Enterprise Cyber Risk Management

A Toolbook for Healthcare Boards and Executives

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

A Governance Institute Strategy Toolbook **Summer 2021**

A SERVICE OF

nrc HEALTH

The Governance Institute®

The essential resource for governance knowledge and solutions®

1245 Q Street, Lincoln, NE 68508
(877) 712-8778

GovernanceInstitute.com
/The Governance Institute
/thegovinstitute

Jona Raasch	Chief Executive Officer
Cynthia Ballow	Vice President, Operations
Kathryn C. Peisert	Managing Editor
Glenn Kramer	Creative Director
Kayla Wagner	Senior Editor
Aliya Flores	Editor

The Governance Institute is a service of NRC Health. Leading in the field of healthcare governance since 1986, The Governance Institute provides education and information services to hospital and health system boards of directors across the country. For more information about our services, please call toll free at (877) 712-8778, or visit our Web site at GovernanceInstitute.com.

The Governance Institute endeavors to ensure the accuracy of the information it provides to its members. This publication contains data obtained from multiple sources, and The Governance Institute cannot guarantee the accuracy of the information or its analysis in all cases. The Governance Institute is not involved in representation of clinical, legal, accounting, or other professional services. Its publications should not be construed as professional advice based on any specific set of facts or circumstances. Ideas or opinions expressed remain the responsibility of the named author(s). In regards to matters that involve clinical practice and direct patient treatment, members are advised to consult with their medical staffs and senior management, or other appropriate professionals, prior to implementing any changes based on this publication. The Governance Institute is not responsible for any claims or losses that may arise from any errors or omissions in our publications whether caused by The Governance Institute or its sources.

About the Author

Bob Chaput is the author of the book, *Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know about Enterprise Cyber Risk Management (ECRM)*. He is also the Founder and Executive Chairman of Clearwater, a provider of healthcare compliance and cyber risk management solutions.

Prior to founding Clearwater in 2009, Chaput served as CIO and then as Executive Vice President—Operations Services at Healthways, Inc. Before Healthways, Chaput founded and served as President and CEO of the American Technology Group, Inc.

Chaput spent six years at Johnson & Johnson, serving as Vice President of Networking & Computing Services, and then as Vice President and General Manager of Technology Consulting Services. Prior to that he spent 12 years at GE, serving in various technology and management assignments.

His career includes assignments as an educator, including serving as an adjunct faculty member teaching courses in computer programming, project management, and technology certifications at Southern Vermont College, ITT Technical Institute, Belmont University, and Quinnipiac University.

In addition to an M.A. in mathematics from Clark University and a B.A. in mathematics from the Massachusetts College of Liberal Arts, Chaput has earned numerous certifications in technology and cybersecurity, including: Certified Information Systems Security Professional (CISSP), Health Care Information Security and Privacy Practitioner (HCISPP), Certified in Risk Information Security Controls (CRISC), Certified Information Privacy Professional/US (CIPP/US), Certified Ethical Hacker (C|EH) and NACD CERT Certificate in Cybersecurity Oversight.

Chaput is committed to educating healthcare industry leaders about cyber risk management through articles, presentations, and Webinars. He was a contributing author to two books: Wolters Kluwer's *Health Law and Compliance Update* and the American Society of Healthcare Risk Management (ASHRM)'s *Health Care Risk Management Fundamentals*. His insights about cyber risk management have been published in *Modern Healthcare*, *CISO Mag*, *Health Law Connections,* the Health Care Compliance Association's *Compliance Today*, The Governance Institute's *BoardRoom Press, HealthITSecurity*, *HealthcareInfoSecurity* (Information Security Media Group), and *The Wall Street Journal (WSJ) Pro Cybersecurity*.

Note: this toolbook is adapted from Bob's book, *Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)* (Nashville: Clearwater, 2020).

Acknowledgements

Bob and The Governance Institute thank the following individuals and their organizations for spending time sharing their ECRM stories, which make up the accompanying case studies for this toolbook, as well as the case example lessons included within this toolbook:

- Jason R. Joseph, Senior Vice President and Chief Digital and Information Officer, Spectrum Health
- Mitchell Parker, Chief Information Security Officer, IU Health
- Adam Zoller, Chief Information Security Officer, Providence St. Joseph Health

The case studies are available here.

The Governance Institute

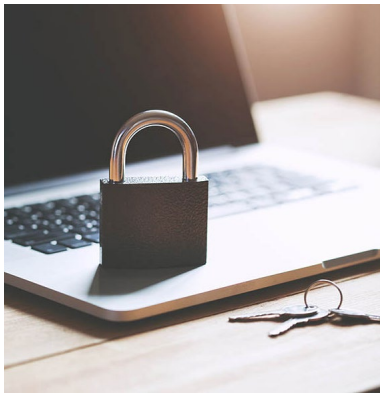
The Governance Institute provides trusted, independent information, tools, resources, and solutions to board members, healthcare executives, and physician leaders in support of their efforts to lead and govern their organizations.

The Governance Institute is a membership organization serving not-for-profit hospital and health system boards of directors, executives, and physician leadership. Membership services are provided through research and publications, conferences, and advisory services. In addition to its membership services, The Governance Institute conducts research studies, tracks healthcare industry trends, and showcases governance practices of leading healthcare boards across the country.

Table of Contents

The Current State of Healthcare Cyber Risk

Cyber attacks on hospitals and health systems are increasing in frequency and severity. Welcome to healthcare's new normal. Healthcare organizations have been a target for cyber attackers since well before the pandemic. But as healthcare organizations accelerated digital initiatives in response to the pandemic, cyber attackers took notice of increased vulnerabilities and escalated their assaults on healthcare systems. One study found a 9,851 percent increase in attempted attacks per endpoint between 2019 and 2020.[1] Another study found that healthcare hacking incidents increased by 42 percent in 2020, resulting in more than 40 million healthcare records being exposed or compromised.[2]



Part of this increase can be attributed to increased exposures in the wake of the pandemic. Healthcare organizations rapidly rolled out telehealth and other virtual healthcare delivery methods. They also took steps to accommodate remote employees. In the rush to increase accessibility to data, systems, and devices, cyber risk management was often overlooked.

But it's not just the pandemic that has put healthcare organizations at increased risk. The healthcare ecosystem is changing in ways that make cyber risk management more challenging. While the industry's evolution has increased access and efficiency, many of the changes have also increased the industry's attack surface. For example:

- Healthcare organizations are managing exponentially increasing volumes of data.
- Healthcare organizations have become more dependent on cloud-based applications, remote services, and Internet-connected medical and monitoring devices.
- Healthcare organizations have been expanding healthcare delivery outside the walls of the facility via telehealth and other virtual care options.
- Data-sharing with third-party partners has become a necessary part of doing business, for everything from sharing patient records to support the continuum of care, to billing, insurance verification, and other tasks associated with revenue cycle management.

1 "VMWare Carbon Black Explores the State of Healthcare Cybersecurity in 2020," *HIPAA Journal,* February 8, 2021.
2 "2020 Saw Major Increase in Healthcare Hacking Incidents and Insider Breaches," *HIPAA Journal,* March 16, 2021.

- Merger and acquisition activity has increased dramatically in the healthcare industry over the past several years, creating larger entities with vastly more complex IT networks to manage and protect.

Any one of these activities is enough to warrant an assessment of your organization's cyber risk management posture. But the fact is that many organizations are dealing with two or more of these changes at once. And few healthcare organizations have taken the time to ensure that the cyber risks associated with these activities have been addressed.

The consequences of neglecting to address cyber risk can be severe. A ransomware attack can shut down services and put your patients' lives at risk. A data breach can result in millions of compromised or exposed patient records, leading to penalties, fines, legal and other fees, settlements, and reputational damage for your organization. The risk of harm to your patients and your organization from a cyber incident has become too significant to ignore.

Introduction to Enterprise Cyber Risk Management

In order to understand enterprise cyber risk management (ECRM), it is important to connect it with the oversight role of a hospital or health system board.

The role of fiduciary includes the obligation to execute fiduciary duties. Among these duties is the *duty of care*, which requires that "a board member will act in a manner consistent with the way a prudent businessperson would carry out similar work under similar circumstances. It means that you act in good faith at all times, and it means that you seek out the relevant and pertinent information necessary to make good decisions and undertake proper actions."[3]

Board members' fiduciary duties encompass oversight of enterprise risk management (ERM). Board members, in collaboration with C-suite executives, are obliged to identify the most significant risks to their organizations and to decide how to allocate resources to mitigate those risks. Healthcare enterprises face many different kinds of risks, including risks related to:

- Clinical quality of care and patient safety
- Financial stability
- Emergency preparedness
- Legal and regulatory compliance
- Merger and acquisition (M&A) activity
- The privacy and security of patient data/protected health information (PHI)

It can be argued that cyber risk management should be at the top of the list of enterprise risks because of the way cyber risk interacts with every other area of risk a healthcare organization faces. For example, a successful cyber attack can compromise quality of care and result in harm to patients. An attack that results in a data breach can threaten an organization's financial stability due to the associated financial and reputational consequences. A successful ransomware attack can cripple operations and require a fallback to emergency procedures. Effective cyber risk management is key to compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other legal and regulatory requirements applicable to healthcare organizations. Cyber incidents can also derail M&A plans.

In other words, it is simply not possible to separate "cyber risk management" from your enterprise's overall risk management program. That is why I always refer to cyber risk management as *enterprise* cyber risk management, or ECRM.

3 The Governance Institute, *On Board! An Orientation to Healthcare Governance (video)*, 2020.

What Is ECRM?

