SolarWinds Federal Cybersecurity Survey Report

January 2019

solarwinds government

Market Connections® Research you can act on.

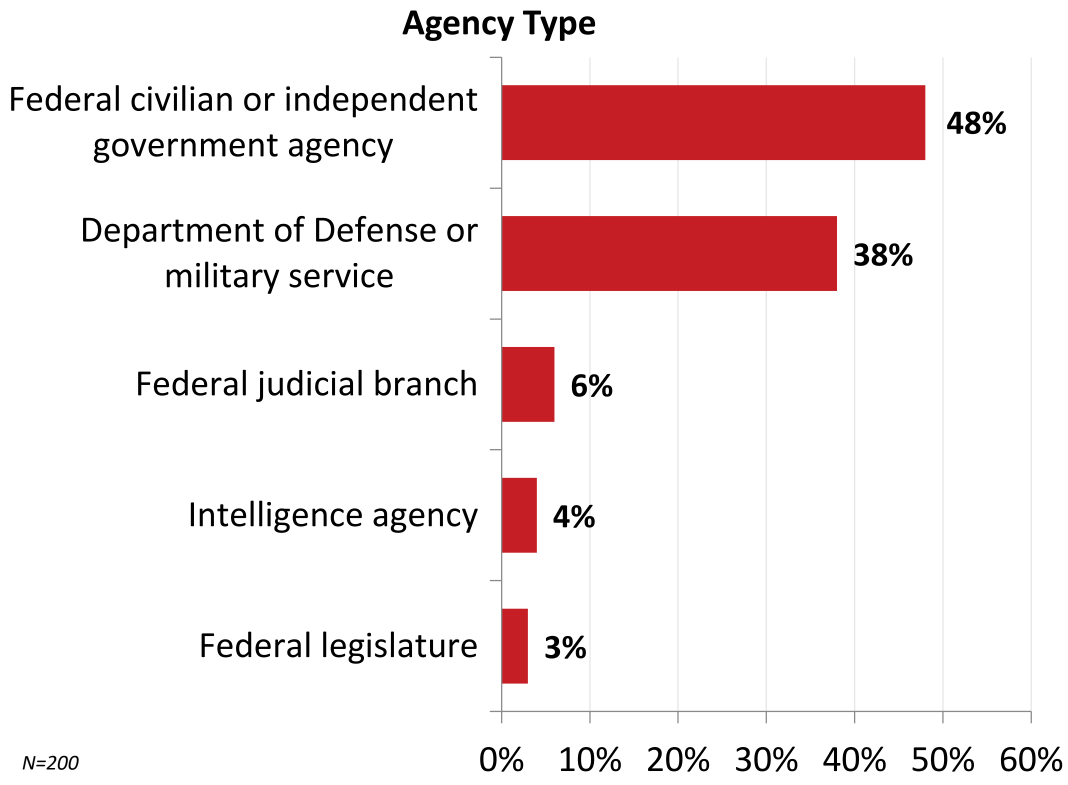
Methodology

SolarWinds contracted Market Connections to design and conduct an online survey among 200 federal government IT decision makers and influencers in December 2018 and January 2019. SolarWinds was not revealed as the sponsor of the survey.

PRIMARY OBJECTIVES:

- Determine challenges faced by IT professionals to prevent IT security threats
- Quantify sources and types of IT security threats
- Identify specific plans, processes, regulations, mandates, and tools that contribute to or challenge agencies’ management of risk
- Address the ability to prevent and detect insider threats:
  - Accidental and malicious
  - Third-party contractors and regular employees
- Assess perceptions of IT security training

Organizations Represented



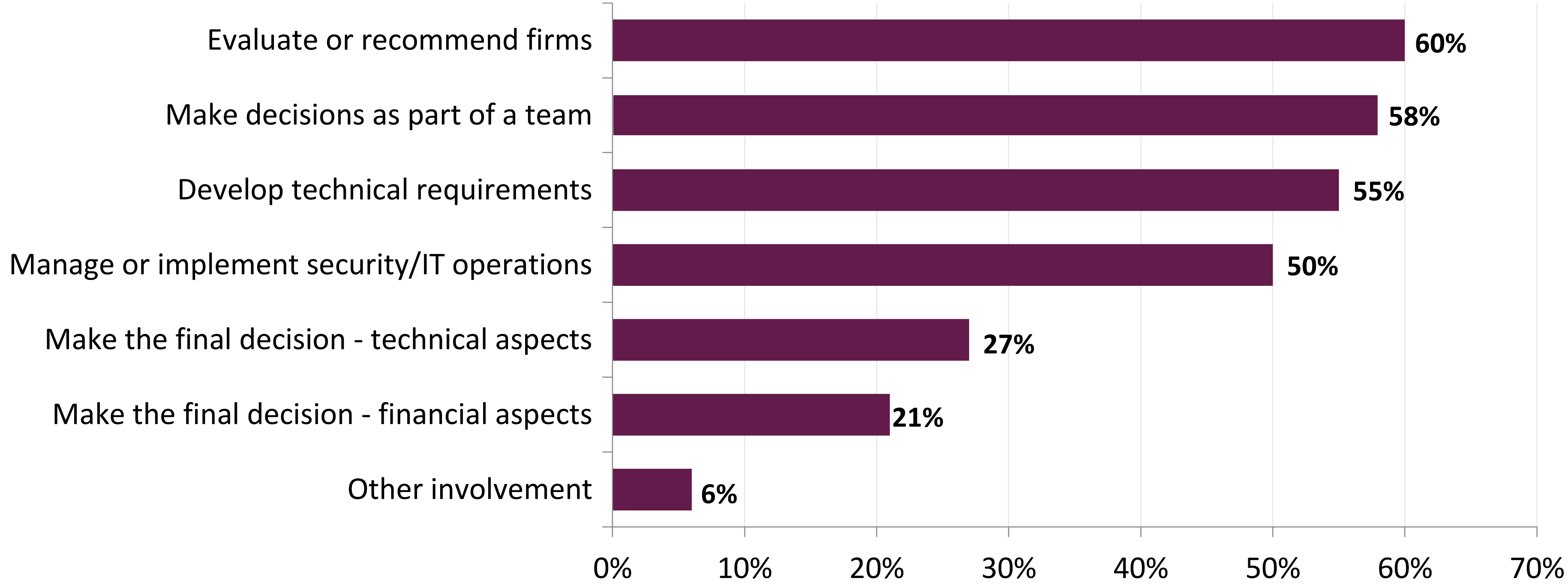
N=200

Sample Organizations Represented (in alphabetical order)	
Air Force	Department of Labor (DOL)
Army	Department of State (DOS)
Department of Commerce (DOC)	Department of Transportation (DOT)
Department of Defense (DOD)	Department of Treasury (TREAS)
Department of Energy (DOE)	Department of Veteran Affairs (VA)
Department of Health and Human Services (HHS)	NASA
Department of Homeland Security (DHS)	Navy/Marines
Department of Housing and Urban Development (HUD)	Securities and Exchange Commission (SEC)
Department of Justice (DOJ)	Social Security Administration (SSA)

solarwinds

Decision-Making Involvement

All respondents are knowledgeable or involved in decisions and recommendations regarding IT operations and management and IT security solutions and services.



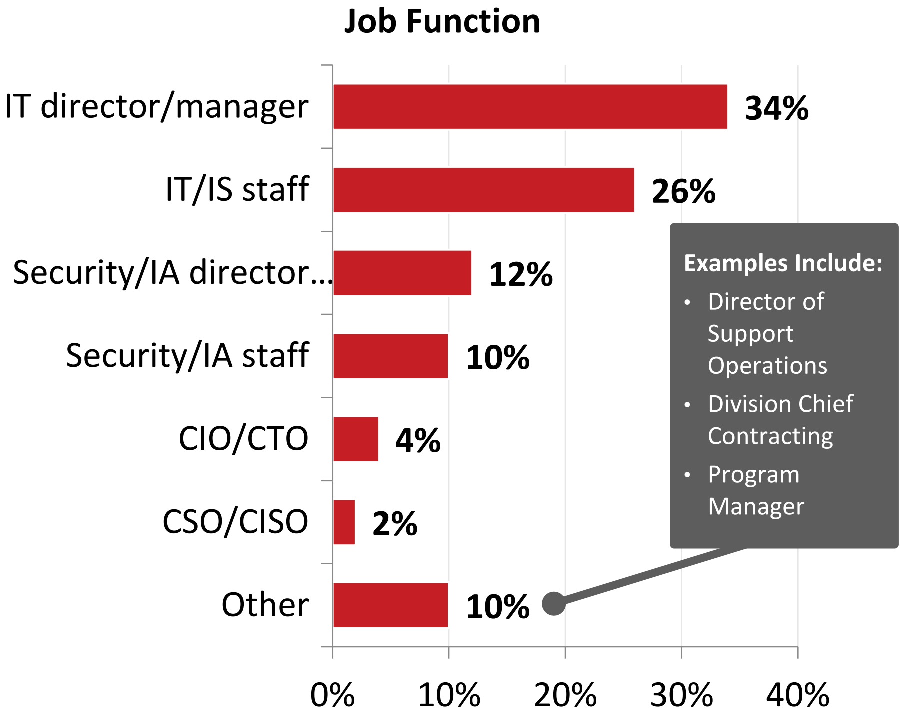
N=200

Note: Multiple responses allowed

Q *How are you involved in your organization's decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)*

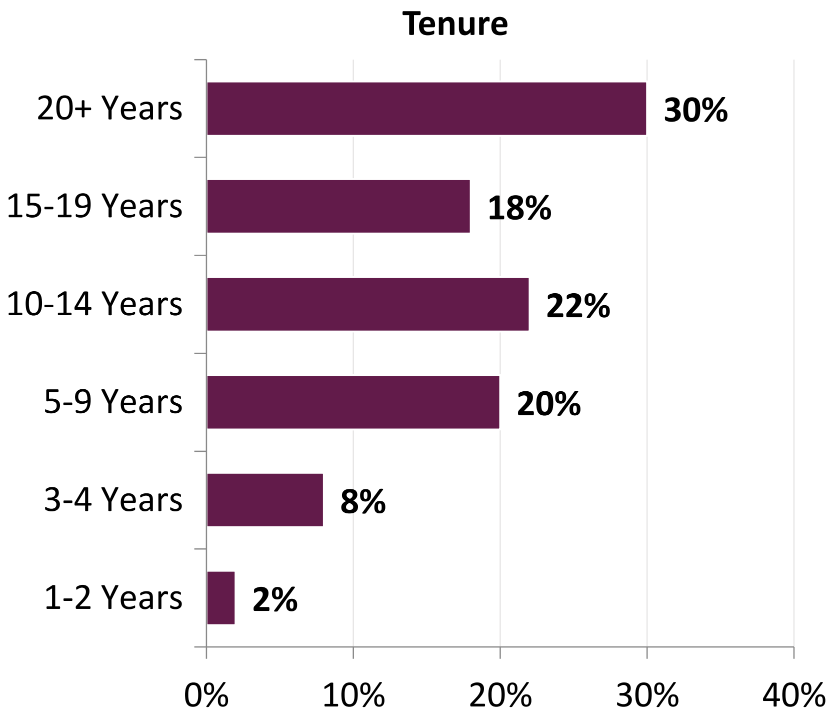
Job Function and Tenure

A variety of job functions and tenures are represented in the sample, with most being IT management and working at their current agency for more than 20 years.



Examples Include:

- Director of Support Operations
- Division Chief Contracting
- Program Manager

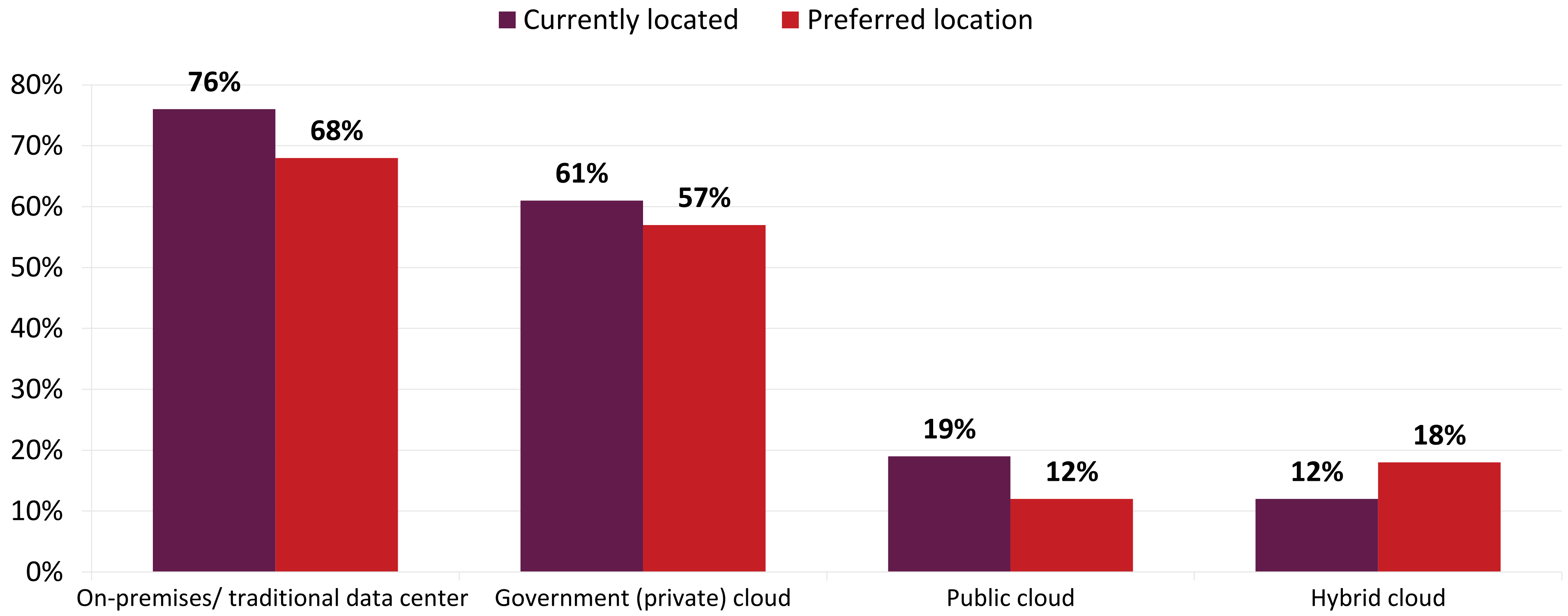


N=200

Q *Which of the following best describes your current job title/function? How long have you been working at your current agency?*

Location of IT Security Products

IT security products are located primarily on-premises or in a private cloud. The respondents' preferred location of these products is similar to the current location.



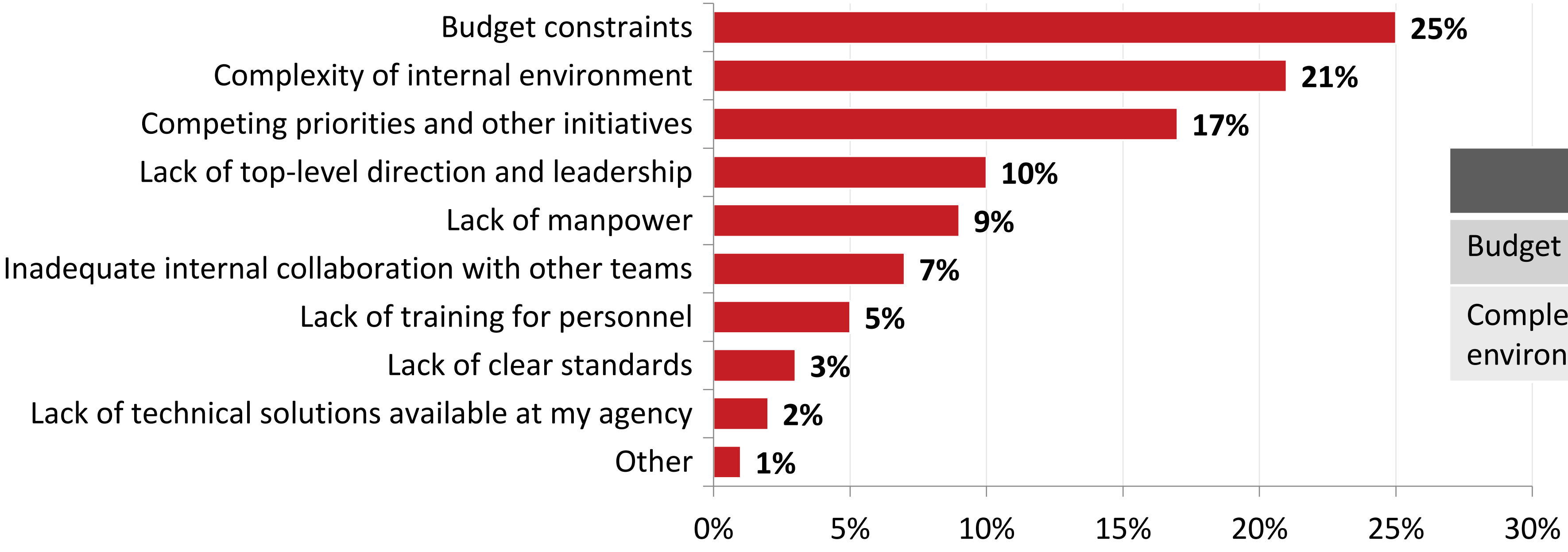
N=200

Note: Multiple responses allowed

Q *Where are the IT security products your organization uses currently? Where would you prefer these products to be located?*

IT Security Obstacles

Budget constraints top the list of significant obstacles to maintaining or improving agency IT security. While budget constraints have declined since 2014, the complexity of the internal environment as an obstacle has increased.



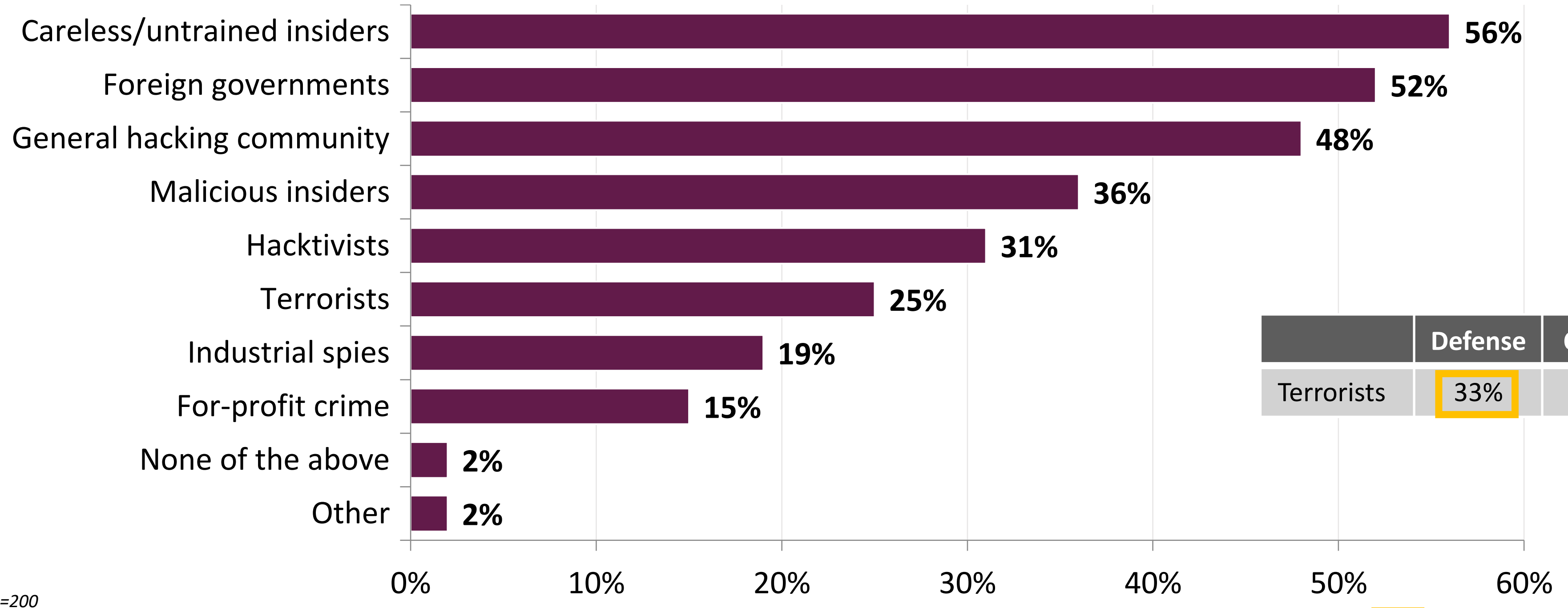
	2014	2018
Budget constraints	40%	25% ⬇
Complexity of internal environment	14%	21% ⬆

N=200

Q *What is the most significant high-level obstacle to maintaining or improving IT security at your agency?*

Sources of Security Threats

Careless/untrained insiders and foreign governments are noted as the largest sources of security threats at federal agencies.



	Defense	Civilian
Terrorists	33%	19%

N=200
Note: Multiple responses allowed

□ = statistically significant difference

Q *What are the greatest sources of IT security threats to your agency? (select all that apply)*

Sources of Security Threats - Trend

All sources of security threats have increased since 2014. Six of the eight threat sources are at an all-time high.

	2014	2015	2016	2017	2018
Careless/untrained insiders	42%	53%	48%	54%	56%
Foreign governments	34%	38%	48%	48%	52%
General hacking community	47%	46%	46%	38%	48%
Hacktivists	26%	30%	38%	34%	31%
Malicious insiders	17%	23%	22%	29%	36%
Terrorists	21%	18%	24%	20%	25%
For-profit crime	11%	14%	18%	17%	15%
Industrial spies	6%	10%	16%	12%	19%

N=200
Note: Multiple responses allowed

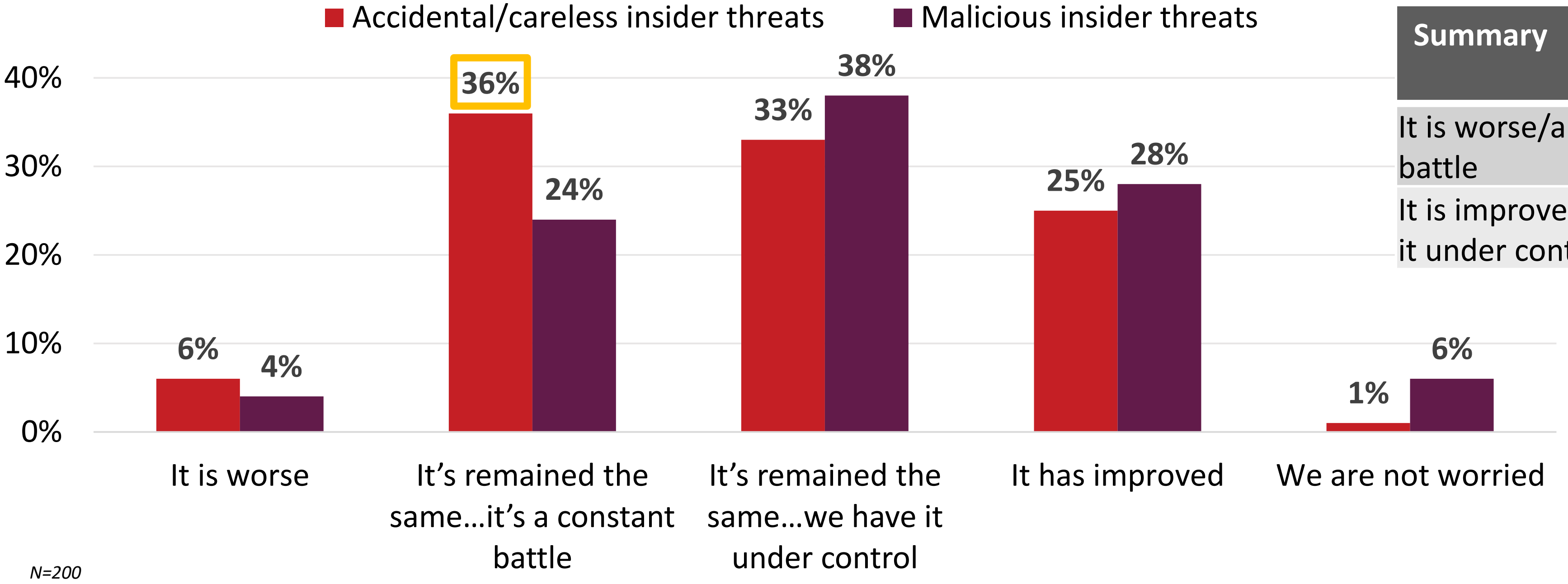
■ = top three sources

□ = statistically significant difference from 2017

Q *What are the greatest sources of IT security threats to your agency? (select all that apply)*

Agencies’ Ability to Prevent and Detect

A significantly greater proportion of respondents note their ability to detect and prevent careless insider threats is a constant battle relative to malicious insider threats.



N=200

Summary	Accidental / careless	Malicious
It is worse/a constant battle	42%	28%
It is improved/we have it under control	58%	66%

Improved	Defense	Civilian
Malicious	38%	22%

□ = statistically significant difference

How would you describe your organization’s ability to prevent and detect insider threats over the last two years?

solarwinds

Detection and Prevention Improvement

Improved strategy and processes to apply security best practices is noted most often as a reason careless insider threats have improved or remained in control.

Employee background checks is noted most often as a reason malicious insider threats have improved or remained in control.

Policy and Process		
Reasons that insider threats have improved or remained in control	Careless Insider Threats	Malicious Insider Threats
Improved strategy and processes to apply security best practices	58%	44%
Employee background checks	41%	48%
Increased investment in security posture improvement	39%	45%
Leadership buy-in to improve security posture	34%	35%

Accidental/careless insider threats n=116, Malicious insider threats n=132

■ = top reason □ = statistically significant difference

Q *In your opinion, what are the main reasons (i.e., tools and/or processes) your organization's ability to prevent and detect insider threats has improved or remained in control?*

Detection and Prevention Improvement (continued)

Regarding basic security hygiene, end-user security awareness training is noted most often as a reason careless insider threats have improved or remained in control. Patching is noted most often for malicious insider threats.

Basic Security Hygiene		
Reasons that insider threats have improved or remained in control	Careless Insider Threats	Malicious Insider Threats
End-user security awareness training	47%	41%
Network access control	45%	43%
Patching	43%	45%
IT configuration management and reporting	41%	37%
Identity and access monitoring tools	39%	43%
IT asset management and reporting	31%	32%

Accidental/careless insider threats n=116, Malicious insider threats n=132

■ = top reason

Q *In your opinion, what are the main reasons (i.e., tools and/or processes) your organization's ability to prevent and detect insider threats has improved or remained in control?*

Detection and Prevention Improvement (continued)

Regarding advanced security tools, intrusion detection and prevention tools is noted most often as a reason careless and malicious insider threats have improved or remained in control.

Network traffic encryption is also a top reason noted for malicious insider threats.

Advanced Security Tools		
Reasons that insider threats have improved or remained in control	Careless Insider	Malicious Insider
Intrusion detection and prevention tools	42%	36%
Endpoint and mobile security	34%	27%
Web application firewalls	34%	29%
Fire and disk encryption	34%	32%
Network traffic encryption	34%	36%
Web security or web content filtering gateways	33%	29%
Internal threat detection/intelligence	30%	32%
SIEM	28%	33%
Advanced endpoint protection	28%	19%
Advanced security threat analytics	28%	25%
Mobile device management or mobile-specific security tools	26%	27%
Next generation firewalls	24%	25%
Cloud app security management	22%	18%
Threat hunting	21%	21%
Endpoint forensics	19%	22%

Accidental/careless insider threats n=116, Malicious insider threats n=132

■ = top reason

Q *In your opinion, what are the main reasons (i.e., tools and/or processes) your organization's ability to prevent and detect insider threats has improved or remained in control?*

Difficulties with Insider Threats

Lack of training, an increase in the number of devices and the volume of network activity are noted most often as reasons for difficulties with careless or malicious insider threats.

The increase in use of cloud apps and infrastructure is also one of the top reasons for malicious threats.

Reasons that insider threats are worse or are a constant battle	Careless Insider Threats	Malicious Insider Threats
Lack of employee training/awareness	43%	31%
Increase in the number of devices with access to data	41%	35%
Volume of network activity	40%	42%
Lack of IT/security staff	35%	16%
Use of mobile devices, that are not limited to secure environments	28%	29%
Lack of IT staff training	28%	25%
Increased use of contractors that access network	27%	16%
Cost of sophisticated tools	23%	29%
Inadequate visibility into users' network activity	21%	29%
Inadequate change control practices	21%	18%
Pressure to change IT configurations quickly more so than securely	21%	20%
Inadequate monitoring of storage devices	17%	24%
Complexity or multitude of monitoring tools	17%	20%
Increased use of cloud apps and infrastructure	12%	31%
Inadequate configuration management of IT assets	11%	24%

Accidental/careless insider threats n=82, Malicious insider threats n=55

■ = top reasons □ = statistically significant difference

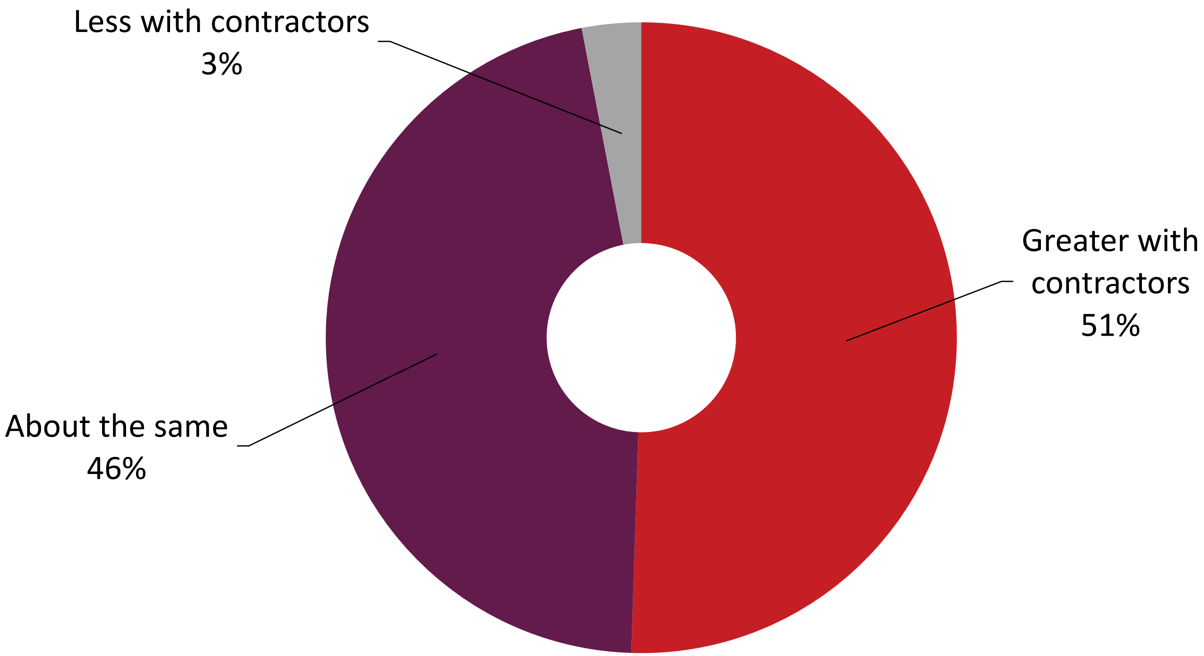
Q *In your opinion, what are the main reasons your organization's ability to prevent and detect insider threats has worsened or has been a constant battle?*

IT Risks: Contractors vs. Regular Employees

About half believe that IT security risks are greater with contractors.

Slightly less than half see the risks the same with contractors and regular employees.

Compared to Regular Employees, the IT Risks are…

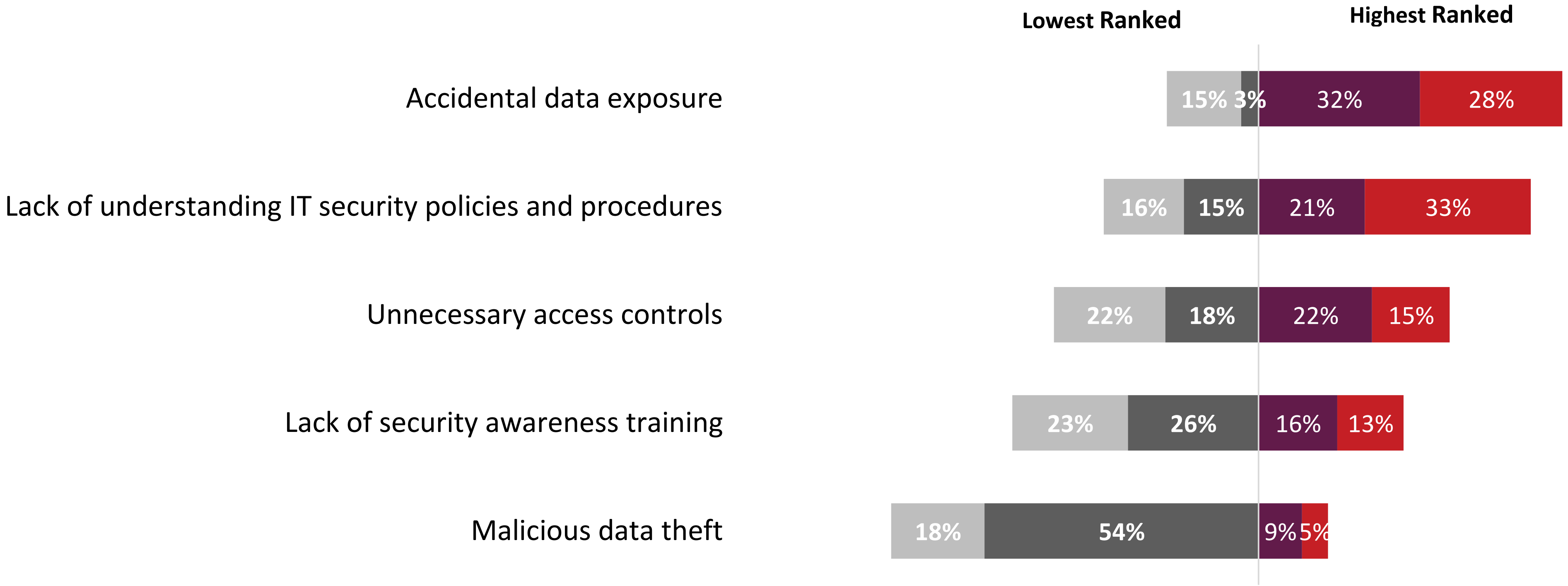


N=200

Q *Do you believe the IT security risks associated with hiring third-party contractors and/or temporary workers are greater or less than regular agency employees?*

Associated IT Security Risks - Ranked

Accidental data exposure and the lack of understanding of IT security policies and procedures are the risks associated the most with an agency's contractors and/or temporary workers.



Q *Please rank the following IT security risks that are associated with an agency's third-party contractors and/or temporary workers. A rank of number one means that in your opinion, it is the highest risk. Number two means it places second in your mind and so forth.*

Causes for Accidental Insider Breaches

Accidently exposing, deleting, or modifying critical data is the number one common cause associated with careless insider breaches from both regular employees and contractors.

Access to resources that are not necessary to do their job and using unsecured networks/Wi-Fi are more frequently noted as breaches from contractors.

	Regular employees	Contractors
Accidentally exposing, deleting, or modifying critical data	44%	48%
Access to data and resources that are not necessary to do their job	36%	46%
Using unsecured networks/Wi-Fi	32%	42%
Using personal devices that are against policy	39%	40%
Data copied to insecure devices	42%	40%
Poor password management and/or weak passwords	44%	36%
Device loss/thefts	38%	35%
Sharing passwords	28%	34%
Not applying/installing security updates	32%	32%
Incorrect disposal of hardware	16%	20%

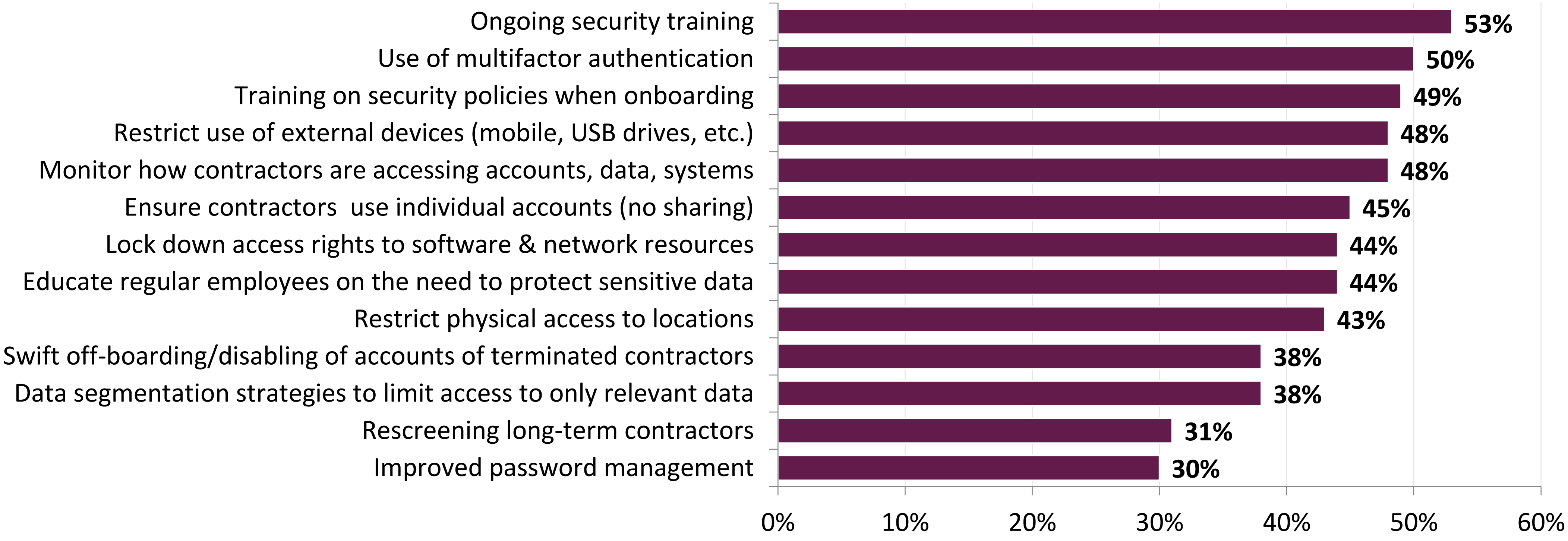
N=200
Note: Multiple responses allowed

■ = top three □ = statistically significant difference

Q *What are the most common causes of accidental/careless insider breaches from regular employees and contractors/temporary workers?*

Best Ways to Reduce Risks

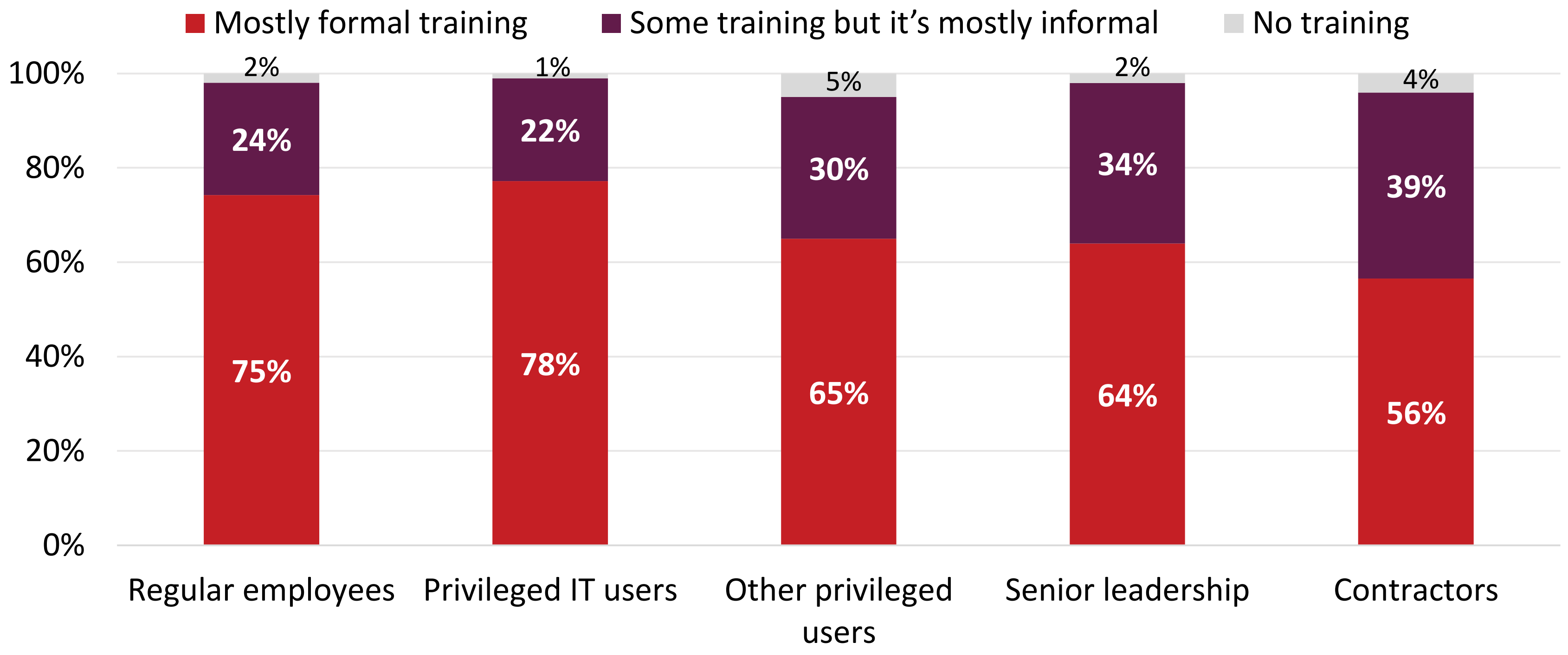
About half indicate the best way to reduce the risks associated with contractors is training (onboarding and ongoing), multifactor authentication, restrictive use of external devices, and monitoring the access of accounts, data, and systems.



Q *What are the best ways to reduce IT risks that are often associated with using third-party contractors and/or temporary workers?*

IT Security Training by User Type

Three quarters note regular employees and privileged IT users are provided formal IT security training. Over half indicate contractors receive formal training as well.



N=200 Due to rounding percentages may not add up to 100%

Reasons for No Formal Security Training

48% - Investment is made for other types of IT security safeguards

46% - Takes time away from day-to-day responsibilities

43% - Too costly

35% - Upper management doesn't feel it is important

	Defense	Civilian
Upper mgmt. doesn't feel it's important	21%	45%

N=127
Note: Multiple responses allowed

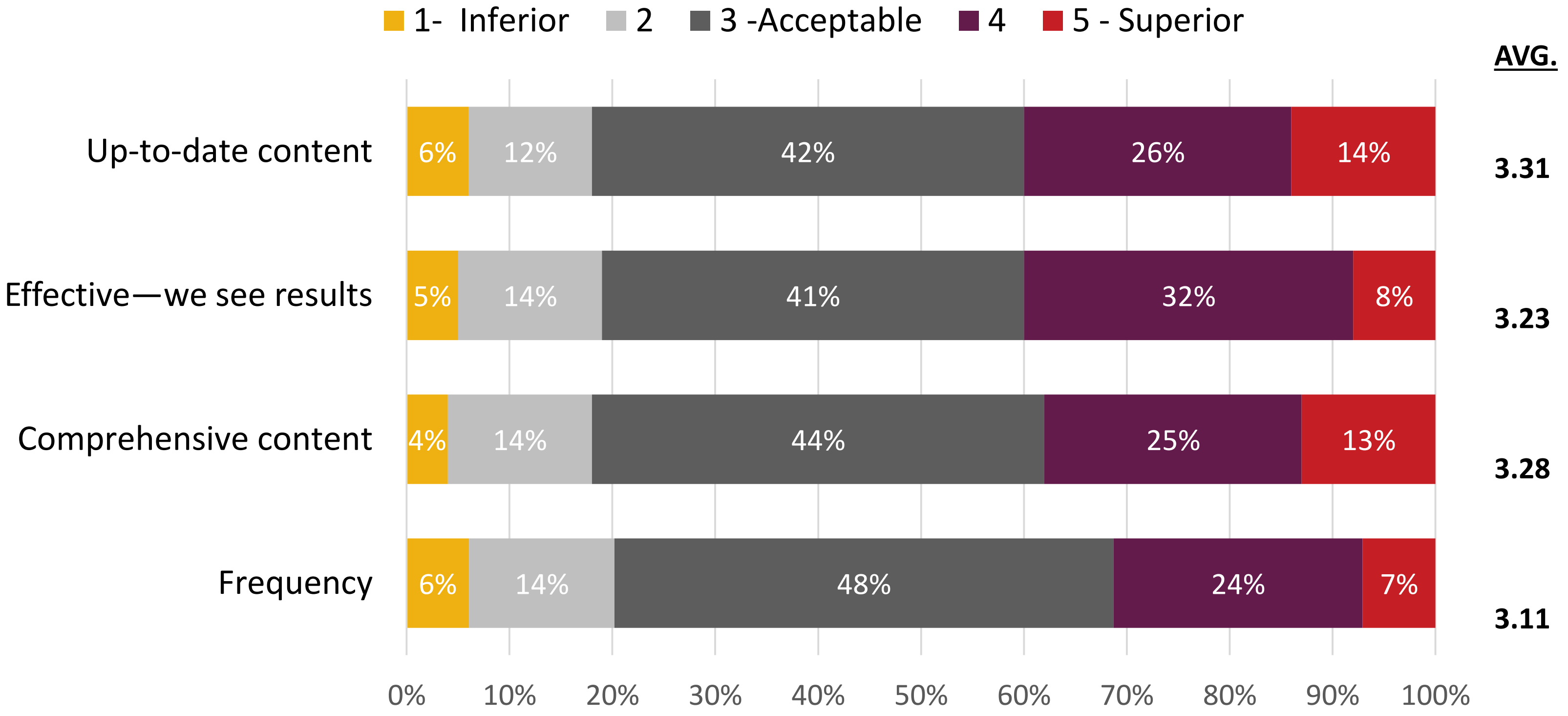
□ = statistically significant difference

Q *What type of IT security training is provided to the following types of individuals at your organization? What are the reasons your organization does not use formal IT security training for all types of workers?*

solarwinds

Rating of Agency IT Security Training Efforts

On average, respondents rate their IT security training efforts “acceptable” though defense respondents give higher ratings for comprehensiveness and effectiveness relative to those from civilian agencies.



4/5-Superior	Defense	Civilian
Comprehensive content	47%	31%
Effective—we see results	48%	34%

□ = statistically significant difference

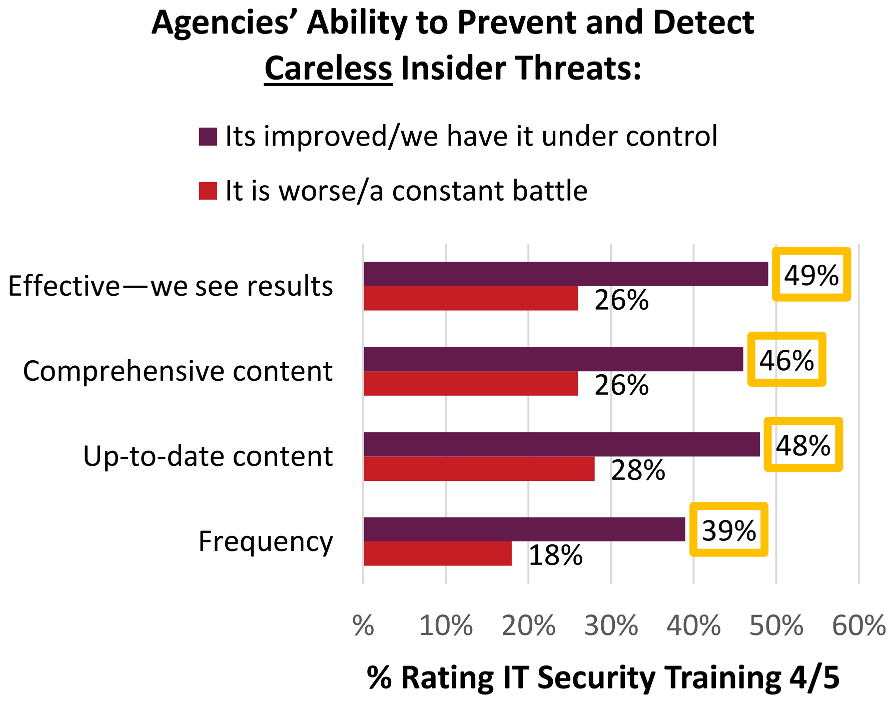
N=200 Due to rounding percentages may not add up to 100%

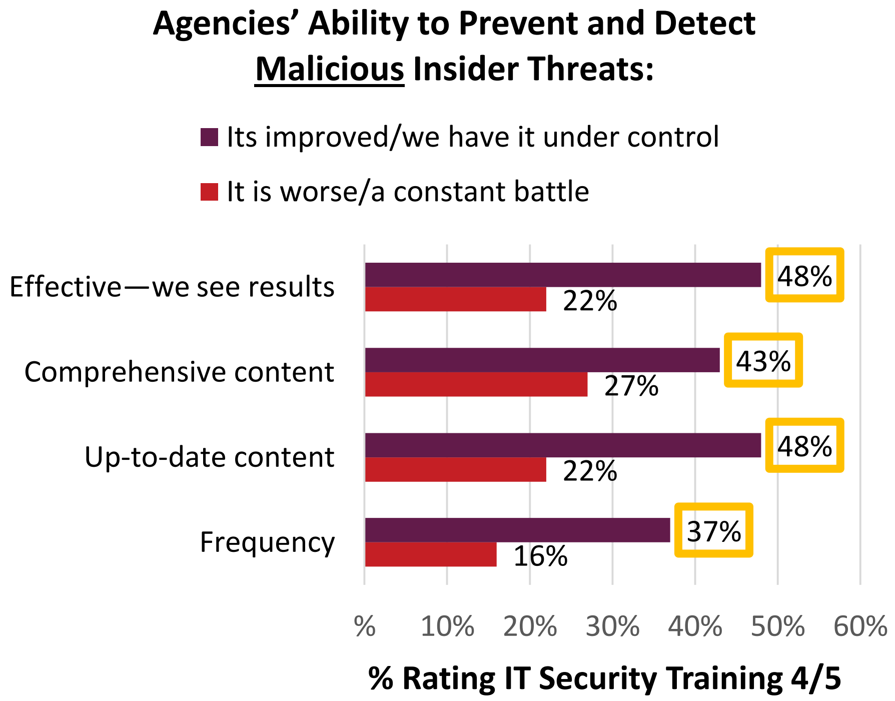
Q *How would you rate your organization’s overall IT security training efforts on the following factors?*

solarwinds

Training Ratings By Ability to Prevent Insider Threats

Respondents that indicate their insider threats (both careless and malicious) have improved or are under control are more likely to rate their IT security training highly.





□ = statistically significant difference

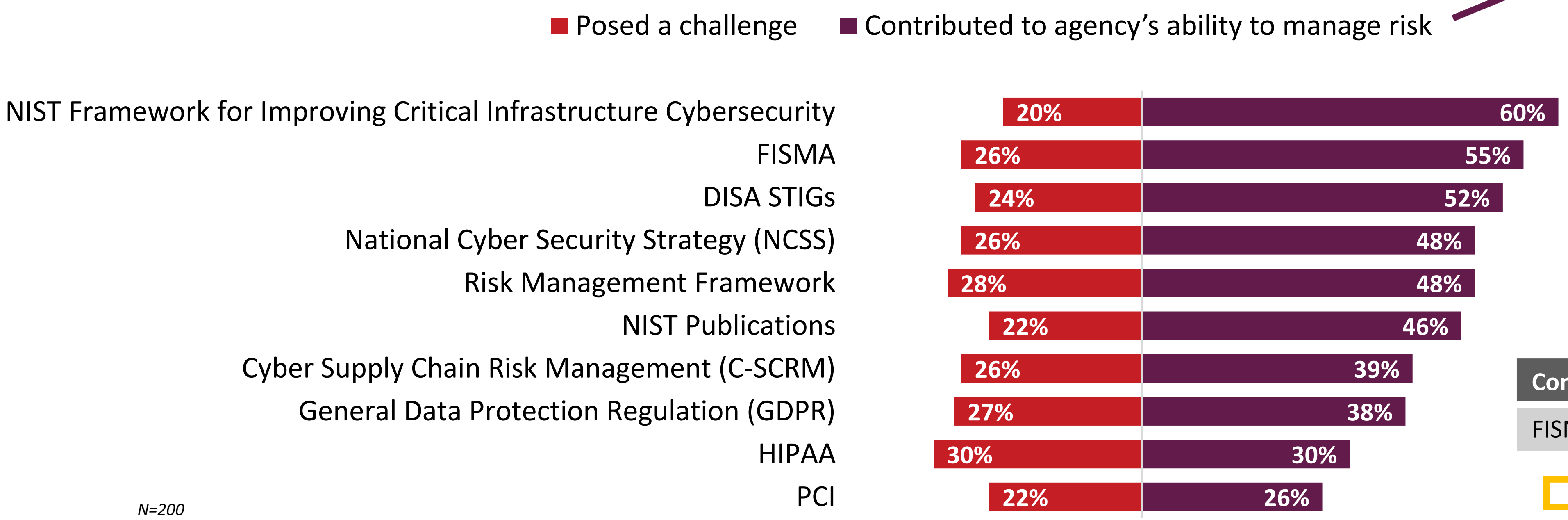
N=200

How would you rate your organization's overall IT security training efforts on the following factors?
How would you describe your organization's ability to prevent and detect insider threats over the last two years?

Managing Risk

Respondents most often note NIST Framework for Improving Critical Infrastructure Cybersecurity and FISMA as contributing to agencies' ability to manage risk.

Overall, more federal IT decision makers currently view regulations and mandates as contributing to their agencies' ability to manage risk as part of their overall security posture relative to 2017 (24%).



N=200

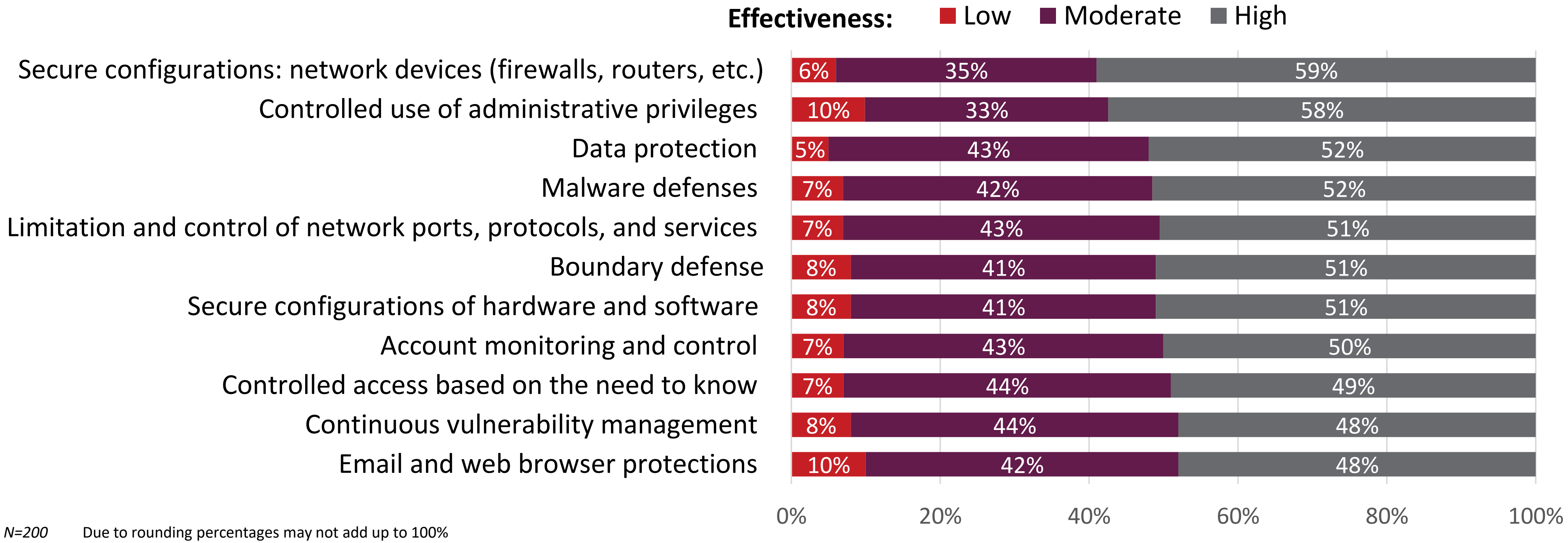
Contributed	Defense	Civilian
FISMA	45%	62%

□ = statistically significant difference

Have the following specific plans, processes, regulations, and mandates contributed to your agency's ability to manage risk as part of its overall security posture in the past 12 months? Or have they posed more of a challenge?

CIS Framework – Effectiveness of Current Practices

There is little variance in respondents' opinions of the effectiveness of their organization's current tools, policies, and practices at improving security for the CIS security framework controls. The highest effectiveness ratings are seen for secure configurations of network devices and controlled use of administrative privileges.

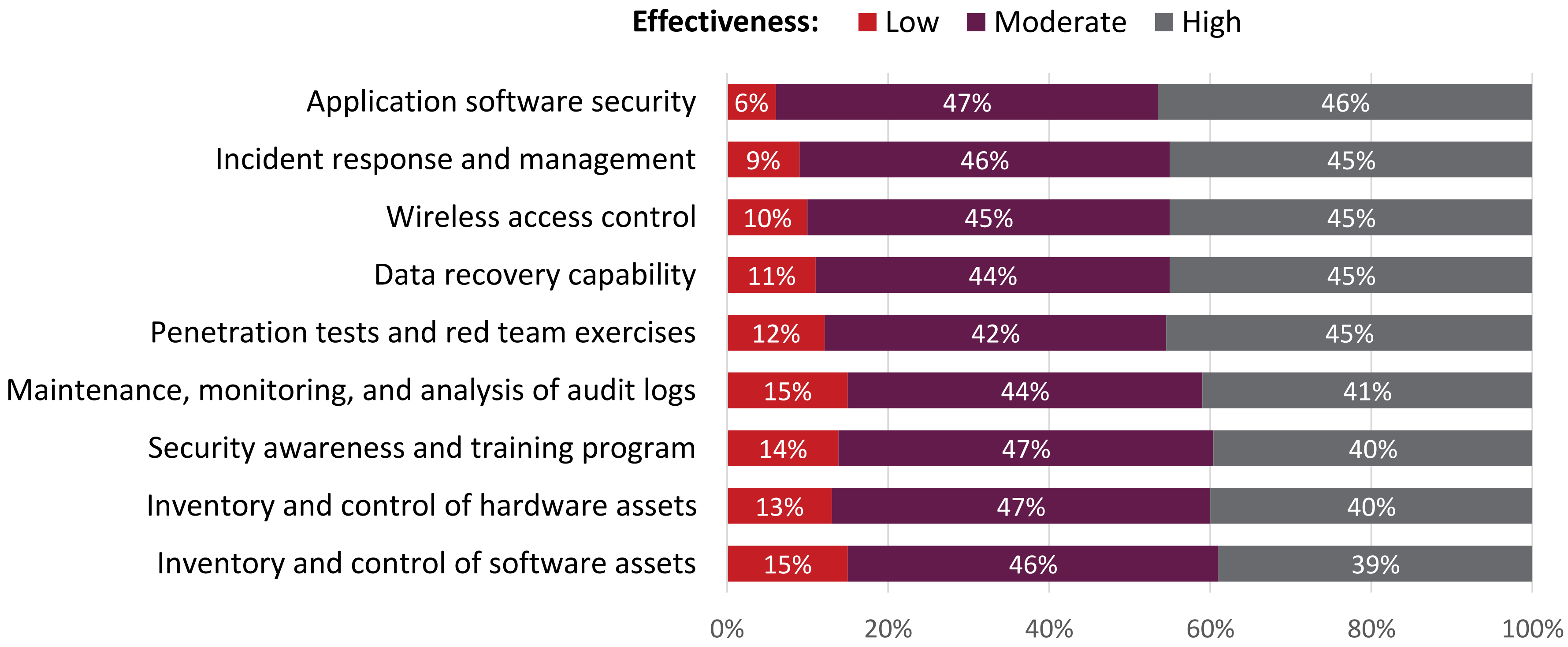


N=200 Due to rounding percentages may not add up to 100%

Q *In your opinion, how effective are your organization's current tools, policies, and practices at reducing risk and improving overall IT security posture for each of the following Center for Internet Security (CIS) security framework controls?*

CIS Framework – Effectiveness of Current Practices

Though few rate their organization's effectiveness as low, the greatest proportion is seen for maintenance, monitoring, and analysis of audit logs, security training programs, and the inventory and control of hardware and software assets.



N=200 Due to rounding percentages may not add up to 100%

Q *In your opinion, how effective are your organization's current tools, policies, and practices at reducing risk and improving overall IT security posture for each of the following Center for Internet Security (CIS) security framework controls?*

Examples of Comments

We went cloud crazy and are also overly reliant on contractors. The former directly, and immediately, shuts down over 90% of our business operations when there is no internet connectivity. The latter are government-paid insider threats whose sole mission is partial solutions, and expanding long-term business, and withholding key info, services, or other from the naive and ignorant government client in order to secure future funding.

LOGISTICS, NAVY

Automated user training covers the basics, but sets a very low baseline. We can do better.

DIVISION CHIEF, ARMY

There is redundant and inefficient security on endpoints—specially desktops and notebooks. Traditional antivirus and scanning is not keeping up. It also adds tremendous processing overhead and degrades user experience. New ways of delivering security, such as network analytics and threat detection via AI, must be considered soon.

IT DIRECTOR, ARMY

We seem to be doing a rather good job of protecting public records. Need better upfront training for employees.

SYSTEMS LAN MANAGER, SSA

There is a fundamental failure of mid-level and senior-level leadership to grasp the need for security. They tend to feel that security is an impediment to doing the scientific mission.

IT OFFICER, NIH

Interest in IT security occurs only after an incident. Then after the dust settles (investigations, reviews, numerous warning and alert memos), it’s back to the same business as usual. No true concrete steps are taken, in my opinion.

DIRECTORATE EXECUTIVE, ATF

Security guidance needs to be produced internally much faster—how to take external direction and policy and provide guidance to program managers, operators, and developers. Now the solutions are being implemented with a best guess and the guidance comes next, leading to either compliance failures or the need to redo everything.

IT DIRECTOR, DOD

We need more consequences for programmers and others who consistently resist, break, or evade best IT security practice.

TEAM LEADER, HHS

Q *Please feel free to share any other comments or concerns regarding your agency’s unique security challenges or success stories.*

Key Takeaways

Careless insider threats continue to be a top security threat at federal agencies.

- There has been no significant decline or change in the top three threat sources to federal agencies. These include careless/untrained insiders, foreign governments, and the general hacking community.
- Careless insider threats continue to be the number one source of IT security threats. Significantly more respondents note their ability to detect and prevent careless insider threats as a constant battle relative to malicious insider threats. More believe they have seen improvement or have malicious insider threats under control.
- Organizations point to a lack of training, use of more devices, and the volume of network activity as the most common reasons behind careless or malicious insider threats. Notably, increased use of cloud apps and infrastructure is also one of the top reasons for malicious threats.

Key Takeaways

Strategies relating to policy, process, and basic security hygiene provide the foundation to improving and controlling insider threats at federal agencies. A variety of advanced security tools add to that success.

- Improved strategy and processes to apply security best practices is noted most often as a reason careless insider threats have improved or remained in control. Employee background checks is noted most often as a reason malicious insider threats have improved or remained in control.
- Regarding basic security hygiene, end-user security awareness training is noted most often as a reason careless insider threats have improved or remained in control. Patching is noted most often for malicious insider threats.
- Regarding advanced security tools, intrusion detection and prevention tools is noted most often as a reason careless and malicious insider threats have improved or remain in control. Network traffic encryption is also a top reason noted for malicious insider threats.

Key Takeaways

Revealing a difference of opinion, about half believe IT security risks are greater when dealing with contractors and temporary workers, while slightly less than half consider the risks about the same.

- Regardless of the difference in opinion of what type of employee has a higher security risk, the top cause associated with careless insiders is the same: accidently exposing, deleting, or modifying critical data.
- Relative to regular employees, access to resources that are not necessary to do their job and using unsecured networks/Wi-Fi are more frequently noted as breaches from contractors.
- About half mention the best way to reduce the risks associated with contractors is through onboarding and ongoing training, multifactor authentication, restricted use of external devices, and monitoring the access of accounts, data, and systems.

Key Takeaways

IT security training is seen as a way to reduce IT risks associated with contractors and a top basic security hygiene practice necessary to prevent and detect careless insider threats.

- The majority note implementing formal IT security training for all types of employees. Regular employees and privileged IT users are more likely to receive formal training than contractors
- On average, respondents rate their IT security training efforts acceptable. Though respondents rating their organizations’ IT security training highly are also more likely to mention their ability to prevent and detect insider threats has improved or is under control.

Contact Information

Laurie Morrow, VP, Research Strategy, Market Connections, Inc.

LaurieM@marketconnectionsinc.com
703-378-2025

Lisa M. Sherwin Wulf, Senior Director of Marketing - Government, SolarWinds

Lisa.SherwinWulf@solarwinds.com
703-386-2628
www.solarwinds.com/government
LinkedIn: SolarWinds Government

solarwinds government • Market Connections® Research you can act on.