Better Together

How Integrating Enterprise Risk Management Can Strengthen Federal Cybersecurity

SEPTEMBER 2021

PARTNERSHIP FOR PUBLIC SERVICE

Deloitte.

About the Authors

About the Partnership

The Partnership for Public Service is a nonpartisan, nonprofit organization that works to revitalize the federal government by inspiring a new generation to serve and by transforming the way government works. The Partnership teams up with federal agencies and other stakeholders to make our government more effective and efficient.

About Deloitte

Deloitte provides industry-leading audit, consulting, tax and advisory services to many of the world's most admired brands, including nearly 90% of the Fortune 500® and more than 5,000 private and middle market companies. Our people work across the industry sectors that drive and shape today's marketplace — delivering measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to see challenges as opportunities to transform and thrive, and help lead the way toward a stronger economy and a healthy society. Deloitte is proud to be part of the largest global professional services network serving our clients in the markets that are most important to them. Now celebrating 175 years of service, our network of member firms spans more than 150 countries and territories. Learn how Deloitte's more than 312,000 people worldwide make an impact that matters at www.deloitte.com.

Table of Contents

Introduction

Every day, federal agencies handle huge volumes of sensitive information—from the personal data of those who receive government benefits to national security information analyzed by the intelligence community. Digital systems store, manage and process much of this data, making critical government operations vulnerable to cyberattacks.

Yet, since 1997, the Government Accountability Office's biannual High-Risk List has identified cybersecurity as a crucial area requiring more attention from federal agencies.[1] And as agencies continue to modernize their digital operations, new cybersecurity challenges compound existing ones, posing even greater risk to effective government operations. For example, in 2020, the widespread SolarWinds attack affected multiple federal agencies and highlighted the need for government to prioritize cybersecurity.[2]

It is critical for the federal government to strengthen its cybersecurity risk management. To do so, federal cybersecurity programs can partner with their agencies' enterprise risk management functions, an approach highlighted in recent guidance from both the National Institute of Standards and Technology and the Office of Management and Budget. Enterprise risk management, or ERM, is a practice used to methodically identify, prioritize, address and monitor all risks, including the cybersecurity risks that threaten the success of an organization's mission. In our 2020 report, "Mastering Risk," the Partnership for Public Service and Deloitte detailed recent advances in federal ERM, and called for agencies to more frequently and actively integrate ERM with other risk functions like cyber risk management.

In spring 2021, the Partnership and Deloitte organized a working session for experts and practitioners in ERM and cybersecurity. Participants discussed how agencies can use ERM programs and principles to enhance the effectiveness of cybersecurity initiatives, noting in particular how ERM can help evaluate cybersecurity risks with a strategic lens and bring those risks to the attention of agency leaders. This issue brief summarizes these discussions and highlights several leading practices used by agencies that work at the intersection of ERM and cybersecurity.

1 Government Accountability Office, "Ensuring the cybersecurity of the nation." Retrieved from bit.ly/3elxEHL.
2 Government Accountability Office, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response." April 22, 2021. Retrieved from bit.ly/3hRWMxc.

Why Federal Agencies Should Integrate Cybersecurity and ERM

Many government agencies have robust cybersecurity programs overseen by chief information and chief information security officers. Agencies can build on that strong foundation by better coordinating their cybersecurity programs and ERM activities. In turn, agency leaders can be better positioned to fully assess, monitor and make decisions about cybersecurity risks. Discussions in our working session revealed several ways that this increased coordination can help ensure effective and secure federal operations, thus enabling government to better carry out its mission.

Bridge communication gaps between agency leadership, staff and technical experts

During our working sessions, federal cybersecurity practitioners discussed the challenge of communicating complex information about threats and vulnerabilities to agency leaders who may not have in-depth technical knowledge. This communication gap can have serious consequences—if leaders don't understand the information presented to them and the risks associated with that information, they may not make the necessary decisions or investments to safeguard the agency's cybersecurity. Federal ERM programs have the tools and expertise to help agencies develop a comprehensive risk register. A good risk register can clearly articulate the full picture of an agency's cybersecurity risks and serve as a resource to help agency leaders understand, prioritize and address those risks.

