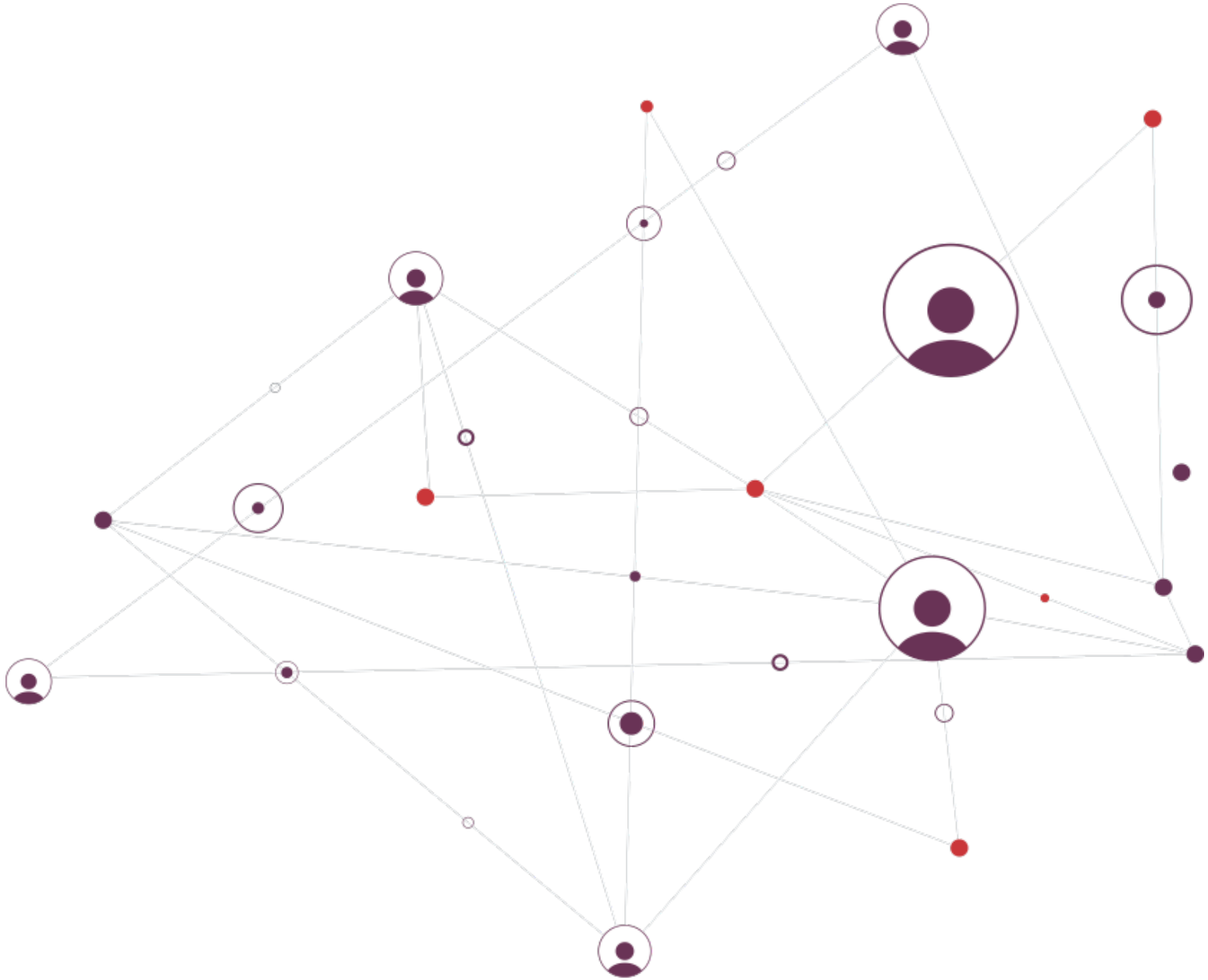
Market Connections™
Research you can act on.