At its most fundamental level, risk management is about managing the possibility of loss or harm. ECRM specifically focuses on risks related to information assets—i.e., PHI (the data), systems, and devices. In particular, ECRM focuses on threats to the *confidentiality, integrity,* and *availability* of PHI.[4] Note that these three characteristics are distinct from each other. For example, a data breach could compromise the confidentiality of PHI, whereas a ransomware attack could compromise the availability of PHI.

For risk to exist, there must be three components: an asset, a threat, and a vulnerability. The asset-threat-vulnerability combination is known as a "risk scenario." An example of an ECRM risk scenario for a healthcare organization might include: a laptop containing PHI (the asset); a thief who wants to steal the laptop (the threat); and the fact that the laptop lacks encryption (the vulnerability). I use the notation {asset-threat-vulnerability} to indicate a risk scenario.

Other variables—beyond the {asset-threat-vulnerability} combination—are also at play when assessing risk. When evaluating risk scenarios, three additional variables must be considered: likelihood, impact, and controls:

- *Likelihood* refers to the probability that a given threat is capable of exploiting a given vulnerability
- *Impact* refers to the extent of the harm that can occur if a vulnerability is exploited
- *Controls* are the measures, safeguards, strategies, methods, and tools used to mitigate risk by lowering the likelihood or impact

Applying the concepts of likelihood, impact, and controls to each risk scenario is essential for rating, and then prioritizing, risks. For example, the *likelihood* of the {laptop-thief-no encryption} scenario is high, considering the frequency of laptop theft. The *impact* depends on the scope of the compromise of information, with respect to factors such as the number of patient records breached, operational downtime, and organizational cost. Finally, *controls*, such as encrypting all of the organization's laptops, serve to mitigate the risk.

The ultimate purpose of incorporating ECRM into your organization's overall risk management program is to protect your organization's data, systems, and devices from potential compromises of confidentiality, integrity, and availability.

4 The HIPAA Security Rule specifically states that covered entities and business associates must "ensure the confidentiality, integrity, and availability of all electronic protected health information." See 45 CFR § 164.306(a)(1).

Three Essential Tasks

ECRM is composed of three essential tasks or activities. The board is responsible for providing leadership and oversight of these three activities.

1. Conduct Risk Analysis

The foundational activity of any ECRM program is to identify, and then prioritize, all of your organization's unique cyber risks. The single biggest deficiency I observe in ECRM programs across the industry is the failure to invest in cybersecurity in a way that is based upon an organization's unique risks.

Too often, healthcare organizations use a one-size-fits-all checklist of cybersecurity methods and controls. Using a generic checklist for cyber risk management is like borrowing your neighbor's "to-do" list to manage your day. You have unique priorities, responsibilities, and obligations that determine your to-do list. Your neighbor's priorities, responsibilities, and obligations are different from yours—which is why you can't share the same to-do list.

The same logic applies to ECRM. Your organization is unique—and not just by virtue of its unique vision, mission, strategy, values, and services. Your organization is also unique in terms of information assets. No other organization has exactly the scope and configuration of information assets that yours has. No other organization deploys its data, systems, and devices in precisely the same manner as yours does. So, in order to create an effective ECRM strategy, you have to begin with an inventory of your information assets. In addition to creating an inventory of assets, your organization must also evaluate the other components of risk, including identifying every possible risk scenario (e.g., {laptop-thief-no encryption}) and assessing the likelihood and impact of each scenario in order to assign a risk rating.

Conducting a risk analysis is essential to effective ECRM—and it is also a significant and complex undertaking. A risk analysis is not something that can be conducted, documented, or maintained using a simple Excel spreadsheet. Specialized software can help organizations efficiently perform an enterprisewide, comprehensive risk analysis across all ePHI assets and medical devices, evaluate reasonably anticipated threats and vulnerabilities, assess risk, and manage risk remediation.

2. Determine Risk Appetite

The second critical ECRM activity is that the organization must discuss, debate, and settle on an appetite for cyber risk. This task relies on the context of the first task, conducting a risk analysis. One of the work products resulting from a comprehensive risk analysis is the creation of a risk register. A risk register catalogues the hundreds of thousands of risks unique to your organization (see **Exhibit 1**).

Exhibit 1: Sample Excerpt from a Risk Register

Asset	Threat Source/Event	Vulnerability	Likelihood	Impact	Risk Rating
Laptop	Burglar steals laptop	No encryption	High (5)	High (5)	25
Laptop	Burglar steals laptop	Weak password	High (5)	High (5)	25
Laptop	Burglar steals laptop	No asset tracking	High (5)	High (5)	25
Laptop	Careless user drops laptop	No data backup	Medium (3)	High (5)	15
Laptop	Lightning strikes home	No surge protection	Low (1)	High (5)	5
Laptop	Shoulder-surfer views screen	No privacy screen	Low (1)	Medium (3)	3
Etc.	There are dozens more risk scenarios to consider with each category of laptops.				

Source: Bob Chaput, Executive Chairman, Clearwater.

The risk register provides the foundation for informed decision-making related to cyber risks. As shown in **Exhibit 1**, the likelihood and impact of each risk scenario has been analyzed, resulting in a unique risk rating. The board and C-suite now have the information they need to determine the organization's risk appetite: the level of risk the organization is willing to assume.

For example, if an organization sets its risk appetite at 15, then the organization would simply accept risks rated at 14 or below, but treat all risks rated at 15 or above. Likewise, if an organization sets its risk appetite at 5, it will accept risks rated at 4 or below, but treat all risks rated at 5 or above.

Why wouldn't an organization set its risk appetite at zero? Organizations have a finite amount of resources available for managing risk. Theoretically, an organization could choose to treat every risk on the register, but in reality, that would be cost prohibitive. In addition, it might not make strategic sense to allocate resources for risks with low ratings.

3. Manage Risk

Finally, the organization has to make an informed decision about how to manage each risk. Risks that are rated below your risk appetite are risks that you *accept*. For risks at or above your risk appetite, you have to determine whether you will *avoid*, *mitigate*, or *transfer* that risk. These four choices—accept, avoid, mitigate, or transfer—are fairly standard in the treatment of any type of risk.

An example of ECRM risk mitigation would be to implement a mobile device management (MDM) solution to include all laptops, so that even if a careless employee lost a laptop, the laptop could be located and/or remotely wiped to prevent access to its contents. An example of risk transfer would be to increase an organization's cyber liability insurance limits to help cover potential damages.

The goal of risk treatment is to lower the risk rating of risks that are above your organization's risk appetite, such that the risk rating is at an acceptable level—i.e., below your risk appetite. The countermeasures, safeguards, or controls that are implemented to treat risks at or above your organization's risk appetite form the basis of your organization's cybersecurity strategy.

The Board's Approach to ECRM

An oft-used phrase that describes the board's role is, "eyes open, nose in, fingers out." This way of thinking can be applied to a board member's approach to ECRM as well:

- **"Eyes open":** understand what it means to have an effective ECRM program in place.
- **"Nose in":** understand where your organization is in relationship to legal requirements, best practices, and standards related to ECRM, and provide leadership with respect to closing any gaps between established ECRM practices and your organization's approach.
- **"Fingers out":** leave the details of execution to your organization's appropriate executives and team members.

The most effective way for the board to provide ECRM leadership is to apply this philosophy to three broad areas of responsibility: setting the tone, becoming ECRM enablers (not experts), and mandating best practices.

1. Set the Tone

The board plays a critical role in setting the tone for an organization's ECRM program. If the board takes ECRM seriously and views it as a business risk issue, this perspective will be communicated to the rest of the organization. If, on the other hand, the board dismisses ECRM as strictly an "IT problem," this is the message that will be conveyed.

The board's actions communicate the importance of ECRM within the organization. For example, if the board establishes and supports a governance structure that prioritizes ECRM, that priority is communicated throughout the enterprise. Likewise, if ECRM becomes a standing agenda item at every board meeting, it establishes a culture that supports the importance of ECRM discussions at every level of the organization.

Setting the tone also means establishing context for the prioritization of ECRM. The board's messaging lays an important foundation for creating a cyber-risk-aware culture throughout the organization. Key assumptions that are important for the board to communicate include:

- Cyber risk management is a business risk issue, not an IT problem.
- Cyber risk impacts all healthcare organizations. No single organization is immune from cyber risk.
- An effective cyber risk management program requires the engagement of all stakeholders, including patients, staff, clinicians, executives, the C-suite, and board members.
- Effective ECRM is a proactive undertaking, even though it also incorporates best practices for how to deal with the aftermath if a cyber incident occurs.
- A robust ECRM program is a business enabler that can help organizations securely deploy consumer-centric, technology-based innovations that engage customer trust and encourage customer confidence.

2. Become ECRM Enablers, Not Experts

As a board member, you do not need to become a cybersecurity expert to lead your organization's ECRM efforts effectively. The board's role in ECRM is at the strategic, not tactical, level. Technical details about current cyber threats and advances in specific controls and safeguards are best left to your internal and external experts.

At the strategic level, however, only the board and C-suite have the business-wide perspective and authority to ensure that your organization's ECRM efforts align with your overall strategic goals and ERM program. Only the board and the C-suite have the scope and power to allocate scarce resources strategically, including human resources, capital expenditures (CapEx) and operating expenses (OpEx), to establish, implement, and mature an effective ECRM program.