Increase understanding of cyber-related risk

Integrating cybersecurity and enterprise risk management can also help ERM professionals better understand an agency's cyber risks. ERM programs can work with cybersecurity professionals to connect information on cyber risks and vulnerabilities to information about other agency programs and strategic priorities. These efforts enable ERM professionals to better understand and monitor cybersecurity risks in relation to other elements of an organization's risk profile. As a result, ERM practitioners are able to more fully grasp the agency's overall risk. At the same time, the urgent nature of cybersecurity work means that practitioners must constantly focus on addressing immediate threats and often lack the time to step back and assess the full scope of cybersecurity risks. By connecting cyber risk to other agency priorities, ERM can help cybersecurity practitioners think more strategically about how to manage these risks.

Bring risks to the attention of agency leaders

Once ERM practitioners have analyzed how cybersecurity risks relate to other agency programs and strategic priorities, they can work with cybersecurity experts to elevate critical issues and areas to agency leadership. This coordination can help agency leaders more efficiently and effectively respond to rapidly evolving cybersecurity threats. For example, at our working session, officials from the State Department shared that the agency's Office of Global IT Risk uses ERM principles to frame technical information about cybersecurity risks for agency leaders and then relays their decisions about risk tolerance back to technical staff as it evaluates specific programs and systems. "If we're going to have a conversation at the organizational level, we need to have it in the context of how leaders deal with decisions on a regular basis," said Peter Gouldmann, director of the Office of Global IT Risk. "We have to look at the strategic implications." ERM programs, with their broad view of risk, can also help leaders assess trade-offs and make decisions about how to manage cybersecurity risks while also addressing the other risks an agency faces.

Although relatively new, the idea of closer coordination between federal ERM and cybersecurity programs is gaining traction in government. For example, in October 2020, the National Institute of Standards and Technology released "Integrating Cybersecurity and Enterprise Risk Management," an overview of how agencies can integrate the two disciplines. "[Agencies] have generally treated these areas as separate and created some silos... this document talks about how [ERM and cybersecurity] can work in concert," said Stephen Quinn, senior computer scientist at NIST and one of the document's authors.

The document demonstrates that NIST recognizes the critical relationship between cybersecurity and ERM, and details how an integrated approach can help agencies better identify, assess and manage cybersecurity risks. Quinn also noted that NIST is now developing further guidance that can help agencies align their cybersecurity and ERM programs.

Leading Practices for Aligning Cybersecurity and ERM

Cybersecurity threats and vulnerabilities continue to be a primary concern for agency leaders across government. To better manage these risks, federal ERM practitioners should closely coordinate with cybersecurity programs. This type of integration is critically important for agencies' enterprise risk management and cybersecurity functions.

The good news is that many agencies have already started this integration. As this process continues, ERM, cybersecurity and digital transformation practitioners should keep in mind several leading practices generated by our working sessions:

Use common terminology. To collaborate effectively, ERM and cybersecurity teams should build a common terminology to identify, prioritize and communicate cyber risks. This terminology should be useful to technical experts and accessible to organizational leaders.

Make information actionable. Agencies should go beyond using ERM to generate knowledge about cybersecurity risks—they must make this information actionable. Risk information should be analyzed and then distributed to the leaders who work every day to manage cybersecurity efforts.

Connect risk governance and align leadership. ERM and cyber risk management processes should be interconnected, with leaders from each group working together and having joint discussions to promote information sharing and collaboration. Risk owners and those managing risks on a day-to-day basis should also work collaboratively.

Incorporate risk appetite and risk tolerance. These ERM concepts refer to how much risk an agency is willing to accept in pursuit of its strategic objectives. Using these concepts in relation to cybersecurity risk can help agencies prioritize and monitor top cybersecurity risks and identify which cyber events and activities agency leaders are willing to accept.

