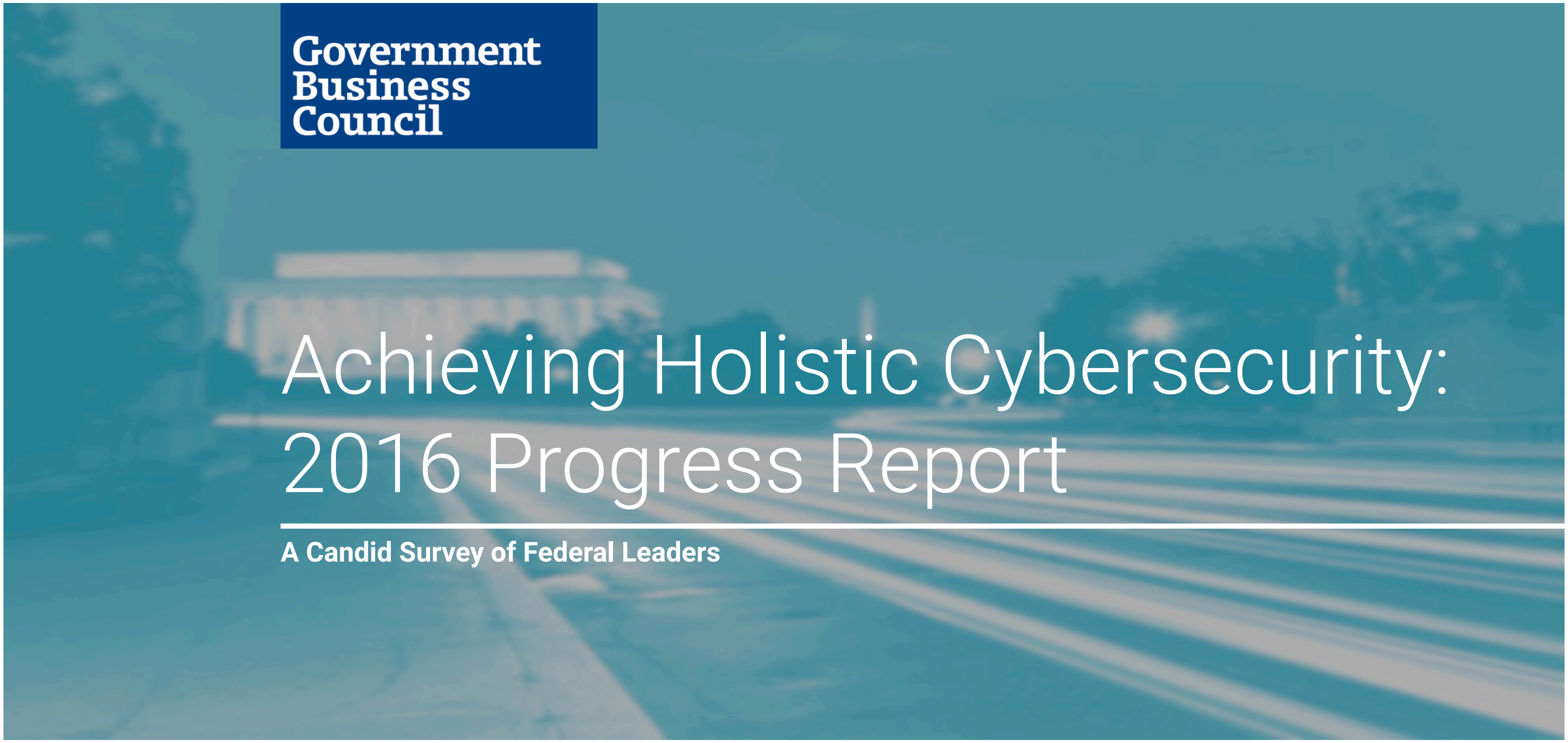


Government Business Council

Achieving Holistic Cybersecurity: 2016 Progress Report

A Candid Survey of Federal Leaders

Underwritten by

DELL Security

April 2016

Table of Contents

Overview

—

Purpose

The past few years have seen an explosion of cyber attacks, and with the 2015 Office of Personnel Management (OPM) breaches underscoring the vulnerability of government data, agencies are racing to implement proactive, holistic cybersecurity measures. In order to learn more about the current state of agency cybersecurity, Government Business Council (GBC) and Dell Security undertook an in-depth research study. This survey is a follow-up to a previous June 2014 GBC study and serves to measure changing perceptions and experiences of federal leaders regarding the present threat landscape.

—

Methodology

Government Business Council and Dell Security released a survey on February 23, 2016 to a random sample of *Government Executive, Nextgov,* and *Defense One* print and online subscribers. 464 senior-level federal employees completed the survey, including those at the GS/GM 11 to 15 grade levels and members of the Senior Executive Service. 54% of respondents are GS/GM 13 and above, and all are familiar with cybersecurity. Respondents include representatives from over 30 federal agencies, including both defense and civilian agencies.

To view a full demographic detail, methodology, and findings of the previous June 2014 survey, please click here.

“Cyber threats cannot be eliminated entirely, but they can be managed much more effectively. And we can best do this by aligning and focusing our efforts, by properly funding necessary cyber investments, by building strong partnerships across government and industry, and by drawing on the best ideas and talent from across the country to tackle this quintessential problem of the 21st century.”

Federal CIO Tony Scott

“Strengthening & Enhancing Cybersecurity for the 21st Century,” July 2015.

Executive Summary

—

Federal leaders are significantly less confident in agency cybersecurity than they were two years ago

In 2014, a substantial majority of respondents felt that their agency's defensive measures were capable of successfully combating cyber threats. Confidence has since decreased dramatically – just 35% of respondents in 2016 are confident or very confident in their agency's ability to protect information systems. Fewer than 1 in 3 feel confident in their agency's ability to protect employees' personal information or keep up with evolving cyber threats.

—

Workforce hygiene continues to be an overarching point of concern when it comes to top cyber threats

Respondents identified email embedded with malware and phishing/spear phishing as top cyber threats – both targeting workforce cyber literacy and awareness. Moreover, they most commonly identify cybersecurity personnel and workforce education as cyber defense elements in need of significant improvement, indicating major gaps in the organizational side of agency cybersecurity more so than in technical/structural security.

