COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

NIST guidance tackles how to integrate cyber-security with ERM



By Jaclyn Jaeger | Thu, Oct 22, 2020 10:34 AM

New guidance from the National Institute of Standards and Technology (NIST) aims to demystify a process with which many companies across all industries have long struggled: how to seamlessly integrate cyber-security risk into an overall enterprise risk management program.

The intent of the guidance—formally called **NISTIR 8286**, "Integrating Cybersecurity and Enterprise Risk Management (ERM)—is "to help improve communications (including risk-information sharing) between and among cyber-security professionals, high-level executives, and corporate officers at multiple levels," NIST said. It's a particularly helpful document for corporate officers—including chief information security officers, chief risk officers, chief compliance officers, and others—because it explains in significant detail what cyber-security data to collect, what analyses to perform, and how to usefully consolidate cyber-security risk information into an overall ERM program.

The highly anticipated release of the guidance followed two back-and-forth public comment periods that garnered hundreds of responses. "The comments were extremely helpful in producing a much better, more relevant guide for the community," says Stephen Quinn, senior computer scientist in NIST's Information Technology Laboratory.

Composing a document that's relatable to both private sector and government was not an easy feat. "We received a good deal of comments that we were embarking on an impossible task," Quinn says. "Yes, it was an impossible task, but I like to think we have furthered the discussion."

At the core of the guidance, NIST strongly encourages the use of a risk register—a spreadsheet-like tool already widely used by many companies—to effectively integrate cyber-security risk management (CSRM) into an overall ERM program. As defined by the Office of Management and Budget (OMB) in the guidance, a risk register is a "repository

of risk information" that contains a description of a particular risk, the likelihood of it happening, its potential impact from a cost standpoint, how it ranks overall in priority relevant to all other risks, the risk response, and who owns the risk.

As NIST noted, companies can add more data fields as they see fit, but each risk register should evolve and mature as changes in current and future risks occur. Typically, risks are tracked at the individual system level, flow up through the organizational/business-unit level, and ultimately to the enterprise level.

Following this same construct, the guidance goes into significant detail describing each element of a cyber-security risk register and, helpfully, provides a template. As with all other risks, "cybersecurity risks need to be documented and tracked in cybersecurity risk registers in order to support better management of cybersecurity risks at the enterprise level," NIST said.

However, CSRM still poses challenges for many companies. As NIST pointed out, cyber-security risk data often is presented as a "perpetually red heatmap or at such a volume as to be impractical. Therefore, it is not surprising that higher levels of an organization or enterprise tend to struggle with understanding cybersecurity risk."

Cyber-risk as an opportunity

Taking a page from OMB, NIST further encourages that a risk register "identify all sources of uncertainty, both positive (opportunities) and negative (threats)." This topic especially garnered a lot of feedback. "There were really strong opinions on this in both directions," Quinn says.

The idea here is that opportunities inform decisions by senior leaders for setting the risk appetite and tolerance as much as the threats that could result in negative consequences. Consider the example of a new online service that provides an opportunity for the company to innovate, "so leadership has directed the organization to take a little more risk and potentially improve revenues," NIST said.

"Alternatively, perhaps other business units have suffered some cybersecurity attacks, and stakeholders have reevaluated the likelihood and impact criteria," NIST said. "In either case, the ability to adjust the effective management of cybersecurity risk supports broad enterprise objectives as part of ERM."

Where cyber-security opportunities are included in a risk register, NIST recommends updating the risk response column using one of the following response types and describes the meaning of each:

- **Realize**: Eliminate uncertainty to make sure the opportunity is actualized.
- **Share**: Allocate ownership to another party that is better able to capture the opportunity.
- **Enhance**: Increase the probability and positive impact of an opportunity (e.g., invest in or participate with a promising cyber-security technology).
- **Accept**: Take advantage of an opportunity if it happens to present itself (e.g., hire key staff, embrace new cyber-security technology).

The comment field of the risk register should also be updated to include information "pertinent to the opportunity and the residual risk uncertainty of not realizing the opportunity," NIST said. Upon their completion, risk registers—including cyber-security risk registers—ultimately are shared by chief risk officers with senior management, so that risks can then be aggregated, normalized, and prioritized, with the company's key risks compiled into an enterprise risk profile.

"Currently, many organizations do not conduct these activities in consistent, repeatable ways," NIST said. "Quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are mostly done in an ad hoc fashion and are not performed with the rigor used for other types of risk. Improving the risk measurement and analysis methods used in CSRM, along with widely using cybersecurity risk registers, would enhance the quality of the risk information provided to ERM."

This is a lost opportunity, because through this process of aggregating and normalizing risk register information, the NIST guide states, chief risk officers and risk committees can realize many benefits, including, for example:

- Reporting actual and potential risks from threats and system failures to information and technology;
- Normalizing risk management across the enterprise—for example, if different exposure scales were used in two business units, a "high risk exposure" in one may represent a "moderate risk exposure" under the same conditions in another;

- Providing executives with information to measure and understand potential exposure for achieving strategic, operations, reporting, and compliance objectives;
- Informing operational risk mitigation activities and relating these to enterprise mission and budgetary guidance to prioritize and implement appropriate responses; and
- Producing enterprise-level risk disclosures for required filings and hearings or for formal reports as required (e.g., after a significant incident).

The NIST guidance further discusses the importance of continuous monitoring and cites the use of key risk indicators (KRIs) as one example. “Cybersecurity KRIs can be positive, such as the number of critical business systems that include strong authentication protections,” NIST said. “They also can be negative, such as the number of severe customer disruptions in the last 90 days.”

Fostering a risk-aware culture is another means to achieve continuous monitoring. Specifically, NIST recommended the following measures, among others:

- Encourage employees to look for cyber-security risk issues before they become significant;
- Educate employees on the impact of cyber-security risk and why effective cyber-security risk management is an important part of everyone’s job;
- Conduct risk response exercises to train employees in recognizing, reporting, and responding to cyber-security risk scenarios; and
- Enable an environment where employees and partners may openly and proactively report potential risk situations without fear of reprisal.

If corporate officers take just one message from NIST’s guidance, it is this: If cyber-security risks are to be truly understood by senior management and anchored into an overall ERM program, cyber-security risk cannot be tracked in a vacuum but rather must be treated like any other risk, tracked in an enterprise-wide risk register. This ensures all risk decisions made by senior management are holistically weighed against the company’s overall risk appetite and risk tolerance and that limited resources are effectively optimized to support business objectives.

For companies seeking further clarity, more guidance is on the way. As NIST's flagship document on cyber-security and ERM integration, NISTIR 8286 is the first in a series. "The series will be a decomposition of sections and concepts in the order they are presented," Quinn says. Next in the series (expected to be published sometime within the next month) is NISTIR 8286A, which discusses risk appetite and risk tolerance in greater detail.

RATE THIS RESOURCE

Select your rating

