Deloitte.

Federal CFO Insights
Guarding against cyber threats

Although many cyber-attacks do not make national headlines, they can hurt an organization in any number of ways, from simply vandalizing its website to shutting down networks, perpetrating fraud, and stealing sensitive information. For many agencies, the need to establish an enterprise-wide approach to preventing and responding to such attacks has required increasing attention from agencies' CIOs and Directors.

With the increasing number of cyber incidents, Federal agencies have good reason to ask 'How likely is it to happen to us, and what are we doing about it?' And in this issue of CFO Insights for Federal finance executives, we examine how to take a more risk intelligent view of cyber threats and outline steps agencies can take toward more effective cyber threat risk governance.

Taking a risk intelligent view of cyber threats

The questions of "how vulnerable is my agency" and "what can I do mitigate against cyber threats" are the thoughts that agency risk committees should consider across a broad range of areas — compliance risk, reputational risk, and others. When it comes to cyber risks, however, the term "cyber threat" is often misunderstood or may be underestimated, so these high-level questions may not produce answers that adequately address the threat.

Unless an agency is already quite sophisticated in its cyber threat risk management practices, it may not yet have the risk management infrastructure and/or governance elements in place to support a robust discussion around a fully integrated risk management function. For instance, leaders may not have agreed on risk definitions, risk tolerances, or metrics specific to cyber threat risk, or an agency might not have fully implemented the technology tools and expertise to collect and report cyber threat-related information effectively. In many organizations, the active, integrated involvement of senior leadership outside the CIO function is critical, providing the mission-based impact and context to an otherwise one-dimensional view of cyber risk.

This integration of cyber threat is pivotal in the larger understanding of risk posed to an agency by cyber attackers. If an organization is new to the conversation around integrated IT Risks Management, a first step is to ask the senior leadership team four questions about specific information security practices that are essential to effective cyber threat risk management:

- How do we track what digital information is leaving our agency and where that information is going?
- How do we know who is really accessing our systems, and from where?
- How do we control what software is running on our devices?
- How do we limit the information we voluntarily make available to a cyber adversary?

Highly effective cyber risk management processes are repeatable, clearly defined, well-documented, and aligned with an agency's larger IT Risk Management (ITRM) and Enterprise Risk Management (ERM) frameworks. The agency may measure and monitor process effectiveness and efficiency, as well as apply continuous improvement techniques to enhance performance.

The Cyber Threat Risk Management Maturity Model

A function of the natural evolution of cyber-attack methods, many agencies' more mature capabilities focus on measures, such as firewalls and passwords, aimed at limiting access to the agency's network. Even though these protective mechanisms are essential, they alone may not be sufficient to thwart the skilled attacker. Cybercriminals are becoming increasingly adept at infiltrating commercial and Federal networks without triggering an intruder alert. Once they are inside, they can easily siphon information off a network unnoticed unless an agency is actively looking for signs of suspicious activity.

To help defeat cybercriminals who make it past the front-line access controls, a cyber threat risk management program or set of protocols should include not only the protective cyber measures, but incorporate all of the fundamental cyber framework building blocks outlined in the emerging Cyber Security Framework, developed by the National Institute of Standards and Technology (NIST). To be effective, a cyber threat risk management program should employ techniques, technologies, and processes that not only protect the information systems, but monitor the current state of events, react to potential threats, and continuously improve those underlying processes that secure the organization. For instance, an effective program will also be able to identify and restrict the transmission of suspicious communications until their legitimacy is verified, for example, with technologies that electronically "quarantine" the communication while appropriate checks take place. This coupling of the preventative, detective and mitigating controls not only increases the effectiveness of the program as a whole, it layers the defenses of an agency, increasing the likelihood of identifying a cyber attack.

Characteristics of a mature cyber threat risk management capability

Risk governance (Agency Director, Chief Operating Officer, Senior leadership):	**Communication:** Ongoing dialogue with management; critical metrics and key performance indicators (KPIs) agreed upon and monitored in real time.
Risk infrastructure (Owned by CIO and senior management, which are responsible for implementing and maintaining the people, process, and technology elements needed to make risk management "work"):	**People:** Senior management team has the background knowledge and current information to actively integrate cyber threat risk into broader ERM decisions; enterprise uses cyber threat intelligence to help manage risk in all classes (not just cyber threat risk) to within defined tolerance levels. **Process:** Processes addressed by continuous improvement efforts, including automation and other enabling technologies where appropriate; structured cyber threat risk management program integrated with broader IT risk management and enterprise risk management programs. **Technology:** Technology used to automate not just threat monitoring and alerts, but also other security processes such as malware, forensic analysis, and threat assessment.
Risk ownership (Functions and program):	In addition to the preceding attributes, incentives designed specifically to reward key personnel based on their cyber threat risk management performance.

Steps toward more effective cyber threat risk governance

The following 10 steps can provide a high-level guide for establishing a cyber threat risk governance program, and the approach discussed above can provide a fair start toward understanding an agency's capabilities for managing and mitigating the ever-present risk that cyber threats pose today. However, neither the 10 steps below or approach discussed above are intended to substitute for a formal, rigorous IT security assessment performed by specialists.

- Stay informed about cyber threats and their potential impact on your agency.
- Recognize that cyber threat Risk Intelligence is as valuable as traditional business intelligence.
- Hold an agency's senior executive accountable for cyber threat risk management.
- Provide sufficient resources for the agency's cyber threat risk management efforts.
- Require management to make regular, substantive reports on the agency's top cyber threat risk management priorities.
- Expect executives to establish monitoring methods that can help the agency predict and prevent cyber-threat-related issues.
- Leverage the NIST Cyber Security Framework to guide your development of a robust, comprehensive IT security capability.
- Expect executives to track and report metrics that quantify the business impact of cyber threat risk management efforts.
- Monitor current and potential future cybersecurity-related legislation and regulation.
- Recognize that effective cyber threat risk management can give your agency more confidence to take certain "rewarded" risks (e.g., adopting cloud computing) to pursue new value.

Exploring cyber threat risk with an agency's senior leadership can yield value beyond helping to improve governance over this area of risk alone. It also can lead to a more productive dialogue between an agency's executives and oversight about IT risk management in general and greater engagement on all aspects of IT risk.

Primary contacts

Kevin Brault
Principal, Security and Privacy
Federal Leader, Cyber Security
Deloitte & Touche LLP
kbrault@deloitte.com

Henry Ristuccia
Global Leader and Co-Leader,
Government, Risk and Compliance
Deloitte & Touche LLP
hristuccia@deloitte.com

Deloitte *Federal CFO Insights* are developed with the guidance of Roger Hill, Principal, Federal CFO Program Leader, Deloitte & Touche LLP; and Philippe Podhorecki, Manager, Federal CFO Program, Deloitte Consulting LLP.

About Deloitte's Federal CFO Program

The Federal CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help Federal finance leaders stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a leader's career — helping Federal CFOs manage the complexities of their roles, tackle their company's or agency's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's Federal CFO Program, visit our website at www.deloitte.com/us/FederalCFO.

Endnotes

1. *CF Disclosure Guidance: Topic No. 2 — Cybersecurity*, Division of Corporate Finance, U.S. Securities and Exchange Commission, October 13, 2011
2. For more information, read *Risk Intelligent Governance in the Age of Cyber Threats — What You Don't Know Could Hurt You*