—

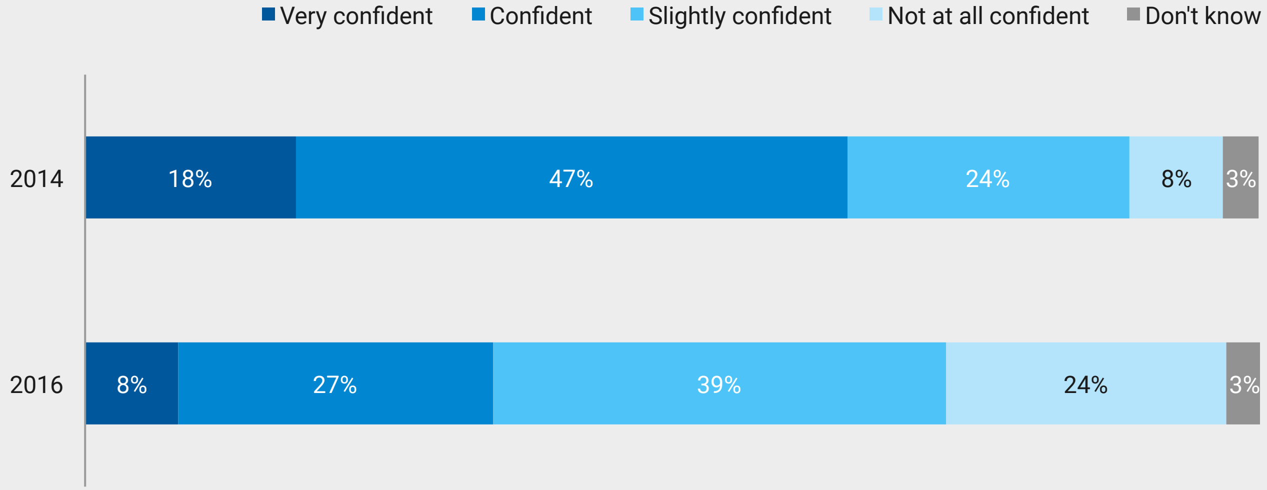
Agencies face a range of challenges in bolstering cyber defenses

While respondents remain largely confident in the security of networked physical devices and information systems, they still express greater uncertainty toward organizational capabilities than they did two years ago. Furthermore, agencies have yet to make meaningful progress in leveraging the Internet of Things (IoT) or in implementing IoT cybersecurity. Budget constraints, procurement delays, and bureaucratic inertia are most commonly identified as obstacles to more comprehensive defense measures, suggesting that organizational barriers present a greater challenge than technical issues with regard to agency cybersecurity enhancement.

Confidence in Federal Cybersecurity

Federal employees have lost confidence in overall agency information security

How confident are you in the ability of your department/agency to protect information systems from cyber intrusions?



Percentage of respondents, n=424 and 461, respectively
Note: Percentages may not add up to 100% due to rounding

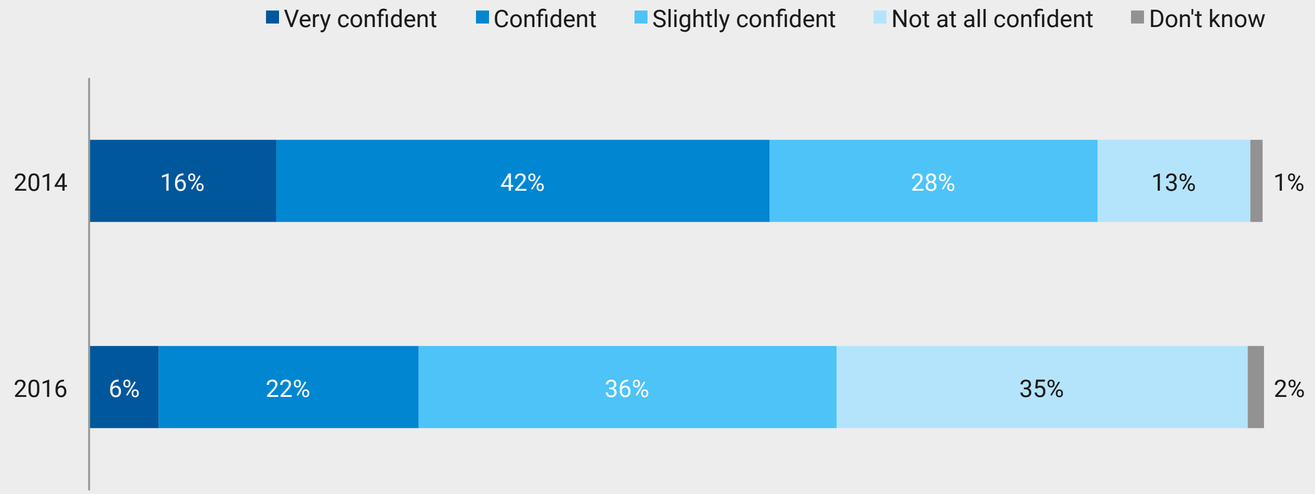
Federal leaders are significantly less optimistic about their department/agency's overall information security capabilities than they were two years ago – while 65% of 2014 respondents were confident or very confident in their department/agency's ability to protect information systems from cyber intrusions, only 35% of respondents currently express the same degree of confidence.

30-pt. drop

in respondents indicating that they are confident or very confident in agency information security.

Respondents are less confident in the security of their personal information / Confidence in Federal Cybersecurity

How confident are you in your department/agency’s ability to protect your personal information?



Percentage of respondents, n=424 and 464, respectively
Note: Percentages may not add up to 100% due to rounding

