The State of Cybersecurity from the Federal Cyber Executive Perspective

KPMG

An (ISC)² Report

EXECUTIVE SUMMARY

THE REALITY THAT CYBER ATTACKS ONCE CONSIDERED PREVENTABLE ARE NOW REGARDED AS INEVITABLE has long been understood and acknowledged by cyber professionals, but this reality is just now reaching the masses due to media coverage of high-profile breaches in recent years. The increased public scrutiny has added to the federal government's enormous task of defending itself against an infinite number of attackers.

> **"THE PLAYING FIELD IS TILTED IN FAVOR OF THE ADVERSARY. TO ALTER THIS REALITY, A FUNDAMENTAL SHIFT IS REQUIRED IN HOW THE GOVERNMENT APPROACHES CYBERSECURITY."**
>
> –SECURITY DIRECTOR, CIVILIAN AGENCY

In March 2016, (ISC)² and KPMG LLP surveyed a targeted pool of executive-level government officials and contractors with the goal of reporting the state of cybersecurity from federal cyber experts whose purview included an enterprise-wide perspective. Responses were collected both anonymously online and during individual interviews, covering a range of topical areas that are key to understanding the state of cybersecurity today. This included professional development, governance and standards, resource and program management and risk management and resiliency.

KEY FINDINGS

- An alarming **59% of respondents say that their agency struggles to understand how cyber attackers could potentially breach their systems**, with 40% of respondents unaware of where their key assets are located.

- **65% of respondents disagree that the federal government as a whole can detect ongoing cyber attacks.**

- The **lack of accountability was a consistent theme throughout** the survey results, as some respondents were unable to identify a senior leader at their agency whose sole responsibility is cybersecurity.

- Leaders are realizing that **people can be their organization's greatest cybersecurity asset or greatest liability**, with 42% of respondents indicating that people are currently their agency's greatest vulnerability to cyber attacks.

- When asked of the effectiveness of the Cybersecurity Sprint, **52% of respondents disagreed that the Cyber Sprint improved the overall security of federal information systems**. 25% of respondents said their agency made no changes in response to the Office of Personnel Management (OPM) data breach that occurred in June 2015.

- **Only 67% of respondents believe their agencies can appropriately respond to a cyber incident**. 40% of respondents surveyed believe their agency's incident response plan is not effective in responding to cyber attacks, even after the OPM data breach.

- The overwhelming technology solution recommended by respondents was the **need for predictive analytics.**

- **Cybersecurity is quickly moving away from a "one size fits all" set of standards**, but the many compliance requirements do not allow for sufficient customization.

- Respondents indicate that **certain departments within agencies do not view cybersecurity as important to their departmental functions**, the most notable being human resources, purchasing/procurement and communications/PR.

DETAILED SURVEY FINDINGS BY TOPICAL AREA

To assess its current state, cybersecurity must be identified as an organization-wide challenge and responsibility, not just a concern of the information technology department. With the OPM data breach behind them, a Presidential transition in front of them and accountability top of mind, there is one theme that remains foundational to how federal cyber executives view future progress – that people can be an organization's greatest cybersecurity asset or its greatest liability. The message that effective cybersecurity programs start and end with the human factor is the underpinning of the data found throughout the following topical areas.

"PEOPLE CAN BE AN ORGANIZATION'S GREATEST CYBERSECURITY ASSET OR ITS GREATEST LIABILITY.

Professional Development

Federal executives overwhelmingly identified people (employees, contractors and system administrators) as their greatest vulnerability with regard to a potential cyber attack – greater than the vulnerability represented by smart devices, e-mail servers, enterprise applications and systems and other forms of technology.

Since people can be an organization's greatest asset in improving its cybersecurity efforts, training and job satisfaction should be key areas of focus and prioritized as areas for dedicated resources.

A civilian agency security director said, "Our user base must become more informed and active in both detection and reporting. We have the 'See Something, Say Something' campaign in the kinetic space – we need the same diligence in cyberspace." This point is reaffirmed by the fact that for many large-scale and recent breaches, the exploited weaknesses were not highly technical attacks.

Among respondents, training, education, recruiting and certification are widely viewed as essential to improving the state of cybersecurity, with 50% of respondents identifying training/recruiting as one of their top three areas for applying proposed Cybersecurity National Action Plan (CNAP) resources.

"ADVANCING AN ORGANIZATION'S SECURITY AGENDA NO LONGER RESTS UPON EDUCATING ITS CYBER WORKFORCE; RATHER, ITS ENTIRE WORKFORCE MUST BE EDUCATED IN CYBER.

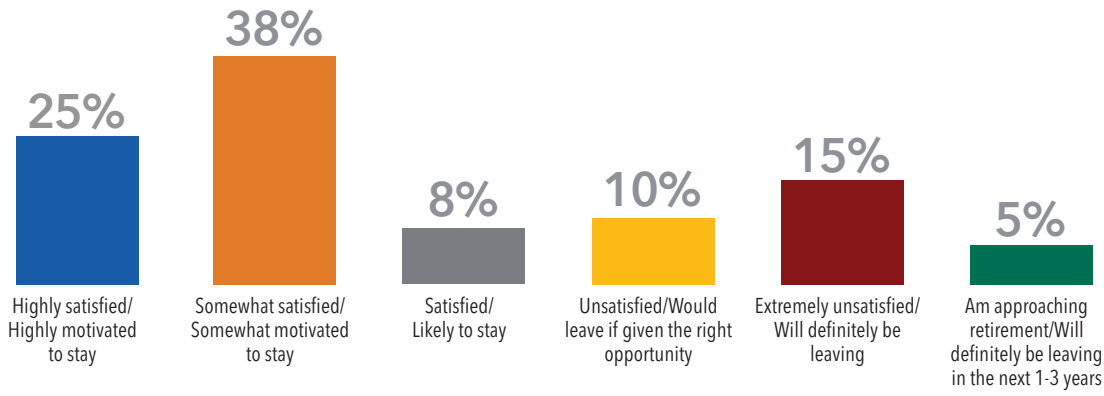
It is imperative to create more awareness and vigilance across the organization through regular and continuous cyber hygiene trainings and simulation drills, rather than annual awareness seminars with ineffective PowerPoint presentations. In addition, 77% of respondents support mandatory professional certification for all government personnel working on cybersecurity systems.