Connect cybersecurity and enterprise risk registers. Standardized risk registers at the organizational level can help agencies incorporate cybersecurity risk activities into overall decision-making about risk.

Examine risks at the organizational level. Agencies should develop an organization-wide understanding of their cybersecurity risks, including enterprise-level risks and risks faced by subcomponents and major offices. In July 2019, GAO reported that 11 of the 23 Chief Financial Officers Act agencies it reviewed had not fully established a process for assessing agencywide cybersecurity risks by compiling system-level risks.[3] This gap prevents agencies from getting a full picture of the risks they face.

3 Government Accountability Office, "Cybersecurity: Agencies need to fully establish risk management programs and address challenges." July 25, 2019. Retrieved from bit.ly/38DWV2p.

Additional Areas for Exploration

The ideas generated in our working session provide a starting point to help agencies more effectively coordinate and integrate their ERM and cybersecurity efforts. These sessions also brought up several questions that merit additional exploration. Further research could explore:

- Ways ERM can help support the development of a risk-based cybersecurity strategy.
- Ways ERM and cybersecurity programs might use data to further understand cybersecurity risks.
- The common terminology practitioners in these two disciplines can use to communicate effectively.
- The organizational capacity ERM and cybersecurity programs should build to coordinate successfully.

Appendix I: Methodology

Between April and July 2021, the Partnership and Deloitte hosted a working session for enterprise risk management and cybersecurity professionals to discuss the intersection of these disciplines and examine how ERM principles and concepts can support federal cybersecurity. Additionally, we solicited comments from experts at the Government Accountability Office to hear their recommendations for agencies on these topics.

Appendix II: Acknowledgements

The individuals listed below generously offered their input on this issue brief. We greatly appreciate their time and counsel. However, the contents of this issue brief may not reflect the views of the federal employees who participated. Additionally, the views of participating federal officials do not necessarily reflect positions or policies of the federal government or its agencies.

Peter Gouldmann
Director, Global IT Risk
Department of State

Nick Marinos
Director, Information Technology and Cybersecurity
Government Accountability Office

Stephen Quinn
Senior Computer Scientist and Program Manager
National Institute of Standards and Technology, Department of Commerce

Appendix III: Project Team

PARTNERSHIP FOR PUBLIC SERVICE

Elizabeth Byers
Associate Manager, Research, Analysis and Evaluation

Loren DeJonge Schulman
Vice President, Research, Analysis and Evaluation

Samantha Donaldson
Vice President, Communications

Barry Goldberg
Editor

Lindsay Laferriere
Senior Manager

Katie Malague
Vice President, Government Effectiveness

Andrew Parco
Digital Design Associate

Jessica Reynoso
Associate

DELOITTE GOVERNMENT & PUBLIC SERVICES

Cynthia Vitters
Managing Director, Enterprise Risk Management Practice Leader
Deloitte & Touche LLP

John Basso
Senior Manager, Enterprise Risk Management
Deloitte & Touche LLP

Dave Mader
Chief Strategy Officer, Deloitte Consulting Civilian Sector
Deloitte Consulting LLP

Ryan Murphy
Manager, Enterprise Risk Management
Deloitte & Touche LLP

Greg Stavrou
Senior Consultant, Enterprise Risk Management
Deloitte & Touche LLP

Mark Stofanak
Analyst, Enterprise Risk Management
Deloitte & Touche LLP

PARTNERSHIP
FOR PUBLIC SERVICE

1100 New York Ave NW
Suite 200 East
Washington, DC 20005

ourpublicservice.org
(202) 775-9111

partnershipforpublicservice
@PublicService
rpublicservice

Deloitte.

1919 North Lynn Street
Arlington, VA 22209

deloitte.com
(571) 882-6254

DeloitteUS
@Deloitte
deloitte

Cover Photo: shutterstock.com