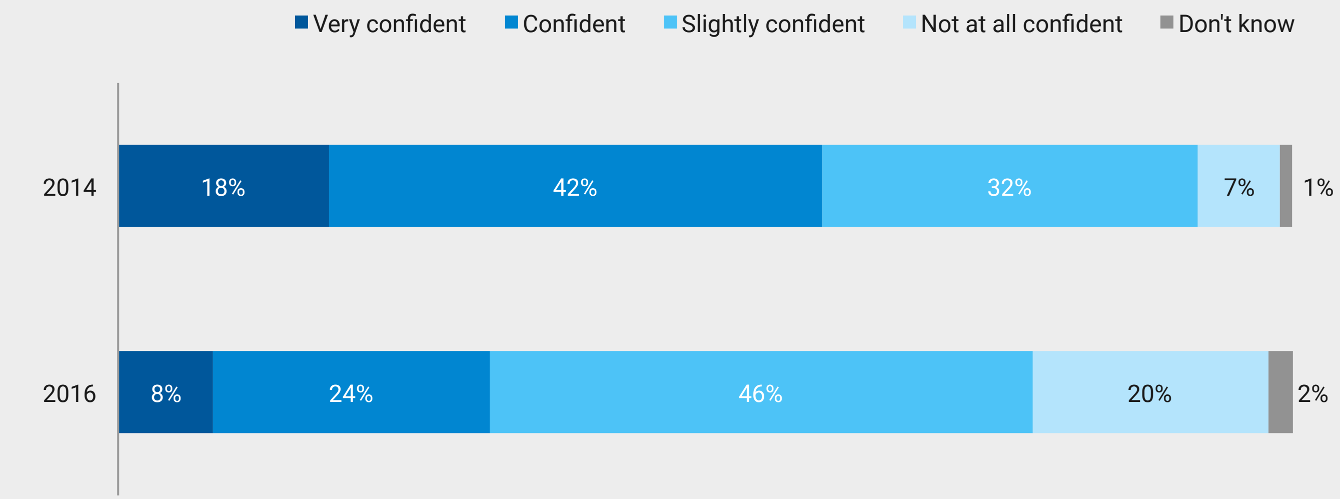
Lack of confidence in organizational cyber defenses extends to personal information security. Only 28% of federal leaders are confident or very confident in their agency/department’s ability to safeguard their personal information, compared to 58% two years ago.

30-pt. drop

in respondents indicating that they are confident or very confident in personal information security.

Respondents are unsure of their organization’s ability to keep pace with evolving cyber threats / Confidence in Federal Cybersecurity

How confident are you in your department/agency’s ability to keep up with evolving cyber threats?



Percentage of respondents, n=424 and 433, respectively
Note: Percentages may not add up to 100% due to rounding

Fewer than 1 in 3 respondents are confident or very confident in their agency/department’s ability to keep up with evolving cyber threats – a marked decrease from the 60% confidence level in 2014.

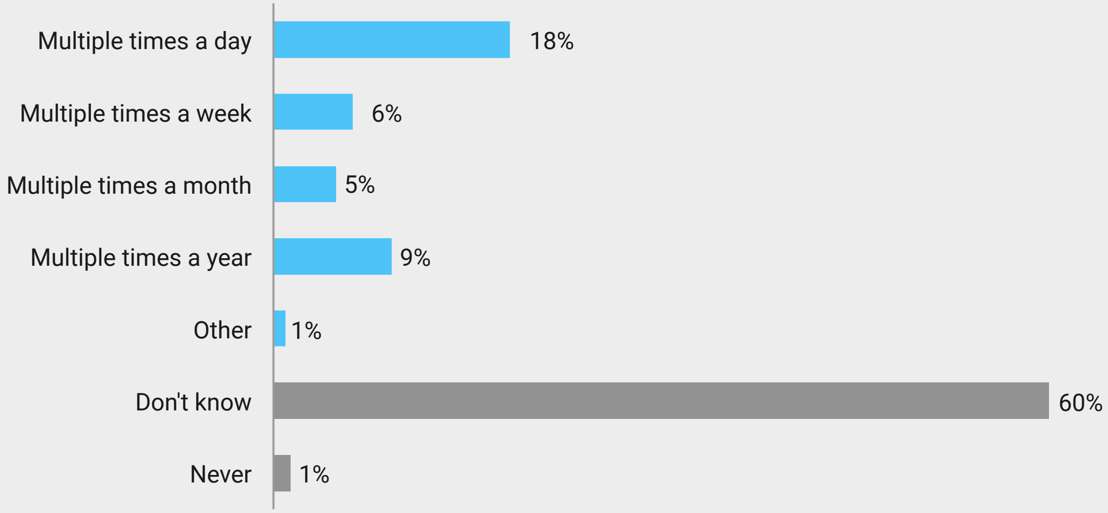
28-pt. drop

in respondents indicating that they are confident or very confident in their agency’s ability to keep up with evolving cyber threats.

Breaking Down the Cyber Threat

Federal employees are largely uncertain of the current cyber threat landscape

To your knowledge, how often is your department/agency the target of a cyber intrusion?



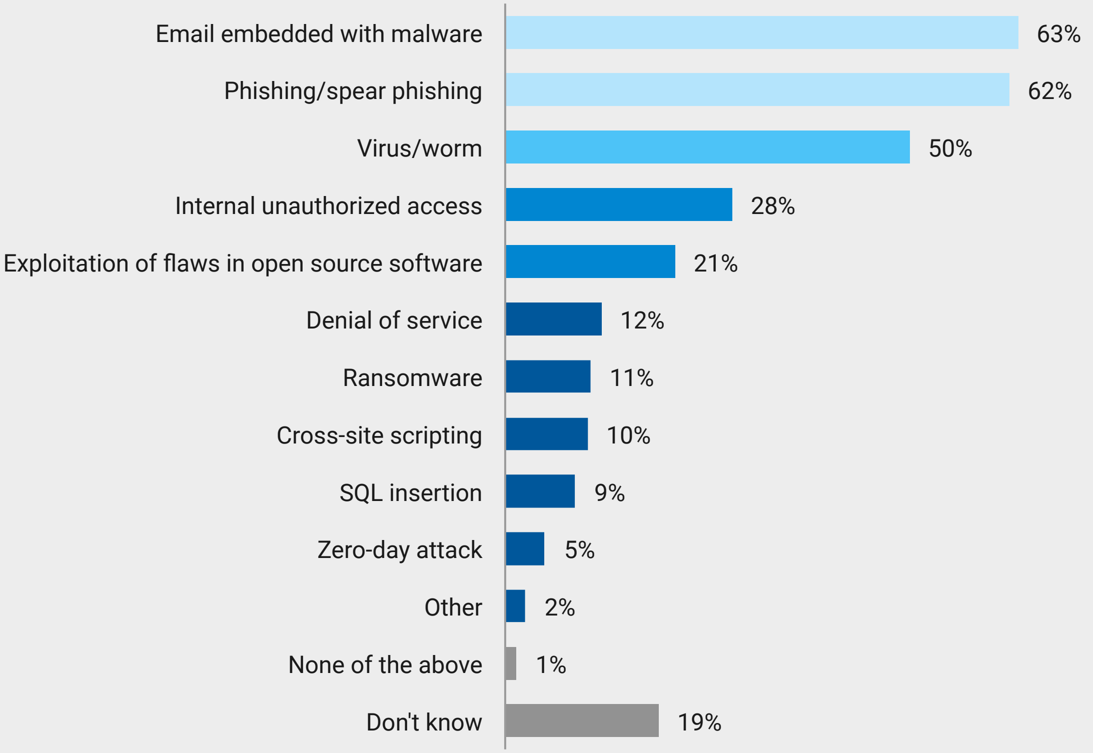
Percentage of respondents, n=462
Note: Percentages may not add up to 100% due to rounding

38% of federal employees indicate that their organization is targeted by cyber intrusions at least a few times a year. However, a majority of respondents (60%) do not know how often their agencies are targeted – a major increase from 20% of respondents in 2014. This surge suggests that federal employees are significantly less certain about the present-day threat landscape – perhaps in the wake of recent high-profile attacks such as the 2015 OPM breaches.

