
010010100
010010100
010010100
010010100
010010100
Risk
Data
Risk
Information

Prioritizing Information Technology Spending Through Cyber Risk Assessments

By: Deborah Golden; Rebecca Tyler, CISA; Danielle Eucker, CISA, CIA, PMP; and Joseph Meyers, JD, MS, Security+, CISSP

Changes and emerging trends in federal information technology (IT) make it critical for federal chief information officers (CIOs) and chief financial officers (CFOs) to work together to understand their organizations' challenges, and collaborate on strategies and solutions to defend against cyber threats. As federal agencies begin to move their operations to shared services platforms and continue to modernize their systems (e.g., retiring legacy systems, migrating to the cloud, launching digital services), allocation of financial resources and focus on cybersecurity spending become increasingly important given the threat environment, the necessity to understand the risks posed within that environment, and the imperative to invest in strategies to address those risks. In an effort to support agencies through this ever-evolving cyber environment, the federal government proposes increasing its fiscal year (FY) 2017 cybersecurity budget.[1]

What's at Risk?

The effects of cybersecurity incidents extend well beyond IT departments and the originating agencies, as system and network borders no longer restrict static data. Dynamic interconnections among entities (e.g., third parties, customers and the public) encourage free flow of data where the "system boundaries" are often beyond an agency's physical walls. Consequently, bilateral transference of risk is shared continuously, where federal agencies introduce risks to outside parties, while third parties and/or external entities introduce risks to federal agencies. For federal agencies, the cost of an incident may include retribution (e.g., the Office of Personnel Management (OPM) must cover the cost [estimated at $330 million][2] of credit-monitoring service and identity theft insurance for those affected by its 2015 breach of 22 million background investigation records, including federal employees, civilians and their dependent children — approximately 28 million people;[3] however, the longer-term effects of a data breach may affect citizens closer to home). When a federal agency is breached, the types of stolen data may expose those affected to financial, identity and privacy-related compromises of information. In addition to financial data, federal agencies have access to unclassified, personally identifiable information (PII), as well as protected health information (PHI). Examples of PII include Social Security Numbers, addresses, phone numbers, credit card numbers, military history and fingerprint scans. Examples of PHI include specific health/dental records/history, medical test results, vital statistics and X-rays. The risks are immeasurable, and the threat actors associated with these events may target financial and other personal information using sophisticated technologies to breach networks undetected.

Considerations for Improving Cyber Risk Management Practices

Sophisticated cyberattack methods, combined with widespread changes in the IT landscape, create greater risks for federal agencies. In addition to mechanisms and strategies currently in place, federal agencies should consider expanding their portfolio of solutions/procedures to manage increased and complex risks. To that end, enterprise-level risk mitigation across the full lifecycle of protection, detection and incident response to achieve optimal security, vigilance and resilience can be a challenge for many agencies. As such, it is critical for CFOs and CIOs to prioritize cyber preparedness along with financial and mission-critical

TOP FIVE Reasons Federal Financial Managers Should Be Diligent about Managing Cyber Risk

1. Federal agencies are not spending their resources efficiently; despite increasing budgets and spending, risks are not mitigated and attacks are not thwarted.
2. Actual cyberattack and security breach recovery costs may exceed the budget.
3. Protecting data (federal employee data, citizen data and trade secrets) is a part of civic duty.
4. Limiting taxpayers' financial exposure is a part of civic duty (e.g., OPM's data breach, which indirectly affects taxpayers and directly affects 28 million people).
5. Federal CIOs are required to responsibly manage IT resources to be compliant with applicable laws or regulations, and to secure against cyber threats.

activities. In an effort to address evolving federal requirements (e.g., the Federal Information Technology Acquisition Reform Act (FITARA)) and to keep pace with the demands of IT modernization while managing cyber risk, agencies should:

1. include a cyber risk assessment in support of an overall enterprise risk management (ERM) program;
2. confirm IT budget is reflective of the results of the cyber risk assessment and that training and incident response costs are incorporated;
3. improve employee training to increase awareness and keep up with changes in technology and threat actors; and
4. develop an incident response plan, and conduct mock incidents to test the plan and improve resiliency.

Here, we'll dive deeper into mechanisms that agencies may use to address these components of cyber risk management.

1 *Cyber Risk Assessment*

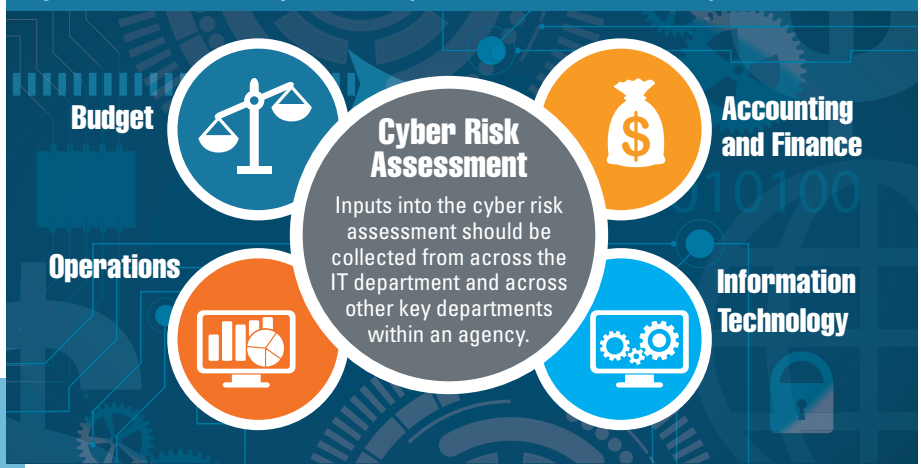
Compliance with internal controls should not be mistaken for security — cybersecurity is not a check-the-box exercise. Design, implementation and effective operation of internal controls over information security is important — however, it can be a challenge to update internal controls to keep pace with the rapidly changing landscape of cyber threats. Establishing a team to design and perform regular cyber risk assessments may help agencies proactively monitor and better protect against — as well as respond to — cyber threats.

During cyber risk assessments, federal agencies should leverage their existing ERM programs to enable a closer examination and risk-based evaluation of IT spending. Most federal agencies follow the Government Accountability Office (GAO) framework for understanding risk exposure throughout the organization in the performance of their annual enterprise risk assessments. Using the GAO framework for these assessments aids agencies in identifying high-level risks related to IT, but they may not explore cyber threats, cyber risk, or cybersecurity vulnerabilities at the appropriate level to evaluate IT spend plans.

Cyber risk should be one component of this overall risk assessment — and the methodology used to perform the cyber risk assessment should be designed with input from IT as well as other key (financial, operational and management) departments within the agency, as depicted in **Figure 1**. The resulting register of risks should be shared with those same departments for risk scoring (and weighting) or "risk sensing," using a methodology that considers, but is not limited to, likelihood and impact of risk.

The cyber risk assessment may leverage the commonly accepted Risk Management Framework (RMF)[4], which provides the context to evaluate the results and prioritize spending. After assessing the applicable security controls in the RMF, identified deficiencies are standardized, with likelihood and

Figure 1. Assessment of Cyber Risk Requires Collaboration across Departments



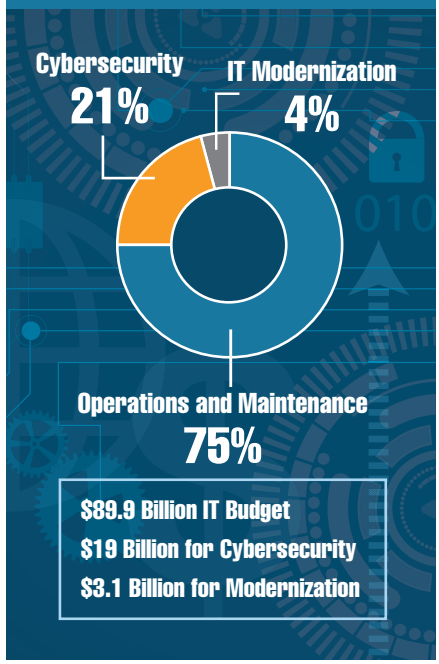
impact scores for each vulnerability. Combined with historical audit data and existing cyber data (e.g., scan results and patch levels), each vulnerability is assigned a composite score. The vulnerabilities with the highest scores pose the greatest threats. Applying analytics to existing IT, financial, and operational data sets adds a proactive and preventive layer to the cyber risk assessment and facilitates a comparison of the benefits to mitigating specific risks against the corresponding costs (e.g., financial, loss of trust and weakened security) of risk mitigation. The final product is a "normalized" hierarchy of vulnerabilities that may be used to drive a prioritized list of investments to reduce the surface area of threat vectors to the federal agency. This approach enables the CFO and CIO to make better-informed IT spending decisions, and provides the basis for the CIO to understand and potentially accept and/or mitigate risks for vulnerabilities that are not remediated.

❷ *IT Budget*

The federal government increased its proposed IT budget by 35 percent to $89.9 billion for FY17 — of which $19 billion is dedicated to cybersecurity and an additional $3.1 billion is allocated to an IT Modernization Fund[5] (see **Figure 2**). This IT Modernization Fund is intended to bolster agencies' momentum toward cloud computing solutions, digital service offerings, and shared services, as agencies continue to upgrade from outdated technologies and systems to better serve their missions.

Federal CIOs are responsible for the management and oversight of the IT budget to support the execution of agency mission and objectives. The objective of FITARA is to provide appropriate visibility and involvement of agency CIOs in the management and oversight of IT resources to support the successful implementation of cybersecurity policies and to prevent interruption or exploitation of program services.

Figure 2. Breakdown of FY17 Federal IT Funding



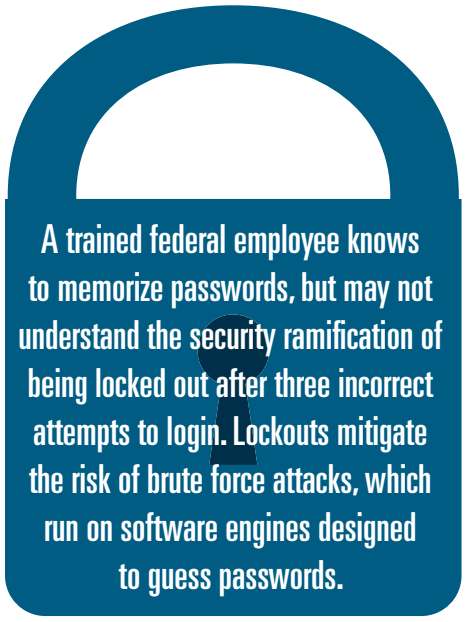
FITARA was enacted in December 2014 and explained further in Office of Management and Budget (OMB) Memorandum, *Management and Oversight of Federal Information Technology* (M-15-14), which was released in June 2015. OMB M-15-14 provides implementation guidance for FITARA and IT management practices, including enhanced transparency and improved risk management in IT investments, federal data center consolidation, expansion of training, and software purchasing.

With increased emphasis on FITARA, aimed to align IT resources with agency missions, goals, programmatic priorities and statutory requirements, the CIO's job performance may be more heavily scrutinized, including decisions on investments in training and cybersecurity, as well as incident response initiatives. By aligning IT spending with the results of the cyber risk assessment, federal CIOs may streamline compliance with FITARA while maintaining focus on mission objectives and reducing risk.

3 *Training Federal Employees on Cybersecurity*

While working toward modernization goals, federal agencies are at a competitive disadvantage in recruitment and retention of top talent needed to achieve modernization. Studies have demonstrated that senior-level software engineers can make approximately $33,000 more annually than their federal counterparts; and entry-level software engineers' average salaries are $14,000 more annually than their federal counterparts'.[6] This insight forces federal agencies to be more strategic in cyber spending, because agencies not only need to remediate vulnerabilities, but must achieve their mission while endeavoring to hire and retain top talent despite salary discrepancies between the federal and commercial markets. As such, training of federal cyber employees and prioritization of cyber risk management efforts (and corresponding spending) is key for enhancing security.

Federal employees are trained on basic cybersecurity principles (e.g., physical security and safeguarding data) through standard onboarding and annual training requirements, but cyber risk management is something different altogether. The rapid progression of technology exponentially increases the importance of more robust and ongoing training so employees' knowledge and awareness increases with the pace of change in the cyber threat landscape.



There is a distinction between what an employee needs to know and what they should understand to do their part in protecting federal agency systems and data. A trained federal employee knows to memorize passwords, but may not understand the security ramification of being locked out after three incorrect attempts to login. Lockouts mitigate the risk of brute force attacks, which run on software engines designed to guess passwords.

Security is everyone's responsibility; and a highly burdened workforce requires targeted and efficient training to provide useful (and relevant) information and education in the least amount of time. Investing in level-specific training and innovative delivery models may prevent or lessen the impact of cyberattacks and breaches and could cost agencies a fraction of the incident recovery expenses. By expanding the curriculum of cybersecurity training offerings beyond role-based training to include simulation-based training and gamification, federal employees may learn from real-world scenarios in a dynamic environment (e.g., in-person and online gaming simulations). Some examples of role-based training include:

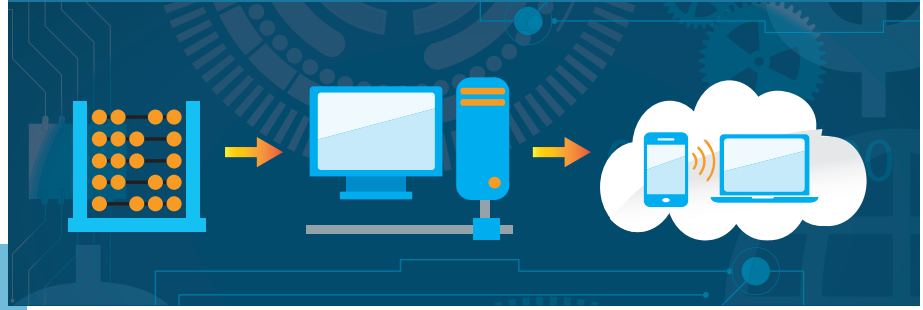
Non-IT personnel

Introductory, foundational cybersecurity training should include topics such as how to handle suspicious emails and links, the role social media can play in cyberattacks and how to report suspicious activity. This level of training can be updated to address new threat vectors and techniques, and should be easily consumed by non-IT personnel.

IT personnel

In addition to receiving the same foundational training as non-IT personnel, IT personnel should also receive training relative to cyber threat analytics and cyber reconnaissance tactics that can be deployed to more accurately measure and mitigate threats. For managers and program area leads within the IT department, scenario-based incident response training should also be mandatory.

Figure 3. Training Should be Commensurate with Current Technology Environment and Trends



Executive-level training

Where IT personnel may receive training on the theories and concepts of cybersecurity, federal executives should receive tactical training. In addition to receiving foundational training, federal executives should attend mandatory scenario-based incident response training so they are well-prepared to make decisions in the event of a security incident.

As depicted in **Figure 3**, as agencies move toward digital platforms and grant access to users from a multitude of devices, there is an increasing need for cybersecurity measures and training.

4 *Incident Response*[7]

Security breaches, data breaches, cyberattacks — these are terms used in reference to cybersecurity incidents, and each describes a slightly different type or categorization of incident. A security breach is any incident, whether intentional or unintentional, that results in unauthorized access to data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A data breach is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository. A cyberattack is a deliberate exploitation of computer systems, technology-dependent enterprises and networks — also known as a computer network attack. Cyberattacks use a variety of vectors or methods to gain unauthorized access and alter computer code, logic or data, resulting in disruptive consequences that can compromise the confidentiality, integrity, or availability of information systems and their data. These attacks are often perpetrated to commit cybercrimes such as information and identity theft. Measuring the number and severity of incidents challenging, since there is no standard method to count or report them; however, in 2013, the Pentagon reported it thwarted 10 million cyberattack attempts per day.[8]

Agencies should follow the approach for incident response planning as outlined by NIST SP 800-61 Revision 2: "Computer Security Incident Handling Guide." In addition to updating incident response plans regularly and including the results in the cyber risk assessment, federal agencies should employ advanced analysis and detection capabilities (i.e., cyber reconnaissance methods) to augment existing solutions. By expanding the inputs to continuously monitor the threat landscape, the cyber risk assessment lifecycle will flow into employee training initiatives and incident response plans, which are tailored to current and specific threats and risks. Federal spending on cybersecurity management should, in turn, be based on the prioritization of threats and risks.

Conclusion

Federal CIOs — working alongside CFOs and other agency leaders throughout the cyber risk assessment process — will have improved visibility and insight into cybersecurity threats and risks, and their potential impact on achieving agency objectives. This coordination and collaboration will also provide an increased understanding of agency-wide cybersecurity training and incident response requirements. It is imperative that CFOs, CIOs and leadership personnel establish innovative and repeatable means to advance efforts in understanding and mitigating the ever-evolving cyber threats.

Endnotes

1. www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. Accessed Aug. 31, 2016.
2. fcw.com/articles/2015/09/10/opm-breach-cost.aspx. Accessed Aug. 31, 2016.
3. Ibid.
4. csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. Accessed Aug. 31, 2016.
5. fedscoop.com/federal-it-2017-budget-proposal-obama-administration. Accessed Aug. 31, 2016.
6. www.bah.com/insights/2009/07/42415933. Accessed Aug. 31, 2016.
7. Definitions of security incidents adapted from www.techopedia.com/dictionary. Accessed Aug. 31, 2016.
8. www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/. Accessed Aug. 31, 2016.

Deborah Golden, a principal with Deloitte & Touche LLP, leads the Federal Cyber Risk Services practice and has 20 years of information technology, security and privacy experience. She specializes in providing cybersecurity and identity and access management services to federal, life sciences and health, and financial services clients.

Rebecca Tyler, CISA, a senior manager with Deloitte & Touche LLP with 15 years of experience, specializes in IT strategy and governance — including enterprise cybersecurity strategy planning and execution, information security governance and audit remediation, as well as IT risk management framework development and implementation. She primarily serves clients in the federal health sector.

Danielle Eucker, CISA, CIA, PMP, a senior manager with Deloitte & Touche LLP, specializes in risk management, business process and IT controls design and implementation, and internal audit. Her recent work includes cybersecurity strategy planning and implementation, and IT security remediation.

Joseph Meyers, JD, MS, Security+, CISSP, a senior consultant with Deloitte & Touche LLP, specializes in cloud-based, host-based, and biomedical device cybersecurity. He serves federal clients in the national defense, civilian and health sectors.