Board members need to understand ECRM at the strategic/conceptual level in order to provide effective oversight, but they should not be dictating the technical details of the organization's ECRM program. To fulfill your responsibilities as an ECRM enabler:

- Become educated, individually and as a board, about ECRM.
- Evaluate your organization's current security posture (at a strategic level).
- Ensure your organization's ECRM program aligns with your organization's vision, mission, strategy, values, and services.
- Determine *how* your organization will conduct ECRM—again, not at the tactical level, but at the strategic, enterprise level.
- Verify that your organization has conducted, and continues to maintain, a comprehensive risk analysis.
- Decide what your organization's risk appetite will be.
- Provide oversight and leadership for risk treatment decisions at the strategic level.
- Require continuous business process improvement principles be applied to your organization's ECRM program to advance the maturity of your program over time.

3. Mandate Best Practices

Mandating best practices is another area in which board members have a critical leadership role—again, at the strategic, not tactical level. Mandating best practices does not mean hearing about the latest and greatest technological controls (e.g., anti-malware software or Intrusion Detection Systems (IDS)) and passing that information on to your Chief Risk Officer (CRO) or Chief Information Security Officer (CISO).

Instead, mandating best practices is about understanding and providing leadership for the foundational practices that underpin your organization's ECRM program. An effective ECRM program starts with *how* you approach ECRM at the strategic level.

The good news is that standardized, strategic best practices for ECRM have already been developed and documented in publicly available, free resources provided by the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce. The NIST Cybersecurity Framework was created in response to a 2013 Presidential Executive Order designed to increase the sharing of cybersecurity threat information across industries and to result in a framework

for reducing risks to critical U.S. infrastructure.[5] The initial framework development and subsequent updates included the participation of more than 2,000 people across a wide range of impacted industries. The strength, relevance, and effectiveness of the NIST Cybersecurity Framework is directly related to the open, inclusive, process that was used to develop and update it.

One of the many strengths of the NIST Cybersecurity Framework is that it is applicable across all industries, including healthcare. The framework has many strengths that make it particularly well-suited to provide a strategic foundation for ECRM in the healthcare industry. To name just a few of its advantages, the NIST Cybersecurity Framework:

- Facilitates ECRM governance
- Leverages current standards, guidelines, and best practices from internationally recognized sources (e.g., COBIT 5, ISA 62443, IOS/IEC 27001)
- Aligns with HIPAA requirements
- Has been endorsed by industry leaders, including the Healthcare Information Management and Systems Society (HIMSS)
- Has already been adopted by a majority of healthcare organizations in the U.S.
- Has become the standard for the U.S. Government (including programs administered by the Centers for Medicare & Medicaid Services)
- Is customizable, scalable, and affordable

More information about the NIST Cybersecurity Framework, as well as supporting resources, are available online. The guidance found in the NIST Cybersecurity Framework and supporting documents can help board members provide strategic leadership for their ECRM programs.

5 National Institute of Standards and Technology (NIST), "History and Creation of the Framework" (Web page), updated November 21, 2019.

ECRM Is a Team Sport

Board engagement, leadership, and oversight is absolutely essential to establishing, implementing, and maturing your organization's ECRM program. Tactical expertise, while not the board's responsibility, is also important. But for an ECRM program to be effective, it requires the engagement of everyone across the breadth and depth of your organizational structure.

Consider the many ways cyber attackers can gain access to your organization: a single employee targeted by a spear phishing attack (a targeted, fraudulent email) could provide an opening for downloading ransomware onto the network. A man-in-the-middle (MitM) attack could insert itself into communications between a clinician's remote device and the hospital network. A third-party services vendor could have unaddressed vulnerabilities that result in the vendor's system, and then the hospital's system, becoming infected with malware.

Also consider the scope of resources—from financial resources (CapEx and OpEx), to human resources, to technical resources—that need to be deployed to effectively manage cyber risk. When you consider the scope of the risks, as well as the breadth of resources that need to be deployed to address those risks, it becomes clear that ECRM is a "team sport." ECRM is not the responsibility of a single officer or a single department: it is the responsibility of everyone in the organization. A key way to enable enterprisewide engagement in cyber risk management is by establishing a strong governance structure.

The Critical Role of Governance

A simple way to think about governance is to pose it as a set of interrelated questions:

- Who makes what decisions?
- How and when do they make those decisions?
- What data and facts do they use to make those decisions?

In my experience working with organizations to establish, implement, and mature ECRM programs, I have found that a three-tiered ECRM governance model is most effective, although the model will vary by the size and resources of each organization. The three tiers in this governance model include:

- *Tier 1*: The full board or designated board committee (e.g., audit and compliance committee or a specific ECRM oversight council or committee) sets direction and provides oversight.
- *Tier 2*: An ECRM executive steering committee (including the CEO and his/her full team) ensures execution of the ECRM program.
- *Tier 3*: An ECRM cross-functional working group (depending on your organization, this may include representatives from legal, risk management, finance, human resources, audit, compliance, privacy, information technology, clinical engineering, security, quality, and/or others as appropriate) executes the steps to establish, implement, and mature the ECRM program.

A small organization might use a simplified version of this model, for example, by combining Tier 2 with Tier 3. On the other hand, a large, complex organization with multiple lines of business might add additional tiers or establish the three-tiered model within each line-of-business. In any case, it is also important to assign your internal audit organization with overall assurance responsibility to provide an independent opinion on the ECRM program to the board. **Exhibit 2** illustrates how the three-tiered ECRM governance model might work in a large organization.

Exhibit 2: Example of a Three-Tiered ECRM Governance Structure

Source: Bob Chaput, Executive Chairman, Clearwater.

Each of the three tiers should have a formal, written charter that delineates the group's decision-making authority, structure, scope of responsibilities, work processes to be followed, etc. If your organization has a project management office (PMO), the PMO can help with chartering and facilitating the groups. In order to facilitate ECRM oversight, it is important that each governance group has appropriate training, as well as access to ECRM expertise, sourced internally or externally.[6]

Once these three tiers of governance are in place, an appropriate starting point is the development of your organization's ECRM framework and strategy document (i.e., your organization's strategic approach to ECRM, which I recommend you base on NIST guidance). The right governance structure—such as the three-tiered model described here—supports ECRM at every level of the organization.

6 Larry Clinton, et al., Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards, National Association of Corporate Directors (NACD) and Internet Security Alliance (ISA), 2020. This publication is a great resource for those participating in governance at the board level.

Case Study Lessons: Third-Party Risk

All three of the cybersecurity leaders from the organizations profiled in the accompanying case studies for this toolbook (IU Health, Providence St. Joseph Health, and Spectrum Health) emphasized the significant potential of third-party vendor risk negatively impacting a healthcare organization. Each leader referenced the SolarWinds example. As Mitch Parker, IU Health's CISO explained, "The number one area my team focuses on is third-party risk. We have a significant third-party risk team aligned with supply chain and system operations. Asking vendors tough questions [about how they handle security] is more important than ever." Adam Zoller, CISO at Providence, said, "If the vendor doesn't invest in cybersecurity, we may choose a different vendor. Or we may go back to the vendor and require them to put in remediation steps in order for us to do business with them. Having security provisions in the contracts with every vendor is absolutely critical." Jason Joseph, Chief Digital and Information Officer at Spectrum, concurred, "The board needs to have confidence that our third-party vendors have a certain level of maturity regarding cybersecurity."

The three leaders provided the following questions that they pose to vendors before entering into a relationship with them, to determine how seriously vendors are handling security and thus assess the cyber risk of entering into a relationship with that vendor (all of which require written assurances/inclusion in contracts):

- Are they handling Protected Health Information? If they are, do we have a Business Associate Agreement?
- What assurances do we have of their security? Do they have a current HITRUST or ISO 27001/27017/27018 certification? Do they complete an annual risk assessment and plan?
- Does their hosting have SOC2 certification?
- Do they conduct source code analysis and testing?
- Do they integrate their authentication with your own enterprise portal or active directory as opposed to standing up their own?
- Do they use good encryption?
- Do they keep their software up to date? More importantly, do they keep their third-party components that they leverage up to date as well?
- Are you able to secure and lock down the applications?
- How will we be notified if there is an issue?
- Do they have cyber liability insurance?

Zoller recommends that you don't start from scratch to find vendors that are strong in their security protocols. Talk to industry peers and seek information from trusted associations such as HIMSS or Health-ISAC.

How the Organizational Structure Helps—Or Hinders—ECRM

In addition to the governance structure, the organizational structure impacts the effectiveness of the ECRM program. For example, do you know where the chief security officer (CSO) or chief information security officer (CISO) sits in your organization? In the not-too-distant past, CSOs or CISOs commonly reported to the organization's chief information officer (CIO), who might, in turn, report to the organization's CEO. This legacy structure grew out of the idea that cyber risk management is a technical subset of the IT department. However, this is not an accurate portrayal of the role of the CSO/CISO in today's healthcare enterprise.

Cyber risk management does include technical strategies that must be implemented and executed by the CIO and their team. But the most important role of the CSO/CISO is to identify, communicate, and address cyber risks in the context of ERM. Cyber risks are not limited to the technical infrastructure of the organization; cyber incidents can cause harm to patients, as well as harm that impacts the finances, operations, and reputation of the entire enterprise. As such, the CSO/CISO is more appropriately placed at a senior executive level, reporting directly to the chief risk officer (CRO) or to general counsel. Alternatively, the CSO/CISO might report to the CEO, chief operating officer (COO), or chief financial officer (CFO).

There are three problems with having the CSO/CISO report to the CIO. The first problem, as already noted, is that information security/cyber risk management is an enterprisewide function that transcends the IT department. The organizational structure needs to reflect the true scope of the CISO role. The second problem is that there is an inherent conflict between the CIO's role and the CISO's role. The CIO has a mission to deploy and maintain applications, with a minimum of friction for end users. The CISO, on the other hand, may have to restrict access in order to ensure security. Having the CISO report to the CIO sometimes means that frictionless accessibility will take precedence over security management.