6 in 10

respondents aren’t aware of often their department/agency is the target of a cyber intrusion.

Significant Cyber Threats



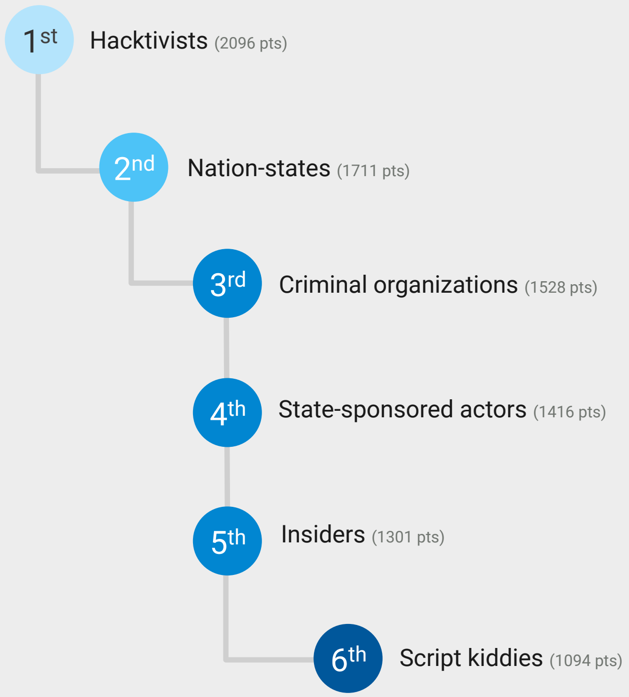
Percentage of respondents, n=457
Respondents were asked to select all that apply

When asked about significant cyber threats to their department/agency, respondents most commonly identify email embedded with malware (63%) and phishing/spear phishing (62%) – selections that are largely aligned with 2014 top identified threats. All stem from human interaction, suggesting that insider threats may constitute the most pressing risk to agency cybersecurity. Respondents also highlight ransomware (11%) – a new answer choice in the 2016 study – as an emerging threat.

Hacktivists are identified as the greatest source of cyber threats / Breaking Down the Cyber Threat

Greatest Cyber Threat Sources

Ranked by respondents in order of threat severity



1st Hacktivists (2096 pts)

2nd Nation-states (1711 pts)

3rd Criminal organizations (1528 pts)

4th State-sponsored actors (1416 pts)

5th Insiders (1301 pts)

6th Script kiddies (1094 pts)

Ranked by Borda count, n=437

When asked to rank cyber threat sources based on the severity of the threat they pose to agencies, most federal employees select hacktivists as the top threat source, followed by nation-states and criminal organizations. Interestingly, insiders are ranked second to last despite being the source of top respondent-identified cyber threats.

Respondents were asked: “Please rank the following sources of cyber threats based on the severity of the threat you believe they pose to your department/agency.”

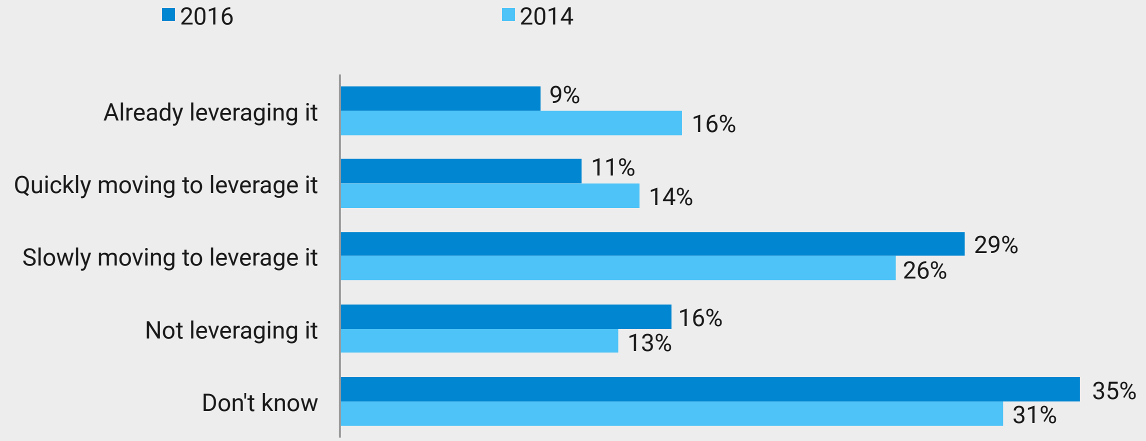
Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. Each respondent’s top answer choice receives the maximum score of n points for that respondent, where n is equal to the total number of options. Each subsequent choice receives 1 less point than the one ranked ahead of it. Unranked answer choices receive zero points. Please see Appendix for further detail.

The Internet of Things

Agencies are still in the early stages of leveraging the Internet of Things

Technology experts have identified the "Internet of Things" (IoT) as a quickly growing IT phenomenon. The term refers to the network of physical devices and systems (e.g., consumer electronics, smart appliances, vehicles, energy grids) capable of collecting, processing, and exchanging data automatically via the Internet.

Which of the following best describes the extent to which your department/agency is leveraging the "Internet of Things"?