Often overworked and holding highly stressful positions, cyber practitioners face a lack of resources, causing frustration that can lead to high rates of turnover. Approximately 25% of federal respondents noted dissatisfaction with their position and a willingness to leave their agency. Given the extreme nature of the existing shortage of cyber talent and the enormous task of filling the workforce pipeline, agency and government leadership must address job satisfaction of the existing cyber workforce.

The cyber workforce of the future will not resemble the workforce of the past, or even of the present. The extreme shortage of qualified professionals, the demand for specialized training, the aging federal workforce (also known as the "silver tsunami") and the focus on managing risk is reshaping the role of the cyber practitioner. Continued attention and efforts need to not only focus on promoting the need for the increasing number of capable professionals entering the cybersecurity field, but resources must be dedicated to retaining the existing cyber talent at all levels.

FIGURE 1.

How satisfied and motivated are you to remain at your agency?



Governance and Standards

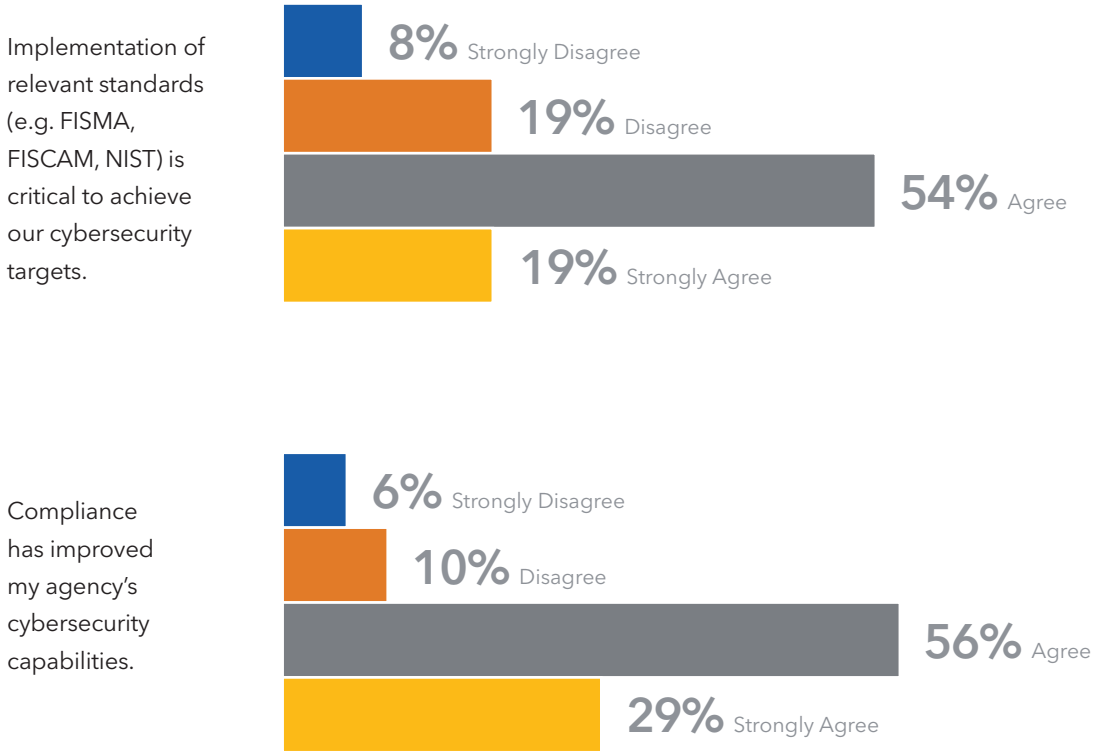
Federal cyber executives are continuing to see greater awareness of their respective missions by federal leaders, but not enough improvement in the security posture of the federal domain. Prevention begins with governance and requires installing fundamental measures and placing responsibility within the organization. The survey responses show that federal agencies have implemented a number of activities around managing security, including policies, training or increasing the role of mandated compliance. Respondents largely agree that these changes are making a difference in protecting our nation's data.

85% of respondents agreed that compliance with federal mandates has improved their agency's cybersecurity capabilities. Implementation of relevant standards, such as NIST, FISMA and FISCAM, are thought to be critical to achieving cybersecurity targets by 73% of respondents. While respondents recognized that compliance has improved their agency's cybersecurity capabilities, many believe there is an overwhelming amount of information that can seem like time-consuming "check the box" activities to cyber practitioners. Sound cybersecurity practices must go beyond compliance.

> **"THE [NIST CYBERSECURITY FRAME–WORK] MODEL IS SIMPLE IN FORM AND SEEMS TO BRIDGE THE GAP BETWEEN RISK MANAGEMENT MATURITY AND IT SECURITY."**
>
> – SECURITY DIRECTOR, CIVILIAN AGENCY

FIGURE 2.

Federal cyber executives agree that compliance is improving cybersecurity.