The final problem with having the CSO/CISO report to the CIO is related to resource allocation. When cyber risk management is viewed as a subset of the IT department, it is likely to be under-resourced, because the CIO's focus is cost management rather than risk management. Reporting to a CIO can limit the CSO's ability to implement ECRM effectively.

Interestingly, the three organizations we profiled have not established a reporting structure per these recommendations; their structure is the traditional CISO-CIO-CEO reporting path. However, the three leaders provide pertinent information directly to the board on a regular basis (which is described in more detail later). They also have separate budgets and teams devoted to cybersecurity, rather than being considered a subset of the IT budget and team. Finally, they all are integrated and aligned with the CRO and enterprise risk team. At IU Health, Parker works closely with and provides his board report to the CRO, who then presents the information to the board.

> "ECRM must be a board- and executive-led initiative, with engagement across and up and down your entire organization."

The Roles of the C-Suite and Other Executives

Although the CSO/CISO may be point person for the technical execution of the ECRM strategy, every C-suite executive has a role to play. The following examples were adapted, with permission, from the original *Cybersecurity Cheat Sheets for the C-suite and Board* developed by the Advisory Board:[7]

- *Chief Audit Executive (CAE)*—Audit executives already play an integral role in ERM. Given the unique relationship CAEs have with their boards, they have the opportunity to:
  - » Ensure that ECRM is formally integrated into the organization's audit plan.
  - » Insist on making ECRM a "team sport," encompassing all departments.
  - » Lobby to make ECRM discussions an agenda item at every board meeting.
  - » Provide the C-suite executives and board with assurance that the ECRM program is working, through internal IT and security audits and coordinated external audits.
  - » Help the organization estimate the potential cost of a data breach to your organization.
- *Chief Human Resources Officer (CHRO)*—Threat sources healthcare organizations face include malicious insiders, careless insiders, and workforce members who simply make a mistake and open a malicious email. The implementation of an organization's cybersecurity program depends heavily on members of the workforce being well-trained and performance-measured on privacy and security policies and procedures. The CHRO can contribute to the success of the organization's ECRM program in multiple ways, including:
  - » Ensuring that the right privacy, security, compliance, and risk management talent is on board to operationalize the organization's ECRM program
  - » Assisting in the development of privacy and security policies and procedures
  - » Assisting with the development and delivery of privacy, security, and breach notification training to all members of the workforce
  - » Enforcing sanction policies to ensure all members of the workforce are held accountable for privacy and security
- *Chief Medical Officer (CMO)*—ECRM has become a patient safety and professional liability matter for hospitals and health systems. With the digitization of healthcare, clinicians across your organization are now dependent on data, systems, and devices that impact patient safety, quality of care, and access to care. The CMO contributes to the success of your ECRM program in many ways and can:

7 Advisory Board, *Cybersecurity Cheat Sheets for the C-Suite and Board,* updated May 9, 2019.

  - » Help the organization "connect the dots" between the confidentiality, integrity, and availability of data, systems, and devices, and quality care, safe care, and timely access to care.
  - » Ensure that clinicians have a seat at the table as new security controls are considered and take into account the impact of the implementation of security controls on clinician productivity and morale.
  - » Advocate for "security-by-design" that ensures risks are considered before new healthcare data, systems, or devices are implemented.
  - » Make ECRM and cybersecurity a standing and ongoing training program for all clinicians.
  - » Advocate that your business continuity plans remain current and consider the potential adverse patient impact if critical data, systems, and devices become unavailable.
- *Chief Financial Officer (CFO)*—A core theme of this toolbook is to help your organization make more informed decisions about the allocation of scarce human and financial resources to your ECRM program. The CFO, as a core member of the executive team, has a unique view of financial resources across the organization. To fulfill his or her cyber risk responsibilities, he or she should:
  - » Understand and communicate the financial consequences of the compromise of the confidentiality, integrity, and availability of critical data, systems, and devices.
  - » Work with C-suite colleagues to establish appropriate OpEx, CapEx, and human resource budgets to manage cyber risks to an acceptable level in the organization.
  - » Establish the financial analysis methods that your organization will use to judge the value or return on investment (ROI) of cybersecurity investments.
  - » Participate in and support making ECRM an executive-led, cross-functional initiative outside the sole purview of the CIO and/or CISO.

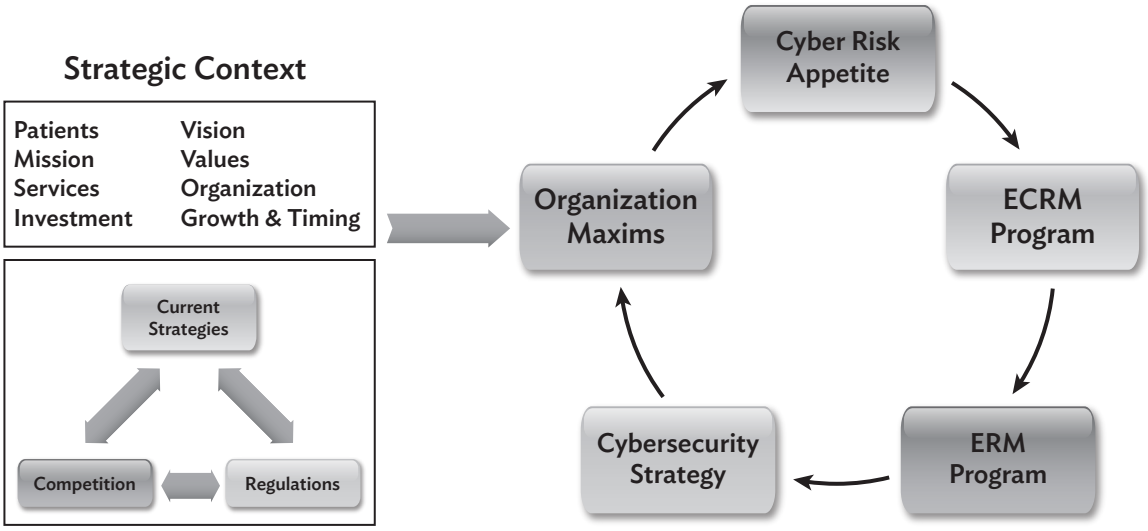
ECRM Strategic Goals

At the tactical level, your ECRM program must be based on your organization's unique information assets (data, systems, and devices). At the strategic level, your ECRM program must align with your organization's unique vision, mission, strategy, values, and services. The board's ECRM leadership and oversight, and the C-suite's implementation of ECRM, takes place in the context of your organization's particular priorities and business objectives. Your organization's ECRM decisions and strategies should reflect that alignment.

Aligning ECRM with the Organization

Aligning ECRM with the organization means taking strategic context (vision, mission, strategy, values, and services) into consideration when establishing, implementing, and maturing your organization's ECRM program. **Exhibit 3** illustrates a model for driving alignment in cybersecurity strategy.

Exhibit 3: Model for Driving Alignment in Cybersecurity Strategy



Source: Bob Chaput, Executive Chairman, Clearwater.

NIST emphasizes the importance of ECRM alignment with the organization's vision, mission, strategy, values, and services in *Managing Information Security Risk (SP 800-39)*. NIST notes that large, complex healthcare organizations may be focused on one or two primary missions, but that these missions are supported by myriad business functions and organizational components:

> "While all of these organizational components and associated missions/business functions are likely to be important and play a key role in the overall success of organizations, in reality they are not of equal importance. The greater the criticality of organizational missions and business functions, the greater the necessity

> for organizations to ensure that risks are adequately managed. Such missions and business functions are likely to require a greater degree of risk management investments than missions/business functions deemed less critical."[8]

NIST goes on to state that "the determination of the relative importance of the missions/business functions and hence the level of risk management investment" is a decision that is made at the organizational level, executed at the business process level, and which directly influences activities that take place at the information systems level.

Five Essential Capabilities

One of the means by which the board and C-suite can align ECRM with the organization is by developing strategic objectives that simultaneously advance the organization's mission and strengthen cyber risk management. I recommend that healthcare organizations establish strategic objectives that address five critical core capabilities of the organization: governance, people, processes, technology, and engagement. Focusing on this specific set of capabilities will help your organization grow and mature a cyber-risk-aware culture that supports your ECRM program.

For each critical area described below, I have included an example of a strategic ECRM objective, an example of an enabling objective, and an example of a key performance indicator. These examples are not meant to be limiting or prescriptive, but only to give examples of how strategic objectives facilitate ECRM program effectiveness.

1. Establish Appropriate Governance

With respect to ECRM governance, the role of the board is to set direction and provide ongoing oversight. In other words, the board establishes and communicates, "This is where we are going (with respect to ECRM), and this is why we are going there." C-suite executives and their teams are then responsible for execution.

Sample Strategic ECRM Objective:
Incorporate ECRM into strategic decision making and ongoing business planning.

Sample Enabling Objective:
Set the ECRM framework, process, and maturity model by which ECRM will be performed consistently throughout your organization.

This means the C-suite and board would consult with internal and external subject-matter experts to understand the alternatives for a framework, a process, and a maturity model, respectively. Establishing such a model by which your organization will conduct its ECRM work enables the incorporation of ECRM into ongoing strategic decision making and business planning.

8 NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* NIST Special Publication, 800–39, March 2011.

Sample KPI:
Extent of alignment of your cybersecurity strategy with your business strategy and objectives.

For example, if one of your key business initiatives this year is establishing a new ambulatory surgery center (ASC) line-of-business, but all of your cybersecurity resources and projects are focused on securing the hospital-based electronic health record (EHR) system, it demonstrates a lack of alignment between your cybersecurity strategy and your business strategy.

2. Resource Skilled People

The success of any business program or initiative requires employing the right number of people with the right skills, knowledge, experience, and passion about the subject matter. (Note that I'm using "employing" in a generic sense here—lack of cybersecurity talent is one of the challenges impacting cyber risk management programs at healthcare organizations. As a result, many organizations are turning to outside experts to provide ECRM services.)

Fitting your ECRM program with the right number of people often requires organizations to leverage a combination of internal and external resources. Leveraging internal resources includes not only hiring skilled ECRM staff but also creating a risk-aware culture throughout your organization. In addition, part of your leadership responsibility as board members is to build understanding of the value and benefits of your ECRM program in order to justify the resources allocated to support it.

Sample Strategic ECRM Objective:
Establish a high degree of knowledge of your chosen ECRM framework, process, and maturity model among the people throughout your organization responsible for execution.

Sample Enabling Objective:
Establish clear delegation of program responsibility.

For example, to support board oversight, establish a cross-functional executive committee and a subordinate, cross-functional working group, to help establish, implement, execute, and mature your organization's ECRM program.

Sample KPI:
Percentage of employees who have completed relevant professional training.

For example, appropriate training at the board and C-suite level could include the Cyber Risk Oversight Certificate offered by NACD. The NACD course, which is designed specifically for board members, covers cybersecurity leadership, cybersecurity literacy, and risk preparedness.[9]

3. Adopt Industry-Standard Processes

At the most basic level, a process is a specific way of doing something. Organizations with a mature ECRM process have formal, well-documented, and consistently

9 Click here for more information about the NACD Cyber Risk Oversight Certificate Program.

followed policies, procedures, and practices for risk management. These policies and procedures help ensure a risk management process that is predictable, measurable, and controlled, and which aligns with the principles of continuous process improvement (CPI).

As with other core capabilities, healthcare organizations can benefit by referencing standards-based guidance on cyber risk management processes, rather than trying to create their own from scratch.[10]

Sample Strategic ECRM Objective:
Adopt NIST-based ECRM processes (as described in NIST SP 800–39 *Managing Information Security Risk* and NIST SP 800–30 *Guide for Conducting Risk Assessments*).[11]

Sample Enabling Objective:
With respect to process, NIST recommends four steps:

1. Frame your approach to ECRM.
2. Assess your risks.
3. Respond to risks.
4. Monitor your risks.

A sample enabling objective would be: complete the first of these four steps. This step involves deciding upon and recording your approach to ECRM in an overarching framework and strategy document. This document will include your chosen approach (e.g., NIST-based), define your key terms (e.g., "likelihood," "impact," "risk rating"), specify your risk appetite, and articulate your current-year strategic objectives. The framework and strategy document should also serve as the basis of your ECRM training program.

Sample KPI:
Progress toward the development of your organization's ECRM framework and strategy document (version 1.0) as measured against your specified production schedule and final delivery date.

4. Employ Relevant Technology

Nearly all healthcare industry organizations already employ technology tools and automation to streamline clinical, administrative, and operational processes. Technology tools can also enable ECRM workflows and efficiency. More importantly, technology tools are essential for the scalability of your ECRM program.

As noted previously, a typical healthcare organization has thousands, if not tens of thousands, of information assets (data, systems, and devices). Multiply that by the other variables that comprise the risk scenario {asset-threat-vulnerability}, and a typical healthcare organization may be looking at more than 100,000 different risk scenarios that must be analyzed in order to complete a comprehensive risk analysis.

10 NIST is an excellent resource for standards-based guidance on cyber risk management, which have been developed by experts from across industry verticals, are vetted, and are freely available to the public.

11 NIST, March 2011; NIST, Guide for Conducting Risk Assessments, NIST Special Publication 800–30, September 2012.

It is simply not possible to complete—and maintain—an adequate risk analysis without using an appropriate technology and automation solution. And since the results of your risk analysis serve as the foundation for your ECRM strategy, it is critical to have the right ECRM technology solution in place. That means using standards-based technology. The advantage of using standards-based technology is that standards (such as the NIST Framework) have been developed, vetted, and successfully deployed across multiple organizations in multiple industries. Standards-based technology delivers consistent, predictable, repeatable, and measurable results, with the added benefit of explicit recognition (in the case of NIST) by the U.S. Department of Health and Human Services Office for Civil Rights (HHS/OCR) as a valid approach to ECRM. (OCR is the agency tasked with enforcing the HIPAA Privacy, Security, and Breach Notification Rules).

Ultimately, the technology and automation tools you use to support your ECRM program will range from strategic-level solutions (such as ECRM software) to operational-level solutions (such as a security information and event management [SIEM] system). The technology with the greatest relevance to the board and C-suite is the ECRM software solution, which provides the foundation for the ECRM program and should include appropriate board and C-suite-level dashboards and reporting with the information needed to execute ECRM leadership and oversight responsibilities.

The right technology tools are critical to establishing, implementing, and maturing your ECRM program. The wrong solution—or, alternately, the deployment of different software solutions in different areas of your organization—will seriously undermine the effectiveness of your ECRM program.

Sample Strategic ECRM Objective:
Implement technology and automation tools to support strategic, tactical, and operational aspects of your ECRM program.

Sample Enabling Objective:
Oversee the implementation of a standards-based (e.g., NIST-based) ECRM software solution to operationalize your organization's approach to ECRM.

Sample KPI:
The number/percent of your organization's total information assets (data, systems, and devices) under the management of your chosen ECRM software solution.

5. Ensure Organizational Engagement

The success of your ECRM program depends on the extent to which the entire organization is actively engaged in ECRM. Everyone in your organization has a role to play in your program. Even if your board and C-suite are providing appropriate leadership and oversight, if your organization's other executives, managers, and workforce members are not engaged in your ECRM program, it will fail. Without engagement and ownership of risks by line-of-business, process, and functional leaders, risk-related decisions will be made by people without the full strategic business view. This is why engagement is so critical.

All organizations have (or should have) an ECRM plan that describes the broad, strategic objectives to be pursued. At the same time, requiring departments to develop their own ECRM plans (within the context of your organization's overall

ECRM framework and strategy) can help enforce accountability for risk management throughout the entire organization.

Sample Strategic ECRM Objective:
Ensure line-of-business, process, and functional leaders are engaged in the ECRM program.

Sample Enabling Objective:
Include specific ECRM performance goals in all line-of-business, process, and functional leaders' annual objectives.

Depending on the ECRM maturity of your organization, in your first-quarter goals, you might explicitly require that each leader complete an inventory of all information assets for which they have responsibility. If your organization is further along in maturity, your objective for all line-of-business, process, and functional leaders might be to complete a comprehensive risk analysis for the most critical information assets under their purview. The ultimate objective would be for all line-of-business, process, and functional leaders to conduct a comprehensive risk analysis for all of the information assets under their purview and to update the analysis on a regular basis (including, for example, whenever there are changes in information assets, technology assets, or personnel).

Sample KPIs:
(*Quarter One KPI*) The number/percent of line-of-business, process, and functional leaders who have completed an inventory of all information assets for which they have responsibility.

(*Quarter Two KPI*) The number/percent of line-of-business, process, and functional leaders who have completed a comprehensive risk analysis for the most critical information assets under their purview.

(*Quarter Three KPI*) The number/percent of line-of-business, process, and functional leaders who have completed a comprehensive risk analysis for all of the information assets under their purview.

Clearly defining ECRM accountability at the line-of-business, process, and functional-leadership levels is an important step that can help create a culture of engagement around ECRM. The point of enabling a culture of engagement is to ensure that decisions and behaviors that support ECRM become the norm across all levels of your organization. Building the right level of engagement and a cyber-risk-aware culture is a key board responsibility, as it sets the tone for the entire enterprise.

Funding Your ECRM Program

Funding your organization's ECRM program should be framed in the same context as other enterprise business risks—considered part of the normal cost of running a healthcare organization, rather than being viewed as a subcategory of the IT budget.

For most organizations, funding ECRM requires a shift in thinking. Investing in cybersecurity is different from traditional types of healthcare investing. Hospitals and health systems are used to investing in new lines of service or new facilities that promise a significant and measurable ROI, such as buying or creating a joint venture with an ambulatory surgery center. Investing in ECRM, on the other hand, is about investing to prevent something bad from happening. Part of the calculation involved in that investment is considering the likelihood that your organization will experience a significant cyber incident. Unfortunately, the likelihood is substantial—and increasing over time. The 2020 Cybersecurity Survey conducted by HIMSS found seven in 10 organizations experienced significant security incidents in the past 12 months.[12] The healthcare industry has been a primary target for cyber attackers for some time. For healthcare organizations, investing in ECRM is about "when" a cyber attack occurs rather than "if."

Cost Repercussions of NOT Funding ECRM

In an ideal world, it would be great to be able to quantify the return on ECRM program investments. Clear ROI examples within ECRM are rarely possible, however. This is due to the unpredictable nature of cyber events, along with the breadth of the potential impact on your particular organization.

But while the ROI of ECRM investments is not readily accessible, another approach is to consider the costs of *not* investing in ECRM. As a board member, in addition to understanding that it is more likely than not that your organization will experience a significant cyber incident, you should also have a rough idea of the potential cost of such an incident.

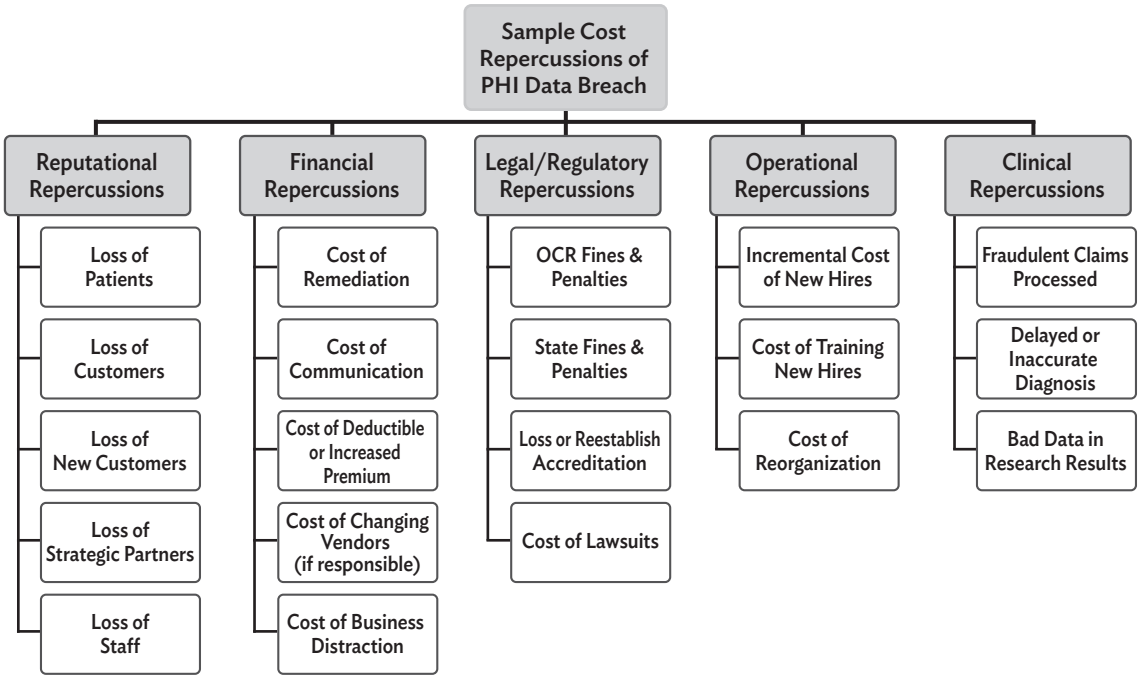
The potential costs of data breaches have been studied in detail. The Ponemon Institute conducts annual research to calculate data breach costs. Its 2020 report found that the average cost of a healthcare data breach (globally) is $7.13 million per incident. The cost per incident for healthcare is higher than for any other industry studied.[13] The report also found that data breach costs carry over for years. A longtail cost analysis showed that while 61 percent of costs occur in the first year, 24 percent of costs occur in the second year, and 15 percent of costs occur after two years.[14]

12 HIMSS, 2020 HIMSS Cybersecurity Survey, p. 4.
13 Ponemon Institute/IBM Security, *Cost of a Data Breach Report 2020*, p. 12.
14 *Ibid.*, p. 59.

While the results of the Ponemon analysis are interesting, global averages are not especially helpful when it comes to estimating your organization's unique loss exposures. The Ponemon analysis does not address your organization's unique set of information assets, threat sources, threat events, likelihood, and other factors that must be considered.

A useful tool that can help you develop a more customized estimate of the potential cost of a data breach for your organization is a publicly available costing model based on a report originally developed in 2012 by the American National Standards Institute (ANSI), The Santa Fe Group, the Internet Security Alliance (ISA), and leaders from other healthcare organizations. The report and the associated *Cost of a Data Breach Excel Model* was updated in 2017. The model enumerates the most tangible of the many costs associated with a data breach (see **Exhibit 4**).[15]

Exhibit 4: Sample Cost Repercussions of PHI Data Breach



Source: Bob Chaput, Executive Chairman, Clearwater. Adapted from The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security, *March 2012.*

15 The "Cost of a Data Breach Excel Model" from the American National Standards Institute, *The Financial Impact of Breached Protected Health Information: 2017 Update,* can be downloaded from the *Stop the Cyber Bleeding* book resource page.

> "At the end of the day, I am a cost center and a risk reduction function. I am here to enable the system and our caregivers; I can't directly help patients get better. But if you're on the Internet, no matter how small you are, you're a target. No one is immune."
>
> *—Adam Zoller, CISO, Providence St. Joseph Health*

The model details costs across five broad categories: reputational, financial, legal and regulatory, operational, and clinical. In the reputational repercussions section, loss of current and new revenues, loss of insurer/health plans, and loss of strategic partners and staff are quantified and estimated. Estimated financial repercussions include remediation costs, notification costs, and cyber insurance and third-party business associate switching costs. The model estimates various legal and regulatory costs, including OCR fines and penalties, state fines and penalties, and lawsuits. The costs of corrective actions are also considered.

Operational repercussions include the potential costs of adding new staff and reorganization to strengthen your organization's compliance and ECRM posture. Finally, in the category of clinical repercussions, the costs considered are focused on professional liability exposures from a cyber-driven medical or hospital malpractice lawsuit.

Using this model may help you develop a more accurate estimate of your organization's unique loss exposures, which can help you justify the investment in your ECRM program. However, it is important to note that even this model does not account for every possible cost.

The real point is that your organization will spend money on cybersecurity one way or another. The question is: Would your organization rather make those spending and allocation decisions proactively, with your organization's best interests as the driver? Or will your organization's spending occur reactively, in response to a cybersecurity incident?

A Note about "ECRM Debt"

Over the past decade, hospitals and health systems transitioned rapidly to digital records, largely due to the incentives and penalties included in CMS's EHR Incentive Program, also known as Meaningful Use (MU). The Meaningful Use program (now subsumed into CMS's Promoting Interoperability [PI] Program) offered billions of dollars in incentives to hospitals and clinicians to digitize clinical records.

The MU program emphasized clinical applications and data interoperability over information security (even though MU did include objectives that specifically addressed information security). As a result, many organizations implemented EHR solutions without allocating funds to manage the cyber risks associated with EHR implementation.

This is what I refer to as "ECRM debt." As a rule, when healthcare organizations undertake any kind of digital transformation, every program, project, or initiative should include not only an examination of the cyber risk implications, but also a budget for addressing those implications. By and large, this did not happen during the

race to collect Meaningful Use incentive money. This has left the healthcare industry with a huge ECRM debt—dollars that should have been spent on managing cyber risk simultaneously with EHR and related systems implementation. The cyber risk implications of those projects now need to be addressed.

Going forward, hospitals and health systems need to not only address their ECRM debt, but also put practices in place to ensure funding for ECRM for all new projects. Rather than thinking of ECRM as a line item in or percentage of your IT cost budget, think of your ECRM spend in terms of a percentage of each line-of-business, process, and functional leader's revenue budget.

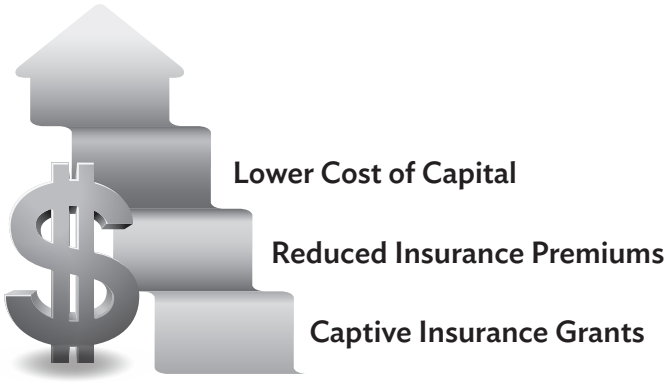
The best way to ensure that you don't incur additional ECRM debt going forward is to withhold approval of any initiatives, projects, or programs involving healthcare data, systems, or devices, unless and until specific and appropriate funding has been designated for cyber risk management. Successful ECRM outcomes can best be achieved by building ECRM into business programs and initiatives—following the principle of "security-by-design"—rather than trying to add ECRM after the fact.

Potential Sources of Funding for Your ECRM Program

As healthcare organizations move to institutionalize funding for ECRM throughout the organization, they are challenged to find funding, since investing in an ECRM program does not produce a new revenue stream. However, there are ways in which implementing a strong ECRM program can positively impact your organization's bottom line. A strong ECRM program may:

- Lower the cost of capital
- Be leveraged to reduce insurance premiums
- Make use of captive insurance grants (see **Exhibit 5**)

Exhibit 5: Three Specific Sources of ECRM Funding



Source: Bob Chaput, Executive Chairman, Clearwater.

Realizing Lower Cost of Capital

Access to capital is vital—without it, healthcare organizations would be unable to acquire new technologies, start new lines of business, renovate facilities, or offer new programs. In order to stay competitive, healthcare organizations have to maintain access to capital at low rates.

ECRM is playing an increasingly important role in this arena. Credit-rating agencies, including Standard and Poor's, Moody's Investors Service, and Fitch Group, have all implemented or signaled consideration of the financial impact of a cyber attack on an organization's credit rating. In 2018, when Moody's created a new position—Head of Cyber Risk—the Moody's President said, "As with environmental, social, and governance risks, we see cyber risk as an area of increasing relevance to issuers, investors, counterparties, and government authorities as it impacts operational and credit risk."[16]

In 2019, Moody's released a research report which assessed the cyber risk of 35 industry sectors, including healthcare. The healthcare sector—including hospitals, pharmaceutical companies, and medical device manufacturers—was classified as high risk. Of all 35 sectors rated, only three others (banks, securities firms, and financial market infrastructures) were found to be at "high risk."[17]

The report also indicated one of the key factors in Moody's credit analysis going forward may include "the extent of an entity's investment in cyber defenses before an event…."[18] In other words, a robust ECRM program may positively impact your credit rating and help your organization obtain more competitive rates for capital. This benefit can be viewed as an indirect source of funding for your ECRM program.

> "We determine our cybersecurity maturity using the NIST framework's five-point scale and set goals to move higher on the scale. We take the same kind of approach with the same level of importance as we do with finance and financial risk scenarios using S&P and Moody's medians."
>
> *—Jason Joseph, Chief Digital & Information Officer, Spectrum Health*

Leveraging Reduced Insurance Premiums

Insurance premiums are another area—like cost of capital—you can leverage to help fund your ECRM program. It is a common insurance practice to lower premiums when the insured takes actions to reduce risk. For example, your organization may receive more competitive rates for medical professional liability insurance premiums when your organization is able to demonstrate the implementation of training, quality, and patient-safety programs.

The same thing is beginning to happen with cyber liability insurance. Beginning in 2012, the Cybersecurity & Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, held a series of sessions with insurers and other

16 Moody's Investor Relations, "Moody's Names Derek Vadala as Global Head of Cyber Risk for MIS" (press release), October 17, 2018.
17 Moody's Investors Service, "Credit Implications of Cyberattacks will Hinge on Long-Term Business Disruptions and Reputational Impacts" (research announcement), February 28, 2019.
18 *Ibid.*, p. 3.

key stakeholders to discuss the relationship between cyber risk management and cybersecurity insurance. CISA has suggested that:

A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection.[19]

Through conversations with stakeholders, CISA hoped to expand the cybersecurity insurance "market's potential to encourage businesses to improve their cybersecurity in return for more coverage at more affordable rates" and to develop "new cybersecurity insurance policies that 'reward' businesses" for adopting and enforcing best practices—such as implementing a robust ECRM program. In fact, this concept is beginning to play out in the marketplace. As one security expert wrote:

> "While it's pretty straightforward that you can get a safe driving deduction on vehicle insurance or cut the cost of healthcare premiums by signing a non-smoking certification, there is no widely advertised fee-reduction structure for cyber insurance. Yet, implementing cybersecurity best practices and remaining compliant with industry standards will lower your premiums with many carriers."[20]

The key to reducing your insurance premiums as a way to help fund your ECRM program is to collaborate with internal executive colleagues, your cyber risk broker, and carrier underwriter. Get advance buy-in from the underwriter that they will work with you to review your ECRM program and take it into account when pricing your cyber liability premiums. Working together, you can create a win/win scenario that keeps your premium costs down and, at the same time, mitigates the insurer's risk of a large payout.

Captive Insurance Program Grants

As risk management and insurance models continue to evolve, more healthcare organizations are turning to a captive insurance model in innovative ways. The captive insurance model gives organizations more control over the risk management process and can serve as a way to jump-start your ECRM program.

According to a 2020 report on captives by Marsh, a global leader in insurance broking and risk management, "cyber risk tops the list of new areas that regulators see captives writing more frequently."[21]

You may be able to use your captive as a source of funds for your ECRM program even if your captive insurance company does not currently have a cyber liability line. The lines separating medical professional liability, privacy risk, and cyber risk have become blurred. In addition, the costs associated with privacy risk and cyber risk can easily exceed the cost associated with an individual instance of medical professional liability. The captive insurance model is one that healthcare organizations would do well to consider when they are examining cyber risk and exploring how to fund an ECRM program.

19 CISA, "Cybersecurity Insurance" (Web page).
20 Jeremiah Talamantes, "How to Lower Your Cybersecurity Insurance Premiums," RedTeam Security.
21 Marsh & McLennan, *Captives Offer Value in Uncertain Times: Effective Tools to Address Pandemic and Other Risks,* September 2020, p. 9.

The Ideal ECRM Board Meeting

ECRM should be a standing agenda item on a quarterly basis. There are at least four good reasons for this:

1. As a board member, you cannot be effective at providing leadership and oversight for the organization's ECRM program unless you have the opportunity to become informed about and engaged with ECRM and with your organization's specific ECRM challenges.
2. Your organization cannot establish, implement, or mature an effective ECRM program unless that program is integrated into every part of your organization. That integration starts at the top—with the board.
3. Board involvement in ECRM is an expectation of the regulatory bodies that oversee compliance with information security and information privacy laws. According to Leon Rodriguez, former director of HHS/OCR, "Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected."[22]
4. "Board involvement" in ECRM is a documented factor associated with a decrease in the average cost of a data breach.[23]

Too often, the first ECRM meetings in which a board becomes involved occur only as the result of a cyber crisis. If your organization has not yet had a board meeting focused on ECRM, now is the time to do so, even if it is a special, separate kickoff meeting. Seize the opportunity to commit to board education and to begin establishing, implementing, and maturing your ECRM program.

General Logistics

Adhering to a few, general best practices will help ensure that the time your board devotes to ECRM is meaningful and productive. To that end, here are a few guidelines that can help you make the most of ECRM discussion in your board meetings.

Frequency

ECRM should be on the agenda of the full board on a quarterly basis. Depending on the maturity of your ECRM program, as much as 90 minutes of each quarterly board meeting may be required to discuss ECRM risks and treatment, program advancement, current events, and board education. (Note that the frequency of meetings depends upon the specific governance tier being referenced. **Exhibit 6** (on the next page) provides more detail on suggested meeting frequency by governance tier.)

22 U.S. Department of Health and Human Services, "HHS requires California Medical Center to Protect Patients' Rights to Privacy" (press release), June 13, 2013.
23 Ponemon Institute/IBM Security, p. 42.

Exhibit 6: Recommended ECRM Meeting Schedule by Governance Body

Tier	Governance Body	Members	Function	ECRM Meeting Frequency
1	Full board or designated board committee (e.g., audit & compliance committee or a specific ECRM oversight council)	Full board or designated committee	Sets direction and provides oversight.	Quarterly
2	ECRM executive steering committee	CEO + his/her full team	Ensures execution of the ECRM program.	Monthly
3	ECRM cross-functional working group	May include representatives from legal, risk management, finance, HR, audit, compliance, privacy, IT, clinical engeineering, security, quality, and/or others.	Executes the steps to establish, implement, and mature the ECRM program.	Several times per month

Source: Bob Chaput, Executive Chairman, Clearwater.

Presenter

If ECRM has been integrated into your organization's ERM program, it would be appropriate for your chief risk officer (or most trusted risk management executive) to lead the ECRM discussion at the board meeting. If ECRM has not yet been integrated into your ERM program, I recommend you do so. Historically, healthcare CROs have focused on medical malpractice. However, security research and demonstrations are serving as harbingers of the inevitability of cyber-driven medical professional liability lawsuits. It's appropriate for other leaders, such as the CIO, CISO, CFO, CCO, CAE, and CMO, to be present during the ECRM discussion. However, if your CIO or CISO is currently leading the ECRM discussion, it is time to make the change to the CRO.

Presentation Guidelines

Board members often receive ECRM reporting that is too detailed, too technical, and too difficult to interpret. Board members don't need stacks of detailed operational data: they need succinct summaries and actionable insights.

The NACD handbook, *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards*, includes information about how information should be presented to boards. NACD suggests that information for the board should:

- Be relevant to the audience (full board; key committee).
- Be reader-friendly: use summaries, callouts, graphics, and other visuals, and avoid technical jargon.
- Convey meaning: communicate insights, not just information.
  - » Highlight changes, trends, and patterns over time.

  - » Show relative performance against peers, against industry averages, against other relevant external indicators, etc. (e.g., maturity assessments).
  - » Indicate impacts on business operations, costs, market share, etc.
- Be concise: Avoid information overload.
- Above all, enable discussion and dialogue.[24, 25]

Three Critical Subtopics

Each of the following ECRM subtopics should be discussed at every quarterly board meeting. I recommend allocating 30 minutes to each subtopic.

1. Risks and Treatment

The board's oversight responsibilities include ensuring that initial and ongoing risk analysis is being conducted; determining the organization's risk appetite; and the oversight of risk treatment.

Risk analysis: Risk analysis describes the process of identifying, estimating and prioritizing risks to an organization's data, systems and devices. The single largest ECRM issue facing healthcare organizations today is the failure or inability to identify all of their unique risks.

Risk appetite: After you have identified and rated all of your organization's risks, you must decide which risks you will treat, and which risks you will simply accept. Risk appetite is generally defined as the level of risk an organization is willing to assume in order to achieve an acceptable level of risk management. An organization's risk appetite will change over time, as the threat landscape changes and as the resources the organization has allocated to manage risk changes. Setting, communicating, and adjusting your organization's risk appetite is one of the most important board and C-suite responsibilities with respect to your organization's ECRM program.

Risk treatment: Once your organization has identified each possible risk, and assigned a rating based on likelihood and impact, your organization will need to make choices about how to treat risks that are rated at or above your organization's risk appetite level. The organization will accept risks that are rated below your risk appetite. For risks at or above your risk appetite, you will have to determine whether to avoid, mitigate, or transfer those risks.

2. Program Advancement

ECRM is not a once-and-done proposition. The threat landscape is constantly evolving. Your organization is constantly changing, adding new equipment, adding lines of service, expanding delivery methods (e.g., increasing access to telehealth), changing personnel, etc. Any organizational change that impacts your organization's data, systems or devices is going to necessitate a re-evaluation of risks, risk appetite, and consideration of risk treatments. That is why when we talk about ECRM, we

24 Larry Clinton, et al., *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards,* NACD, p. 14.

25 The *Stop the Cyber Bleeding* book resources page also includes examples of board-appropriate presentation slides and handouts that can be uses as a template for board-level ECRM reporting.

talk about establishing, implementing, and maturing an ECRM program. There is always more work to be done. In this respect, your ECRM program is no different than any other program within your organization in which you desire to see continuous improvement.