Percentage of respondents, n=425 and 424, respectively
Note: Percentages may not add up to 100% due to rounding

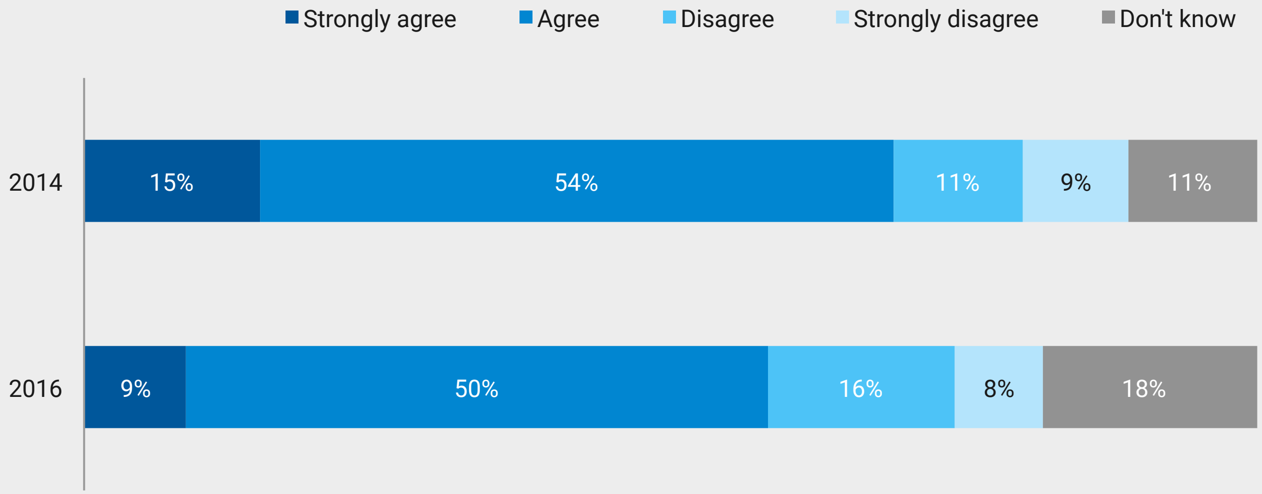
While the IoT has the potential to unlock greater agency effectiveness, agencies have yet to make strides in employing it. Only 20% say that their agency is leveraging or quickly moving to leverage it – a decrease from the 30% of 2014. Defense agencies are also capitalizing on the IoT to a greater extent than other non-defense civilian agencies – 29% of defense respondents say that their agency is leveraging or quickly moving to leverage the IoT, while only 19% of non-defense civilian employees indicate the same.

20%

of respondents feel that their agency is leveraging or quickly moving to leverage the IoT.

Respondents remain largely confident in the security of existing networked physical devices / The Internet of Things

To what extent do you disagree or agree with the following statement: “My department/agency is able to secure its networked physical devices and systems.”



Percentage of respondents, n=424 and 427, respectively
Note: Percentages may not add up to 100% due to rounding

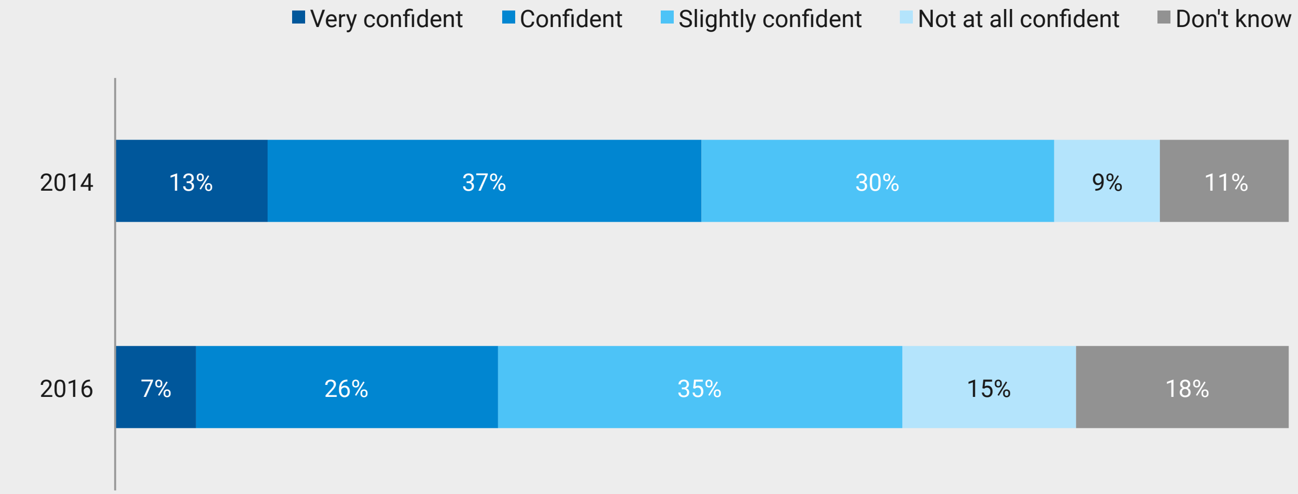
In spite of the potential security risks attached to the IoT, a majority of respondents (59%) agree or strongly agree that their agency is able to secure its networked physical devices and systems. However, this is still a 10-point decrease from the 69% confidence level of respondents in 2014.

10-pt. drop

in respondents who agree or strongly agree that their agency’s networked physical devices/systems are secure.

Respondents are less confident in agency supply chain security / The Internet of Things

How confident are you in the ability of your department/agency to validate the security of its IT supply chain?



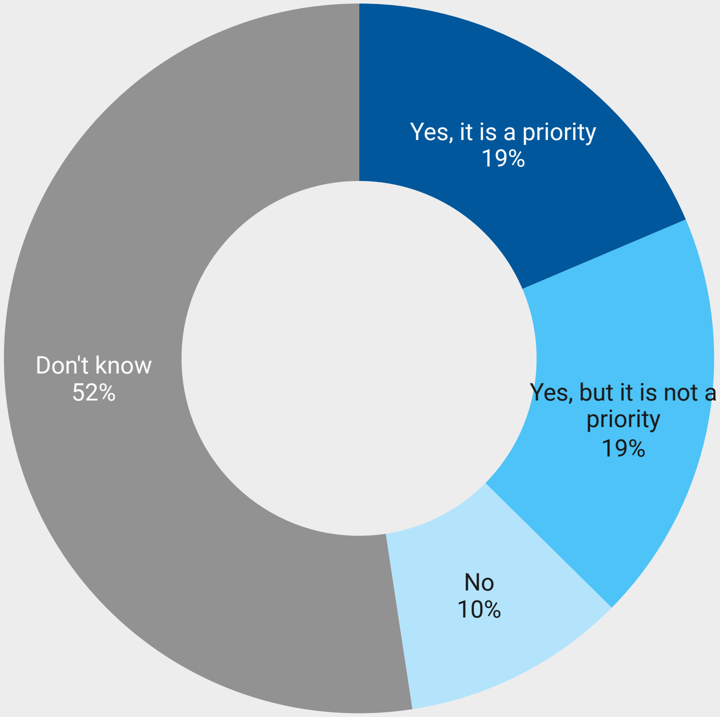
Percentage of respondents, n=424 and 420, respectively
Note: Percentages may not add up to 100% due to rounding

While 50% of 2014 respondents were confident or very confident in the security of their agency's IT supply chain, only 33% of respondents currently express the same degree of confidence. Meanwhile, 50% are just slightly or not at all confident, representing a sizeable level of concern.

