Guidehouse

Applying ERM Programs to Address Cyber Risks

AGA + Guidehouse Panel

Background

On October 23, 2019, the Association of Government Accountants (AGA) hosted a webinar titled "Applying ERM Programs to Address Cybersecurity Risks" as part of AGA's webinar series. The webinar was moderated by Daniella Datskovska, Director, Guidehouse LLP, and covered the role of cyber strategy in federal agencies' ability to identify, prioritize and manage cyber risks, optimize organizational awareness and training, and integrate cyber and Enterprise Risk Management (ERM). In addition, the panelists discussed the July 2019 Government Accountability Office (GAO) Congressional Report, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges."

This paper presents highlights and insights from the webinar's panel discussion and is organized topically by the themes addressed during that panel. Panelists—experts in cyber risk management—concluded that much remains to be accomplished to adequately address cyber risks, and that integrating cyber risk management with operations and enterprise risk management is an important step in maturing the cyber capability. Panelists noted that while leadership understands how to manage operational risks, cyber risk management professionals must be able to more effectively describe cyber risks to leadership in business language. Furthermore, they must understand how cyber risks fit within and can impact the organization's broader mission and mission-support functions.

Key Recommendations from the GAO Report

- Manage competing cyber and operations priorities, including instances when operational needs appear to conflict with cyber requirements
- Implement consistent cyber risk management policies and procedures across an agency
- Incorporate cyber risks into enterprise risk management
- Establish agencies' cybersecurity risk management strategies

The panel included:

- **Nick Marinos**, Director, Information Technology and Cybersecurity, Government Accountability Office
- **Marianne Bailey**, Cybersecurity Lead, Guidehouse LLP
- **Pete Gouldmann**, Enterprise Risk Officer for Cyber, Department of State
- **Amber Simco**, Acting CISO & Division Director at The National Institutes of Health

Cyber Risk in Perspective

Cyber has been included in the GAO's High Risk list since 1997. The need for cybersecurity risk management in government has grown since then, as agencies' digital footprints have increased. The more complex the environment, the more vulnerable it becomes. In essence, agencies increase the attack surface as they fold emerging technologies into legacy systems and move to modernize IT systems. So how bad is it? According to the Govloop eBook Enterprise Risk Management in Today's Digital World:

- 74 percent of the 96 participating agencies have cybersecurity programs that are either at risk or high risk
- 17 of 23 agencies studied by the GAO have not fully established agency- and system-level policies for assessing, responding to and monitoring risk
- 2 of 5 chief information security officers in the 96 participating agencies said they were reviewing NIST's Cybersecurity Framework upon its release

There is no shortage of regulations and guidance in this sphere, including Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and supporting documents from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). So why do gaps in managing cyber risks still exist? The panelists offered some insights about these persistent gaps, as well as guidance on how they might be addressed.

The History of Risk Management in Government

The need for risk management in government has grown along with agencies' digital footprints. That's because the more complex the environment, the more vulnerable it becomes. Here's a look at where governments at all levels stand with risk management.

74%

of the 96 agencies participating in the risk assessment process have cybersecurity programs that are either at risk or high risk.

49%

of agencies can detect and whitelist software running on their systems.

17

agencies out of 23 that the GAO studied have not fully established agency- and system-level policies for assessing, responding to and monitoring risk.

42%

of local government IT officials say their agencies have adopted a cybersecurity framework based on national standards and guidelines.

4%

of 204 local governments in the United States show some aspect of enterprise risk management (ERM).

2 of 5

chief information security officers said they were reviewing NIST's Cybersecurity Framework on release.

80%

of the problem with risk management is cyber hygiene, the Chief Information Security Officer for the Air Force's Office of the Deputy CIO said.

69%

of state cybersecurity budgets went to compliance and risk management in 2016, down from 74% in 2014.

> *"There is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure — ensuring that the systems, products, and services are sufficiently trustworthy throughout the system development life cycle (SDLC) and can provide the necessary resilience to support the economic and national security interests of the United States."*
>
> **Risk Management Framework for Information Systems and Organizations**

Source: Enterprise Risk Management in Today's Digital World, Govloop E-Book 2019

> Cyber is not the bane of existence for cyber professionals, but rather, it is something to be embraced by everyone."

