RSA

WHITE PAPER

DIGITAL RISK IS MISSION RISK

IT MODERNIZATION TRENDS IMPACTING AGENCY MISSIONS

From federal agencies (whether civilian agencies or defense and intelligence agencies) to state and local governments, organizations in the public sector are advancing digital transformation to better serve constituents, protect the homeland, connect citizens with data and increase agency efficiency.

As agencies and their partners work to make government more accessible to citizens through online and mobile experiences, there is a risk that these activities will also make operations and data more vulnerable to cyber attacks.

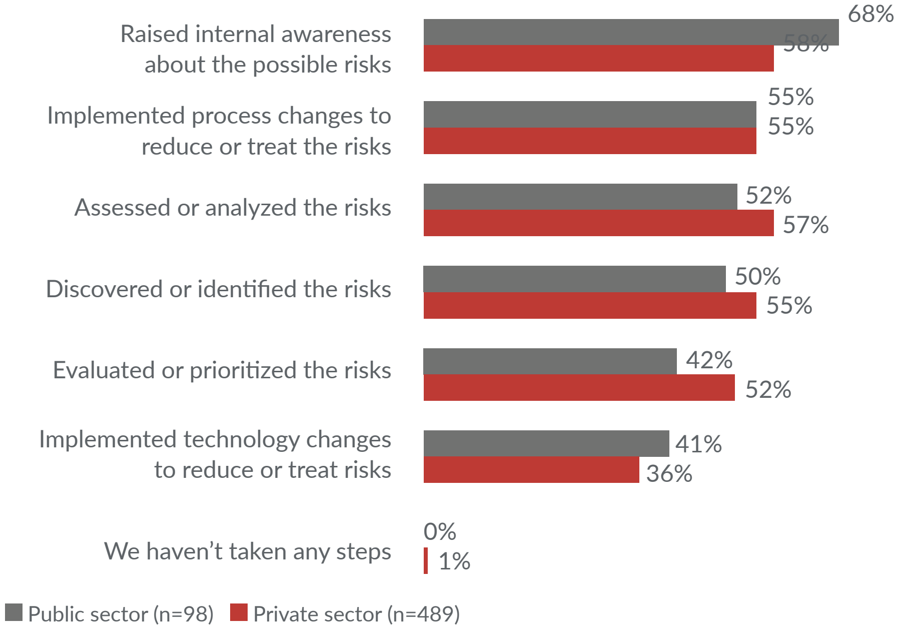
This digital transformation is not an overnight phenomenon. It began with 1990s legislation (Clinger-Cohen Act of 1996)[1] that established agency-level CIOs to oversee and implement IT modernization, and continued through the E-Government Act of 2002,[2] which promoted the use of the internet to improve citizen participation in government and also resulted in the establishment of the Federal Information Security Modernization Act of 2002 (FISMA) to ensure implementation of appropriate security measures as the government transforms. More recently, policies and standards such as Cloud First[3] and Cloud Smart[4] have driven organizations to rapidly advance digital transformation in government. In addition, Executive Orders have outlined administrations' cyber agendas. Through all this change, government IT and security professionals are challenged to ensure that systems and data remain secure and protect sensitive government and citizen data, while remaining open and transparent to stakeholders.

Working both independently and in partnership with other organizations (public and private), government organizations pursuing digital transformation to deliver mission outcomes for constituents face some level of potential for increased risk that could impact the mission. As agencies and their partners work to make government more accessible to citizens through online and mobile experiences, there is a risk that these activities will also make operations and data more vulnerable to cyber attacks—whether by external actors such as nation-states, activists and disgruntled citizens looking to create chaos, or by insider threats across the government workforce. Potential consequences can have major impacts:

- Threats to national security
- Disruptions to public services, utilities and healthcare
- Privacy violations, breaches and exposure of millions of citizens' personal and financial data to criminals on the dark web
- Leaks of classified information resulting in the potential for international or domestic outrage, economic trade impact and placing armed forces in harm's way
- Election tampering that undermines voter confidence in legitimate elections

Organizations in the public sector are acutely aware of the serious nature of digital risk and are taking actions to mitigate. According to the results of the RSA Digital Risk Study, included in the 2019 RSA Digital Risk Report, 68% of public sector respondents reported taking action to raise awareness internally about the possible risks of digital transformation, compared with only 58% of organizations in the private sector. This indicates that public sector organizations are outperforming private sector organizations in educating the workforce about the risks and how to protect themselves and government data and systems from the bad actors.

