solarwinds

SolarWinds Cybersecurity Survey 2022

What is the greatest cybersecurity concern for your peers?

Arthur Bradway

Solutions Architect, Government & Education

Arthur has over 22 years of professional experience in the information technology industry providing sales engineering support for government and education clients, with over five years of experience supporting clients at SolarWinds. During his career, Arthur has provided pre- and post-sales support for government and education clients for networking, performance monitoring, and software engineering products.

Arthur has solid technical knowledge, with business experience in enterprise networking and application architecture. He has excellent problem-solving and leadership skills to deliver both technical and business solutions. He effectively manages and mentors cross-functional teams, and he has successfully managed and deployed complex IT projects within budget and on schedule.

Speaker Photo

Agenda

Cybersecurity Survey 2022: What Is the Greatest Cybersecurity Concern for Your Peers?

- The Cybersecurity Climate Today
- The Seventh Annual SolarWinds® Cybersecurity Survey
- Results & Key Takeaways
- What to Expect in the Future
- Secure by Design: SolarWinds Product Mix
- Q&A
- Resources and Contact Information

The Cybersecurity Climate Today

Cybersecurity Today: Current State of Affairs

The impact of our current geopolitical climate

Bloomberg
U.S. Cyber Firms Seek Tech Standards as Russian Hacking Fears Grow
3h ago SUBSCRIPTION

BBC NEWS
Ukrainian power grid 'lucky' to withstand Russian cyber-attack
1h ago

TechCrunch
Ukraine disrupts attempt by Russian hackers to take down energy provider
4h ago

VICE
Russia's 'Infamous Sandworm' Hackers Tried to Attack Ukraine's Energy Company
3h ago

WIRED
Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine
3h ago

ZDNet
Terrible cloud security is leaving the door open for hackers. Here's what you're doing wrong
3h ago

NBC NEWS
Ukraine foiled Russian cyberattack that tried to shut down energy grid
3m ago · Kevin Collier

The Register
Industrial cybersecurity group gathers lobbying force
1h ago

TechCrunch
Panasonic says Canadian operations hit by 'targeted' cyberattack
1d ago

Bloomberg
Russian Hackers Tried Damaging Power Equipment, Ukraine Says
38m ago SUBSCRIPTION

VICE
T-Mobile Secretly Bought Its Customer Data from Hackers to Stop Leak. It Failed
1h ago

Roll Call
Congress aims for next step to safeguard critical infrastructure
7h ago

CBS NEWS
Russian hackers targeted Ukrainian power company, say Ukrainian officials
1h ago

How Russia's Invasion Triggered a US Crackdown on Its Hackers

MIND MATTERS
Cybersecurity: Put a Lid on the Risks. We Already Own the Lid
22m ago

Cybersecurity Survey:

Overview & Results

Methodology

SolarWinds contracted Market Connections to design and conduct an online survey among 200 federal, 100 state and local, and 100 education decision-makers and influencers in October 2021. SolarWinds was not revealed as the survey sponsor.

Market Connections®
Research you can act on.

PRIMARY OBJECTIVES:

- Determine challenges faced by public sector IT professionals and sources of IT security threats
- Evaluate the importance of IT security products, solutions, and services and rate investment priorities
- Determine familiarity with the White House Cyber Security Executive Order and the perceived impact of its objectives
- Identify if organizations use a zero-trust approach to IT, their motivations and deterrents, and evaluate the Principle of Least Privilege (PoLP)
- Measure the use of teleworking before COVID-19, currently, and in future

Key Findings

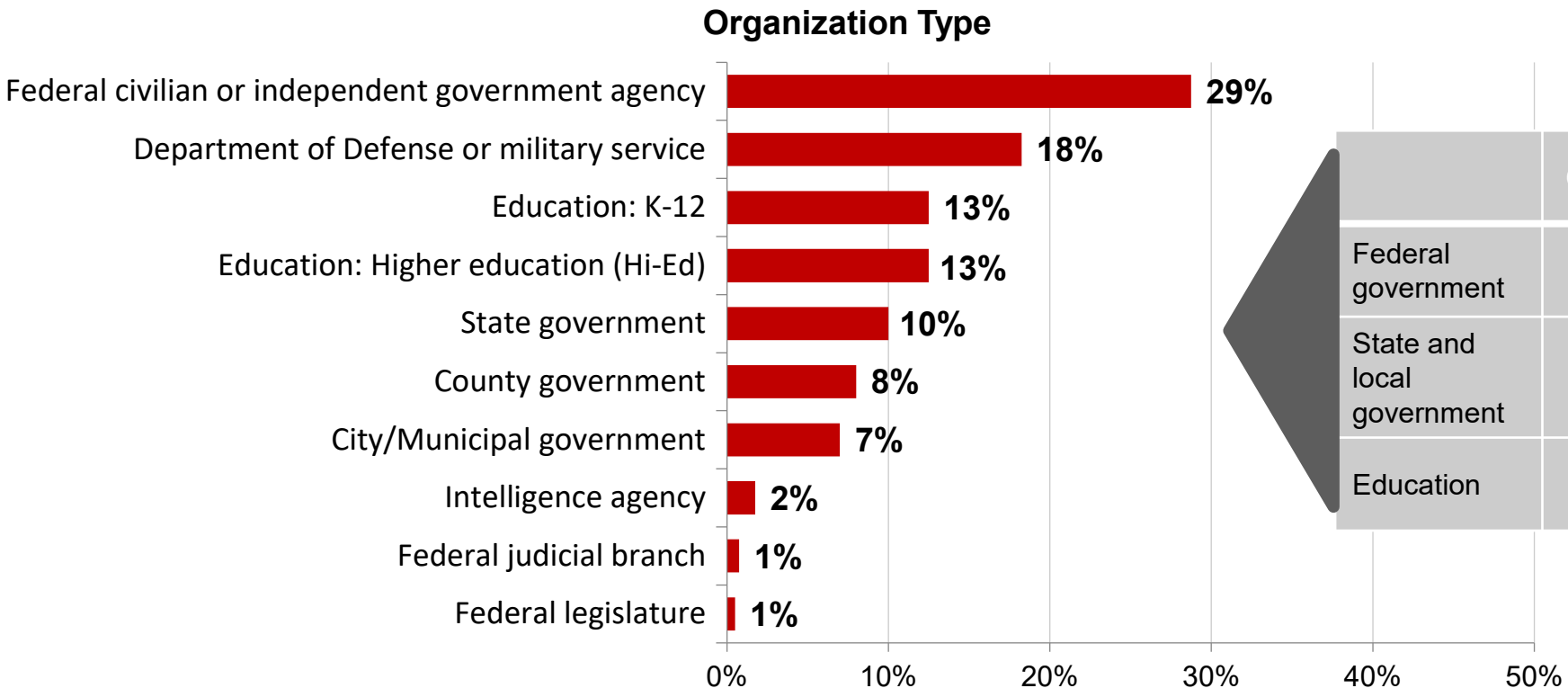
The general hacking community is the largest source of security threats at public sector organizations, followed closely by careless/untrained insiders and foreign governments