Public Sector Cybersecurity Survey Report

February 2023

Presented to: solarwinds public sector

Methodology

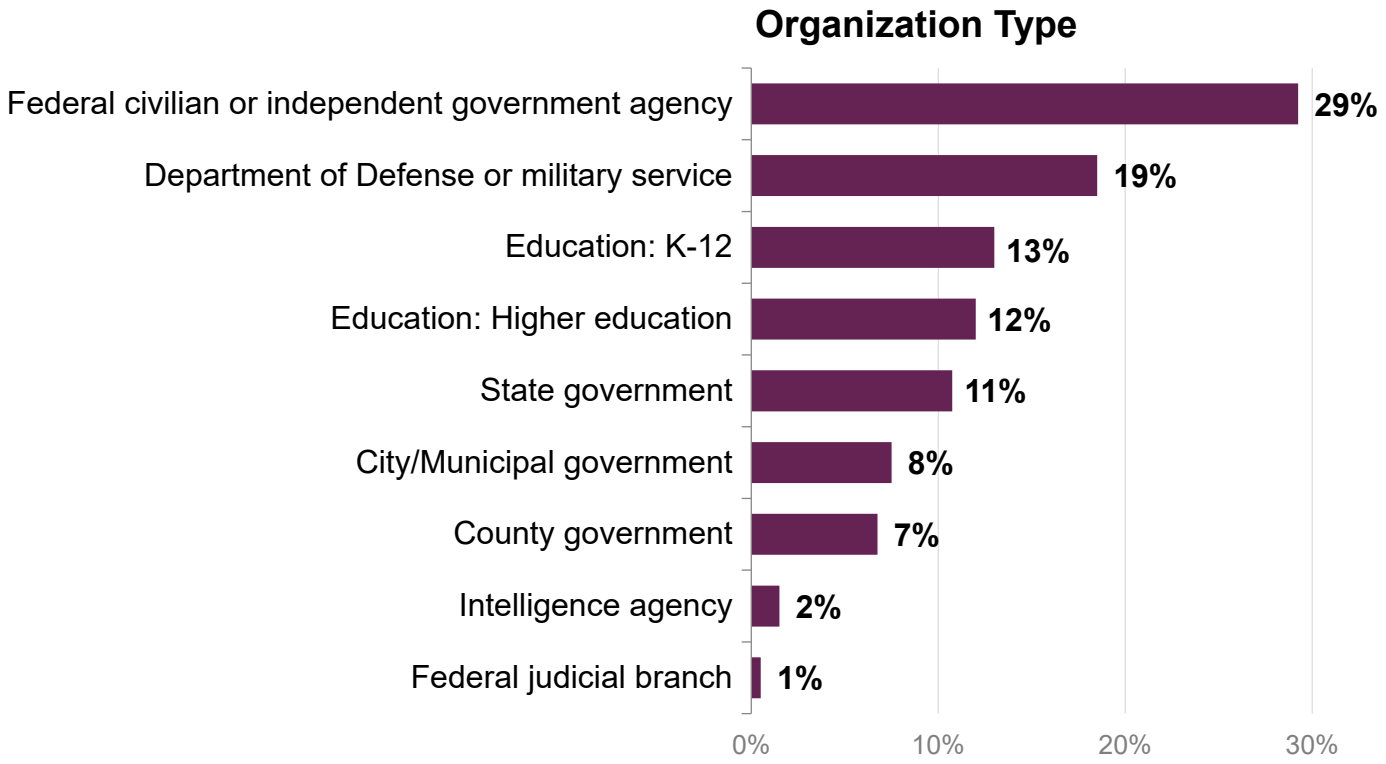
PRIMARY OBJECTIVES:

SolarWinds contracted Market Connections to design and conduct an online survey among 400 Federal, State and Local, and Education decision-makers and influencers in January 2023. SolarWinds was not revealed as the sponsor of the survey.

- Determine challenges faced by public sector IT professionals and sources of IT security threats
- Evaluate the current confidence and concerns of managing the IT environment
- Investigate barriers to the implementation of new IT security solutions
- Determine the importance and concerns with software supply chain security
- Identify if organizations are using a zero-trust approach to IT

Organizations Represented

- All respondents work for the public sector with half in the federal government, one-quarter in state and local government, and one-quarter in education.



