their criticality to the organization is understood. Grant access to systems and data.

Document incident response processes that include critical business functions—such as compliance, public and stakeholder relations, internal communications and general counsel—so everyone understands their roles and responsibilities. Also, automatically enforce proper access to online resources by patients, providers and staff.

Regularly test incident response capabilities at individual and organizationwide response levels.

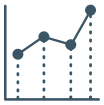
STEP 2: DETECT SECURITY THREATS

To cut through alert clutter and better detect cyber threats, you need a security platform that provides visibility across all environments. To streamline forensic investigation and quickly identify the full scope of an attack, make sure your platform can gather insights from across your IT footprint.

TO EFFECTIVELY DETECT THREATS, YOU NEED:

VISIBILITY

Across logs, network, medical devices and other endpoints (IoMT), gateways and hosts to detect, prioritize and investigate threats



DEEP, ADVANCED ANALYTICS

Including user and entity behavior analytics (UEBA) to rapidly detect anomalies in users' behavior and uncover unknown, abnormal and complex evolving threats

BUSINESS CONTEXT

Including contextual intelligence and data criticality to help prioritize alerts and drive response based on the potential impact to organizations

INCIDENT MANAGEMENT

Including orchestration and automation to make analysts more effective with automation detection and response actions

ACTIONABLE INSIGHTS

Including access and entitlement intelligence, fraud intelligence, threat intelligence and known vulnerabilities to support forensic investigations and determine the full scope of an incidents

STEP 3:
ASSESS THE IMPACT

Security teams typically focus on identifying the scope and technical severity of an incident but may lack the ability to quickly assess its impact on areas such as patient privacy. Giving security teams business and risk context helps them prioritize and orchestrate appropriate responses based on potential business and patient impact.

TO ASSESS THE IMPACT OF AN INCIDENT:

Educate responders about business criticalities within the organization—such as business divisions, products, systems and data—to help them better understand business impact and prioritize accordingly.

Integrate impact analysis into investigations, to help responders understand upstream and downstream relationships and implications.

Conduct cyber risk quantification, to understand the business consequences of attacks on critical financial and medical data.

Incorporate known vulnerability data into investigations. When analysts understand which assets and data types are most vulnerable, they can better prioritize remediation efforts.

STEP 4:
RESPOND TO THE RISK

Centralize incident management both inside and outside the SOC, to ensure a consistent, coordinated and—whenever possible—automated response. This gives stakeholders a clearer understanding of the process, ownership and accountability for each step; how to better mitigate the risk that attacks pose to the organization; and what will be done to address the threat.

	TECHNICAL RESPONSE	ORGANIZATIONAL RESPONSE
INCIDENT: Rapid, Organized Response	Detect and declare incident Identify affected areas Trigger clear, process-oriented escalations Automate and orchestrate to reduce dwell time and contain the threat	Declare incident, automatically invoking organizational response workflows Ensure that business processes are resilient Engage cross-functional teams based on established workflows • Compliance • Legal • Communications • PR
POST-INCIDENT: Address Vulnerability Gaps	Perform forensic analysis Locate assets, applications and protocols for data exfiltration Make security changes	Understand need for new controls or process changes (root cause for systemic issues) Communicate priority and direction to ensure that most valuable and sensitive PHI is protected Use closed-loop process to ensure change management

RSA HELPS YOU MITIGATE ORGANIZATIONAL RISK FROM A CYBER ATTACK

RSA provides an end-to-end solution that combines holistic threat detection with coordinated, cross-functional response. It connects security, risk and business stakeholders and provides advanced capabilities for measuring and mitigating the organizational impact of a cyber attack. With RSA, you get hands-on advisory services to help you assess and mature your organization's ability to detect and respond to a cyber attack.

THE CHALLENGES

The healthcare industry's move to electronic health records has created new patient privacy exposures as records are more easily accessed by consultants, vendors and other third parties for efficient operation, and targeted by cyber criminals.

The organization does not know or control who has access to its systems and data.

The healthcare organization doesn't always know soon enough if their systems and data have been breached.

If a breach does occur, the organization does not know what occurred; how bad it was; what and who were potentially impacted; what was done to stop it; or how are they preventing it from happening again.

HOW RSA CAN HELP

Understand and assess your organization's ability to deal with cyber threats to your healthcare systems and patient data.

RSA RISK & CYBER SECURITY PRACTICE

Improve your ability to detect and respond to cyber threats quickly and efficiently across your systems.

RSA NETWITNESS® PLATFORM

Reduce your risk of external attacks and insider threats with modern, mobile multi-factor authentication; real-time detection of suspicious access and entitlements; and automated, risk-based identity governance controls.

RSA SECURID® SUITE

Detect and respond to fraud threats in your patient-facing digital channels with a combination of actionable fraud intelligence, real-time behavioral analytics and risk-based adaptive authentication.

RSA FRAUD & RISK INTELLIGENCE SUITE

Provide organizational context and coordinate the response and minimize the impact of security incidents to your healthcare organization.

RSA ARCHER® SUITE

Are you prepared to mitigate the risk to your patients and healthcare delivery system from cyber attacks? Take our online assessment to see how you stack up, at **riskassessment.rsa.com**.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

1. Fred Donovan, "Organizations See 878% Health Data Growth Rate Since 2016," *HIT Infrastructure*, May 8, 2019.
2. Dell EMC, *Security Transformation in Healthcare*, September 2017.

RSA®