- Cybersecurity threats from foreign governments are responsible for the greatest increase in concern among public sector respondents
- Lack of training, low budgets and resources, and the expanded perimeter as a result of increased remote work continue to plague public sector security pros
- More than 75% of public sector respondents note their organizations rely on a formal or informal zero-trust approach
- Most public sector respondents realize the importance of IT security solutions and prioritize their investments highly in the next 12 months, with network security software being the top priority

Organizations Represented

Market Connections®
Research you can act on.

RESPONDENT CLASSIFICATIONS



	Count	Percent
Federal government	200	50%
State and local government	100	25%
Education	100	25%

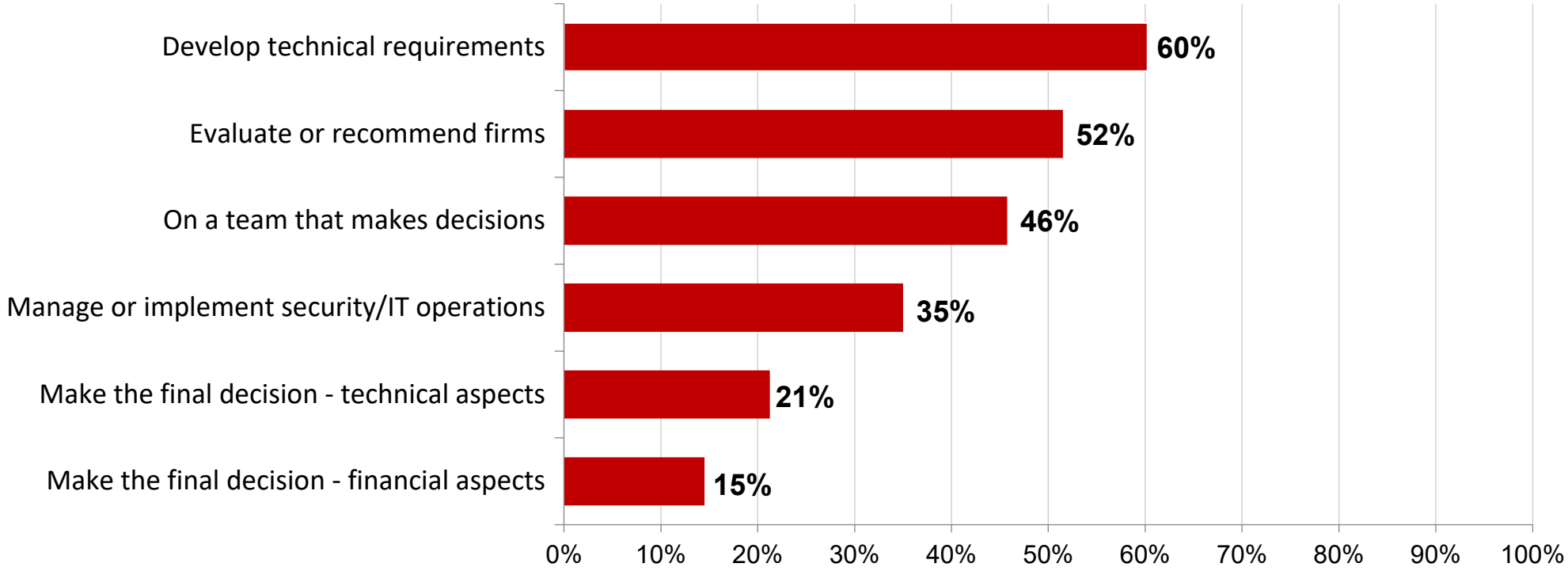
Which of the following best describes your current employer?

Decision-Making Involvement

Market Connections®
Research you can act on.

