Clearwater

Whitepaper

Advancing Enterprise Cyber Risk Management with Executive Engagement

How Sentara Healthcare Made Cyber Risk Management an Enterprise Initiative

Table of Contents

Introduction

While cyberattacks, in general, are increasing across a range of industries, healthcare remains front-and-center for attackers, especially in light of changing environments spurred by the coronavirus pandemic and the push for new technologies to better facilitate patient engagements and services delivery.

While innovation may be much needed, hospitals and health systems that push off cyber risk management to IT departments without looking at the bigger business impact and risk are likely to stay behind the eight ball, and as a result, may unintentionally give attackers an advantage where they already have a head start against most information security teams.

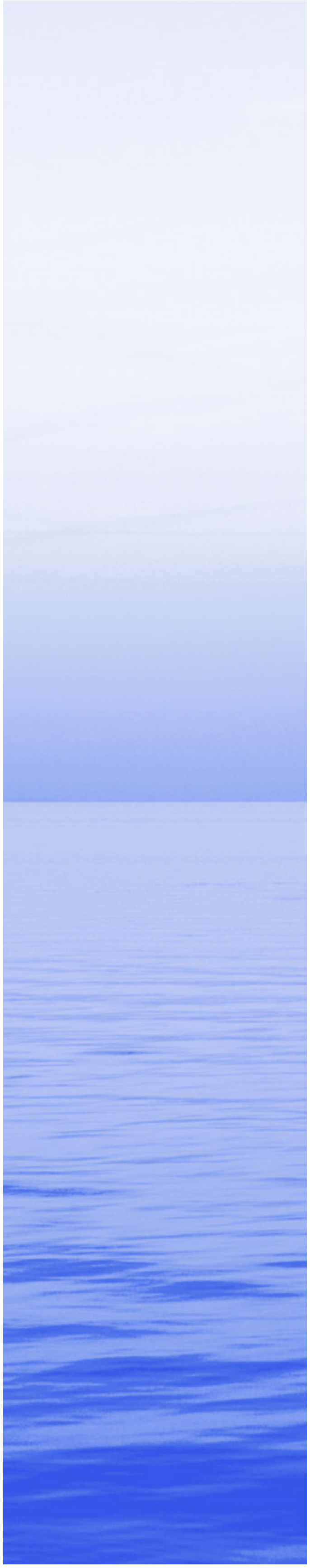
With risks this great, why do some organizations still look at cyber risk management as a siloed, departmental function of the IT team? That's because far too many executives and key stakeholders see enterprise cyber risk management (ECRM) as a technical function, not a strategic imperative that makes the organization more resilient overall.

While your IT team members play a critical role in identifying and mitigating cyber risks, cyber risk management is an issue that has increasingly greater impact on the organization as a whole, where one misstep from an out-of-the-loop team member may have cascading negative, potentially even devastating, effects on the entire organization and patient safety, too.

Here are a few examples of how a single breach within an organization with a disconnected ECRM/business strategy could negatively impact that organization:

- A crippling ransomware attack could lead to patient harm, even death
- A data breach incident could damage reputation and cause business loss
- A compliance violation could lead to lawsuits, settlements, penalties, corrective action plans and other consequences including severe financial impacts

These examples are just a few of many that highlight why ECRM is a business risk issue and not just a technical problem for IT. So if you don't already have an ECRM program in place or your program is immature, how do you take it to the next level and better manage your risks?



The average cost of a data breach in the U.S. is almost $4 million and it takes about 280 days on average for organizations to discover and contain a single breach. Healthcare, unfortunately, spends the most on mitigation, remediation, and recovery, topping other industries at more than $7 million. For organizations without a mature ECRM program, these gaps and risks may exponentially increase, not just in terms of financial costs, but in impact on its people, processes, and reputation.

It starts with a roadmap to executive engagement—one that leads your executives away from the technical sticking points of cyber risk management and into a journey that guides business risk engagement.