Cyber Risk Management Involves Everyone

Cyber risk management should not be a siloed task relegated to cyber professionals, but rather a concern embraced by everyone and shared across an entire agency. One panelist noted that we really have reached the point where we need a "see something, say something" mindset. It is not sufficient to rely on a select few IT professionals to handle cyber risks.

Cyber risk management must move beyond protecting IT assets from unauthorized access, or threats and address the full range of cyber-related concerns. This will result in improved organizational awareness, especially at leadership levels. Many people think of IT as "business-processing systems" instead of "mission systems." IT staff receive in-depth training: a similar level of cyber knowledge should be afforded to non-IT, mission-oriented staff.

On a related note, the GAO recommended that the 23 agencies it reviewed should share cybersecurity experiences amongst themselves to learn from each other and improve individual agency programs.

Cyber Risk Management and ERM Should be Integrated

> When we see organizations that have a good collaboration and coordination between the cyber risk management function and the overall ERM functions, there seems to be a greater chance of success in terms of the maturity of the program."

Risk management itself is not a new concept. Protecting government information and information systems is expected to use risk-based concepts. Given the breadth of cyber risks—encompassing policies, procedures, protocols, hardware, software and people's behavior—incorporating these risks into an organization's ERM program maximizes leadership knowledge and facilitates organization-wide risk-aware decision making.

Yet it continues to be a challenge to bring cyber risks into the broader ERM framework. Cyber and cyber risks encompass a highly technical area, and professionals may feel it is not feasible to articulate risks in a manner that is understood by people outside their discipline. Yet it is critical that this very objective be met, and that cyber risks be clearly stated in business language. Understanding cyber risks in the broader enterprise risk landscape is crucial in aligning risk-response actions with an organization's overall risk profile.

One recommendation for better integration of cyber risk management and ERM is to ensure your CISO or CIO has a seat on the ERM leadership or governance body. Doing so will help facilitate meaningful discussions around the scope and potential enterprise-level impacts of cyber risks, while also providing your CISO/CIO with visibility to possible interrelations among their cyber risks and other enterprise risks.

Government Cybersecurity Documents

- **July 2019:** CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
- **April 16, 2018:** NIST Framework for Improving Critical Infrastructure Cybersecurity
- **May 19, 2017:** OMB Memorandum M-17-25—Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **May 11, 2017:** Executive Order 13800–Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **December 2014:** Federal Information Technology Acquisition Reform Act (FITARA)
- **December 2014:** Federal Information Security Modernization Act (FISMA)

Competing Priorities Between Operations and Cyber Must be Managed

> Leadership knows how to manage risk, we just need to speak in their language. This is why ERM is so important to this effort."

Federal agencies, like private sector companies, have a finite amount of resources, most or all of which must be allocated to the highest-priority needs. Integrating cyber risk management with ERM programs can help ensure equal consideration of cyber needs with other enterprise needs.

Unfortunately, in contrast with more noticeable functional improvements, many security-related improvements are not visible to end-users, and thus do not receive the same level of attention. Employees may also view basic cyber practices—such as multi-factor authentication (MFA)—as burdensome and impeding their work. Improved communications and awareness programs can help by clearly describing the cyber risk that is being addressed, along with its possible consequences—and then explaining how the control is an effective and minimally intrusive measure that results in the successful mitigation of that risk.

Common Cyber Risks of Which Agency Practitioners Should be Aware

> "What makes cyber risk different from other types of risk, is the fact that it is abstract. You can't touch it, you can't see it, you can't hear it."

Third-party risk has been and will continue to be a common cyber risk. Which of your systems do your third parties access, which systems do third parties host or control, how do they access systems, and to what other systems are the accessed systems connected? What access-control technology and protocols are employed? And what tools are available to incentivize your third parties to adhere to requirements or to enforce requirements? Seemingly innocent arrangements can lead to disastrous results.

Insider threats also pose significant cyber risks. These risks can range from a disgruntled current or former employee sabotaging internal systems, to employees unintentionally enabling a spear-phishing attack by clicking on a link in an email. Even more sinister insider threats may exist in the form of planted operatives intent on obtaining sensitive information. Detecting and controlling insider threats should not be the sole purview of IT professionals—all employees must be vigilant. On another front, targeted use of data analytics and artificial intelligence is providing significant advances in detecting anomalies and deviations in the ways systems are accessed and used by employees; such approaches have the capacity to detect attacks on systems in their infancy, well before they become a significant threat.