Steps Taken to Manage Digital Risk



According to the results of the RSA Digital Risk Study, included in the 2019 RSA Digital Risk Report, 68% of public sector respondents reported taking action to raise awareness internally about the possible risks of digital transformation, compared with only 58% of organizations in the private sector.

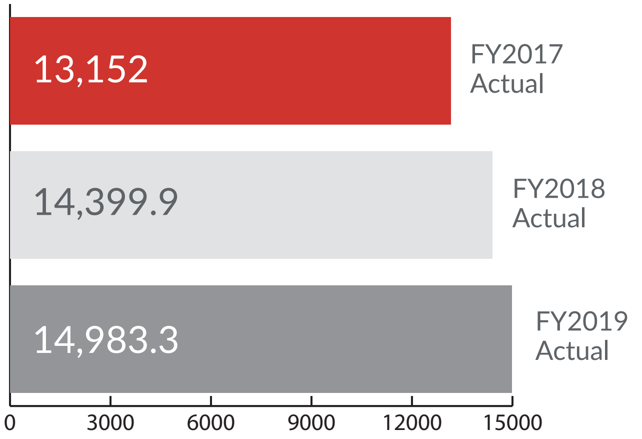
In addition, public sector respondents identified the top three specific areas of digital risk they will be most concerned about over the next two years that must be addressed: the risk of a cyber attack, data privacy risk and dynamic workforce risk.

CYBER ATTACK RISK

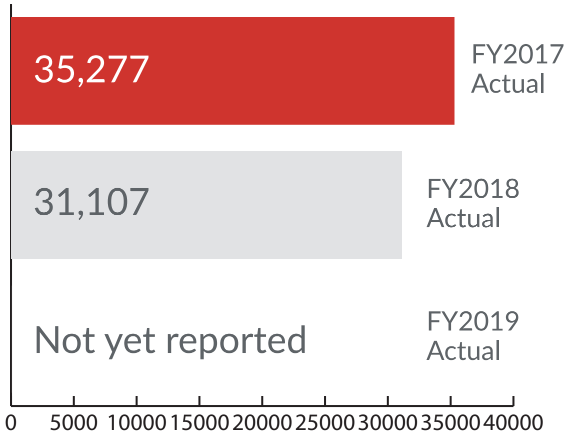
Mitigating cyber attacks has represented the public sector's top risk management objective for the past two years, according to the RSA Digital Risk Study. The importance of managing this risk is underscored by the FISMA Fiscal Year 2018 Annual Report to Congress from the U.S. Government Accounting Office (GAO). This report shows substantial progress towards managing cyber attack risk, such as a 12% decrease in cybersecurity incidents from the previous fiscal year (35,277 in FY17). However, the report also highlights the fact that there were still over 31,10[7] cybersecurity incidents in FY18.[5] This shows that federal agencies face a huge challenge in securing their information and systems from bad actors, making cybersecurity challenges a

Agency Cybersecurity Funding Totals

(in millions of dollars)



FISMA Reported Cyber Incidents



Source: https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

"high-risk issue" for the federal government.[6] An even more recent GAO report listed "ensuring the cybersecurity of the nation" as one of nine high-risk areas warranting particularly focused executive and congressional attention.[7]

Federal agencies are by no means the only public sector organizations experiencing cybersecurity challenges today. Earlier this year, a spate of ransomware attacks in Texas affected 22 municipal governments at around the same time that data networks in Baltimore, the Georgia courts system and a county in Utah were also targeted.[8] It may be reasonable to speculate that smaller governments are more vulnerable to these types of attacks than federal agencies because attackers see them as having fewer resources to invest in cybersecurity. While many of these types of attacks are growing,[9] states and local governments are taking action. For example, states like Texas are providing cybersecurity services and managed security services (MSS) in partnership with private providers, among other tools and support, to offer local governments and public entities cost-effective access to security tools, monitoring and detection.[10] Additionally, states and local governments are scaling up training to help educate their workforce in best practices to be cyber-aware. Simple training such as educating users about phishing emails, how to recognize them and how to respond can help flag potential threats and prevent similar phishing-based attacks.