Meeting ECRM challenges head-on

ECRM is fret with challenges, but those challenges don't have to be program fail points. Teams that effectively overcome these challenges are better poised for ECRM success. That's why it's important, before you step onto your ECRM path, that you understand what some of these challenges look like so you can assemble the right tools to mitigate them into merely speed bumps and not program derailment.

ECRM success begins with getting executive buy-in about why the program is valuable, the benefits of active involvement in cyber risk management governance, and expectation of roles and tasks related to executive leadership participation so together you can overcome common obstacles that negatively impact your resiliency.

Here's a quick look into five common challenges hospitals and health systems encounter with ECRM and how you can address them:

1. Get the board on board with cyber risk as a business risk

Challenge: One of the most obvious—and maybe biggest—challenges of building an effective enterprise cyber risk management program is getting your key stakeholders to understand exactly how and why cyber risk is a real business risk for operational resiliency.

Solution: Share real-world examples of how cyber incidents have affected peers in the healthcare industry. Share information about how the attack occurred, how many records were affected, outline the compliance and regulatory ramifications, and summarize it with a financial impact. You can find a list of current breaches, as well as a historical perspective, from the Office for Civil Rights (OCR). The OCR cases focus on HIPAA violations, but you can use them as a starting point to research the broader impact of peer incidents.

2. Break down technical barriers

Challenge: Cyber risk management and all the tools and resources needed to discover, quantify, prioritize, and remediate risks are complicated and you need specialized skills to understand them. As such, your executives and board members may feel intimidated by all the technical jargon and will pull back, leaving it to your IT team to deal with it.

Solution: The key here is to speak the same language as your key stakeholders. It's not about the details – for example, all the technical steps you need to take to find and fix a risk; it's about the bigger picture. You can overcome this challenge by creating higher-level reports and presentations that quantify the risks with business impact and how they affect organizational goals, planning, and objectives. Look for metrics that are specific, meaningful, and memorable. This will give your leadership team a foundation for understanding ECRM issues today and their impact over time.

3. Shore-up incomplete programs

Challenge: If your ECRM program is missing key elements, your board may see it as underdeveloped and will be challenged to understand its potential and value.

Solution: Before engaging with your key stakeholders, be sure you've established a solid ECRM framework, one that includes governance, people, processes, technologies, and enterprise-wide engagement.

4. Understand resource gaps

Challenge: In some organizations, executives remain so disconnected from day-to-day activities, they can't see the impact of limited resources on organizational security and resiliency.

Solution: Clearly outline resource challenges at the get-go, especially related to people, processes, and technologies, and share a game plan to address those challenges, while highlighting program impact if they're not addressed. For example:

- People: There is a lack of available skilled cybersecurity professionals across all industries, so even if you're given flexibility to hire the right positions, you may struggle finding people to fill them. Could you work with an advisor, contractor, or managed services provider instead?
- Processes: Many organizations, especially as they scale, have disparate and unclear processes, and far too often, many of these processes rely on tedious, manual and repetitive tasks. Could you facilitate process improvements by employing a cyber risk management solution that automates tasks and provides clear, comprehensive insight into all enterprise risks and resolutions?
- Tech: Many organizations are tech-innovation adverse. That's because finding a new solution can be time-consuming and expensive, and there are additional challenges getting team members to adopt new tech. Instead, roadmap your tech needs before you start a buyer's journey. Understand your ECRM program goals, as well as your business goals, and look for a solution that will give you the metrics you need–from a big picture to a granular level—so you can communicate with both your IT professionals responsible for tasks, but also upward to executives.

5. Build longevity

Challenge: Getting your executives and board members to buy-in that ECRM is a program and long-term strategy, not one-and-done activities.

Solution: Remind your stakeholders that ECRM is an ongoing program, one that continually evolves and changes. As your organization scales and your threat landscape changes with it, you'll need ECRM practices that address all those changes, continuously evaluates your risks, and evolves as your organization's business risks and risk tolerance levels change too. Remind leadership that every aspect of ECRM is continuously evolving: your threat landscape is constantly changing, the information asset inventory changes as your organization brings on new systems and new lines of business, and your organization's position on risk tolerance may evolve as you secure high risk assets and more resources become available.