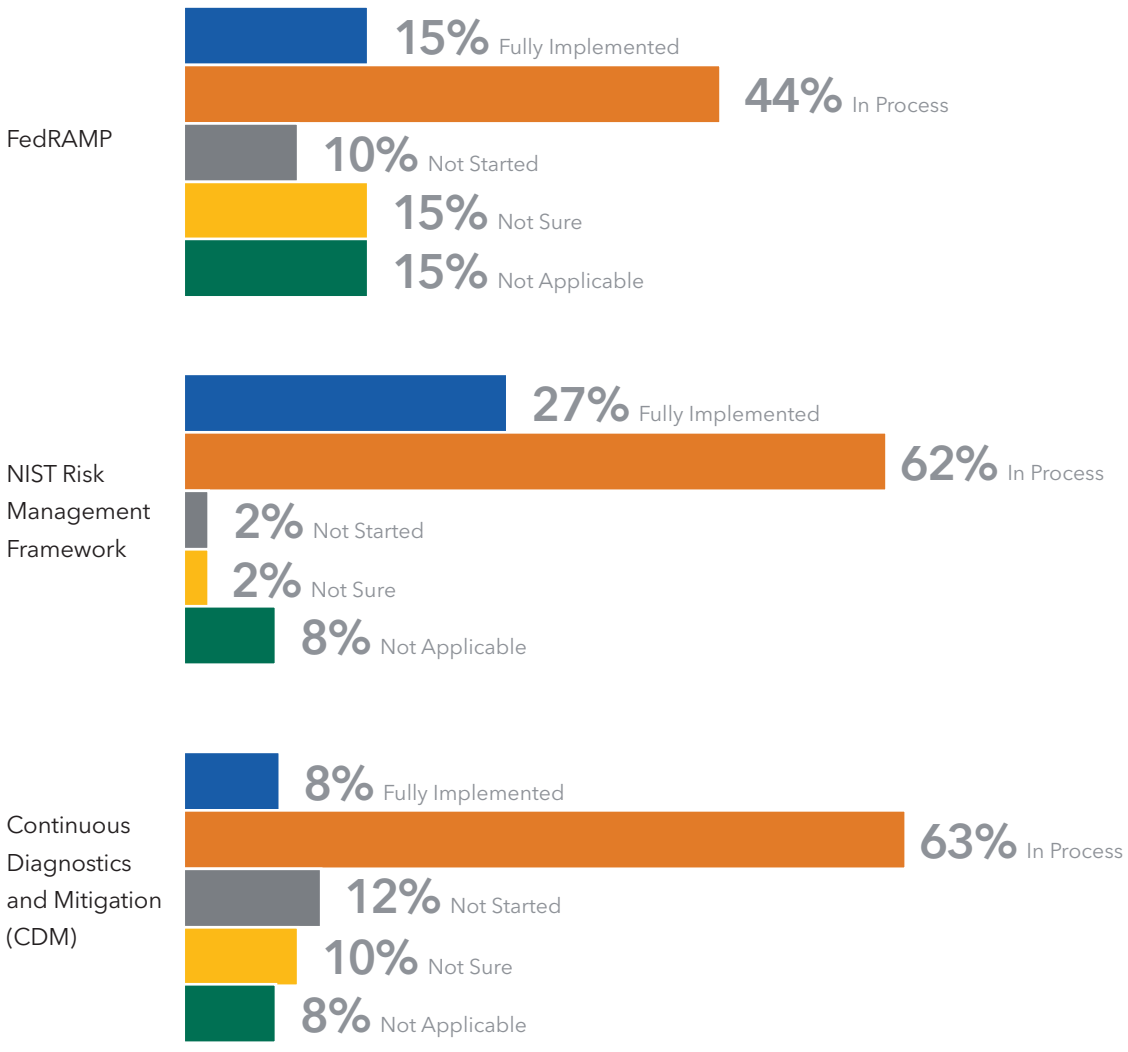


While most respondents consider standards important, the implementation and perceived effectiveness of recent standards are mixed as many agencies have prioritized what they consider most important. For instance, 63% of respondents said that Continuous Diagnostics and Mitigation (CDM) is currently in progress at their agency while 12% said they have not started and only 8% confirmed completion.

The NIST Risk Management Framework (RMF), the successor to DoD Information Assurance Certification and Accreditation Process (DIACAP), is in progress at 62% of the respondents' agencies, while 2% have not started, and 27% noted completion. The Federal Risk and Authorization Management Program (FedRAMP) is in progress at 44% of the respondents' agencies, while 10% have not started, and 15% have completed implementation.

FIGURE 3.

Regarding your agency, what is the implementation status of the following cyber initiatives?