17-pt. drop in respondents who are confident or very confident in their agency's ability to secure its IT supply chain.

Adapting cybersecurity strategy to the Internet of Things is not yet an agency priority / The Internet of Things

To your knowledge, is your department/agency adapting its cybersecurity strategy to accommodate the "Internet of Things"?



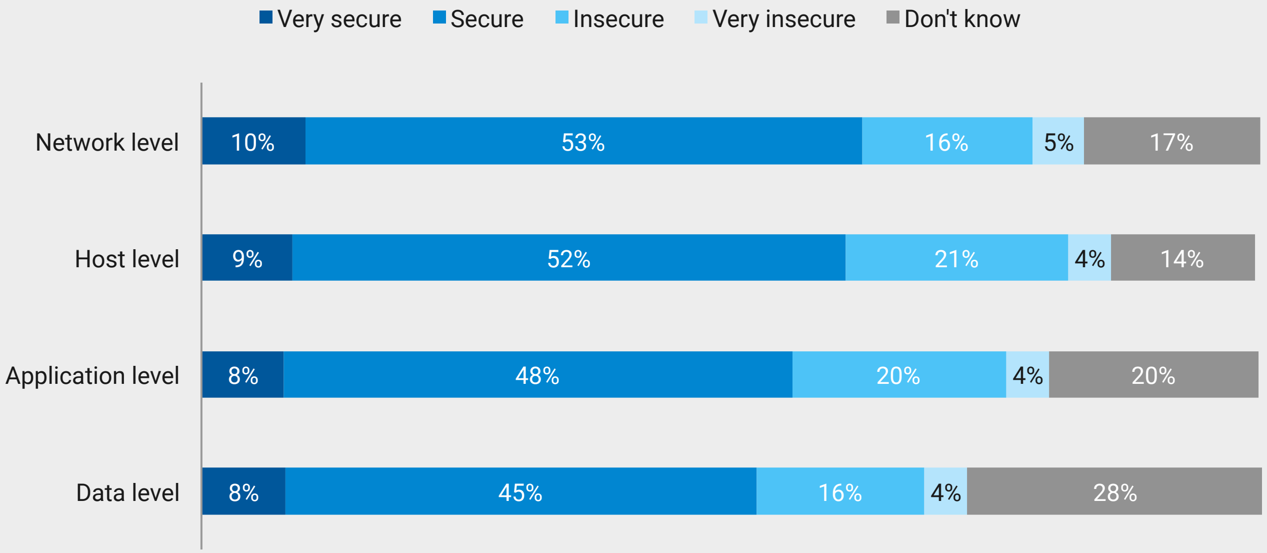
Percentage of all respondents, n=420
Note: Percentages may not add up to 100% due to rounding

Only 38% of federal employees indicate that their agency is implementing IoT cybersecurity – a slight decrease from two years ago. Meanwhile, over half of respondents do not know where their agency stands in adapting cybersecurity to the IoT, suggesting that it is not yet a prominent organizational priority.

Current State of Cyber Defenses

Despite a drop in confidence, respondents still feel that agency information systems layers are secure

To what extent do you believe the following layers of your department/agency's information systems are secure?



Percentage of respondents, n=410
Note: Percentages may not add up to 100% due to rounding

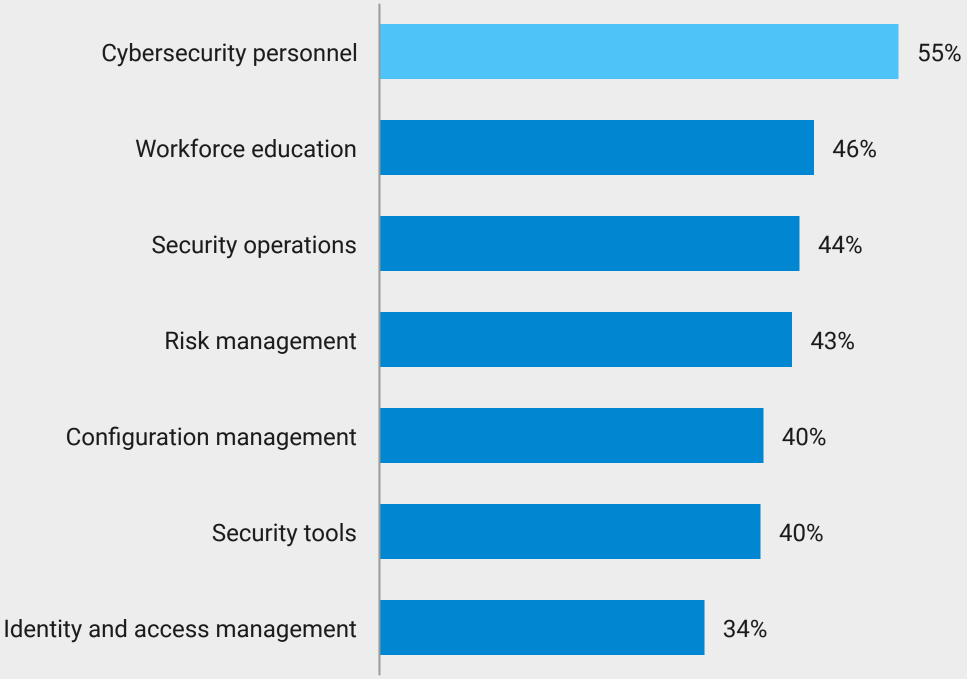
A majority of respondents feel that the network (63%), host (61%), application (56%), and data (53%) layers of agency information systems are secure or very secure. However, this is a marked decrease from 2014, which saw a much larger percentages expressing confidence in network (83%), host (77%), application (72%) and data (72%) security.

16-pt. drop

at least in respondents who feel that the layers of their agency's information systems are secure or very secure.