Real-world ECRM engagement

Based in Norfolk, Virginia, Sentara Healthcare is an integrated nonprofit with 12 hospitals in Virginia and North Carolina. Across all of its facilities, Sentara has more than 28,000 employees and 3,800 provider medical staff, as well as a Level I trauma center, the Sentara Heart Hospital and the Sentara Healthcare Cardiovascular Research Institute, the Sentara Brock Cancer Center and the accredited Sentara Cancer Network, two orthopedic hospitals, and the Sentara Neurosciences Institute.

The Sentara family includes four medical groups, Nightingale Regional Air Ambulance and ground medical transport, home care and hospice, ambulatory outpatient campuses, advanced imaging and diagnostic centers, a clinically integrated network, the Sentara College of Health Sciences and the Optima Health Plan and Virginia Premier Health Plan, which serves 858,000 members in Virginia, North Carolina, and Ohio.

Sentara continually demonstrates its commitment to data security and privacy as an innovative organization that embraces technology to deliver high quality services to its constituents and to support its healthcare teams. In 2020, for example, IDG's CIO 100 recognized Sentara for operational and strategic excellence in information technology, specifically for cross-industry work with cloud-hosted application design, support, and cost optimization.

One area where Sentara continues to shine is in developing and maturing its ECRM program and building executive engagement. To support that initiative, the organization partnered with Clearwater to get more visibility into its cybersecurity risks—across its expansive enterprise—so it can more effectively prioritize remediation for those risks while meeting regulatory and compliance mandates.

Unlike other organizations where teams view cyber risk management as a responsibility that falls solely on the IT department, Sentara understands that cyber risk management is a broader business risk and is working to build a culture where all team members understand how a single incident could harm the organization, including:

- Reputational damage
- Legal consequences (including class action lawsuits)
- Compliance issues

Financial consequences such as fines, fees, penalties, resolution agreements, corrective action plans

While executives and key stakeholders, for example, board members, are generally responsible for business risk management, at this level in many organizations there is often a disconnect with understanding the role cyber risk management plays in assessing and mitigating business risks. That's why Sentara made a commitment to closing that communication gap and empowering its leadership team to become more fully engaged in ECRM, integrating a lexicon that embraces organizational language and culture, while enhancing five critical ECRM capabilities:

1. Governance
2. People
3. Process
4. Technology
5. Engagement

Sentara challenges

Earlier, we discussed common challenges that can derail an ECRM program. Now, let's take a closer look some of Sentara's priorities that Chief Information Security Officer Dan Bowden believes were critical for program success:

Priority 1: Get ECRM on the board and C-suite agenda

ECRM should be a regular agenda item for your executive and board conversations and it's important to build ECRM discussions across all tiers of leadership with a goal of creating a formal governance structure.

Priority 2: Talk about cyber risk in a way that directly aligns it with business-impacting risk

Pointing out impacts of cyber events at peer organizations gives executives real-world insight into what could happen if your organization doesn't invest in—and mature—your ECRM program.

Priority 3: Educate the board and C-suite about foundational cyber risk management concepts

Board members don't need a deep technical understanding of cyber risks, but they should understand basic cyber risk management concepts, for example, the differences between an asset, a threat, and a vulnerability. They should also understand the concepts such as likelihood and impact, which affect risk ratings.

Priority 4: Avoid getting overly technical

Don't overwhelm leadership with too many technical details, but be sure to do a risk assessment that includes an inventory of assets with specific threats and vulnerabilities, and the likelihood and impact associated with each scenario. Risk assessments are required for HIPAA and other compliance standards, so your board should understand what these risks are as they relate to organizational resiliency.

Priority 5: Have ongoing conversations about risk tolerance

Your executive leadership team is responsible for defining organizational risk tolerance, so it's important to make sure they understand what risk tolerance is and how it impacts resources.