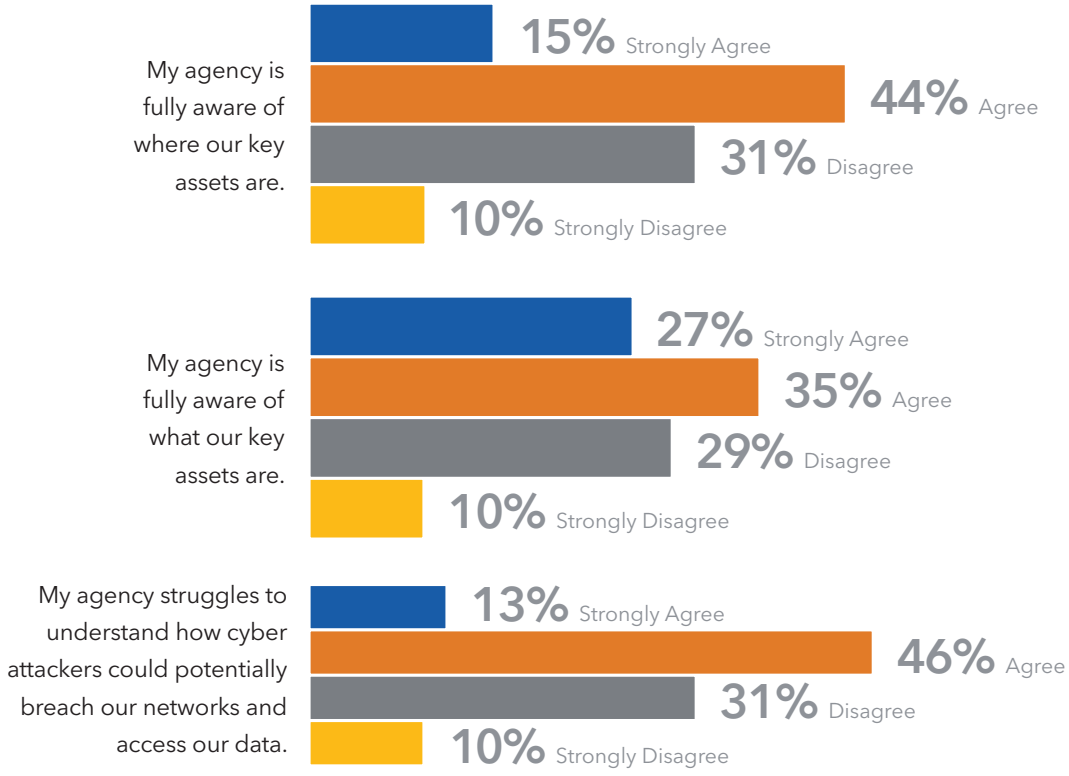
Governance and Standards (cont.)

Knowledge of how agencies' full arsenal of assets can be affected by cyber threats has become very complex, especially with the introduction of systems migrating to the cloud. An alarming 59% of respondents say that their agency struggles to understand how cyber attackers could potentially breach their systems. 62% of respondents indicated that they were fully aware of what their key assets are, but 41% responded that they were unaware of where their key assets are. These results indicate that the network boundary of many agencies may be changing faster than federal executives realize, resulting in new bleeding-edge technologies that may not fit in rigid regulatory or legislative mandates. Cybersecurity is quickly moving away from a "one-size-fits-all" approach as expanding compliance requirements do not allow for enough customization.

> **"[AS A NEW CISO, I WOULD] ASSESS THE STATE OF MY INFORMATION SECURITY CAPABILITIES USING THE CYBERSECURITY FRAMEWORK'S IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER FUNCTIONS. THAT WOULD GIVE ME A SENSE FOR WHERE I AM WELL PREPARED AND WHERE I NEED TO PUT MY ATTENTION."**
>
> – SECURITY DIRECTOR, CIVILIAN AGENCY

FIGURE 4.

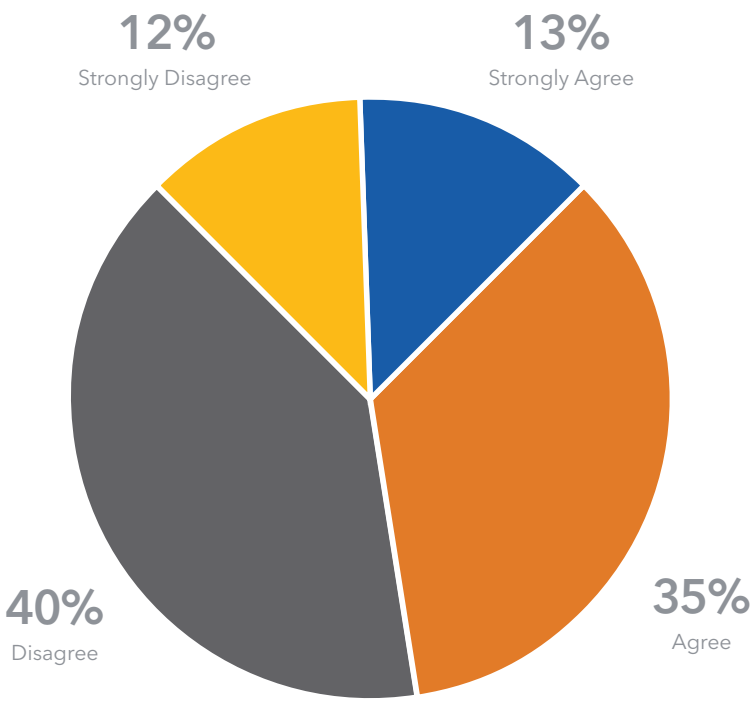
Agencies' cybersecurity awareness and understanding is varied.



Lack of resources and accountability within an organization for cybersecurity may also be dampening the effect of compliance. Approximately one year prior to this survey being conducted, the Office of Personnel Management (OPM) sustained a widely covered data breach that impacted personnel records of 21.5 million current, former and retired federal employees and contractors. As a result, U.S. Chief Information Officer Tony Scott launched a 30-day Cybersecurity Sprint in June 2015 that instructed agencies to immediately take steps to further protect federal information assets and improve the resilience of federal networks. In response to that breach and discovery, 52% of respondents disagreed that the Cyber Sprint response improved the overall security of federal information systems. A former federal CISO cautioned that, "OPM had the breach, and while others were affected, they may not have felt the impact to the pain level needed. The Sprint looks to be turning into a marathon for some agencies – resources, mandates, oversight are all roadblocks to getting agencies started on Tony Scott's vision of security." The challenges in responding to the OPM data breach are discussed further in the next sections.

FIGURE 5.

My agency's response to the OPM data breach ("Cyber Sprints") has improved our cybersecurity.



Resource and Program Management

Cyber professionals face a number of hurdles in advancing their agencies' cybersecurity efforts. When asked for the top three factors that hinder their agency's ability to advance cybersecurity efforts, the top responses were a lack of funding, absence of accountability, lack of understanding and lack of expertise.