Federal leaders indicate greatest cyber gaps are workforce-related / Current State of Cyber Defenses

Cyber Defense Elements in Need of Significant Improvement

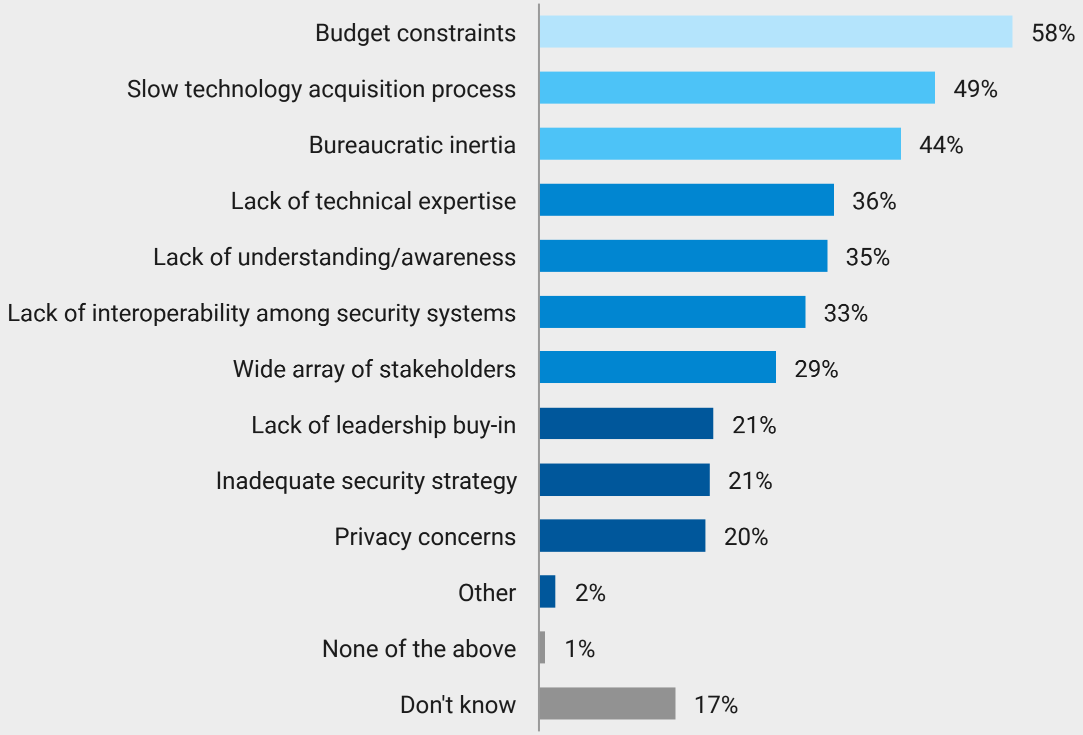


Percentage of respondents, n=390
Respondents were asked to select all that apply

Both 2014 and 2016 survey respondents identified workforce education as one of the top cyber defense elements in need of substantial improvement.

Bureaucratic obstacles continue to present the greatest impediment to enhanced cybersecurity / Current State of Cyber Defenses

Obstacles to Holistic Cybersecurity



Percentage of respondents, n=402
Respondents were asked to select all that apply

When asked about obstacles to a more comprehensive cybersecurity posture, respondents from both 2014 and 2016 tended to identify systemic challenges such as budget constraints, inefficient procurement, and bureaucratic inertia rather than technical barriers.

58%

of respondents cite budget constraints as a barrier to more holistic agency cybersecurity.

Final Considerations

When seeking to achieve a more comprehensive cybersecurity posture:

—

Focus on mitigating both human and technical risks

Federal leaders consistently point to the human element of cyber risks. When it comes to top cyber threats, respondents most commonly identify malware-embedded emails, phishing, and internal unauthorized access as top concerns; in other words, methods that often target agency employees rather than technical or structural vulnerabilities. Furthermore, most respondents believe that agencies should prioritize recruiting cybersecurity personnel and improving workforce cyber literacy. To address these vulnerabilities, organizations might consider enhancing defensive measures to prevent and mitigate insider threats.

—

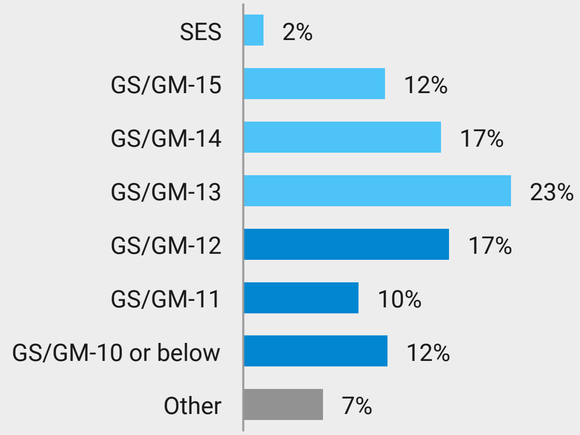
Address the systemic obstacles hindering the implementation of more robust defensive measures

Cyber breaches are an increasingly salient threat to agency information security. However, the federal government appears to still be in the beginning stages of constructing more robust cybersecurity strategies, and respondents cite budget constraints, slow technology acquisition processes, and bureaucratic inertia as the chief barriers to a more holistic agency cybersecurity posture. Moving forward, agencies need to focus on tackling institutional obstacles in order to move forward with bolstering organizational cybersecurity.

Respondent Profile

Survey respondents are largely senior federal leaders

Job grade



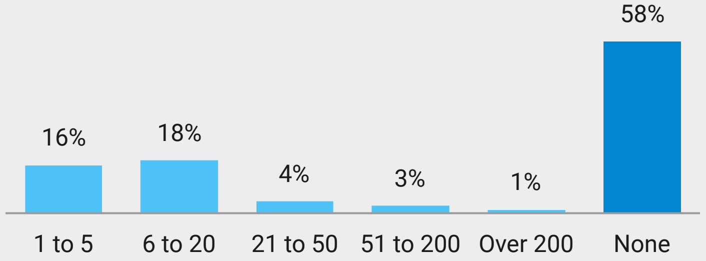
Percentage of respondents, n=404
Note: Percentages may not add up to 100% due to rounding

54%

of respondents rank GS/GM-13 or above, including members of the Senior Executive Service (SES).

"Other" includes those employed under other pay scales or ranking systems (e.g., Military, Foreign Service, Federal Wage System, Executive Schedule, etc.)