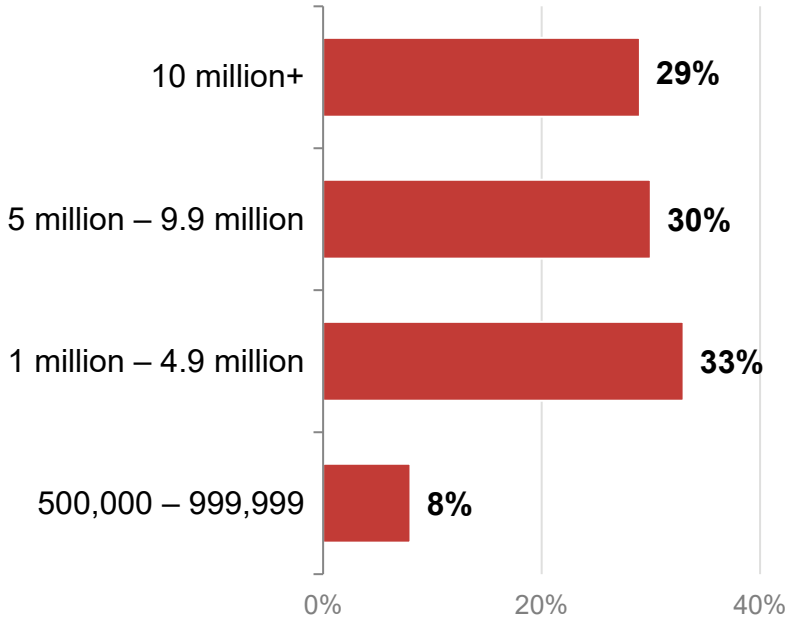
	Count	Percent
Federal government	200	50%
State and local government	100	25%
Education	100	25%

Which of the following best describes your current employer?

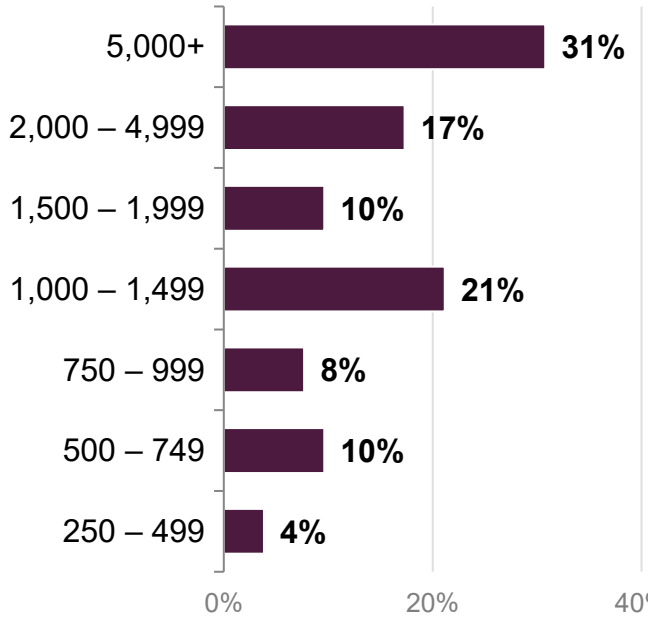
SLED Population and Enrollment

- A range of state and local populations and school enrollments are represented in the sample. Smaller state, local, and education (SLED) populations and enrollments were excluded from participating.