While a lack of information is not viewed as a hindrance, too much information may be causing difficulties. As stated earlier, the amount of compliance information and guidance in the federal domain can be overwhelming for practitioners.

Throughout the survey, respondents identified an absence of accountability as a major challenge. A contributing factor to the lack of accountability is that 21% of survey respondents said that there is not a designated cybersecurity leader at their agency. When the 77% of respondents that said there was a designated leader were asked to identify that person by their title, the results were mixed between the Departmental CISO, CIO, Deputy CIO, Security Director and a number of other responses. The varied responses suggest that more clarity and consistency are needed.

FIGURE 6.

What are the top 3 factors that hinder your agency's ability to advance cybersecurity efforts?

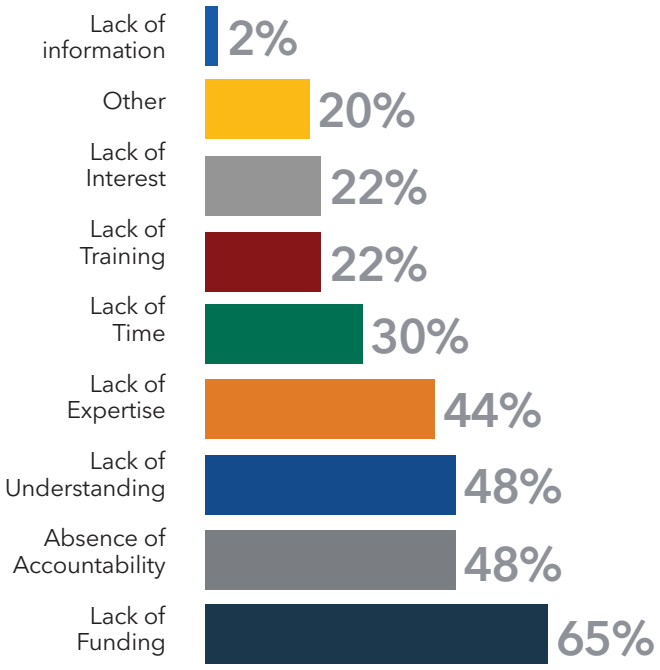


FIGURE 7.

Is there a senior leader(s) in your agency whose sole responsibility is cybersecurity?

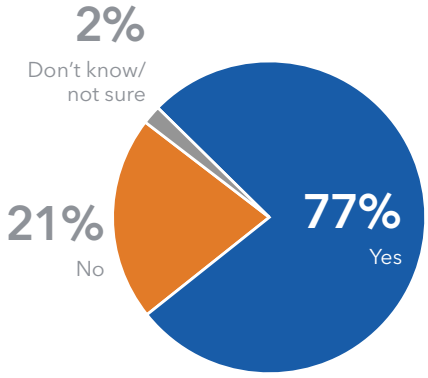
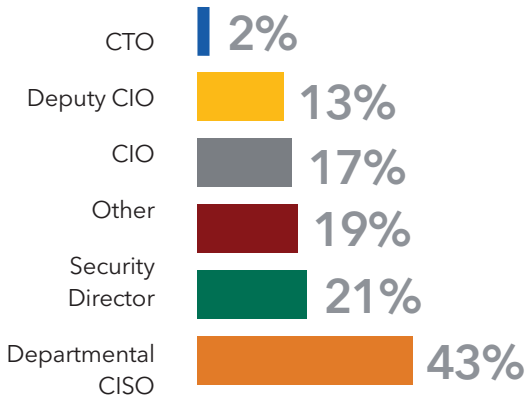


FIGURE 8.

