Building an Effective Enterprise Cyber Risk Management Program

By Bob Chaput, Clearwater

The CEO of a large, national ambulatory surgery center organization once told me, "Taking care of our patients' information is just as important as taking care of our patients." His commitment to information security served as a touchstone for his organization as they built their enterprise cyber risk management (ECRM) program.

A robust, proactive ECRM program is your organization's best defense against cyber attacks. In the first place, if executed properly, an ECRM program will minimize the risk of an incident occurring. But if/when a cybersecurity incident or data breach does occur, an effective ECRM program can help shield you and your organization from claims of negligence or willful neglect.

> With the mass digitization of healthcare and the explosion of electronic healthcare data, systems, and devices, the ability to protect the confidentiality, integrity, and availability of patient information is critical to your organization's success.

In a best-case scenario, you would be able to defend yourself and your organization by honestly and unequivocally communicating the following points:

- Our board has been and is proactively engaged in ECRM.
- Our board has adopted and communicated strong governance principles that require a risk-based (not checklist-based) approach to ECRM.
- Our executive team is responsible and accountable for ECRM and we have formed a cross-functional team of leaders across the organization to execute our ECRM strategy.
- We have adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework and use it as the basis for our ECRM program.
- We have implemented the internationally recognized NIST process for ECRM (NIST Special Publication 800-39 and NIST Special Publication 800-37).
- We engage with our liability insurance brokers on a regular basis to inform our cyber risk-transfer and risk-retention decisions.
- To ensure progress and continuous process improvement of our ECRM program, we monitor all changes in our program, measure our program maturity annually, and execute continuous improvement plans.
- In recognition of the dynamic nature of cyber risks, we conduct ongoing risk analyses and execute risk management plans to ensure any risks we accept are below our risk appetite.

Some of these statements might not be meaningful to you at this point. That's okay. The goal, drawing on my professional experience, is to give you the understanding and actionable information needed to be able to establish or improve your organization's ECRM program. When you have implemented the steps I outline in this article, you will be able to make the statements above, with the confidence and knowledge that you have put into action a program that meets accepted standards of care for managing cyber security risk, protecting your patients and organization from cyber threats.

Key Board Takeaways

The following questions will help you think about the terms and concepts referenced in this article and how they might be applied in your organization:

- Has your organization's C-suite and/or board discussed and agreed upon a common set of definitions related to cyber risk and cyber risk management?
- Have these definitions been documented in your organization's ECRM strategy and communicated throughout the organization via ECRM training?
- Has your organization already, or is it currently, conducting ongoing, rigorous, comprehensive, enterprise-wide risk analysis that would meet the Office for Civil Rights' expectations?
- As C-suite executives and board members, have you discussed, debated, and established your cyber risk appetite?
- If your organization has conducted a risk analysis, are you using the results of that analysis to inform your cyber risk treatment decisions?
- Do you believe the C-suite and board are fully exercising their leadership, oversight, and fiduciary responsibilities with respect to ECRM?

The Bottom Line

Information is literally the "lifeblood" of your healthcare organization. Especially today, with the mass digitization of healthcare and the explosion of electronic healthcare data, systems, and devices, the ability to protect the confidentiality, integrity, and availability

of patient information is critical to your organization's success.

In addition to information, another essential currency in healthcare organizations is trust. There is perhaps no other industry more based on trust than healthcare. Patients entrust their healthcare providers with detailed, sensitive information about themselves, and they trust that this information will be protected. It's important for all of our stakeholders, but especially for our patients, that we maintain their trust by establishing, implementing, and maturing an ECRM program.

Talking about ECRM may seem technical and complex. And yes, it can be both. But it is important to remember that the role of executive leadership and the board is to provide informed direction and oversight for the organization's ECRM approach, activities, and strategy. It is not the board's role to micromanage cyber security efforts in the field, but to provide leadership and guidance that optimizes the organization's cyber security efforts.

It is not the board's role to micromanage cyber security efforts in the field, but to provide leadership and guidance that optimizes the organization's cyber security efforts.

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

understand what it means to have an effective ECRM program in place. "Nose in" means understand where your organization is in relationship to 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. Finally, "fingers out" means leave the details of execution to your organization's appropriate team members.

Many executives and board members struggle with where and how to focus their organization's ECRM efforts. I suggest beginning with the following three steps—keeping in mind that the board's role is to provide oversight for these activities, not to personally implement them:

- Step 1: Identify, and then prioritize, all of your organization's unique cyber risks.
- Step 2: Discuss, debate, and settle on your appetite for cyber risk; i.e., determine what level of risk your organization is prepared to accept.
- Step 3: Address each risk, making informed decisions about which risks you will accept, and which you will address (avoid, mitigate, or transfer) and then execute on that plan.

Healthcare data, systems, and devices are more voluminous, more visible, more valuable, and, at the same time, more vulnerable than ever. The risk of a catastrophic cyber attack on your healthcare organization is real. To address this risk, you must engage in a discussion about what cyber risk is, what the potential impacts could be on your organization, and what steps need to be taken to establish, or improve, your ECRM program.

The Governance Institute thanks Bob Chaput, Executive Chairman and Founder, Clearwater, for contributing this article. This article is excerpted from his soon-to-be-published book Stop the Cyber Bleeding. *To learn more or inquire about obtaining a copy of the book, contact Mr. Chaput at bob.chaput@clearwatercompliance.com.*