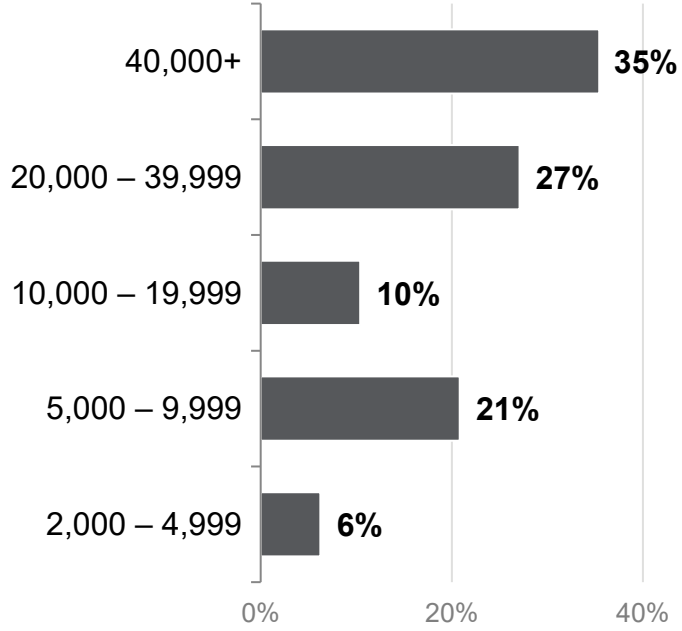
State and Local Population



K-12 Enrollment



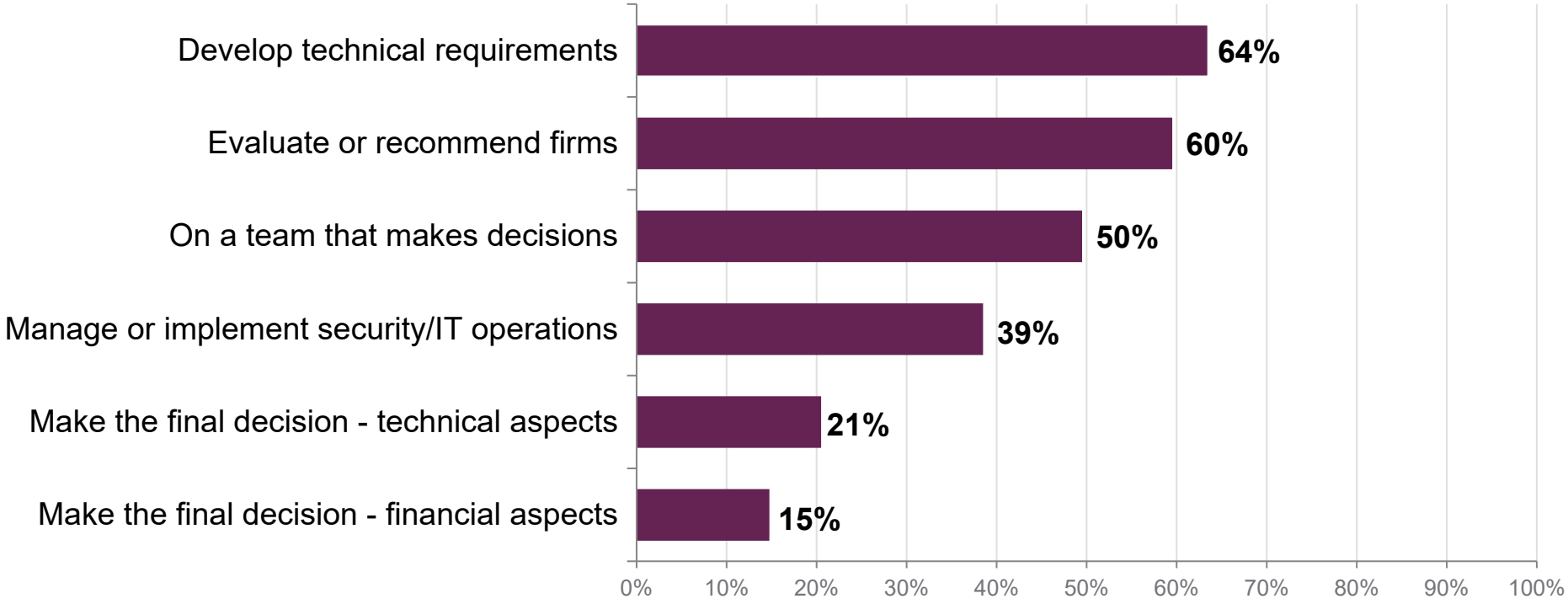
Higher Education Enrollment



[STATE, COUNTY, OR CITY GOVERNMENT] What is the estimated population of the ["state", "county," OR "city"] that you work for?
[EDUCATION: K-12] How many total students are currently enrolled at the school(s) where you are involved with IT security and/or IT operations and management?
[EDUCATION: HIGHER EDUCATION] How many students are currently enrolled at your college or university?