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

RESPONDENT CLASSIFICATIONS



Note: Multiple responses allowed

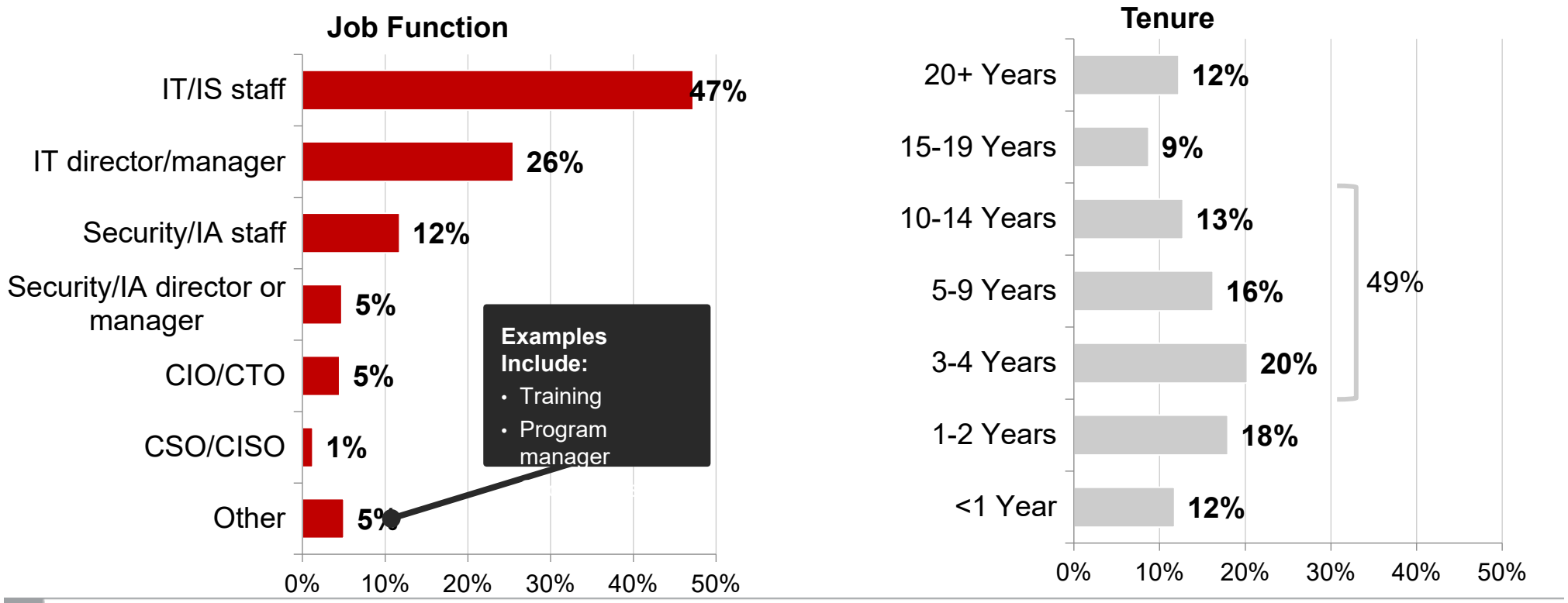
How are you involved in your organization's decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)

Job Function and Tenure

Market Connections®
Research you can act on.

- A variety of job functions and tenures are represented in the sample, with most respondents being IT staff who have worked at their current organization for three to four years; approximately half have a tenure of three to 14 years.

RESPONDENT CLASSIFICATIONS



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

IT Security Obstacles

Market Connections®
Research you can act on.

Budget constraints top the list of significant obstacles to maintaining or improving organizations' IT security.

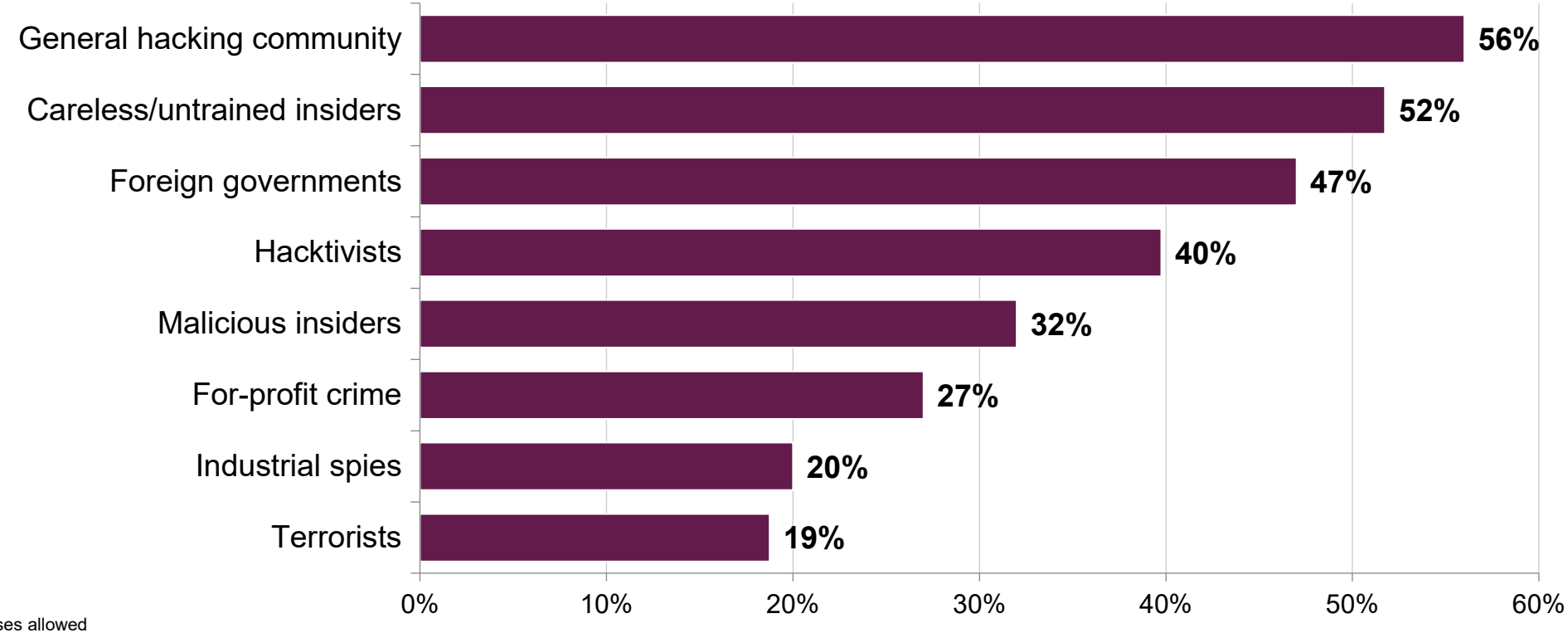
Competing priorities and a complex internal environment also impact IT security improvement.

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

Sources of Security Threats

Market Connections®
Research you can act on.

The general hacking community is the largest source of security threats at public sector organizations, followed closely by careless/untrained insiders.



Note: Multiple responses allowed

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

Sources of Security Threats—Federal Trend

Market Connections®
Research you can act on.

The top three sources of security threats have remained the same for the federal audience since 2014. There are significant increases from 2019 to 2021 for threats from foreign governments, the general hacking community, and hacktivists.

Federal	2014	2015	2016	2017	2018	2019	2021
Foreign governments	34%	38%	48%	48%	52%	48%	59%
General hacking community	47%	46%	46%	38%	48%	40%	56%
Careless/untrained insiders	42%	53%	48%	54%	56%	52%	52%
Hacktivists	26%	30%	38%	34%	31%	26%	42%
Malicious insiders	17%	23%	22%	29%	36%	29%	30%
For-profit crime	11%	14%	18%	17%	15%	20%	27%
Terrorists	21%	18%	24%	20%	25%	22%	23%
Industrial spies	6%	10%	16%	12%	19%	16%	23%

Note: Multiple responses allowed

= statistically significant difference 2019-2020

= top three sources

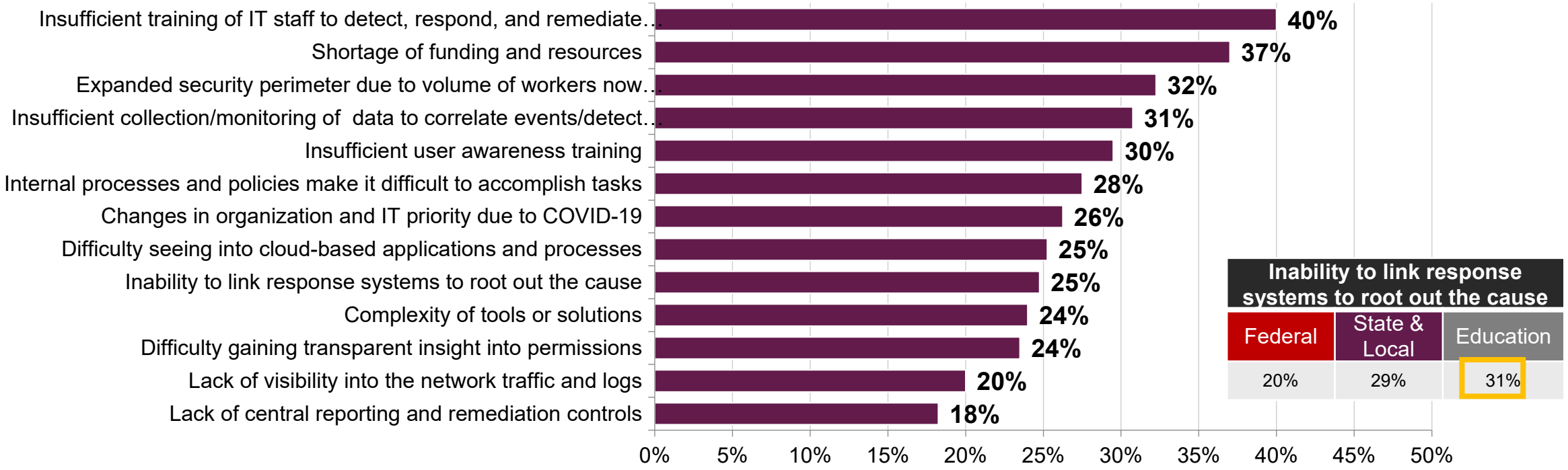
Q *What are the greatest sources of IT security threats to your organization? (select all that apply)*

Impediments to Detection/Remediation of Security Issues

Market Connections®
Research you can act on.

The top impediments to detection/remediation are insufficient training of IT staff and shortage of funding and resources.

Lack of visibility into network traffic/logs or lack of central reporting and remediation are less of an issue.



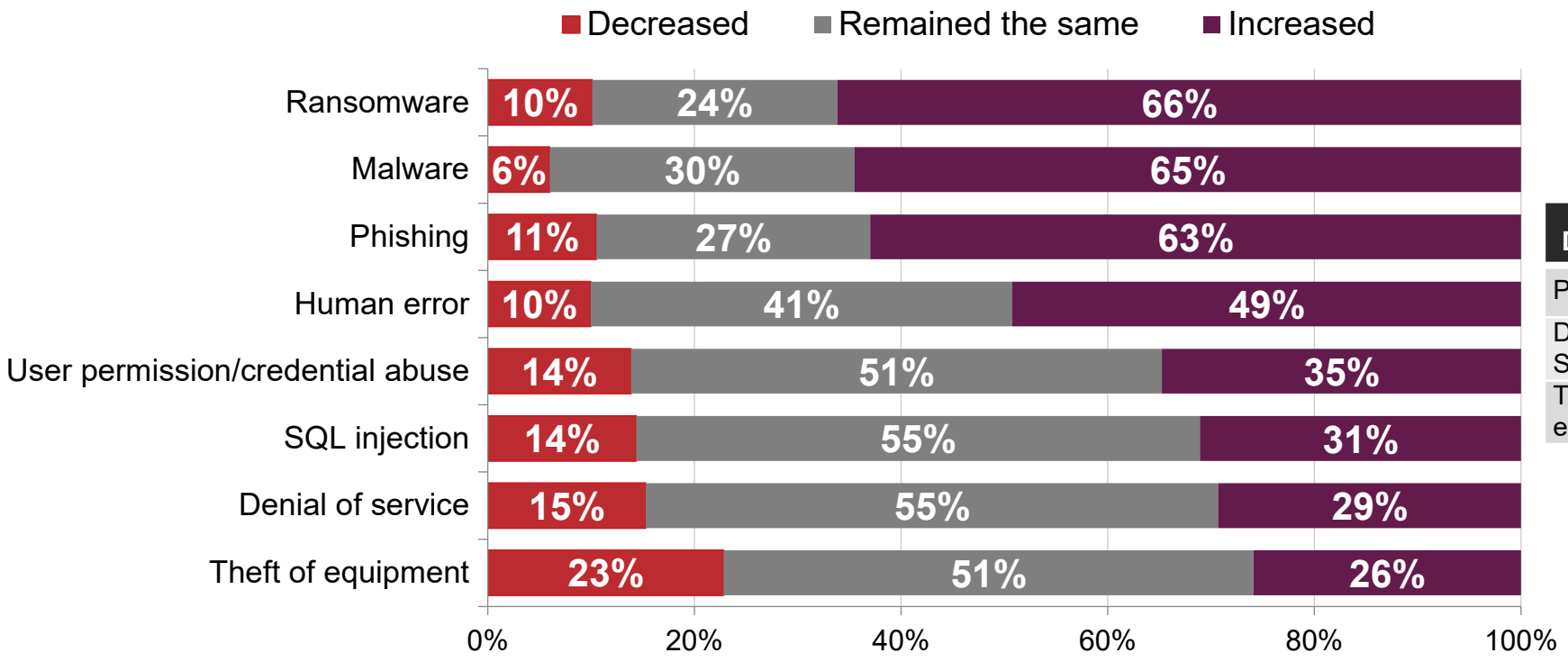
Note: Multiple responses allowed

Which of the following are the greatest impediments to detection and remediation of security issues at your organization?

Concern About Security Breaches Since 2020

Market Connections®
Research you can act on.

Increasing concerns about security breaches, with ransomware, malware, and phishing at the top of the list for the public sector.



Decreased	Federal	State & Local	Education
Phishing	6%	20%	10%
Denial of Service	12%	22%	15%
Theft of equipment	25%	24%	15%

= statistically significant difference

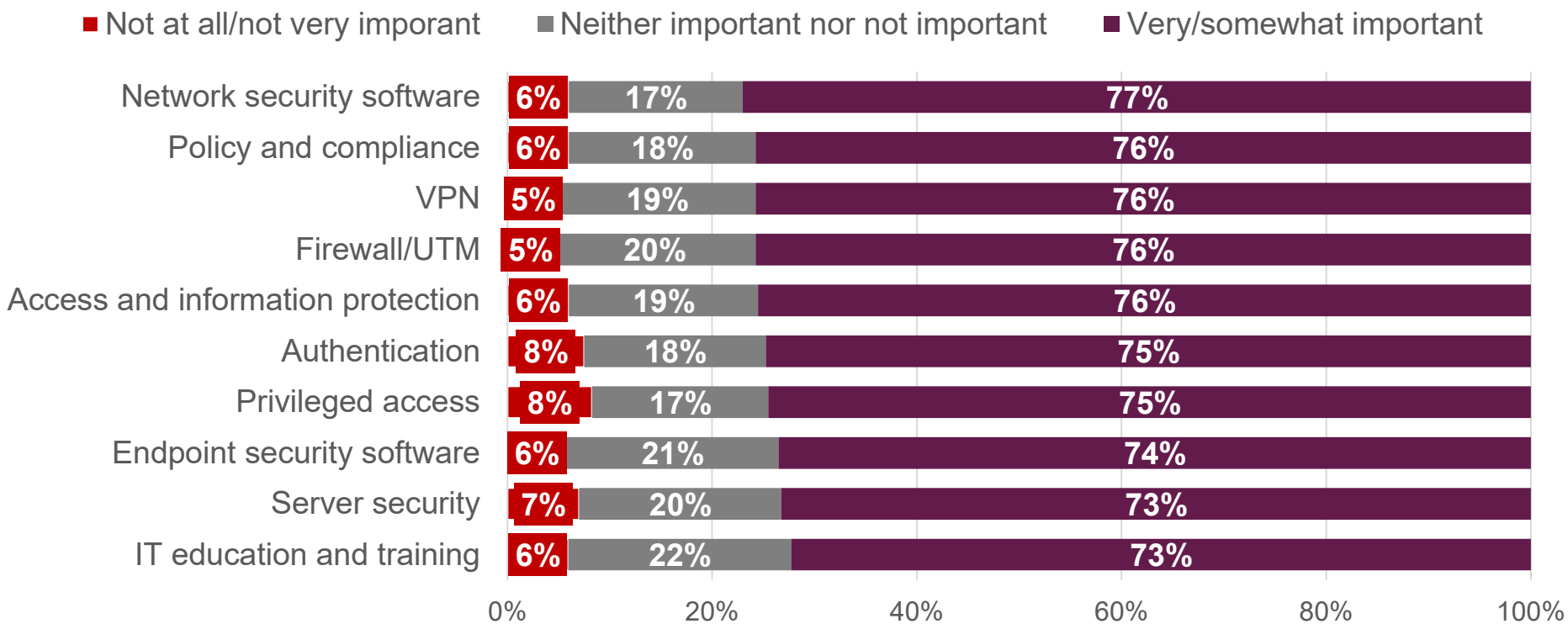
Note: Multiple responses allowed

Compared to 2020, has your level of concern changed regarding the following types of security breaches in 2021?

Importance of IT Solutions—Top 10

Market Connections®
Research you can act on.

When rating the importance of IT security products, solutions, and services in mitigating risk to the organization, network security software rates highest. Of note, all protocols garnered high importance ratings of 50% and up.



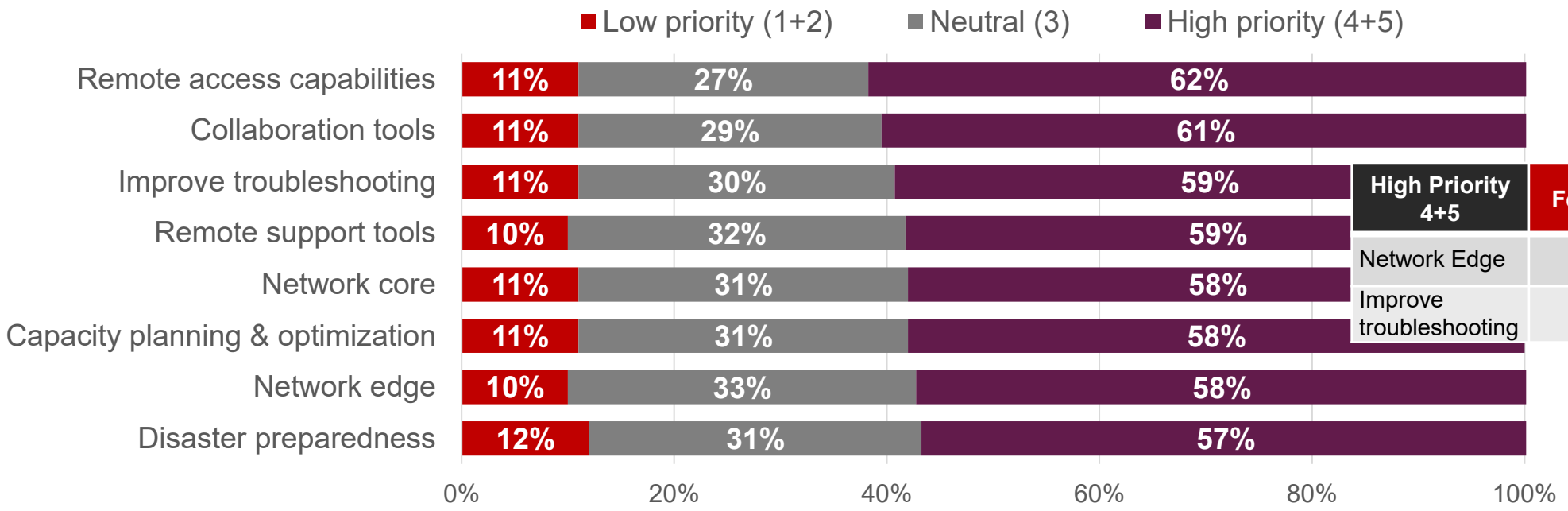
A greater proportion of federal respondents note 19 of the 30 solutions on the survey as important relative to state and local or education respondents.

How important are the following IT security products, solutions, and services in mitigating risk at your organization?

Investment Priorities: Infrastructure

Market Connections®
Research you can act on.

For infrastructure investment, public service organizations place remote access capabilities and collaboration tools as highest priority. All infrastructure investment options hold high priority in general.



High Priority 4+5	Federal	State & Local	Education
Network Edge	58%	48%	66%
Improve troubleshooting	59%	51%	69%

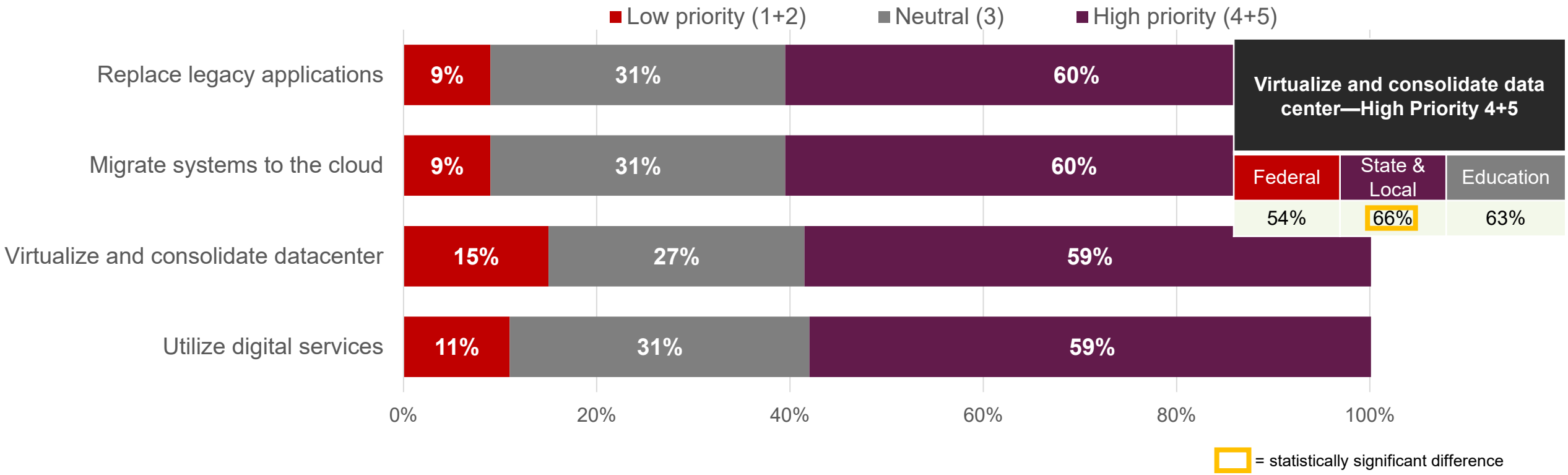
= statistically significant difference

What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

Investment Priorities: IT Modernization

Market Connections®
Research you can act on.

Like other investment priorities, IT modernization categories rate as high-priority. Replacing legacy applications and migrating systems to the cloud hold highest importance.



What are your organization's main investment priorities for the next 12 months (either budget and/or personnel resources)?

The U.S. Government's Response

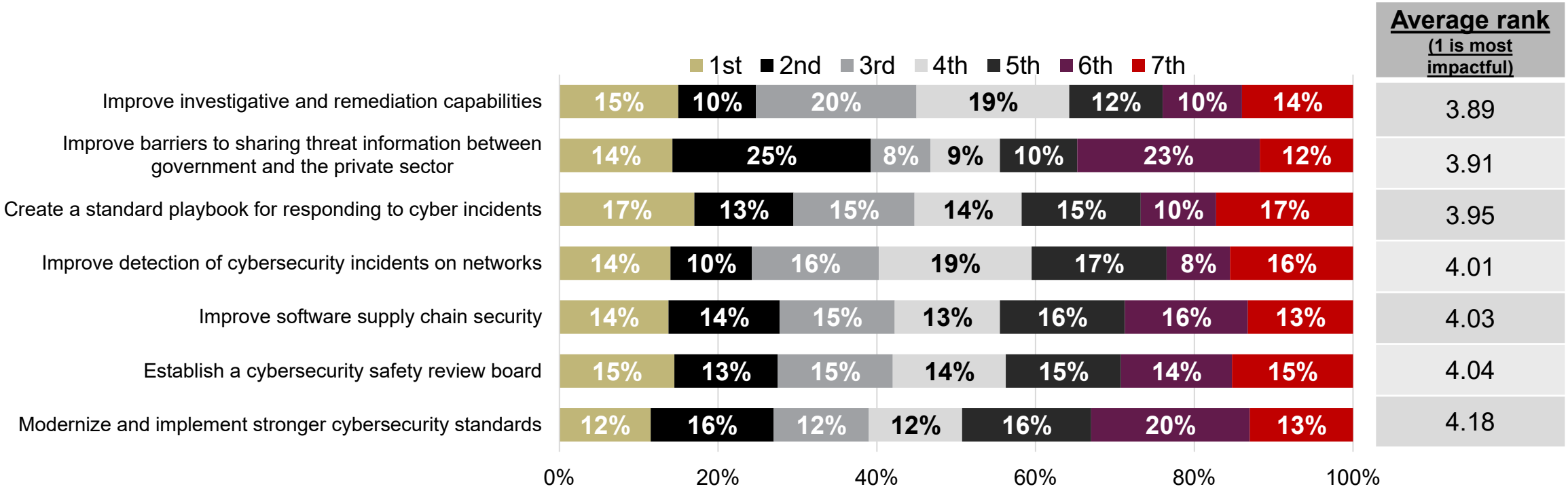
Federal Government mandates, executive actions, breach notifications, public-private partnerships, and more

THE WHITE HOUSE	FACT SHEET: Act Now to Protect Against Potential Cyberattacks	Executive Order on Improving the Nation's Cybersecurity
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY	CISA, FBI and DOE Publish Advisory with Cyber Activity Used by Indicted Russian State-Sponsored Actors	Expansive Federal Breach Reporting Requirement Becomes Law
Homeland Security	Statement from Secretary Mayorkas on Cybersecurity Preparedness	Spending bill includes large funding increase to boost cybersecurity

Investment Priorities: Customer Experience and Digital Transformation

Market Connections®
Research you can act on.

The objectives of the Executive Order ranked as most impactful to improving organizations' cybersecurity and network protection are improving investigative and remediation capabilities and improving barriers to sharing threat information.



The White House's Cyber Security Executive Order includes multiple objectives. Regardless of your familiarity with the Executive Order, please rank the perceived impact of each objective as it pertains to improving your organization's cybersecurity and network protection. (Rank 1 as the most impactful, 2 is the second most impactful, and so forth.)

What to Expect: Looking Ahead

What to Expect in the Future

- Cybersecurity threats from foreign governments are responsible for the greatest increase in concern among public sector respondents.
- Lack of training, low budgets and resources, and the expanded perimeter as a result of increased remote work continue to plague public sector security pros.
- The COVID-19 pandemic drastically changed the work environment for many public sector employees. Though some employees returned to the physical office, large numbers teleworking in the future are expected.
- Most public sector organizations realize the importance of IT security solutions and prioritize their investments highly in the next 12 months, with network security software being the top priority.

Best Practices for Combating Insider Threats

- Know and protect your critical assets
- Develop a formalized insider-threat program
- Deploy solutions for monitoring employee actions and correlating information from multiple data sources
- Clearly document and consistently enforce policies and controls
- Incorporate malicious and unintentional insider-threat awareness into periodic security training for all employees

Build Security into Your Community

- Implement an approach styled after a Secure Development Lifecycle (SDL)
  - SDLs consist of the security processes and activities performed for every software release
  - Although conceived for development, their principles can be applied across your agency
  - For example, by agreeing upon standard security practices for processes that involve sensitive data, you can help instill Information Security (InfoSec) into your agency

Implement Strong IT Controls

- According to respondents in our Federal Cybersecurity Survey*, agencies with evidence of strong IT controls are more likely to possess the hallmarks of strong InfoSec environments
- IT controls consist of procedures or policies that help ensure technologies are being used for their intended purposes in a reasonable manner
  - General controls are used for essential IT processes, such as risk management, change management, security, and disaster recovery
  - Application controls are automatic actions the software takes to help ensure applications are used with authorization, and are properly maintained, monitored, and audited
- Monitoring and management tools can help configure security controls and help ensure effectiveness
- Building strong IT controls requires visibility into your agency's IT infrastructure

Deep Visibility into Agency IT Infrastructure

- Network, application, and system monitoring and management tools provide needed visibility
- These tools are designed to continuously collect data on IT operations and alert on anomalies
  - Performance baselines can help identify threats and provide constant and valuable insight into network activities
    - For example, you can identify irregular bandwidth usage, firewalls with high multicasts or discards, or servers with significant failed login attempts
  - Device tracking provides forensic data that can help locate, identify, and isolate threat sources, or enforce your BYOD/mobility policies
  - Infrastructure performance monitoring metrics can complement your other security tools to help detect and mitigate issues

Configuration Management and Auditing Support

- Configuration management tools can help inventory network device configurations, assess them for compliance, and automate change and configuration management
- Configuration management tools can help implement configuration of security controls and help ensure effectiveness
- Many infrastructure monitoring and management tools also produce audit documentation and reports
- Compliance reporting documents progress and highlights areas that require corrective action

Additional Steps to Help Improve Your Security Posture

- Regularly update your infrastructure inventory
- Identify and protect critical assets
- Plan for and document process changes
- Leverage automated responses when appropriate
- Enforce policies and controls

Secure by Design:

SolarWinds Product Mix

Security Features

Log & Event Manager

A SIEM designed to make it easy to use logs for security, compliance, and troubleshooting

Patch Manager

Automated patching of Microsoft® servers and third-party apps

User Device Tracker

Automated device detection, tracking, and switch port management

Network Configuration Manager

Automated network configuration and change management software

IP Address Manager

Eliminate IP conflicts and save time managing DHCP, DNS, and IP addresses

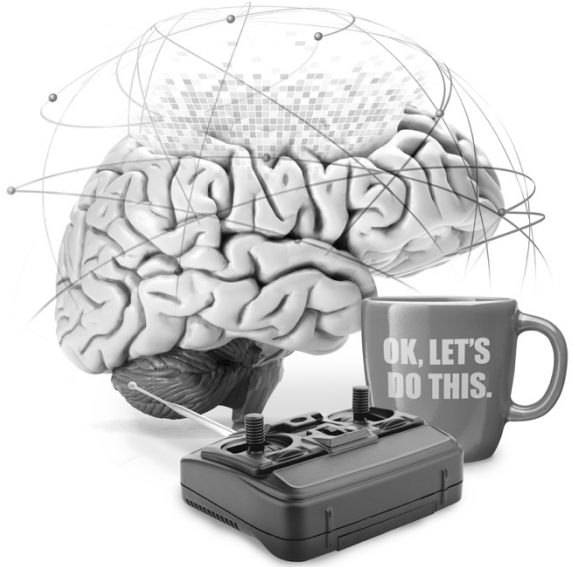
Access Rights Manager

Manage and audit user access rights across your IT infrastructure

Server Configuration Monitor

Track system and application changes in your systems environment

Q&A



Full Report

Get the full report here: https://www.solarwinds.com/resources/survey/solarwinds-public-sector-cybersecurity-survey-report-2021/delivery

Contact Information

Laurie Morrow

VP, Research Strategy, Market Connections

LaurieM@marketconnectionsinc.com

571.257.3845

Lisa M. Sherwin Wulf

Vice President of Americas Marketing, SolarWinds

Lisa.SherwinWulf@solarwinds.com

703.386.2628

Jessica Primanzon

Director Public Sector Marketing, SolarWinds

jessica.primanzon@solarwinds.com

301.672.5351

THANK YOU