Priority 6: Establish formal ECRM governance

Once you've begun engagement with your executives about ECRM, stick with it. Your big-picture goal is to ensure it remains front-and-center in leadership conversations and that these leaders remain actively engaged in ECRM oversight and governance.

Sentara success

After identifying known obstacles for ECRM success, Sentara, with Clearwater's support and help, quickly saw the ROI and benefits of building ECRM executive engagement. Here are a few success takeaways:

1. **Leadership engagement simplifies buy-in when you need additional ECRM resources**

Why: When key stakeholders understand risk management lexicon (assets/vulnerabilities/threats/likelihood/impact) and understand your organization's risk posture, it's easier to explain—and justify—funding requests for additional resources that support or enhance your cyber risk management capabilities.

2. **Leadership engagement helps quantify appropriate risk tolerance levels**

Why: When allocating your ECRM resources, it's critical to understand your organization's risk tolerance levels. As your organization scales and changes—and as your ECRM program matures—this understanding will facilitate conversations about ECRM strategy enhancements related to risk tolerance.

3. **Leadership engagement encourages team members to consider cyber risk impacts when developing new business services or initiatives**

Why: If your organization wants to, for example, improve consumerization by developing a new mobile app for health plan members and a new web portal for patients, you'll want to know if it's a task you can handle in house and what business and cyber risks may evolve from that approach. When that conversation makes it to C-suite, the team should have a general understanding of why ECRM should be included in those discussions and decisions.

4. **Leadership engagement makes it easier to prioritize and plan**

Why: Depending on the size of your organization, there are countless risks to consider, but with limited time and resources, you can only bring the most critical ones to your executives for discussion. By ensuring your leadership team understands key ECRM metrics, you can point out deficiencies and plan for program maturity over time.

5. **Leadership engagement helps advance ECRM program maturity**

Why: Engaged stakeholders and effective ECRM communication will make it easier to explain gaps and weaknesses and support requests for additional resources that will contribute to ECRM program maturity.

Tips for success

Leadership engagement is ECRM critical. Why? Because cyber risk management is a business risk issue and your ECRM program will not be successful without organizational engagement and buy-in. Regardless of your organization's size, you can draw on some of Sentara's best practices to build that engagement and create a culture that supports ECRM success:

Governance

Tip: Your executive leaders should help set your program direction, provide governance for the program, policies, and plans, and help communicate the value of ECRM across your entire organization. Get started by assessing where your organization is now with executive leadership engagement. Then make a plan to get ECRM on that executive agenda and open doors for these important conversations.

Develop a presentation that illustrates cyber risk management as a business risk issue and with quantifiable, real-world examples. Explain basic risk management concepts and terminology. Demonstrate how peer organizations structure their ECRM programs, and keep the conversation ongoing.

People

Tip: When building and maturing your program, seek out skilled professionals with cyber risk management experience beyond just analyzing data and implementing technical controls. You need diverse skills, including soft skills and continuous training.

Processes

Tip: Develop formal, well-documented and consistently followed policies, procedures, and practices that align with industry standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Technology

Tip: Seek out scalable technology tools like Clearwater's IRM|Analysis® that help you conduct risk assessments, manage risk treatments, monitor performance, and create customizable reports to facilitate communication with your key stakeholders.

Engagement

Tip: Get engagement at every level of your organization. While your executives will guide governance and set the tone for your culture, you need ECRM accountability at every level. That means all of your employees, not just leadership team members.

Scaling for the future

While the Sentara team is excited about its ECRM evolution and increasing maturity, they understand that as the organization continues to grow and change, they will have to continuously reassess ECRM, including revisiting practices, processes, technologies, and policies.

Remember, effective ECRM isn't set-it-and forget it. It's dynamic and should evolve as a strategy that continuously focuses on next steps and improvements, while facilitating and expanding executive engagement. It's a journey, not a destination.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact