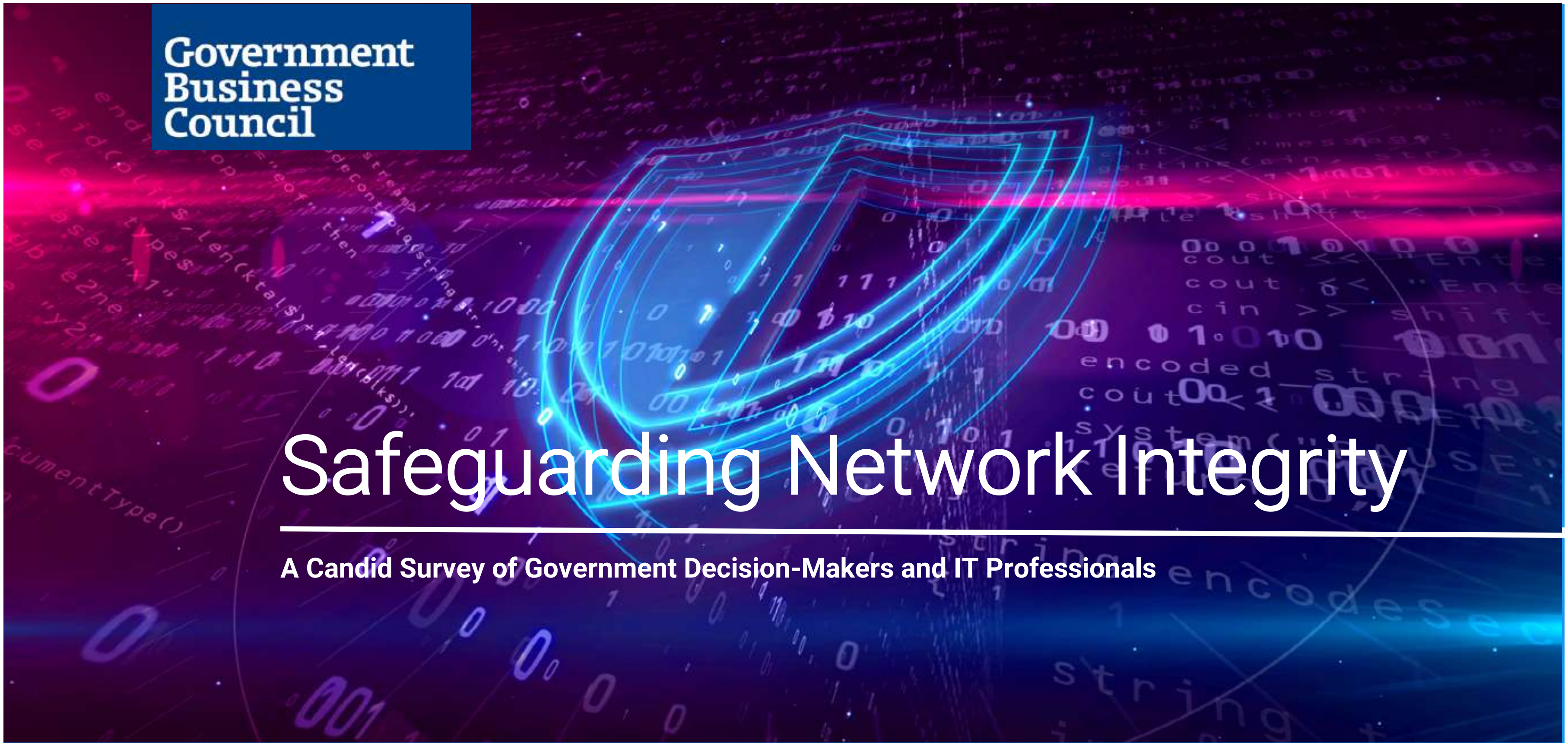


Government Business Council

Safeguarding Network Integrity

A Candid Survey of Government Decision-Makers and IT Professionals

Underwritten by

leidos

May 2020

Table of Contents

—

Overview / 3

—

Executive Summary / 4

—

Research Findings / 5

—

Final Considerations / 25

—

Respondent Profile / 26

—

About / 29

Overview

Purpose

With the global data revolution, cybersecurity has quickly percolated up to among the top priorities of government agencies, requiring them to adapt and employ security strategies. Unanticipated events, such as COVID-19, however, have cast organizations into unchartered territories, energizing cybercriminals to amplify attacks. Government Business Council (GBC) is interested in how agencies are responding. To better understand the current state of cybersecurity in the federal government, GBC conducted an in-depth research study of federal government and defense employees.

Methodology

In April and May of 2020, GBC issued a survey on cybersecurity to the federal government. 358 employees responded, including 57% of respondents identifying as GS/GM-13 or above and 44% of respondents who are involved in their agency's IT. Nearly half of respondents are senior managers.

For more information on respondents, please see the Respondent Profile.

Executive Summary

Federal employees highly value cybersecurity

Respondents value the protection of their agency's networks and systems. In fact, 84% of federal employees think that cybersecurity is vital to ensuring the continuity of agency functions, positioning it among the top priorities for organizations. At least 3 out of every 5 respondents believe that cybersecurity has a high or very high ranking compared to other competing agency priorities.

COVID-19 has escalated cybersecurity demands

Hackers find immense value in the augmented data growth occurring in government agencies and their interest has not gone unnoticed. 73% of federal employee respondents forecast that cybersecurity will be a higher or much higher priority in the future than it is now. Today's situation with COVID-19 multiplies the threat from cybercriminals. 67% of respondents agree that the current pandemic will increase the likelihood of cyber attacks, requiring swift action from agencies to protect their workforce.

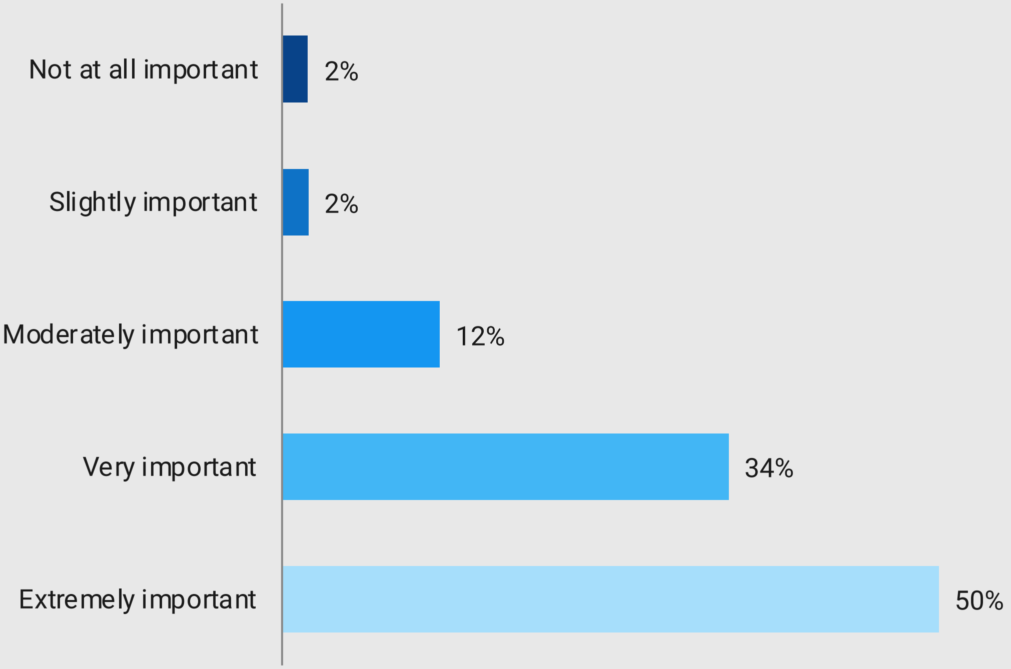
Respondents exemplify the need for cybersecurity reinforcements

Respondents share uncertainty that their agency's cybersecurity controls are sufficient in preventing and combating the existential threat of cyber attacks. 64% of respondents are less than very confident in their agency's ability to successfully address advanced cybersecurity threats. Moreover, 72% of respondents think that their agency's IT department has a less than very good visibility over critical data, suggesting that cybersecurity excellence has yet to be attained.

Research Findings

Cybersecurity is important to respondents' work in the government

How important is cybersecurity in protecting the continuity of your agency's functions?



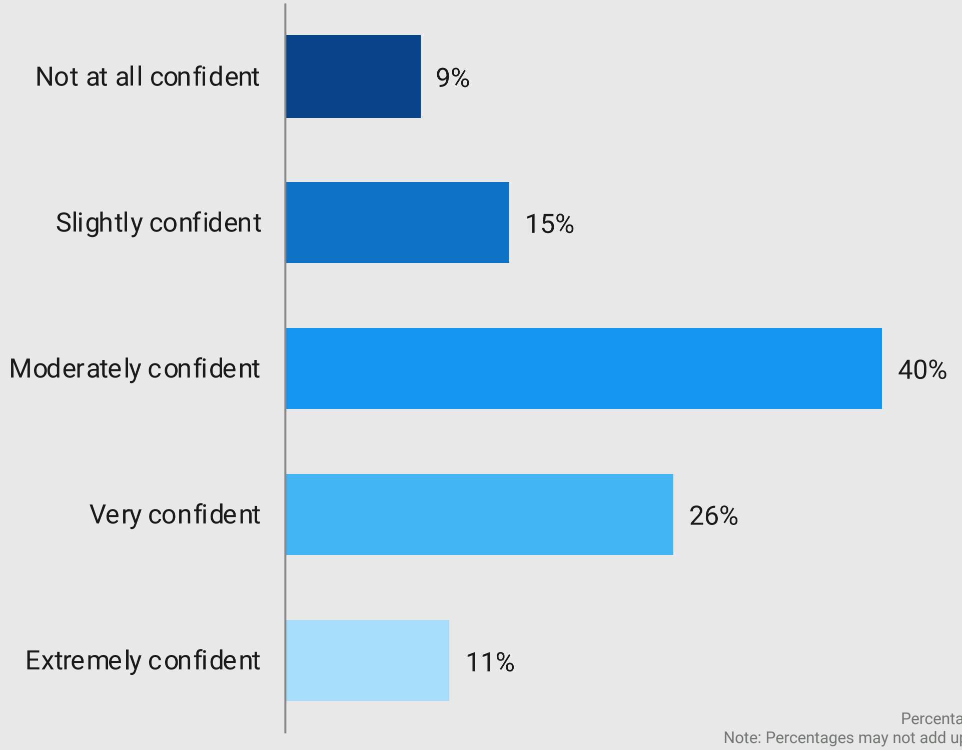
Percentage of respondents, n=334
Note Respondents were asked to select all that apply.

84%

of respondents think that cybersecurity is vital in ensuring the continuity of agency functions.

Federal agencies could build substantially more cybersecurity confidence in their employees

How confident are you in your agency's ability to fend off advanced cybersecurity threats?



Percentage of respondents, n=356
Note: Percentages may not add up to 100% due to rounding

64%

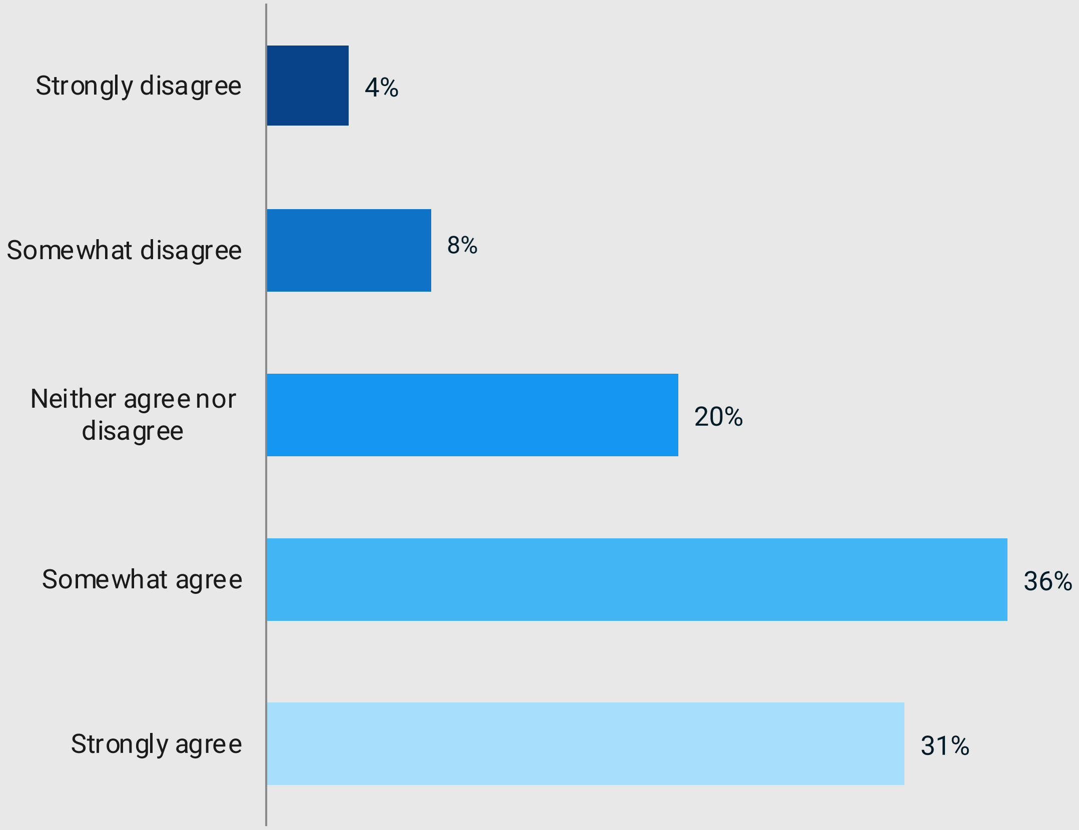
of respondents are less than very confident in their agency’s strength in cybersecurity. DoD and federal civilians share similar sentiments in their agencies’ abilities to fend off advanced cybersecurity threats.

> “
>
> The U.S. government is currently not designed to act with the speed and agility necessary to defend the country in cyberspace….We must get faster and smarter, improving the government’s ability to organize concurrent, continuous and collaborative efforts to build resilience, respond to cyber threats, and preserve military options that signal a capability and willingness to impose costs on adversaries.

Cyberspace Solarium Commission, March 2020

Most respondents believe that disruptive events, such as COVD-19, can increase breaches in their agencies

To what extent do you agree or disagree that major societal disruptions (e.g. COVID-19) increase the likelihood of cybersecurity attacks on your agency?



Percentage of respondents, n=289
Note: Percentages may not add up to 100% due to rounding

Did you know?

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Department of Homeland Security (DHS) released an alert in April 2020 warning of an uptick of cyberthreats during the pandemic.

Cybercriminals are leveraging the telework environment to prey on vulnerable endpoints using tactics such as phishing and malware distribution.

500%

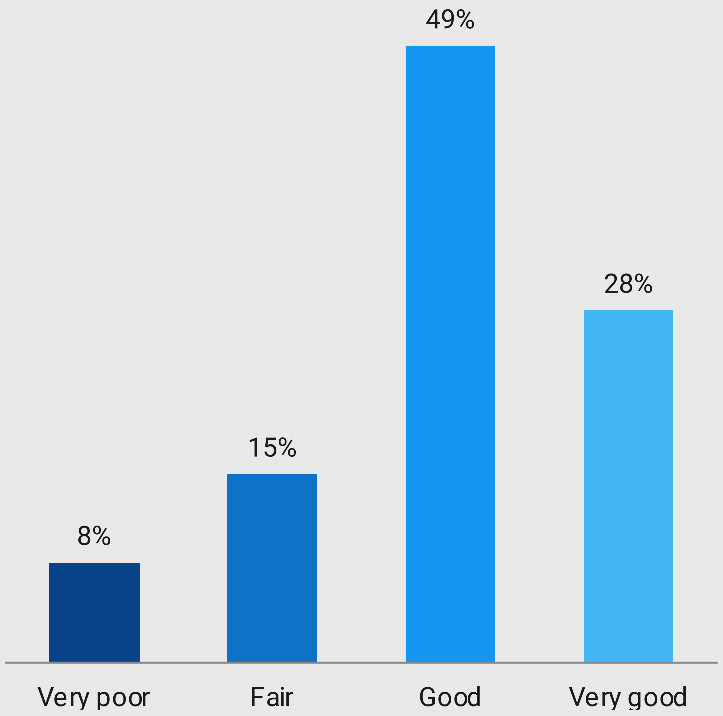
more cyberattacks were targeted toward the World Health Organization (WHO) during the COVID-19 pandemic as health institutions become valuable hacks for cybercriminals.

> “We’re moving into an environment in which there are inevitably going to be greater opportunities for malicious actors.”

Suzanne Spaulding, former Undersecretary for the Department of Homeland Security (DHS)

Opportunity exists to improve data visibility in government agencies

How would you complete the following statement: "My agency's IT department has _______ visibility over all its critical data."



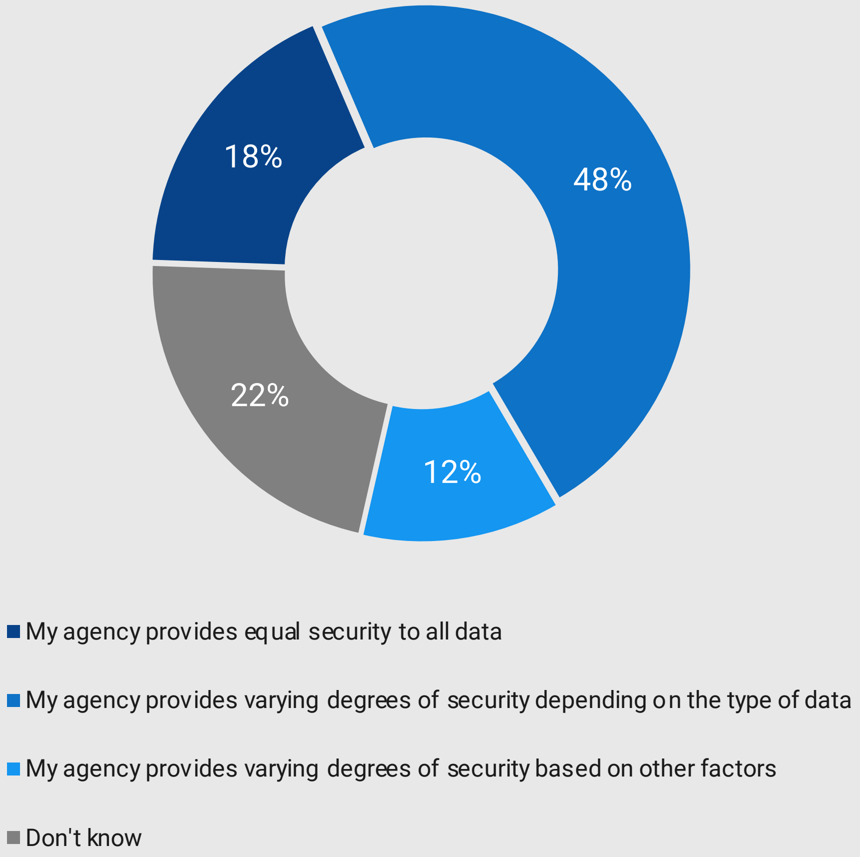
Percentage of respondents, n=39
Note: Percentages may not add up to 100% due to rounding.

72%

of respondents think that their agency’s IT department has good or less than good visibility over its critical data

Agencies are generally selective of the degree of security per data type

Which statement better captures your agency's approach to securing data?



Percentage of respondents, n=328
Note: Percentages may not add up to 100% due to rounding

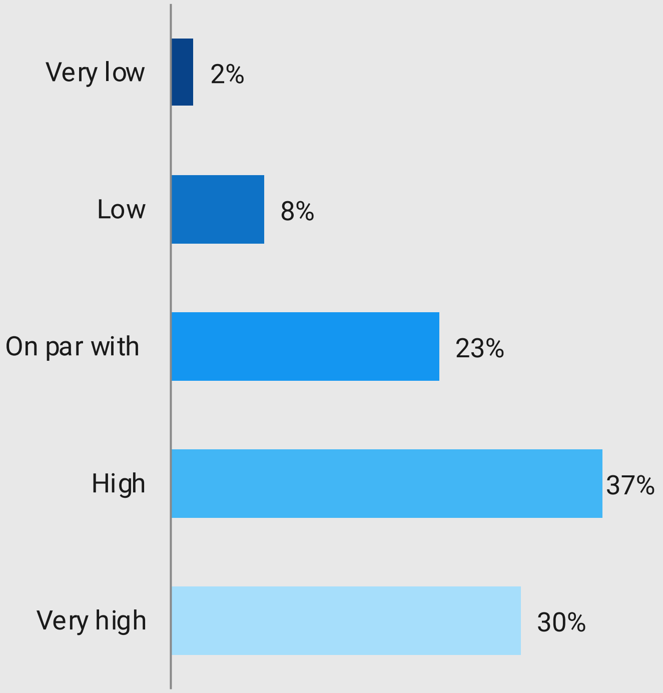
Did you know?

Agencies can classify data to safeguard more sensitive information using methods such as identity access management (IAM) and data encryption.

Data classification can help with compliance of data regulations, including the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).

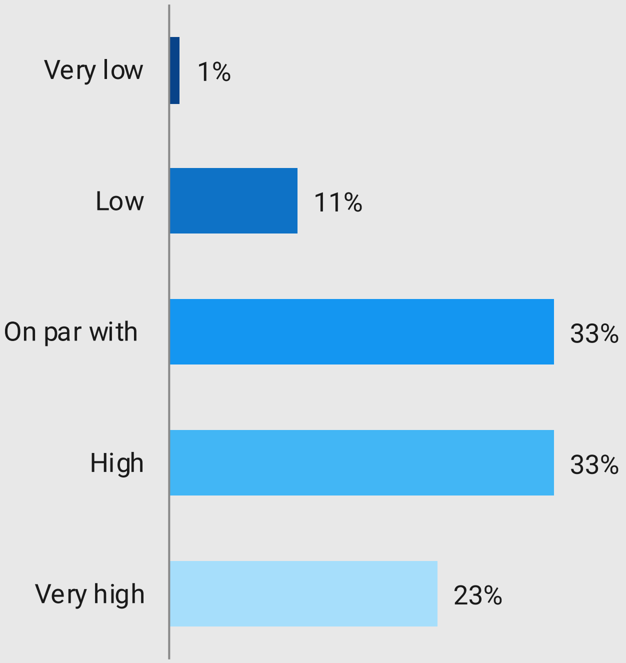
Federal civilians are more likely than DoD employees to say that their agencies rank cybersecurity higher than other competing priorities

Federal Civilians: How does cybersecurity rank relative to other competing priorities in your organization?



Percentage of respondents, n=249
Note: Percentages may not add up to 100% due to rounding

DoD Personnel: How does cybersecurity rank relative to other competing priorities in your organization?



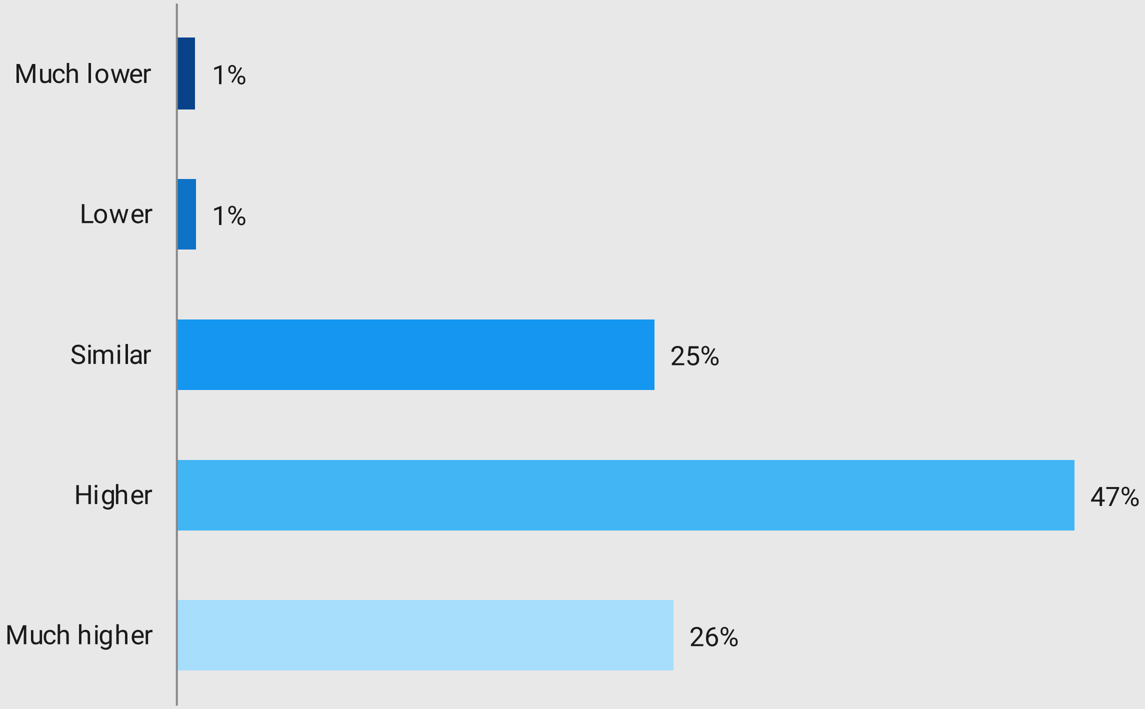
Percentage of respondents, n=101
Note: Percentages may not add up to 100% due to rounding

11%

more federal civilian respondents than defense personnel think that cybersecurity is ranked high or very high compared to other agency priorities.

Respondents involved in IT anticipate heightened cybersecurity priorities in the future

In coming years, I anticipate cybersecurity will have a ______ priority than / as it has today.



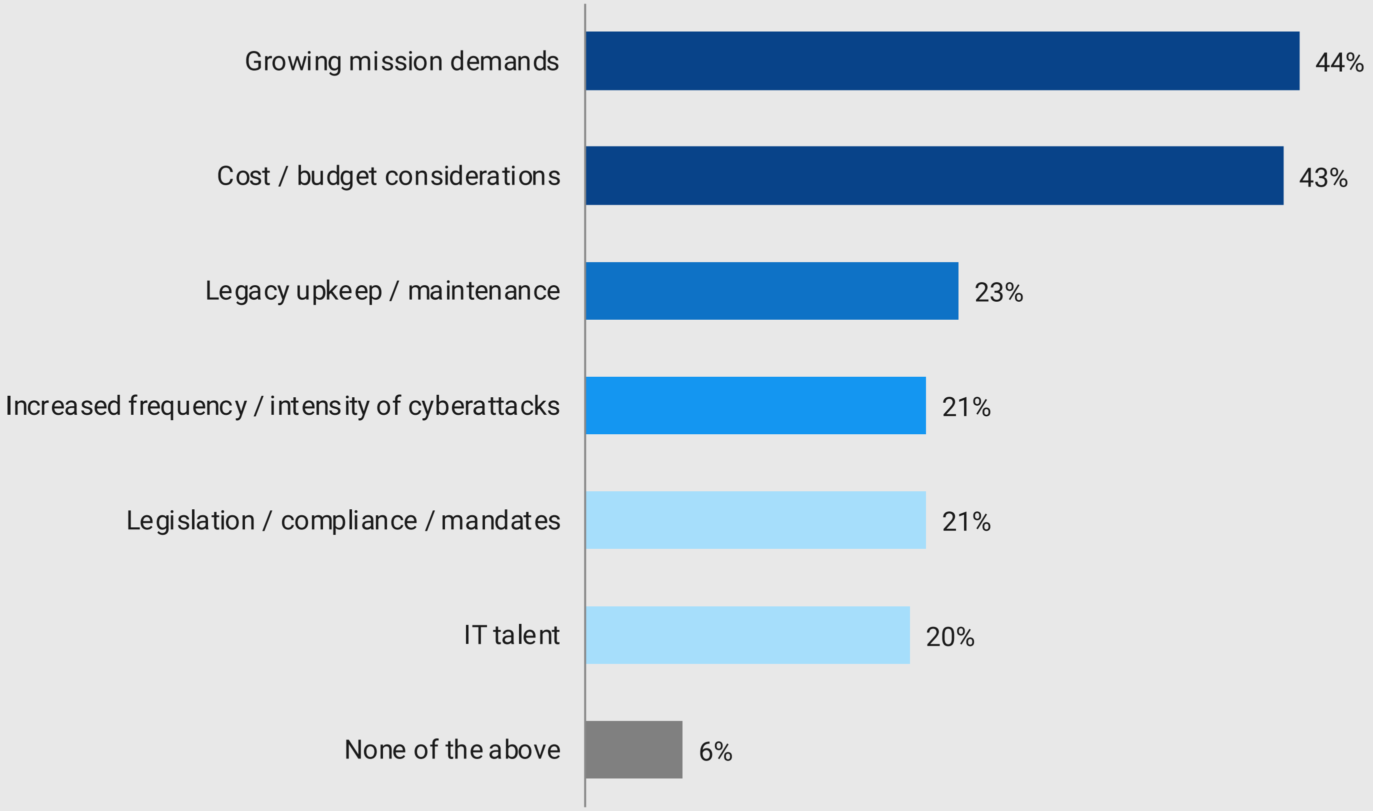
Percentage of respondents, n=154
Note: The data above represents those involved in IT

73%

of respondents think cybersecurity will have a high or much higher priority in the future.

Mission demands and budgets influence agencies’ IT priorities the most

Which factors hold the greatest influence over your organization's IT priorities? Please rank your top 2 choices.



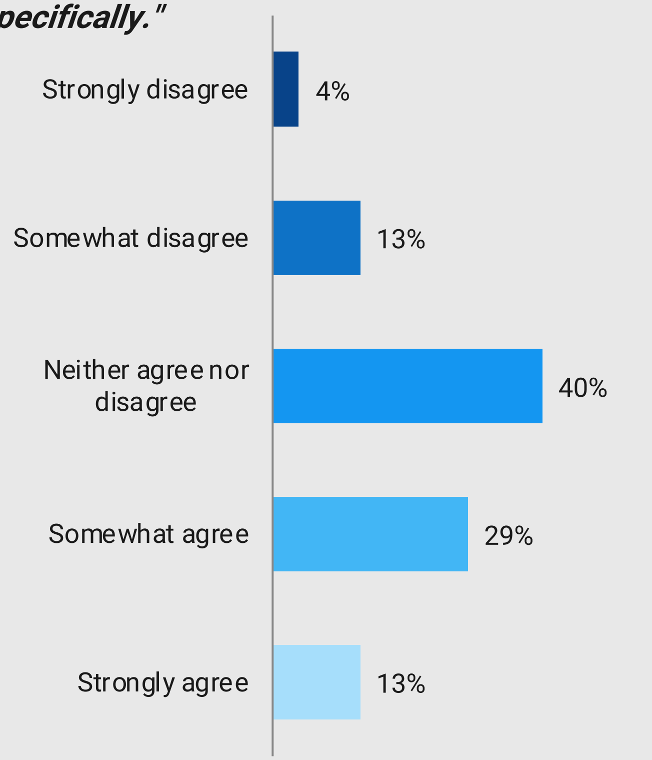
Percentage of respondents, n=333
Note Respondents were asked to select all that apply.

30%

of defense civilian respondents mention legacy upkeep as a top influencer of their organizations’ IT priorities compared to just 20% of federal civilian respondents.

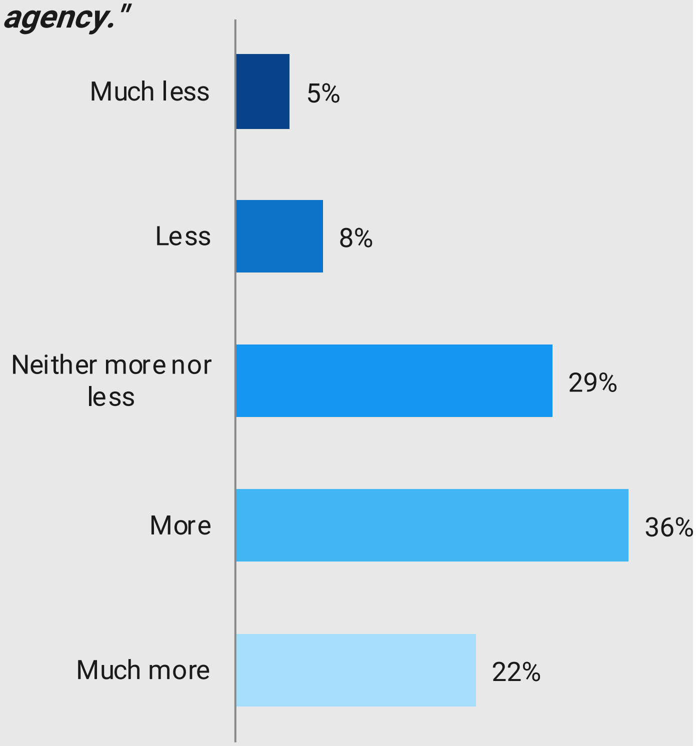
Centralizing cybersecurity funding is more effective than funding managed by different parts of an agency

To what extent do you agree or disagree with the following statement: "My agency allocates sufficient funding to cybersecurity specifically."



Percentage of respondents, n=290
Not shown: 2% of respondents selecting “My agency does not allocate funding for cybersecurity specifically.”

How would you complete the following statement: "It is _____ effective to centralize cybersecurity funding than it is to have such funds managed by different parts of my agency."



Percentage of respondents, n=286
Note Respondents were asked to select all that apply.

36%

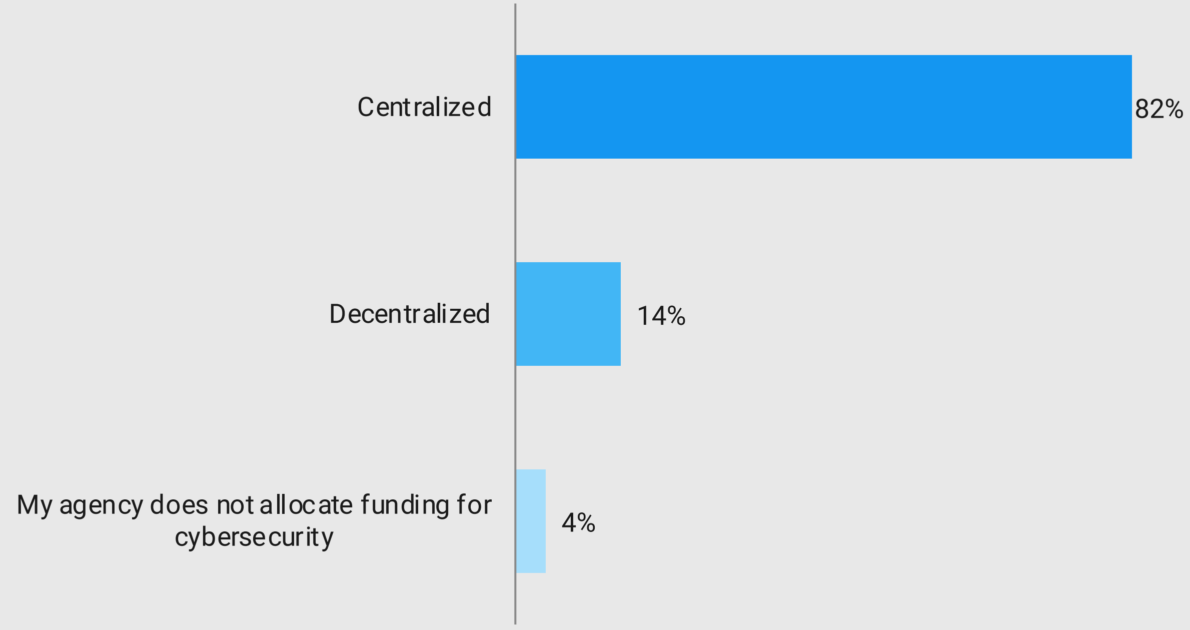
of respondents in positions GS/GM-13 and up somewhat agree with this statement compared to just 18% of those in the lower echelons.

63%

of respondents involved in their agency’s IT think that centralizing funding is more or much more effective compared to 54% of those not involved in IT.

Most respondents note that their agencies have centralized cybersecurity funding

Is cybersecurity funding in your agency centralized or decentralized?



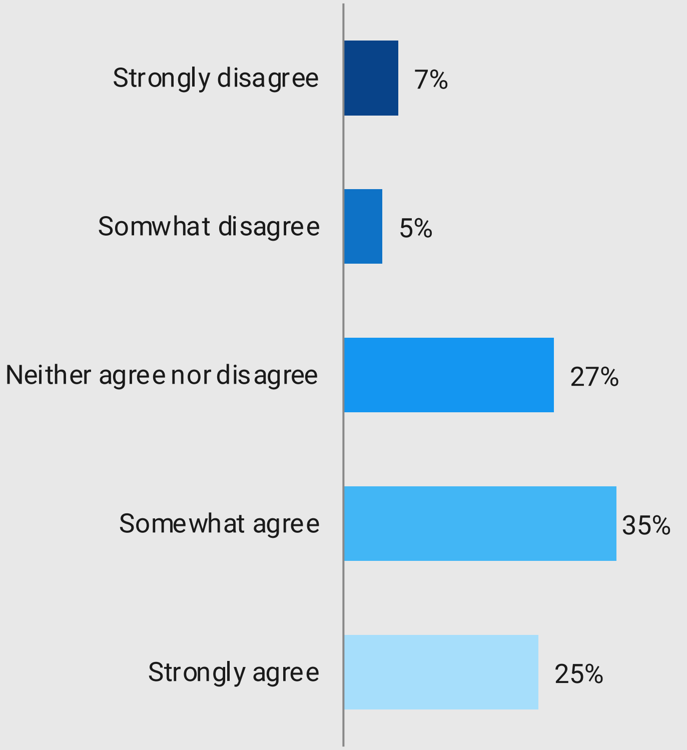
Percentage of respondents, n=125
Note: Percentages may not add up to 100% due to rounding

82%

of respondents say that their agencies centralize funding for cybersecurity. .

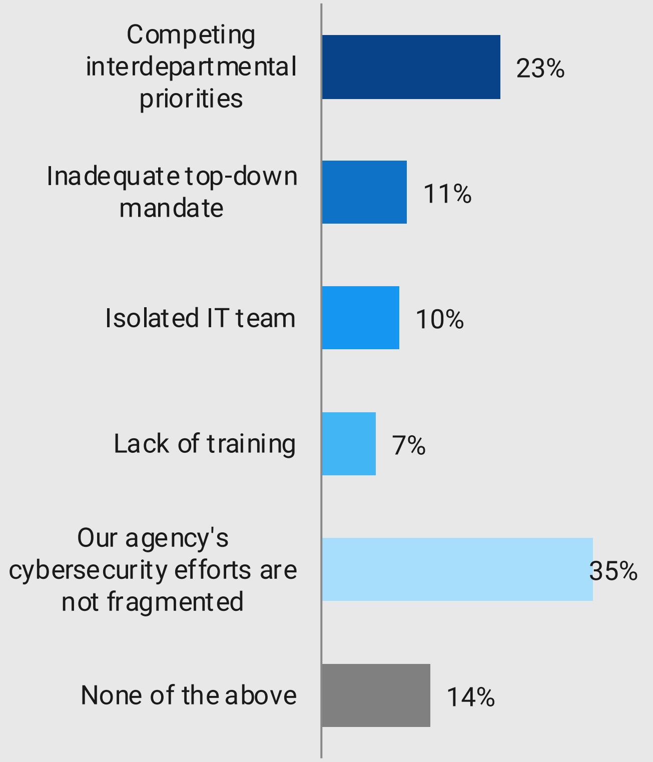
Respondents generally agree that their agencies have a unified cybersecurity plan

To what extent do you agree or disagree with the statement: "My agency has a coordinated incident response plan that covers cybersecurity across my entire agency. "



Percentage of respondents, n=310
Note: Percentages may not add up to 100% due to rounding

Which of the following (if any) is most responsible for fragmented cybersecurity efforts in your agency?



Percentage of respondents, n=299
Note Respondents were asked to select all that apply.

31%

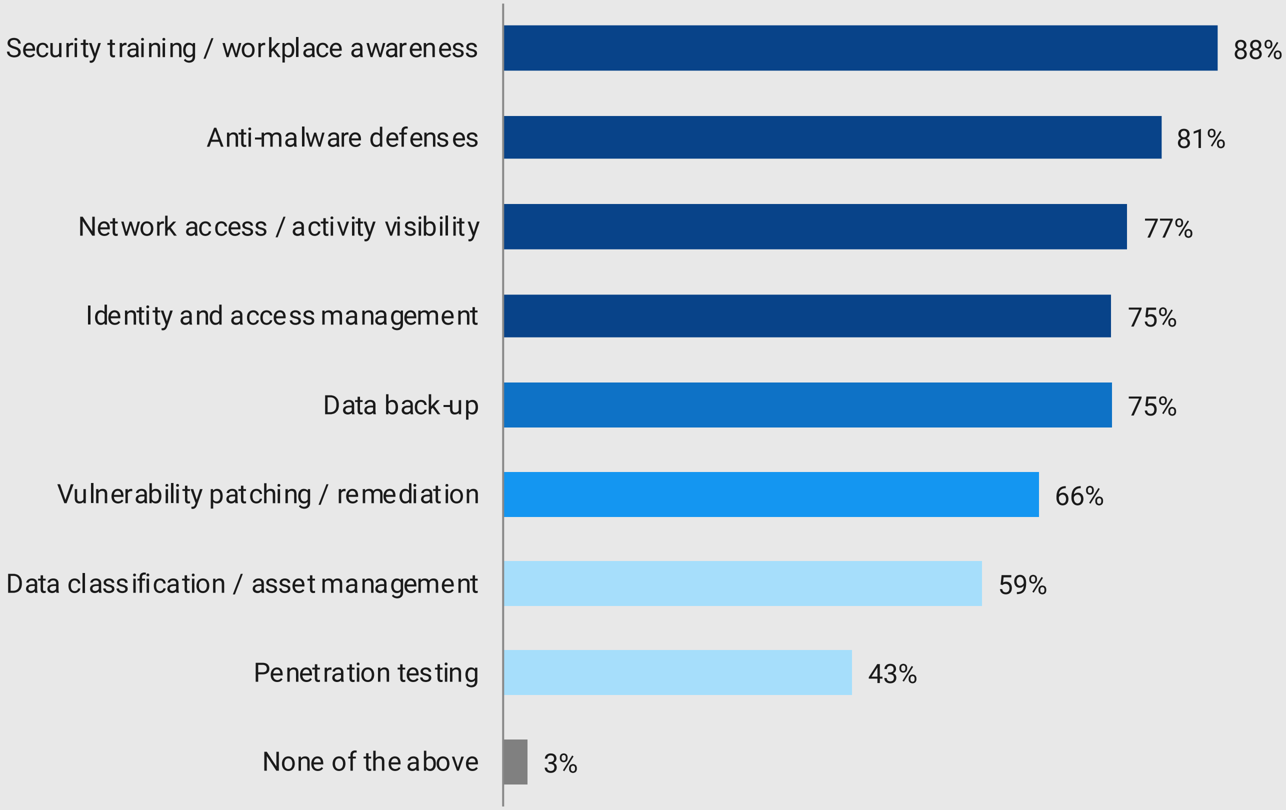
of DoD respondents strongly agree with this statement compared to 22% of federal civilian respondents.

28%

of respondents involved in their agency's IT say that competing interdepartmental priorities fragment cybersecurity efforts compared to just 18% of those not involved in IT.

Less than half of federal respondents say that their agencies use penetration testing to secure their systems

To the best of your knowledge, what cybersecurity controls does your agency have in place? Please select all that apply.



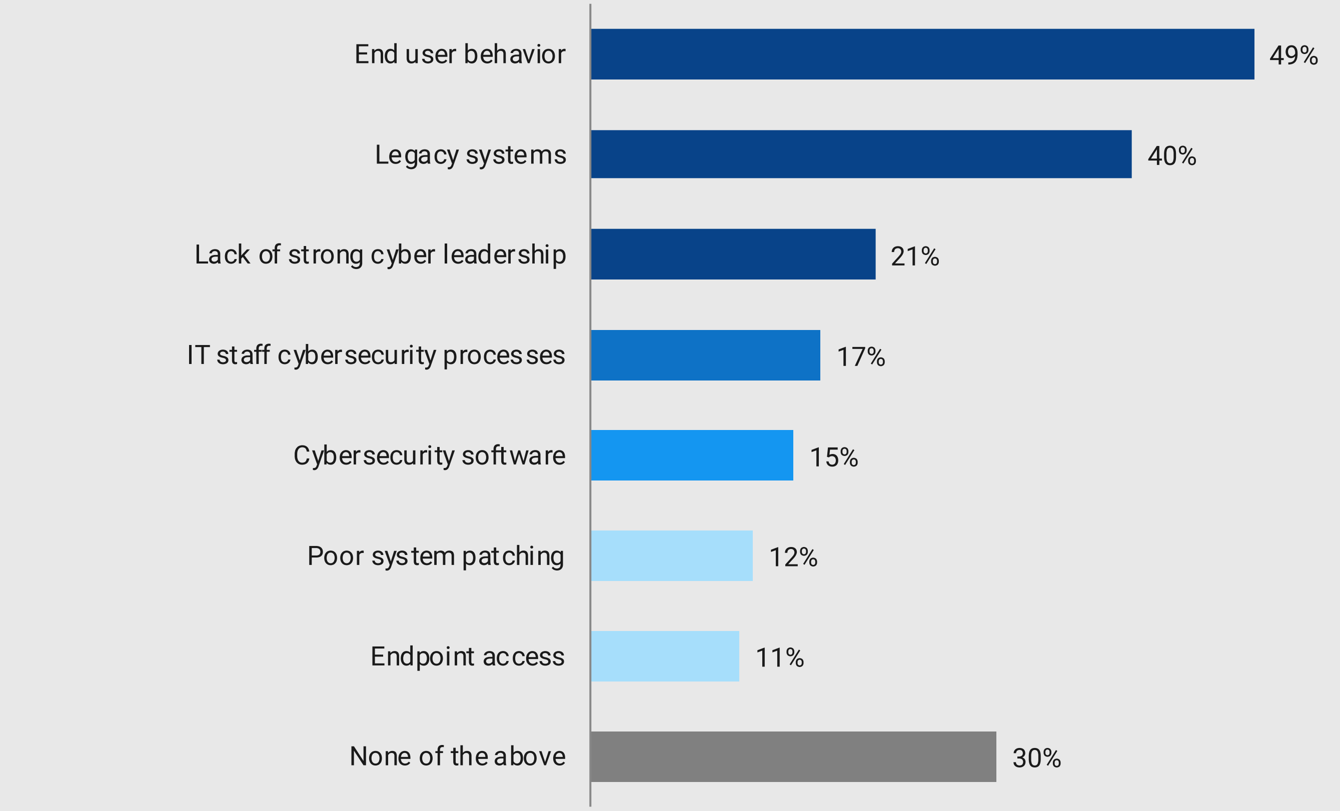
Percentage of respondents, n=358
Note Respondents were asked to select all that apply.

71%

of defense civilian respondents say that their agencies classify data compared to just 54% of federal civilian respondents.

Respondents point to end user behavior and legacy systems as the top factors that deteriorate security

Which of the following are the top causes of cybersecurity deficiencies in your agency? Please select all that apply.



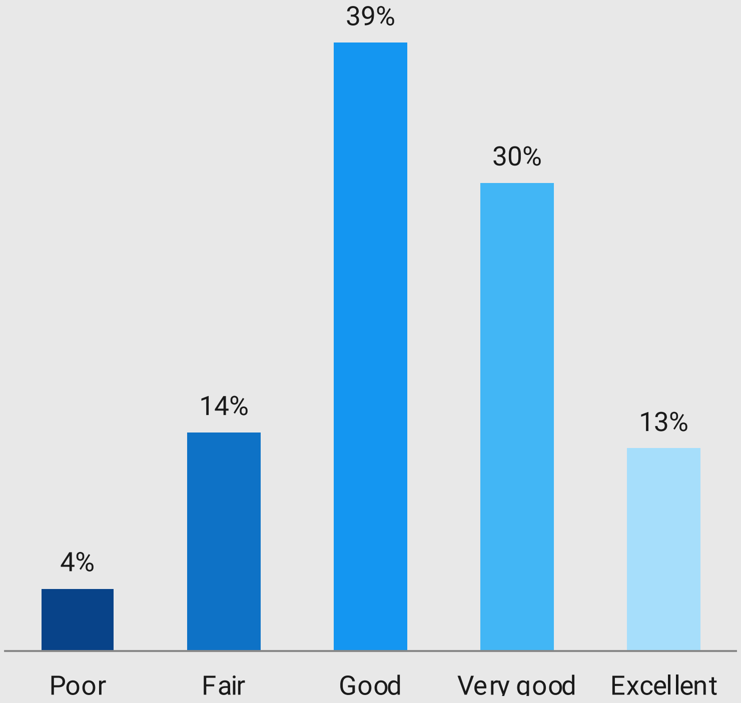
Percentage of respondents, n=358
Note Respondents were asked to select all that apply.

19%

of defense civilian respondents say that their agencies have poor system patching compared to half that for federal civilian respondents.

More than half of respondents think that their agency’s IT resources are good or less than good at defending against cyberattacks

How would you complete the following statement: "My agency's internal IT resources (e.g. staffing, technology) are ____ at preventing and mitigating cyberattacks."



Percentage of respondents, n=286
Note: Respondents were asked to select all that apply.

Did you know?

The number of unfilled cybersecurity jobs increased by more than 50 percent since 2015 across U.S. public and private sectors , according to the Center for Strategic and International Studies.

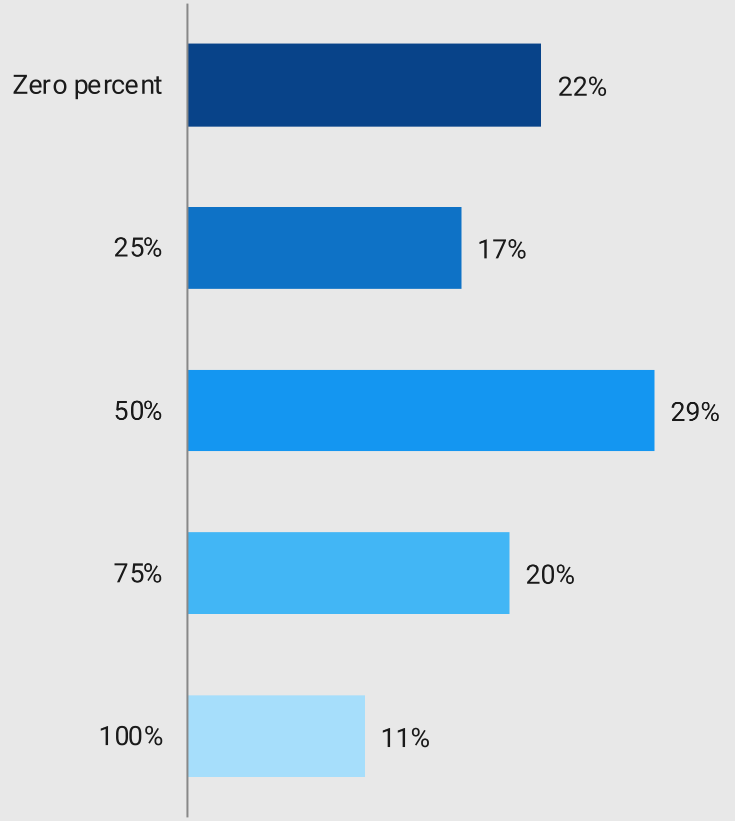
“

Congress should strengthen the Cybersecurity and Infrastructure Security Agency (CISA)…in its mission to ensure the national resilience of critical infrastructure, promote a more secure cyber ecosystem, and serve as the central coordinating element to support and integrate federal, state and local, and private-sector cybersecurity efforts.

Cyberspace Solarium Commission, March 2020

A majority of agencies receive managed services assistance for cybersecurity

To the best of your knowledge, what percentage of your cybersecurity responsibilities are contracted out through managed security services?



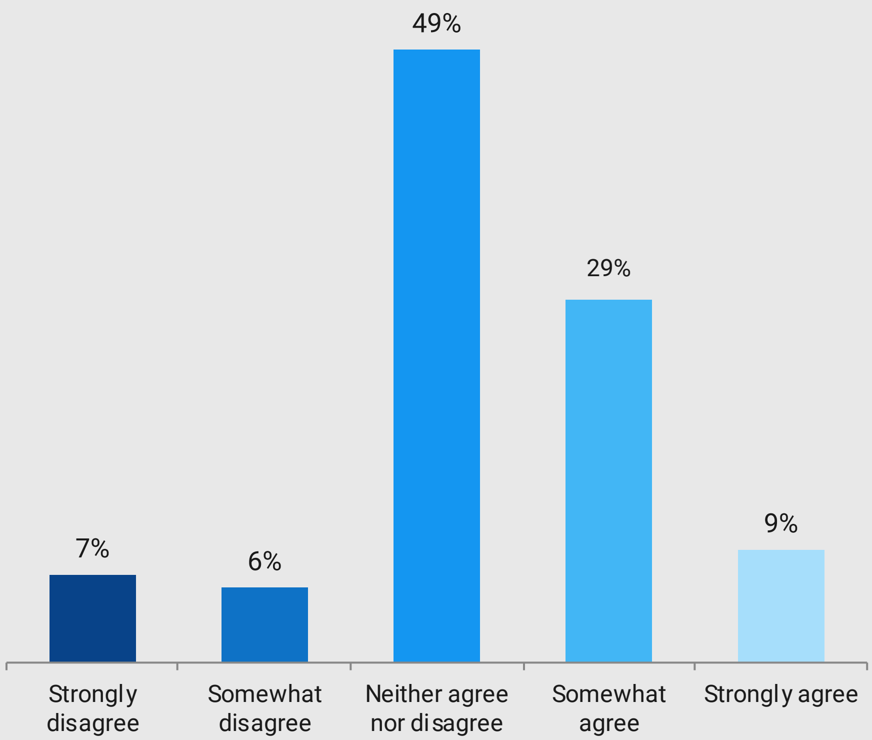
Percentage of respondents, n=89
Note: Percentages may not add up to 100% due to rounding

3 out of 5

respondents involved in their agency’s IT say more than 49% of their agency’s cybersecurity responsibilities are outsourced.

More respondents agree than disagree that their agencies will need third-party services to support their cybersecurity efforts

To what extent do you agree or disagree with the statement: "My agency will require third-party services to support internal cybersecurity resources and practices in the near future."



Percentage of respondents, n=282
Note: Percentages may not add up to 100% due to rounding

38%

of respondents somewhat to strongly agree that their agencies will need third-party cybersecurity services.

Final Considerations

When enhancing agency cyber protections:

–

Invigorate cybersecurity programs

Federal employee respondents express that their agencies lack resources supporting cybersecurity. 57% of respondents say that their internal IT resources (e.g. technology and staffing) are only good or less than good for preventing or mitigating cyberattacks. Only 43% of respondents, for example, note that their agencies utilize proactive cybersecurity methods, such as penetration testing. Agencies aiming to invigorate their cybersecurity controls have turned to managed services with 77% of respondents saying their agency contracts out at least some cybersecurity responsibilities to third parties.

–

Consider all moving parts of securing a network

While respondents clarify a need to invest in cybersecurity technology, other pillars of cybersecurity should be equally attended to, including user behavior and IT infrastructure. Federal employees suggest that IT hygiene could be improved given that 49% of respondents say that end user behavior is a top cause of cybersecurity deficiencies. Additionally, respondents allude to legacy systems as a major barrier to successful cybersecurity, suggesting a need to upgrade to infrastructure compatible with the newest, cutting-edge cybersecurity technology.

Insights from Leidos

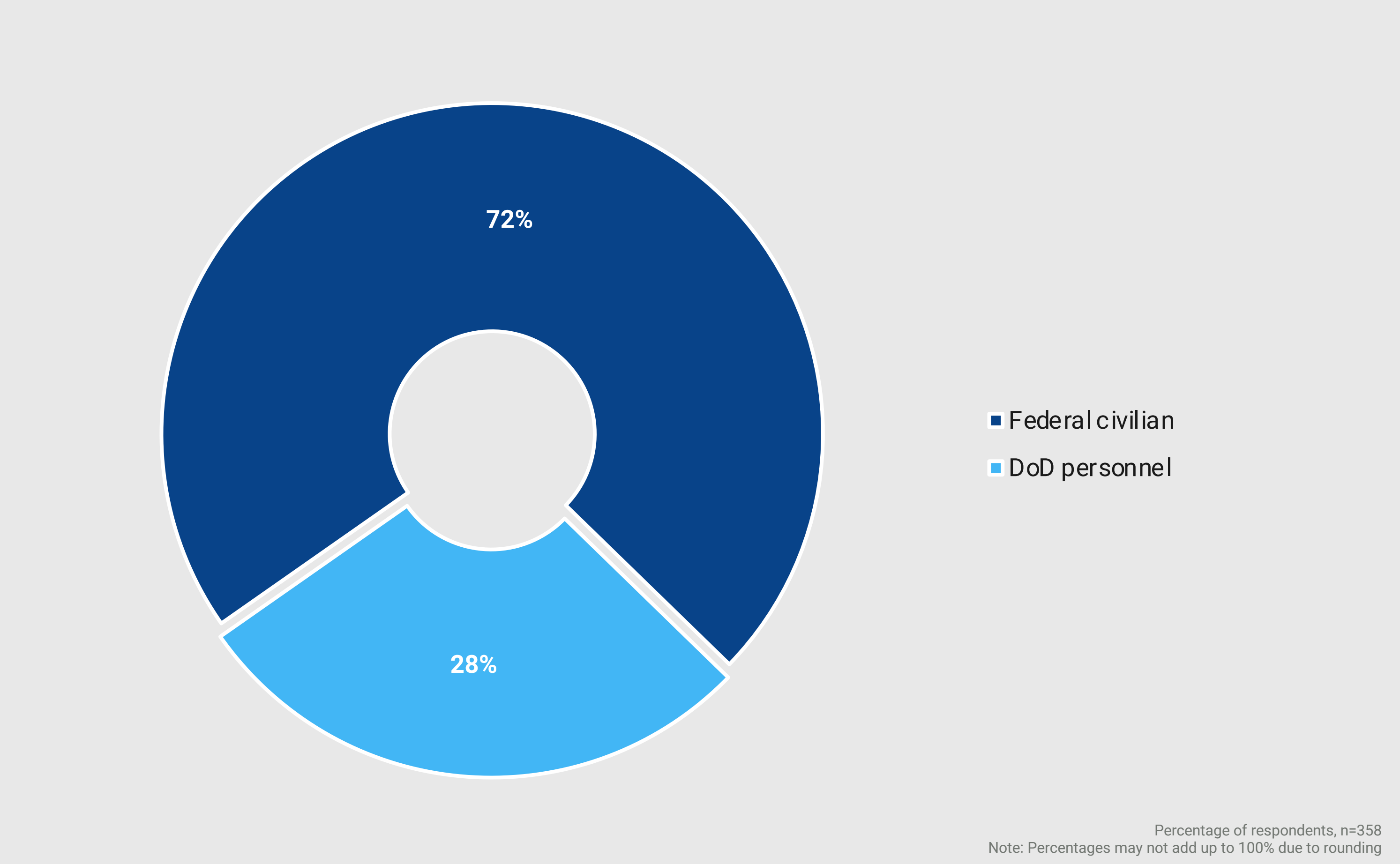
Leidos is a recognized leader in cybersecurity, bringing more than 30 years of experience defending cyber interests globally and delivering advanced capabilities honed from protecting some of the world's most valuable assets. Our solutions and services ensure an adaptive defense strategy, proactive threat protection, and a resilient security posture. We believe that effective cybersecurity solutions:

- Stand by cyber methodologies that enable analysts and ensure cyber resiliency in highly-regulated and mission-critical environments
- Build a strong Risk Management Framework because security, at its core, is a risk analysis and management activity
- Leverage automation and analytics to increase productivity and quality of work
- Target insider threats, providing a truly holistic defense

Strengthen your cybersecurity with Leidos' agile, mission-enabling cyber solutions.

Respondent Profile

A majority of respondents are federal civilians



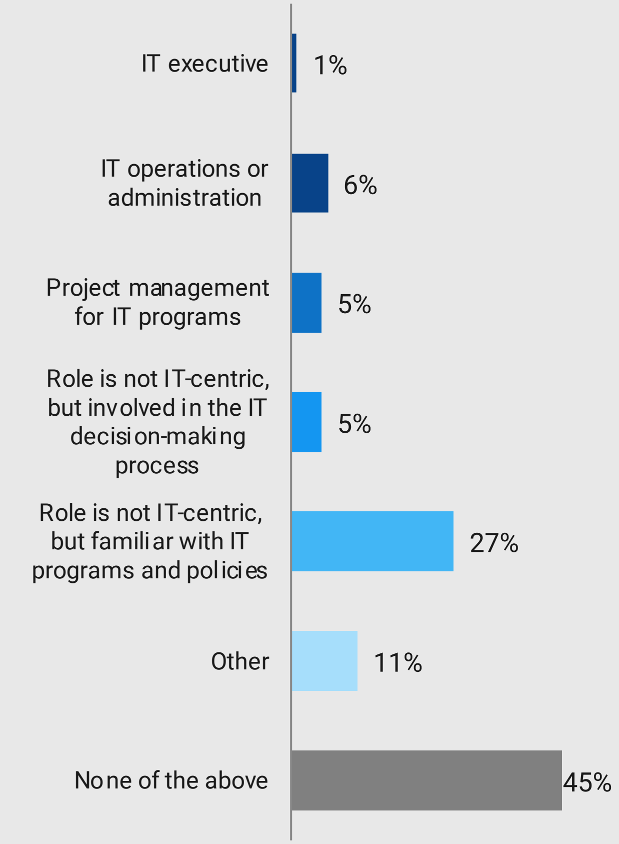
Percentage of respondents, n=358
Note: Percentages may not add up to 100% due to rounding

3 in 4

respondents are federal civilians.

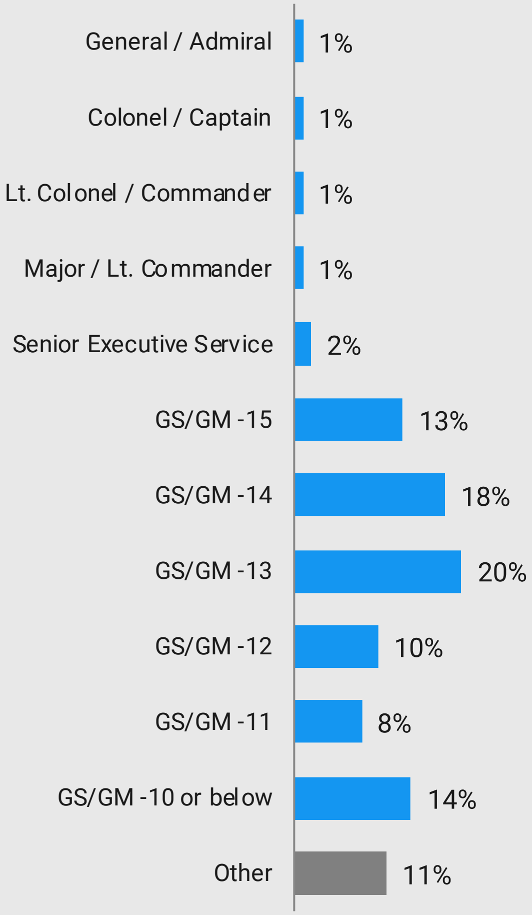
Most respondents are GS/GM-13 and above

Which of the following best describes your involvement with your organization's IT department?



Percentage of respondents, n=358
Note: Percentages may not add up to 100% due to rounding

Job Grade



Percentage of respondents, n=356
Note: Percentages may not add up to 100% due to rounding

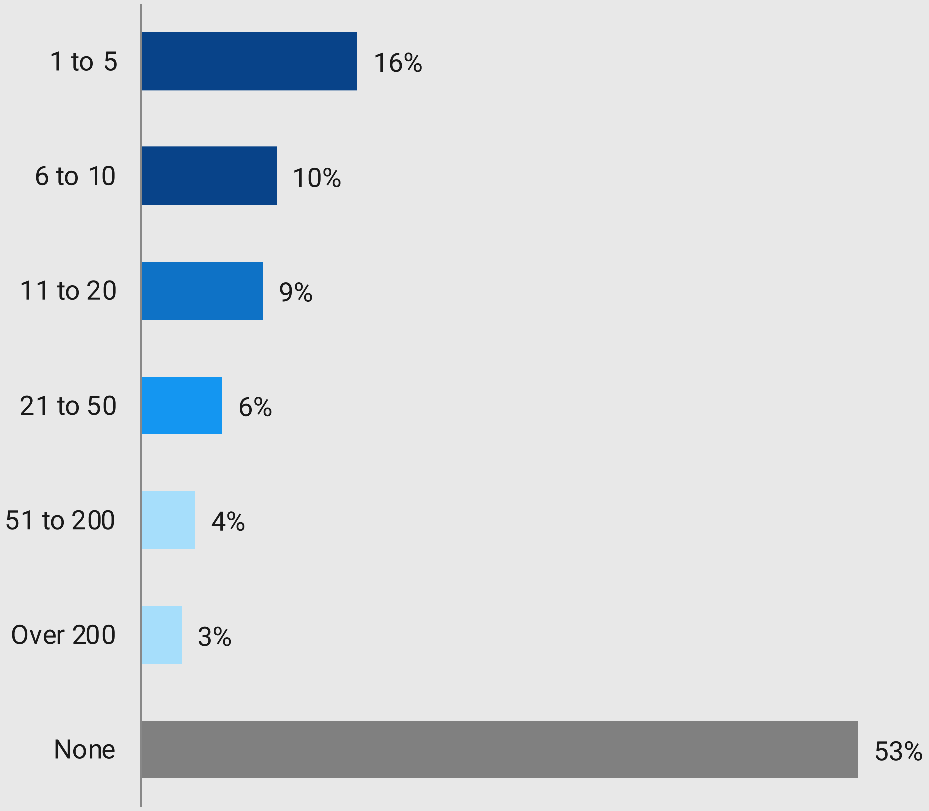
44%

are involved with their agency’s IT.

Respondents were asked to choose which single response best describes their organizational ranking.

Nearly half of all respondents surveyed are senior managers in their agencies

How many people do you oversee in total, either directly or through your direct reports?



Percentage of respondents, n=358
Note Respondents were asked to select all that apply.

About

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. An extension of *Government Executive*'s 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights

Contact

Daniel Thomas
Associate Director, Research & Strategic Insights
Government Business Council
Tel: 202.266.7905
Email: dthomas@govexec.com

govexec.com/insights
@GovExecInsights

About Leidos

Leidos is a recognized leader in cybersecurity across the federal government, bringing more than a decade of experience defending cyber interests globally and delivering advanced capabilities honed from protecting some of the world's most valuable assets. Our solutions and services ensure an adaptive defense strategy, sustainable threat protection, and a mature security posture.

Learn more at: https://www.leidos.com/cyber