3. Relevant Current Events and Board Education

Finally, it is important that every board meeting includes both an update on relevant current events and a board education component.

Relevant current events: The board needs to be apprised of both internal and external events that affect your organization's risk posture. The board should hear about internal events that compromise information assets in a timely manner, rather than waiting for the quarterly board meeting. At the quarterly board meeting, it is important for the board to be briefed on high-profile events, such as data breaches at peer organizations or OCR enforcement actions that have been taken against healthcare organizations. These incidents should be presented in the context of "lessons learned."

Board education: Board education is an ongoing process. Over time, as the right subject matter experts deliver the right content, board members will become more fluent in ECRM topics and therefore better able to execute their ECRM oversight responsibilities. A few examples of effective board member education activities include:

- Hiring outside experts to brief the board on "ECRM 101"
- Engaging outside counsel to discuss the legal implication of a breach
- Inviting external advisors, such as FBI representatives or OCR staff, to discuss the healthcare cyber risk environment.

Finally, don't forget to document all of the board's discussion related to ECRM. Diligent recordkeeping of the boards ECRM discussion and decisions creates an important record that the board is exercising duty of care and reasonable diligence with respect to cyber risk management oversight.

Case Examples: Board Reports that Make an Impact

Zoller reports to the Providence board on a quarterly basis with the following information:

- A programmatic update on the status of projects currently moving forward to directly reduce cyber risk.
- A deep dive on tier 1 incidents.
- A threat spotlight to educate as well as show the board actual threats targeting Providence. "For example, I will show the board screen shots of actual phishing emails that our caregivers are receiving, to demonstrate what the board should be watching out for, that show how threat actors are targeting Providence and the types of information attempting to be stolen," said Zoller.
- Cyber Balance Sheet: pulled from Providence's risk reporting solution, it includes several domains: network defense, vulnerability management, patch management, identity and access management, governance risk compliance (GRC), data protection, and data source quality and asset inventory accuracy. The dashboard uses AI visualization and analytics to show a compelling picture that is easy to understand. "This allows me to have conversations with the board about the actual risks we face, and how we are measuring our progress to address those risks," said Zoller.

Zoller emphasized that this kind of information helps the board to focus on developing a deeper understanding of the actual risks and therefore how to prioritize and allocate resources for risk mitigation.

Joseph takes the approach of helping the Spectrum board understand the system's overall cybersecurity maturity and overall risk—working to quantify it in a way the board can understand, including whether the necessary steps are being taken to mitigate the organization's risk. "I strive to give them objective evidence, from penetration testing to Red Team[26] findings, our list of vulnerabilities, and third-party information," said Joseph. The board typically challenges Joseph with questions such as:

- How do you know this is good enough?
- How do you know this assessment is targeted at the right areas?

In Joseph's experience, it is more impactful to talk about cybersecurity with a story. "The first time I presented to the board, I told them the story of a cyber event that happened through the lens of our framework. I walked them through the story, and I showed them how each part of the NIST model applied to how we handled the event, and if we did not have certain things in place, what would have happened. It helped make some of the concepts more real for the board, beyond the specific language of the framework, beyond compliance, beyond descriptors of risk."

Parker and IU Health's CRO conduct a month-long exercise every September in which they score all of the organization's cyber risks using the same scoring system as they would for other enterprise risks. The exercise includes surveys of all senior executives, and then the top risks are presented by the CRO to the board. "We rank ransomware risk 10 times higher than a hospital closure, which sends a very strong message," said Parker. "The board is used to risk scores in the hundreds; we show them cyber risk scores starting at 4,000 and they know it is something that needs to be dealt with urgently and strategically."

26 "Red Teaming" is a full-scope, multi-layered attack simulation designed to measure how well a company's people and networks, applications, and physical security controls can withstand an attack from a real-life adversary.

20 Questions for Board Members

Board members need to be informed and engaged in order to execute their ECRM oversight responsibilities. When ECRM, including ECRM education, becomes a regular part of the board agenda, it becomes easier for board members to ask relevant questions that facilitate oversight. These questions provide a starting point for thinking about and gathering the information board members need to establish, implement, and mature an effective ECRM program.

10 Questions for Board Members to Ask Themselves

1. As a board member, do you understand how the concepts of *fiduciary responsibility* and *duty of care* relate to your obligation to manage your organization's cyber risk?
2. Do you understand your personal liability as it relates to the robustness of your organization's ECRM program?
3. Do you feel that you have a good understanding of the cyber risks your organization faces?
4. As a board member, have you been updated on the privacy, security, and breach notification regulatory enforcement environment in the last 12 months?
5. Do you have an accurate understanding of how much a data breach could cost your organization? Does your estimate include reputational, financial, legal and regulatory, operational, and clinical costs, as well as intangible costs?
6. How important is it to you to protect your organization from the fines, fees, settlements, and other costs associated with the compromise of confidentiality, integrity, and availability of patient data (e.g., data breach, ransomware attack, etc.)?
7. Does your organization's vision, mission, strategy, values, and services inform your ECRM program?
8. Do considerations about cyber risk inform your organization's business strategy and planning efforts?
9. Does your organization have a good ECRM governance structure in place, that clearly articulates *who* makes *what* ECRM decisions, and *how* and *when*, using what data and facts?
10. Is your organization allocating an appropriate amount of time to ECRM discussions at the board level?

10 Questions for Board Members to Ask Management

1. Is ECRM currently a part of your hospital or health system's overall risk management program? Or is cyber risk management siloed in the IT department?
2. Has your hospital or health system been subject to one or more cyber attacks in the past 12 months?
3. Is your organization's attack surface increasing? Activities that can increase your attack surface—and therefore, increase your cyber risk—include handling increasing volumes of data, expanding the network with IoT and IoMT devices, expanding healthcare delivery outside the walls of the facility via telehealth and other virtual care options, data sharing with business and associates/third-party partners and merger and acquisition activity. There are some, but not all, of the activities that can increase your organization's attack surface. How many of these activities apply to your organization?
4. Is your organization compliant with all relevant regulations and standards, including, but not limited to, Centers for Medicare and Medicaid Services (CMS) regulations (including the expectations and guidance of OCR), HIPAA requirements, General Data Protection Regulation (GDPR) requirements, state and local requirements, and other requirements that may be applicable (depending on the type of institution) including the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and the Payment Card Industry Data Security Standard (PCI DSS)?
5. Has your organization conducted a comprehensive, detailed risk assessment (also known as an OCR-Quality® Risk Analysis) by identifying and rating your organization's unique risks (assets/threats/vulnerabilities)? Have the results of that analysis been communicated to the board and C-suite in an actionable way?
6. Is your organization using a risk-based approach to ECRM or a checklist-based approach? That is, are you making risk-mitigation decisions (e.g., what controls to implement) based on your organization's unique exposures, or are you implementing someone else's checklist of controls?
7. What ECRM framework, if any, has your organization adopted? Is it an internationally recognized, risk-based standard, such as the NIST Cybersecurity Framework? How is it being used?
8. What ECRM process, if any, has your organization adopted? Is it an industry-standard approach, such as that advanced by NIST?
9. Is your organization's current level of ECRM funding adequate to address the ECRM debt your organization has built up over the past 10 years? What "critical" or "high" legacy risks need to be treated as soon as possible?
10. What stage of change is your organization in with respect to establishing, implementing, and maturing your ECRM program? If you have an established ECRM program, is that program improving over time? Is your organization proactively measuring program improvement?

References

Advisory Board. *Cybersecurity Cheat Sheets for the C-Suite and Board*. Updated May 9, 2019.

Chaput, Bob. *Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)*. Nashville, TN: Clearwater, 2020.

Clinton, Larry, Josh Higgins, and Friso van der Oord. *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards*. National Association of Corporate Directors (NACD) and Internet Security Alliance (ISA), 2020.

Cybersecurity & Infrastructure Security Agency (CISA). "Cybersecurity Insurance" (Web page.) Accessed March 13, 2021.

Governance Institute, The. *On Board! An Orientation to Healthcare Governance* (video). 2020.

HIMSS. *HIMSS Healthcare Cybersecurity Survey*. 2020.

HIPAA Journal. "2020 Saw Major Increase in Healthcare Hacking Incidents and Insider Breaches." March 16, 2021.

HIPAA Journal. "VMWare Carbon Black Explores the State of Healthcare Cybersecurity in 2020." February 8, 2021.

Marsh & McLennan Companies. *Captives Offer Value in Uncertain Times: Effective Tools to Address Pandemic and Other Risks*. September 2020.

Moody's Investor Relations. "Moody's Names Derek Vadala as Global Head of Cyber Risk for MIS" (press release). Moody's Investors Service, October 17, 2018.

Moody's Investors Service. "Moody's - Credit implications of cyberattacks will hinge on long-term business disruptions and reputational impacts" (Research Announcement). February 28, 2019.

National Institute of Standards and Technology (NIST). *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30, September 2012.

National Institute of Standards and Technology (NIST). "History and Creation of the [NIST Cybersecurity] Framework" (Web page), updated November 21, 2019. Accessed February 18, 2021.

National Institute of Standards and Technology (NIST). *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800–39, March 2011.

Ponemon Institute, LLC/IBM Security. *Cost of a Data Breach Report*. 2020.

Talamantes, Jeremiah. "*How to Lower Your Cybersecurity Insurance Premiums*." RedTeam Security. Accessed March 13, 2021.

U.S. Department of Health and Human Services. "HHS requires California medical center to protect patients' right to privacy" (press release). June 13, 2013.