Three Essential ECRM 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
2. Determine risk appetite
3. Manage risk

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 observed 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.

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 and assessing the likelihood and impact of each scenario in order to assign a risk rating.

Specialized software can help organizations efficiently perform an enterprise-wide, 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 graphic on the following page).

The risk register provides the foundation for informed decision making related to cyber risks. 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.

© The Governance Institute

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.

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.

© NRC Health