Please select the senior leader(s) whose sole responsibility is cybersecurity

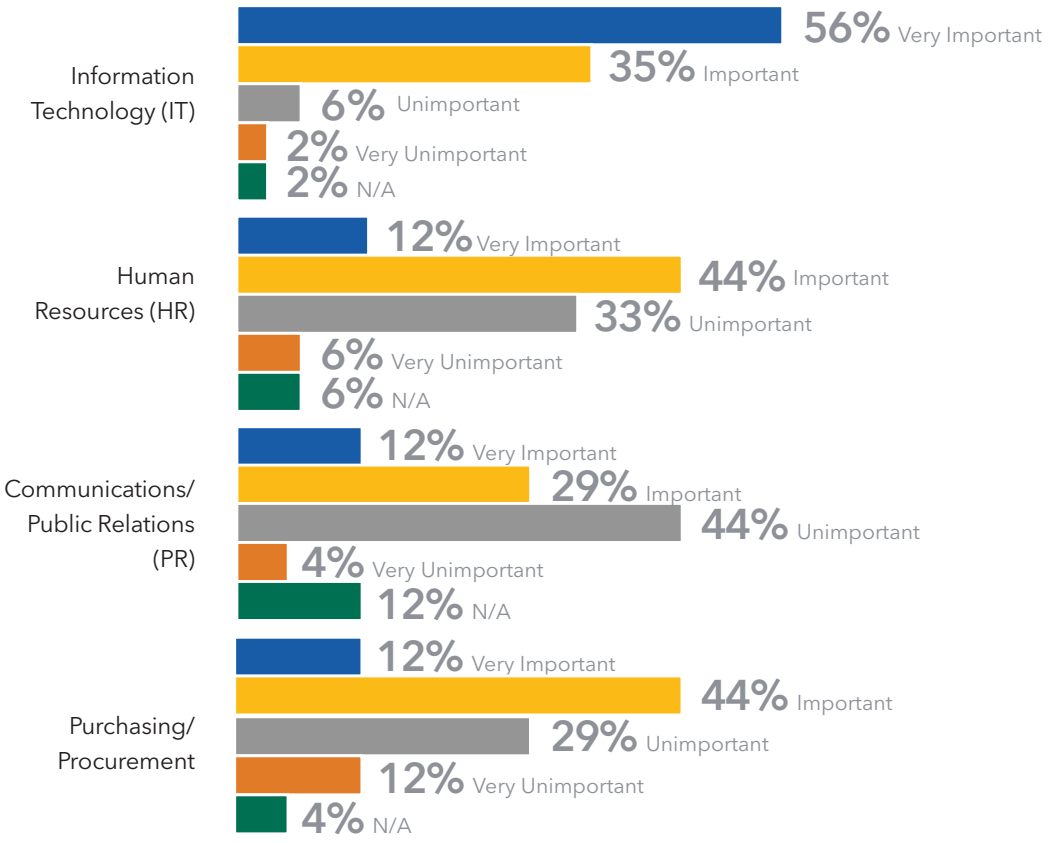


According to cyber executives, certain departments within agencies do not view cybersecurity as important to their departmental functions. To better protect agencies, each department must understand their role in cybersecurity. 39% of respondents noted that human resources departments rank cybersecurity as "unimportant" or "very unimportant." However, human resources should be a component of an agency's cybersecurity program since cyber should be embedded in the organization's culture. Integrating cyber hygiene and awareness in the traditional human resources functions of recruiting, onboarding, training and performance assessment are essential to creating a cyber-educated workforce that can reduce the threat potential. In addition, human resources must nurture the fragile cyber workforce. The White House's recent announcement of plans to appoint a federal CISO may help promote more awareness across all federal functions.

Cyber executives also believe that the purchasing/procurement department does not place enough emphasis on cybersecurity. 41% of respondents said that purchasing/procurement ranks cybersecurity as unimportant or very unimportant. Applying security during the supply chain process of procuring and acquiring information technology and services needs to be a priority. System vulnerabilities are not limited to the operating system that needs constant patching. Every vendor that has touched the system from inception to retirement, to include chip makers, application developers and cloud access security brokers (CASBs), must be assessed as part of an overall risk management process. Finally, 48% of respondents noted that communications/PR departments rank cybersecurity as "unimportant" or "very unimportant." As breaches become more common, internal and external communications departments are feeling the pressure of public reaction and loss of trust. A greater understanding of cyber risk and response will be critical to minimizing fear and increasing citizen confidence.

FIGURE 9.

How do departments in your agency rank the importance of cybersecurity?

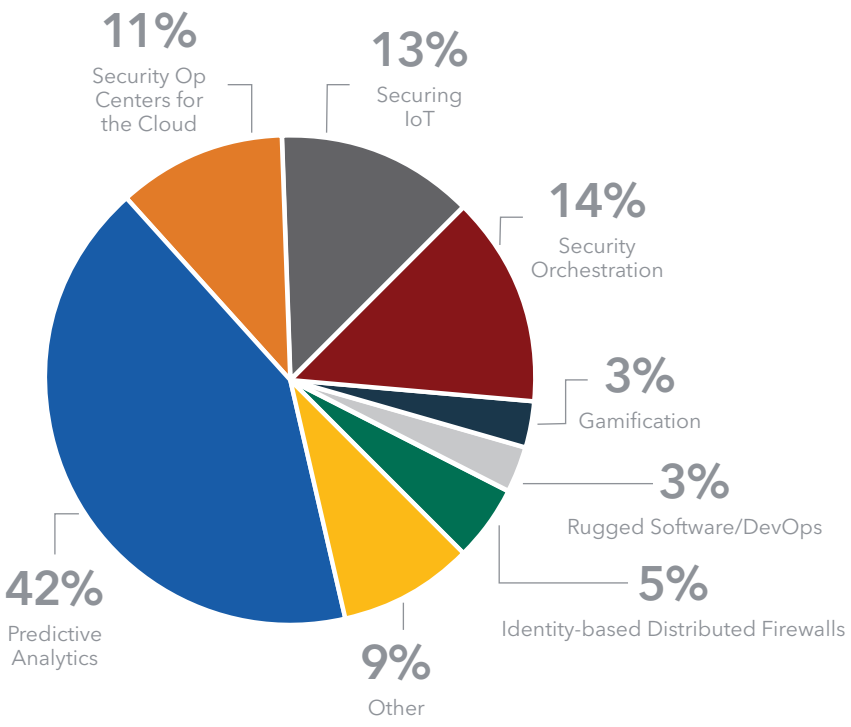


Resource and Program Management (cont.)

Often viewed as the cure, having the latest technology tools does not mean that an organization and its assets are secure. Technology is only as good as the people who design, implement, utilize, monitor and improve it. However, technology solutions continue to be developed to improve the ability to prevent, detect and respond to cyber attacks. Perhaps due to its current hype in the industry, survey respondents identified predictive analytics as the most significant tool by a wide margin. While the promise of predictive analytics is enticing, not enough implementation has taken place in order to accurately measure its effectiveness. A former federal CISO said, "Predictive analysis is a key component of being ahead of the threat and preventing malicious activity rather than cleaning up after the fact. The jury is still out, but I think the verdict is coming soon as we integrate machine data and other sources into the mix for evaluation." On the other hand, a civilian agency security director noted, "Unfortunately, while this [predictive analytics] may help, it is not a silver bullet because our adversaries work to make themselves look like routine users of the network."

FIGURE 10.

Which is the most significant game-changing security technology or solution?

