Benefits of Enterprise Risk Management for a Health Care Organization's View of Privacy and Security Risks

Marti Arvin, Cynergistek

Enterprise Risk Management (ERM) is a big concept. As a starting point, it is important that everyone is on the same page when using this term. ERM has been defined several ways. Chapter One of the *Risk Management Handbook for Health Care Organizations* defines ERM as "an ongoing series of interrelated activities designed to identify, assess, manage, and monitor the risks facing an organization."[1] The American Society for Healthcare Risk Management (ASHRM) further states "Enterprise Risk Management in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connection to total value."[2] The Committee of Sponsoring Organizations (COSO)[3] defined ERM as "a process, affected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[4] But in 2017, COSO changed the definition to state: "Enterprise risk management is not a department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."[5]

Whichever definition is used, ERM is the process of identifying all organizational risks and evaluating and prioritizing when and how to approach these risks. Fundamentally, ERM is about addressing how the risks faced by the organization impact its operational and strategic plans. It is important that everyone in the organization understand their role in the ERM process. Effective ERM is about the whole "enterprise." To evaluate risk on an enterprise level the person or team leading the process must be able to cohesively identify all the risks the organization faces, not just its compliance risks.

Unfortunately, health care organizations have traditionally taken a siloed, non-enterprise approach to risk management. Privacy and compliance risks were often addressed by the compliance office, patient care and malpractice risks by risk management or legal, information security risks by either the compliance office or information technology (IT), and financial risks by the finance office. In this siloed approach, overarching considerations such as reputational and/or brand risks may not be considered. The result is a disjointed, non-strategic approach to risk management with zero consideration of risks across the organization or the "enterprise." With an ever-decreasing financial margin, health care organizations can no longer afford to handle risks in this way.

Another important part of the ERM process is determining how best to address the identified enterprise risks. There are generally five ways to address identified risks:

- *Accept the risk*—the organization has identified and quantified the risk but decided to take no further action and is willing to accept the consequences if the risk occurs.
- *Avoid the risk*—the organization decides certain strategic plans or operational activity will not be initiated or will be discontinued so that the risk is no longer present.
- *Transfer the risk*—the organization transfers the risk in question to a third party, such as through a contractor or insurance coverage.

- *Mitigate the risk*—the organization takes steps to minimize the impact of the risk if it does occur.
- *Exploit the risk*—the organization believes the risk could have a positive impact if it did occur and works on ways to increase the positive impact.

Privacy and Information Security in Enterprise Risk Management

When thinking about ERM, privacy and information security risks for the health care organization are critical considerations. If leaders are just thinking "Have we met the requirements of HIPAA?" it is unlikely all potential risks will be considered and addressed. Health care organizations that have had a significant data compromise appreciate in hindsight the implications and impacts the compromise had across multiple business units.

In health care, the risks associated with information privacy and security non-compliance are often discussed generally, but outcome-specific implications of non-compliance also require consideration. For example, an organization can follow the Health Insurance Portability and Accountability Act (HIPAA) regulations yet still experience significant risk in the privacy and security of its information if a user is not careful and falls prey to a phishing email, resulting in potential exposure of large quantities of data. The organization might have done several things to try to avoid this contingency, such as training, running white-hat phishing exercises, and implementing two-factor authentication, but if the user is careless, all of this was for naught.

When considering overall ERM, the implications of privacy and security risks are much broader than the direct risks in these areas. A ransomware attack is another good example of an organization's need to more broadly assess outcome-specific ERM implications. If the hacker gets into an electronic medical record system requiring the need to go to downtime procedures, the move to paper processes creates a risk cascading effect across other areas. When the electronic system was functioning correctly, for example, getting the right medication to the right patient in an electronic world included several steps to avoid an adverse event. The order was electronically entered and sent to the pharmacy or a medication was withdrawn from an on-unit supply, and the patient's wristband was scanned against the label on the medication to ensure the right medicine was given to the right patient in the right dose.

What if the ransomware attack ultimately prevents one or more of these steps? Even with good downtime procedures, the workforce is being asked to do something in a new way. Sometimes the simplest things can be overlooked when operating under downtime procedures. If the organization's workforce has used the electronic medical record for most of their career, they likely are used to the computer calculating dosages. If the dose of a medication is in milligrams/kilogram and the only patient weight that is available is in pounds, can the end user properly make the conversion? Issues like this could increase the risk of an adverse event such as the wrong patient getting the medication or the right patient getting the wrong dose. If the risk assessment process was siloed and only IT was considering information security risks would this clinical impact be anticipated?