One of the panelists noted a problem regarding basic cyber hygiene with respect to multi-factor authentication (MFA), and the ability to patch vulnerabilities quickly and effectively. MFA significantly improves organizations' capability to limit access to specifically authorized individuals. However, it requires that MFA actually be implemented, and user resistance can arise when they perceive increased burdens to access systems or if they feel uncomfortable providing biometric data (if used). On the response side, once a vulnerability has been discovered or otherwise identified, the ability to quickly and effectively eliminate that vulnerability is perhaps the most critical factor in limiting exposure to potential attacks.

> "We cannot just depend on a select few IT professionals to handle cyber responsibilities. This is really a team sport."

Organizational culture has a lot to do with an agency's level of unaddressed cyber risk exposure, as one panelist noted. In particular, there must be some degree of alignment between the programs being used to address cyber risks and the exposure. Integrating cybersecurity risk into an ERM program can greatly improve the alignment of risks to exposures (or likelihood the risks will occur). Further, a risk-aware culture within an organization improves the ability of all employees to be cognizant of their role in protecting the organization's valuable information and technology assets.

How Would the GAO Advise Agencies to Prepare for a GAO Cyber Audit?

> "Risk management itself is not a new concept. Everything around protecting government information and information systems is intended to be approached from a risk-based methodology."

Audits are an important tool to gauge the ability and status of an organization vis-à-vis dealing with cybersecurity risks. However, when we merely talk about compliance, people often feel that they are taking a test—and thus simply want to get a passing score. The regulated community generally looks at the entire process as a headache that they just want to go away. But those doing the regulating would like people to understand the fundamentals behind the approaches used, and to embrace and accept that GAO auditing practices are the product of sound business processes. When preparing for an audit, consider existing documentation. Take a step back and think about whether key processes you rely on are articulated in specific documents. In addition, bear in mind that all aspects of the audit–including those that may appear challenging—are intended to improve cyber hygiene and risk management. The GAO cannot get to meaningful recommendations without having a constructive conversation with the organization that is being audited. Prepare beforehand, and then ask questions during the initial audit meeting; doing so will ensure a clear understanding of the objectives of the audit and the processes that will be used during the audit.

Conclusion

Government's need for cyber risk management continues to grow, in part due to agencies' increasing digital footprint. Although progress has been and continues to be made, considerable gaps exist. Cyber risk management is the responsibility of everyone in an organization, not just the IT professionals. Perhaps the greatest improvement that has yet to be fully tapped is to integrate cyber risk management into the organization's ERM program. There will always be conflicts between operational objectives and cyber, but solutions can be facilitated via a good understanding and discussion of risks on an enterprise-wide basis. Incorporating cyber risks into an ERM program boosts their visibility for senior leadership and provides cyber risk management professionals with a greater understanding of the interconnectedness of cyber risks with other enterprise-level risks. The net result is a greater understanding of total enterprise risks and better allocation of limited resources to respond to all risks, including those involving cybersecurity.

About Guidehouse

Guidehouse provides your agency with a comprehensive suite of risk management solutions to ensure an increasingly sophisticated threat landscape doesn't compromise your agency's growth, mission or invaluable assets. Identifying and assessing the specific risks you face while arming your team with powerful tools and technologies for potent tactical response is key.

Your agency faces risk every moment of every day. Many of these risks are predictable, relatively benign and easy to avoid. But cyber threats have become stealthier and more insidious. Supply chains have grown more sophisticated. Regulations have gotten ever more complicated. And all this while your data assets have become much, much more valuable.

Today, putting a holistic risk management plan in place is an absolute must for your organization. Guidehouse can help you create and implement such a plan with the precise tools needed to address the unique risks you encounter (cyber, financial, operational, reputational, market, regulatory, supply chain and more). Backed by extraordinary industry expertise and AI-powered analytics, your Guidehouse consultants can help you not just respond to risk, but use it as a catalyst for organizational transformation. While others shy from complex challenges, your agency can learn to embrace them. Guidehouse will help your team become stronger, increase efficiency and grow more agile.

For more information, please visit: **guidehouse.com**

Email: erm@guidehouse.com / **Web:** guidehouse.com / @guidehouse linkedin.com/company/guidehouse/