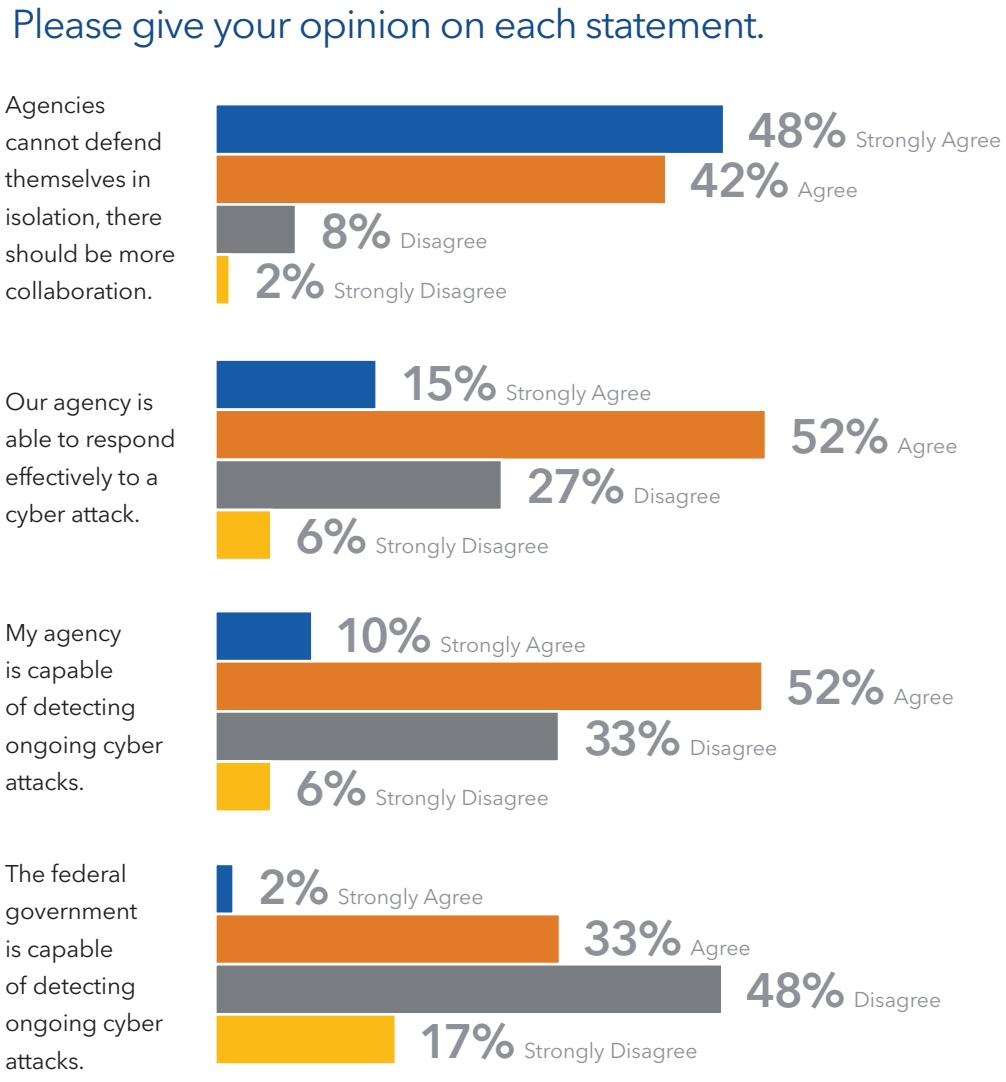


Risk Management and Resiliency

Many organizations lack proper insights, both in terms of the outside threats and in terms of what is at stake for their organizations. This is a serious impediment to proper management of the risks, as managing starts with making informed decisions. While efforts have been made to share more data between industry and government (i.e. Cybersecurity Information Sharing Act), the mantra "what gets measured, gets managed" deserves more attention. Similar to many other risk mitigation strategies, an organization should perceive cybersecurity as a continuous process and not as a one-off solution when developing a monitoring, response and recovery plan.

90% of respondents agree that agencies cannot defend themselves in isolation and believe that there should be more collaboration. However, only 67% of respondents believe their agencies can effectively respond to a cyber incident. Approximately two-thirds of the respondents believe the federal government as a whole cannot detect ongoing cyber attacks. In isolation, 62% of respondents think their agency is capable of detecting ongoing cyber attacks.

FIGURE 11.



Risk Management and Resiliency (cont.)

No agency or cyber environment is the same. In addition to collaboration and agency readiness, agencies should establish policies, processes and procedures that are tailored to their culture, environment, response personnel and, most importantly, operational objectives. In responding to an incident, the incident response plan should be concise and should evolve constantly to remain current with both external trends as well as shifts in business objectives. Only 60% of respondents surveyed believe their agency's incident response plan is effective in responding to cyber attacks, even after the OPM data breach. In order for a response plan to be effective, agencies need to put their plans into action with regular frequency, not when a real event happens.

Instead of incident response, agencies have chosen to make other actions higher priorities. Following the OPM data breach, 35% of respondents said their agency placed more emphasis on preventative measures, like role-based access, multi-factor authentication and monitoring capabilities, while 13% said they focused on defending against the insider threat with more training, security awareness and general cyber hygiene (i.e. locking computer, encrypting sensitive data, securing PIV card). 25% of respondents said their agency made no changes in response to the breach, which raises concern that cyber attacks at other agencies are not driving government-wide action. The lack of accountability may again be the problem and causing this inaction. In commercial industries, companies bolster their cybersecurity practices and policies when a competitor, supplier or business partner suffers an attack because their revenue and shareholder value can be directly affected, for which the CEO and other executives are held accountable. A civilian agency security director stated, "Accountability is not tested in any meaningful way unless there is a catastrophe."

FIGURE 12.

Do you believe your agency's incident response plan is effective in responding to cyber attacks?