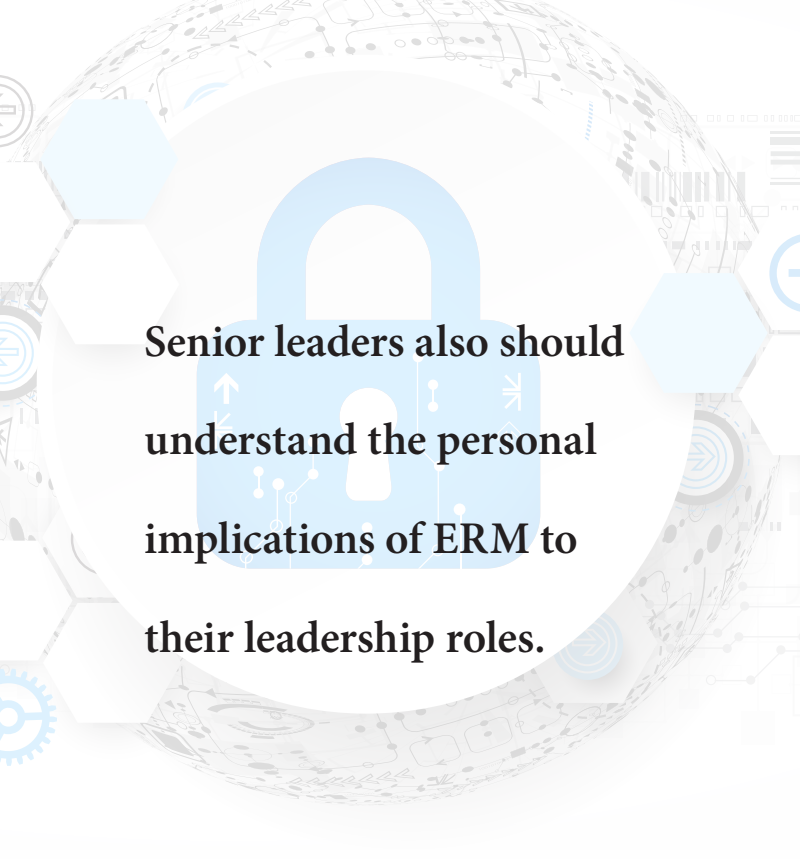
A different clinical impact consideration related to IT is the security of medical devices. This is an area that, again, is often siloed in a health care organization. The machines might be managed by biomedical engineering, but are they considering the security of the device or focused only on ensuring it is inventoried and functions correctly before it is put into operation? If the machine is not secure, it can provide an opening for a hacker to access the organization's network. A bad actor also could potentially change settings on the device, infect devices with ransomware, and hold the organization hostage. This could threaten not only the organization's IT infrastructure and privacy of information but also patient care.

These types of issues underscore why, when an organization is thinking about risk, it needs to have multiple players involved to help ensure thorough and complete consideration of the linkages between risk areas. A scenario where no interdepartmental linkage is found usually is the exception.

The risks around a ransomware attack and downtime procedures include the potential for a significant financial impact such as:

- Cost of unanticipated
  - –overtime for current staff who are dealing with the crisis; and,
  - –supplemental staff to support the day-to-day operations while current staff deal with the crisis;
- Cost of outside expertise like attorneys, forensics firms, other consultants, breach response support;
- Lost revenue because
  - –elective procedures are cancelled; and,
  - –paper documentation is insufficient to support billing for the service;
- Decreased cash flow because
  - –services are postponed; and,
  - –billing is delayed because of the use of paper documents and manual processes.

Fundamentally, ERM is about addressing how the risks faced by the organization impact its operational and strategic plans.



Senior leaders also should understand the personal implications of ERM to their leadership roles.

These are only a few of the ways that information security risk can impact a health care organization financially. There also can be reputational risk if the incident results in the need to notify individuals, the community, and the Office for Civil Rights of the breach.

Senior leaders also should understand the personal implications of ERM to their leadership roles. In an effective ERM program, there is an expectation the senior leaders and members of the board of directors have asked appropriate questions to ensure they are sufficiently informed to make appropriate decisions. There also is an expectation that this group understands their cyber resilience, i.e., the organization's ability to anticipate, adapt to, and promptly recover to normal operations when an event occurs. These expectations tie to overall fiduciary responsibilities.

Unfortunately, all too often when cybersecurity is discussed, senior leaders may tune out if all they hear is "geek speak." Instead, they need to ask questions. They may need to have someone in the room who can translate the "geek speak" into understandable business terms that are more familiar. This will allow them to incorporate ways to address the enterprise risks into the overall business strategy. If issues were brought to their attention but they failed to address them because they lacked a full understanding of the risks, there could be a finding that they breached their fiduciary responsibilities.

Strategies to Address Privacy or Information Security Risks

In an organization exercising ERM processes, all the risks associated with a privacy or information security incident are considered. The organization then embraces a strategic approach to address the risks. Using the ransomware example and the possible five steps of risk management detailed earlier, the organization might consider some of the following actions.

To mitigate risk, the organization may implement a variety of security measures such as data loss prevention, two-factor authentication, a security operations center to monitor network traffic, and alerts so users can identify emails as external and not from their internal colleague.

The organization also may decide to implement mandatory privacy and security training, increase the number of privacy and information security reminders sent to users, and engage in white-hat phishing campaigns to educate users on spotting possible phishing emails. Implementing a strong incident response process also is a mitigation step. The more structured the incident response process the more likely an incident will be detected and contained early, reducing the impact on operations to the organization's significant benefit.