Reports/oversees



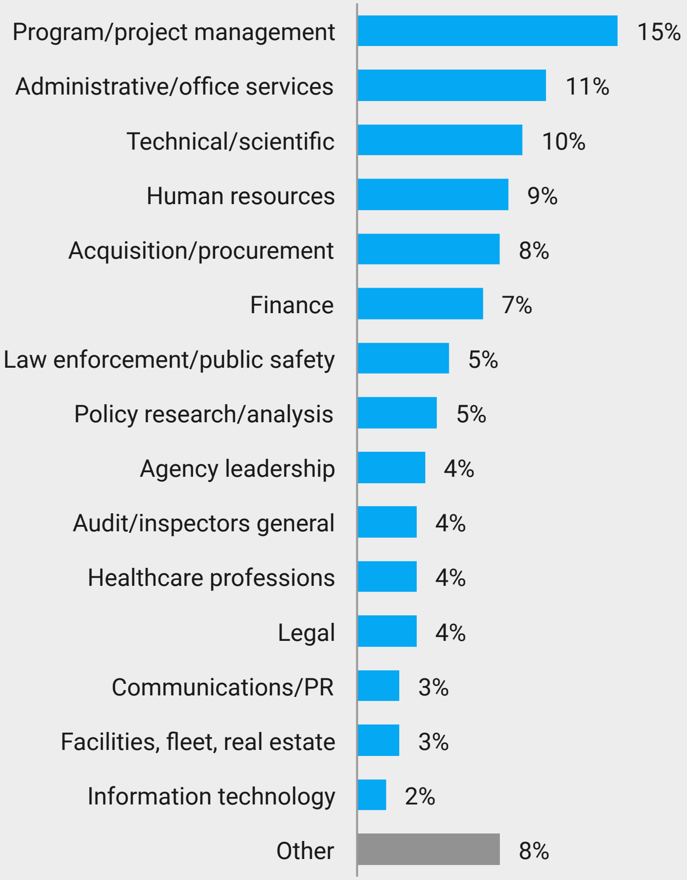
Percentage of respondents, n=404
Note: Percentages may not add up to 100% due to rounding

42%

of respondents are supervisors who oversee at least one employee, either directly or through direct reports.

Respondents represent a wide range of federal agencies and job functions / Respondent Profile

Job function



Percentage of respondents, n=404
Note: Percentages may not add up to 100% due to rounding

Departments and agencies represented

Treasury

Agriculture

Homeland Security

Veterans Affairs

Transportation

Air Force

Interior

Health and Human Services

Justice

Army

Social Security Administration

Navy

Office of the Secretary of Defense

Commerce

Labor

Energy

Small Business Administration

Environmental Protection Agency

General Services Administration

National Aeronautics and Space Administration

Government Accountability Office

Housing and Urban Development

Education

State

Congress/Legislative Branch

Agency for International Development

National Science Foundation

Combatant Commands

Joint Chiefs of Staff

Nuclear Regulatory Commission

Office of Personnel Management

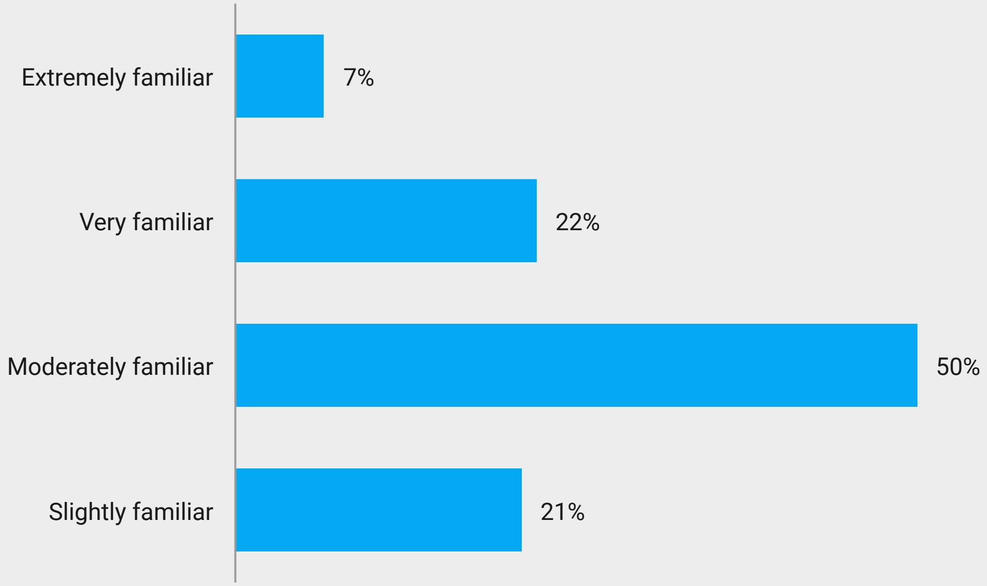
Other Independent Agencies

Respondents were asked to choose which single response best describes their primary job function.

Departments and agencies are listed in order of frequency.

Respondents are familiar with cybersecurity / Respondent Profile

Familiarity with cybersecurity



Percentage of respondents, n=464
Note: Percentages may not add up to 100% due to rounding

Respondents were asked to rate their familiarity with cybersecurity.

Appendix

Please rank the following sources of cyber threats based on the severity of the threat you believe they pose to your department/agency.

	Count per rank						**Total**	**Borda count**
	1	**2**	**3**	**4**	**5**	**6**		
Hacktivists	198	77	77	54	22	9	437	2096
Nation-states	90	93	90	70	45	46	434	1711
Criminal organizations	44	85	89	98	71	47	434	1528
State-sponsored actors	50	73	56	81	110	64	434	1416
Insiders	47	56	55	78	86	113	435	1301
Script kiddies	8	52	68	53	100	155	436	1094
Number of respondents	**437**	436	435	434	434	434	-	-

Ranked by Borda count, n=437

Rankings and total scores are displayed here using the Borda count method, where each answer choice earns points based on the order in which respondents placed them. Each respondent's top answer choice receives the maximum score of n points for that respondent, where n is equal to the total number of options. Each subsequent choice receives 1 less point than the one ranked ahead of it. Unranked answer choices receive zero points.

For instance, if a respondent's ranked choices were 1) hacktivists, 2) criminal organizations, and 3) insiders, those responses would receive 6,5, and 4 points respectively. These points would be added to Borda count of each answer choice.

With 437 respondents and 6 choices, the maximum score possible for any single answer choice (i.e., if every respondent ranked it as their top outcome) is equal to 2622 points (437 x 6).

About

Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight and analytical independence. As an extension of *Government Executive*'s 40 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Report Author: Rina Li

Contact

Mark Lee
Manager, Research & Strategic Insights
Government Executive Media Group
Tel: 202.266.7574
Email: mlee@govexec.com

govexec.com/insights
@GovExecInsights

Dell Security

Dell Security solutions help you create and maintain a strong foundation with interconnected solutions that span your agency. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can meet your mission. http://software.dell.com/govern-protect/.