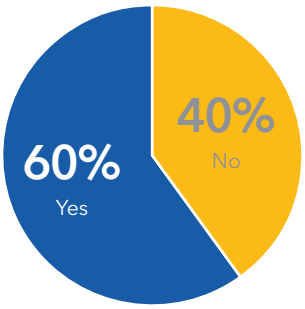
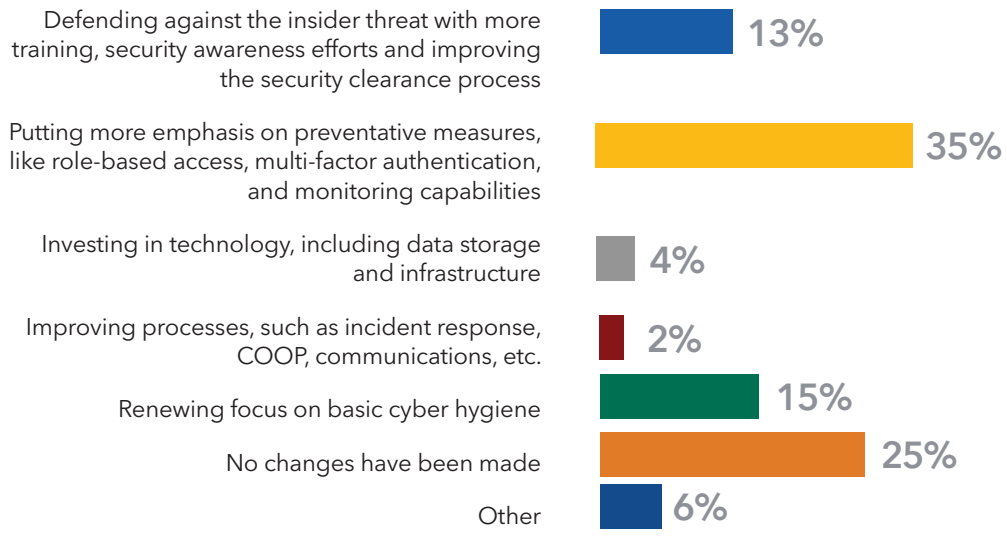


FIGURE 13.

What one thing have you prioritized as a direct result of the OPM data breach?



CONCLUSION

LIKE THE REST OF THE WORLD, FEDERAL CYBER EXECUTIVES ARE ADJUSTING to the fact that cyber attacks have become the new business reality. Each day, attackers are refining their cybersecurity knowledge, skills and tactics while federal agencies are at various stages of cyber preparedness and compliance with federal guidance and legislation.

While the OPM data breach did not directly impact other agencies, it did reveal a number of vulnerabilities common to many. Some improvements were made as a result of the OPM data breach, but most agencies have not yet hit their stride in what they see as a marathon, rather than a sprint, toward progress.

Adding to the general slow pace of government is the approaching Presidential transition and its potential impact on the drivers of cybersecurity progress – legislation, funding and senior leadership. Yet federal executives share the perspective that this is a critical time for the federal government.

> **"UNFORTUNATELY, GOVERNMENT MOVES SLOWLY AND THE ADVERSARY DOES NOT."**
>
> – SECURITY DIRECTOR, CIVILIAN AGENCY

To that end, several encouraging developments are underway – the upcoming appointment of a federal CISO, who can hopefully bridge the gaps between agencies, as well as assume and assign responsibility, and recent budget proposals by the White House that reinforce the federal government's awareness of and commitment to improving the federal government's cybersecurity capabilities.

Based on the survey results, the following recommendations are being made in order to advance the government's cybersecurity progress:

- **More technology is no longer the sole solution** – effectively dealing with cybercrime requires that we place more focus on the human perspective and implement a more balanced and holistic approach as it relates to the people+process+technology equation.
- We must **address the dissatisfaction among the federal cyber executive ranks** and empower them with more authority to make risk-based decisions and, above all, improve the cyber culture within their respective agencies. This will enable **collaboration across all levels and departments within an agency**.
- Advancing an organization's security agenda no longer rests upon educating its cyber workforce, rather **it must educate its entire workforce, across all departments, in cyber**.
- The government's approach to increasing awareness and **vigilance across an agency must include regular and continuous cyber hygiene trainings and simulation drills**, rather than annual awareness seminars with ineffective PowerPoint presentations.
- **Resources must be dedicated to retaining existing cyber talent.** Given the multiple factors working against the government's efforts to build a skilled workforce, existing cyber professionals must be nurtured and rewarded with training and continuing education opportunities.
- As expanding compliance requirements do not allow for enough customization, **the NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond and Recover) are resonating with cybersecurity leaders** and should be further reinforced as the government's baseline for security assessment.

An (ISC)² Report

The State of Cybersecurity from the Federal Cyber Executive Perspective

METHODOLOGY

This report is based on a survey of 54 cyber executives who identified themselves as U.S. federal senior managers or contractors with cybersecurity responsibility in government. The online survey request was distributed to personnel from defense, civilian and intelligence agencies and government contractors and consultants. Results shown in percentages have been rounded and may not total to 100 percent.

ACKNOWLEDGMENTS

(ISC)² and KPMG LLP would like to thank the federal cyber executives for participating in this survey and providing their invaluable insights.

We would like to acknowledge the (ISC)² U.S. Government Advisory Council (USGAC) members for their oversight and guidance in determining the prioritization of the issues addressed in this survey and for the Council's continuing effort to advance the U.S. government cybersecurity workforce.

Finally, (ISC)² would like to thank our research sponsor, KPMG LLP.

CONTACT INFORMATION

Dan Waddell, CISSP, CAP, PMP
(ISC)² Managing Director, North America
Director of U.S. Government Affairs
571-303-1317
dwaddell@isc2.org

Tony Hubbard
Principal and Cyber Leader, Federal Advisory, KPMG LLP
703-286-8320
thubbard@kpmg.com