Transferring the risk may be another option by acquiring a cybersecurity insurance policy. While these policies may not fully transfer all the risk associated with a cybersecurity incident, they often can absorb some of an organization's financial risk. For example, the policy may cover the cost of certain expenses such as outside legal counsel and forensic and breach response support.

It is unlikely that avoidance is an appropriate risk management strategy for any health care organization when dealing with privacy and information security risk, simply because there is often no way to avoid engaging in the activities that create these risks. The organization may asses the cost of certain mitigation steps and determine that instead of implementing those measures, the organization will accept some risks. Or the organization may decide that transferring the risk is too costly. Unfortunately, for many health care organizations this is not the thoughtful process that it needs to be. Too often risk is accepted without fully understanding the implications. It is not an ERM decision made with an understanding of the total risk to the organization's operational functions and strategic plans. Rather, it is a decision based solely on the current impact to the bottom line. This method of risk management has often proven penny wise and pound foolish.

Management Benefits of an ERM Approach

ERM is about understanding an organization's entire risk profile and ensuring the approach to risk matches the organization's risk-tolerance appetite. ERM considers a variety of risks including financial, reputational, regulatory, and operational. Using this approach to risk management permits the organization to be strategic about how to address risk. Considering ways to manage risk can take into account all of the organization's current and planned activities.

For example, an organization's privacy team may identify the inability to perform proactive user monitoring as a risk to the ability to identify improper access to electronic protected health information (ePHI). Another business unit may identify drug diversion as a risk to the organization. If the two groups operate in silos, the organization may miss an opportunity to explore a possible technology solution that addresses both risks. The organization may end up investing in multiple solutions, which generally is less cost effective. If the organization is

engaged in ERM, the likelihood that leadership will be aware of both risks increases the organization's ability to consider a single, more cost-effective solution.

Health care organizations must improve how they address privacy and information security risks, while acknowledging that this improvement cannot be accomplished in a vacuum. Continuing a siloed risk management approach that health care has traditionally taken is not strategic or cost effective. Instead, improving privacy and information security should be part of a broader ERM discussion for the organization. A failure to understand and execute on an ERM approach will invariably leave gaps in the understanding of the strategic and operational risks associated with privacy and information security.

Understanding how these risks relate to the bigger picture will help an organization that thinks it cannot afford privacy and information security risk management activities recognize why such an investment is crucial. The organization can decide to make or forego the upfront investment, but if the decision is to pay later, it is likely the cost will be much higher. C

Marti Arvin is an Executive Advisor at Cynergistek. Arvin has extensive experience in building and managing compliance and research programs, with more than three decades of operational and executive leadership experience that includes compliance, research, and regulatory oversight in academic medical centers and traditional hospital settings. She is a nationally recognized speaker, contributor, and thought leader in the areas of health care compliance and research.

Thanks go out to the leaders of the Enterprise Risk Management Task Force for contributing this feature article: **Michaela D. Poizner**, Baker Donelson Bearman Caldwell & Berkowitz PC, Nashville, TN, (Chair); **Susan N. Goodman**, Tucson, AZ (Vice Chair—Publishing); **Rachel Polzin**, SSM Health, Fitchburg, WI (Vice Chair—Educational Programming); **Lisa Snell Rivera**, Bass Berry & Sims PLC, Nashville, TN (Vice Chair—Member Engagement); **Danene Spaeth**, Providence Health & Services, Renton, WA (Vice Chair—Publishing); **Paul S. Weidenfeld**, Law Offices of Paul Weidenfeld PLLC, Washington, DC (Vice Chair—Educational Programming).

It is unlikely that avoidance is an appropriate risk management strategy for any health care organization when dealing with privacy and information security risk, simply because there is often no way to avoid engaging in the activities that create these risks.

Endnotes

1 Roberta L. Carroll, Gisele A. Norris, and Michael Zuckerman, *Basics of Enterprise Risk Management in Healthcare*, Risk Mgmt. Handbook for health Care Orgs., Vol. 1: The Essentials, Am. Soc'y for Healthcare Risk Mgmt. (6th ed. 2011, Chapter 1), https://books.google.com/books?id=oXxfuGuVpWMC&pg=PT178&source=gbs_toc_r&cad=4#v=onepage&q&f=false.

2 Roberta L. Carroll, *et al.*, Am. Soc'y for Healthcare Risk Mgmt., Enter. Risk Mgmt: A Framework for Success 5 (2014), https://www.ashrm.org/system/files/media/file/2019/06/ERM-White-Paper-8-29-14-FINAL.pdf.

3 COSO was organized in 1985 through a joint initiative of five sponsoring organizations: American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, The Association of Accountants and Financial Professionals in Business, and The Institute of Internal Auditors. The National Commission created by this organizational sponsorship included a mission to provide leadership and guidance in ERM as part of the larger mission of improving organizational governance and reducing fraud.

4 Comm. of Sponsoring Orgs. of the Treadway Comm'n, Enter. Risk Mgmt.—Integrated Framework, Exec. Summary 2 (Sept. 2004), https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf.

5 Comm. of Sponsoring Orgs. of the Treadway Comm'n, Enter. Risk Mgmt. Integrating with Strategy and Performance, Exec. Summary iii (June 2017), https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.