Public sector organizations continue to improve their overall cybersecurity posture while battling with budgetary and resource constraints. Government agencies are adopting common frameworks for cybersecurity, like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), focusing on technology, people and process to identify, detect, protect, respond to and recover from cyber attacks. Organizations are taking a risk-based approach, implementing automation and advanced threat detection to be able to prioritize the threats that matter most. In addition, security leaders across the government continue to implement and improve foundational security protections—for example, multi-factor authentication, identity governance and lifecycle management—to help ensure that there is confidence in who is accessing government information.

> **Security leaders across the government continue to implement and improve foundational security protections—for example, multi-factor authentication, identity governance and lifecycle management—to help ensure that there is confidence in who is accessing government information.**

DYNAMIC WORKFORCE RISK

Today's public service workforce is dramatically changing. Not only are the demographics of government workers evolving as more millennials join public service but there is also continued reliance on, and contributions from, large numbers of contractors to support missions. As in the private sector, public sector organizations are adopting more digital technologies to help their workforce be more productive and efficient at achieving mission outcomes. However, this creates a challenge for government security and risk management leaders to balance the open and fluid flow of information across devices, platforms and the cloud for the diverse workforce against security command and control of resources required to protect citizen and government data.

The challenge is compounded by regulatory mandates, as well as agency and executive-level mandates, that place additional requirements on agencies to achieve access and identity assurance across the public sector ecosystem. The policies to manage the balance are also changing. While government has had insider threat programs for years, the notion of insider threat has evolved. With more and more government data sitting on mobile devices and in the cloud, even just a careless—but not malicious—employee or contractor can be a weak link. Leaving a government-issued laptop on a bus, misplacing a PIV card, transferring data from a government-issued device to a personal or other work device to complete a task—these are all real risks, and even simple mistakes that can lead to data loss. Public sector organizations are doing more to address this issue through training and awareness. As previously mentioned, one finding of the RSA Digital Risk Report is that public sector organizations are doing a better job than their private sector counterparts at raising awareness in the workforce of these digital risks. Continued vigilance and training are key to ensuring that every public servant and contractor is taking responsibility for the security of government data and resources.

Government organizations are constantly working to address data privacy risk through improving access controls to gain better visibility into who has access to data and what they are doing with it, as well as evolving policies for managing data to ensure privacy of the workforce and citizens.

Lastly, the tools that agency security leaders deploy to help make the workforce more productive are evolving as well. Leaders are looking to complement traditional access controls (CAC/PIV) and to employ other controls such as multi-factor authentication, mobile push, biometrics, etc., that use modern authentication approaches to simplify access. This streamlines the processes to gain access for the workforce, but ensures access control across each system. Leveraging risk-based analytics on the back end makes it possible to monitor and detect inappropriate access in new ways that do not cause friction for the workforce user.

DATA PRIVACY RISK

Data privacy is everyone's concern. While high-profile breaches in the commercial world lead the headlines, public sector organizations are not immune. The 2019 Verizon Data Breach Investigations Report found 16% of data breaches to be in the public sector, nearly the same percentage as in healthcare.[11] The National Law Review describes data privacy risk in the public sector as a "less discussed" risk that is moving to the forefront, especially in the wake of the 2019 breach of the Office of Personnel Management (OPM), which exposed personal data in millions of background investigation records and personnel files.[12]

The size of the OPM breach is a sobering reminder of just how much personal data is at risk in government systems. Beyond the millions of people working in the federal government or applying to work there, there are many millions more whose data is in government systems. Government organizations' missions are to serve their constituents. Therefore, securing citizen data and ensuring it is used only for the intended purposes is part of fulfilling the trust that the citizens place in their government. This is paramount to ensuring mission success.

The good news is that government organizations are constantly working to address data privacy risk through improving access controls to gain better visibility into who has access to data and what they are doing with it, as well as evolving policies for managing data to ensure privacy of the workforce and citizens. For example, the Internal Revenue Service has instituted a program to minimize the use of Social Security numbers to authenticate taxpayers.[13] And NIST is expected to soon introduce a framework for data privacy that could serve as a model for not only public agencies but also private businesses—much as the existing NIST CSF does.[14]

The public sector is far ahead of the private sector in raising awareness about digital risk, but still has much progress to make in assessing, prioritizing and treating aspects of that risk to ensure mission success.

CONCLUSION

Today's government organizations continue to modernize how they deliver services to constituents and deliver mission outcomes with technology. As the RSA Digital Risk Study makes clear, managing the risks associated with digital transformation is top of mind for government security leaders. But as digital transformation increasingly defines the work of government today, so too does digital risk. And it's not just the three risks discussed here—it's also the regulatory, operational and other risks that impact agency missions. The stakes are arguably higher for government, and the challenges greater. But one thing not in question is the need to manage the risks associated with digital transformation. Organizations in the public sector that are engaged in digital transformation are keenly aware of this, according to the RSA Digital Risk Study, which indicates the public sector is far ahead of the private sector in raising awareness about digital risk, but still has much progress to make in assessing, prioritizing and treating aspects of that risk to ensure mission success.[15]

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk world at rsa.com

[1] "Information Technology Management Reform Act of 1996," Wikipedia: The Free Encyclopedia, Wikimedia Foundation, Inc., February 19, 2019, 7:45 p.m., https://en.wikipedia.org/wiki/Information_Technology_Management_Reform_Act_of_1996 (accessed October 10, 2019)

[2] "E-Government Act of 2002," Wikipedia: The Free Encyclopedia, Wikimedia Foundation, Inc., April 18, 2019, 2:00 p.m., https://en.wikipedia.org/wiki/E-Government_Act_of_2002 (accessed October 10, 2019)

[3] "OMB announces 'cloud first' policy for agencies, Federal News Network, https://www.federalnewsnetwork.com/technology-main/2010/11/omb-announces-lsquocloud-firstrsquo-policy-for-agencies/ (November 23, 2010)

[4] "From Cloud First to Cloud Smart," Federal Cloud Computing Strategy, https://cloud.cio.gov (accessed October 10, 2019)

[5] "Federal Information Security Modernization Act of 2014: Annual Report to Congress," https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf (Fiscal Year 2018)

[6] "Key Issues: Cybersecurity Challenges Facing the Nation—High Risk Issue," U.S. Government Accountability Office, https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary (accessed October 10, 2019)

[7] "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas," U.S Government Accountability Office, https://www.gao.gov/products/GAO-19-157sp#summary (March 6, 2019)

[8] "22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault," National Public Radio, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault (August 20, 2019)

[9] Allen Kim, "In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks," CNN, https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html (October 8, 2019)

[10] "Cyberdefense for Texas State Government," Fiscal Notes: A Review of the Texas Economy from the Office of Glenn Hegar, Texas Comptroller of Public Accounts https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php (March 2019)

[11] "2019 Data Breach Investigations Report," Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (May 2019)

[12] Kristin Ann Shepard, "Data Privacy Exposure Hits the Public Sector," The National Law Review, https://www.natlawreview.com/article/data-privacy-exposure-hits-public-sector-lessons-opm-data-breach-class-action (August 13, 2019)

[13] "What are we doing to protect taxpayer privacy?" IRS, https://www.irs.gov/privacy-disclosure/what-are-we-doing-to-protect-taxpayer-privacy (October 18, 2019)

[14] Alex Hickey, "Government takes baby steps in data privacy with NIST framework, bill discussions," CIO Dive, https://www.ciodive.com/news/government-takes-baby-steps-in-data-privacy-with-nist-framework-bill-discu-1/550084/ (March 12, 2019)

[15] "RSA Digital Risk Study," RSA Digital Risk Report, 1st Edition, https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf (September 2019)