Decision-Making Involvement

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

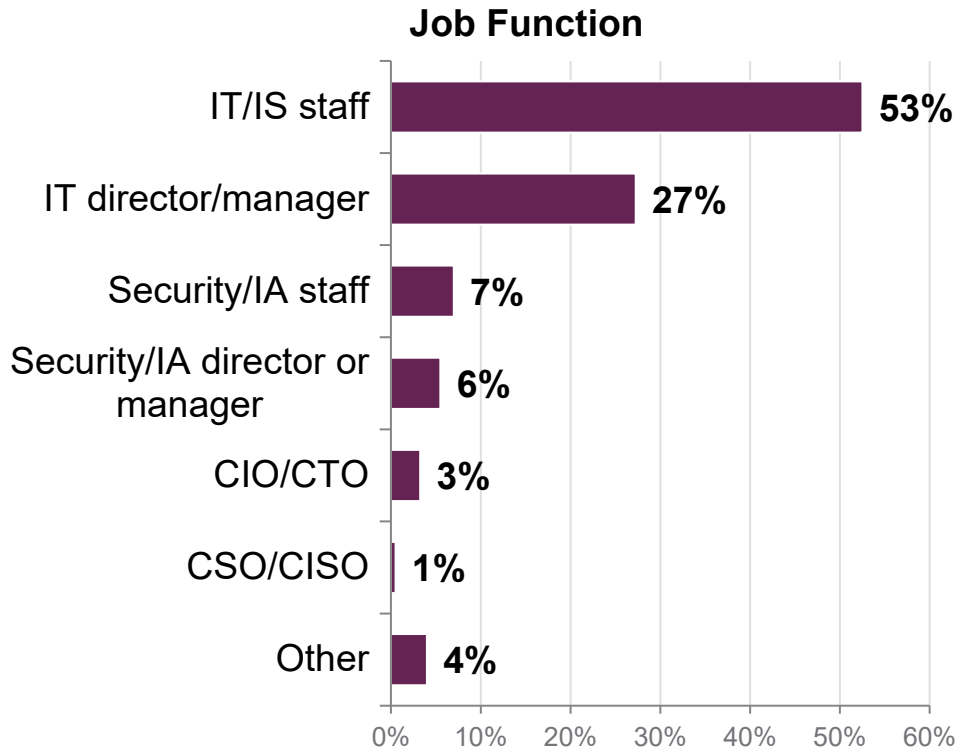


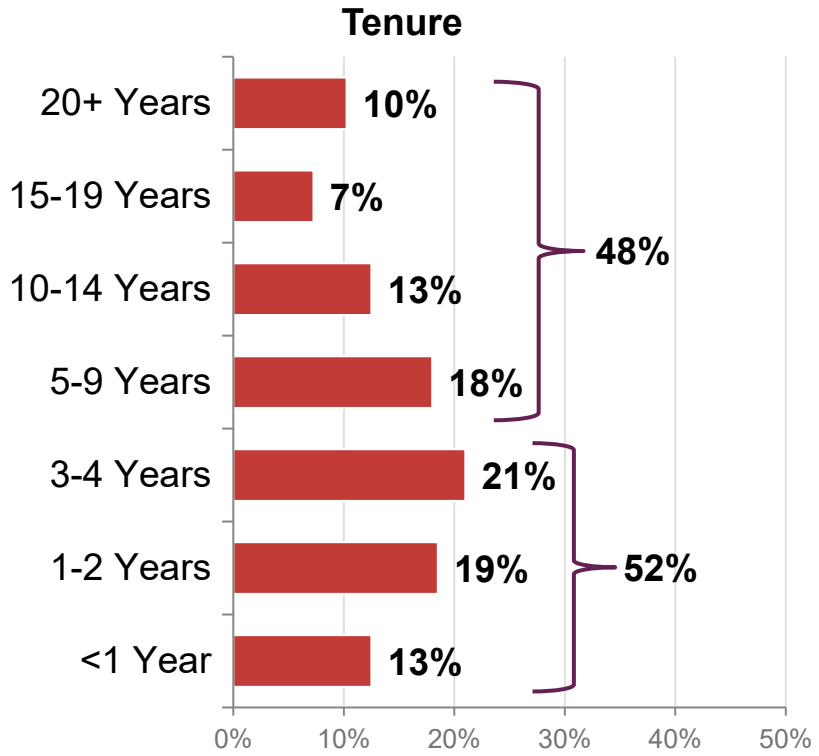
Note: Multiple responses allowed

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

- Most indicate their current job function is IT staff. A variety of tenure levels are represented with just over half (52%) having worked at their organization for less than five years and 48% having worked with their organization for five years or more.

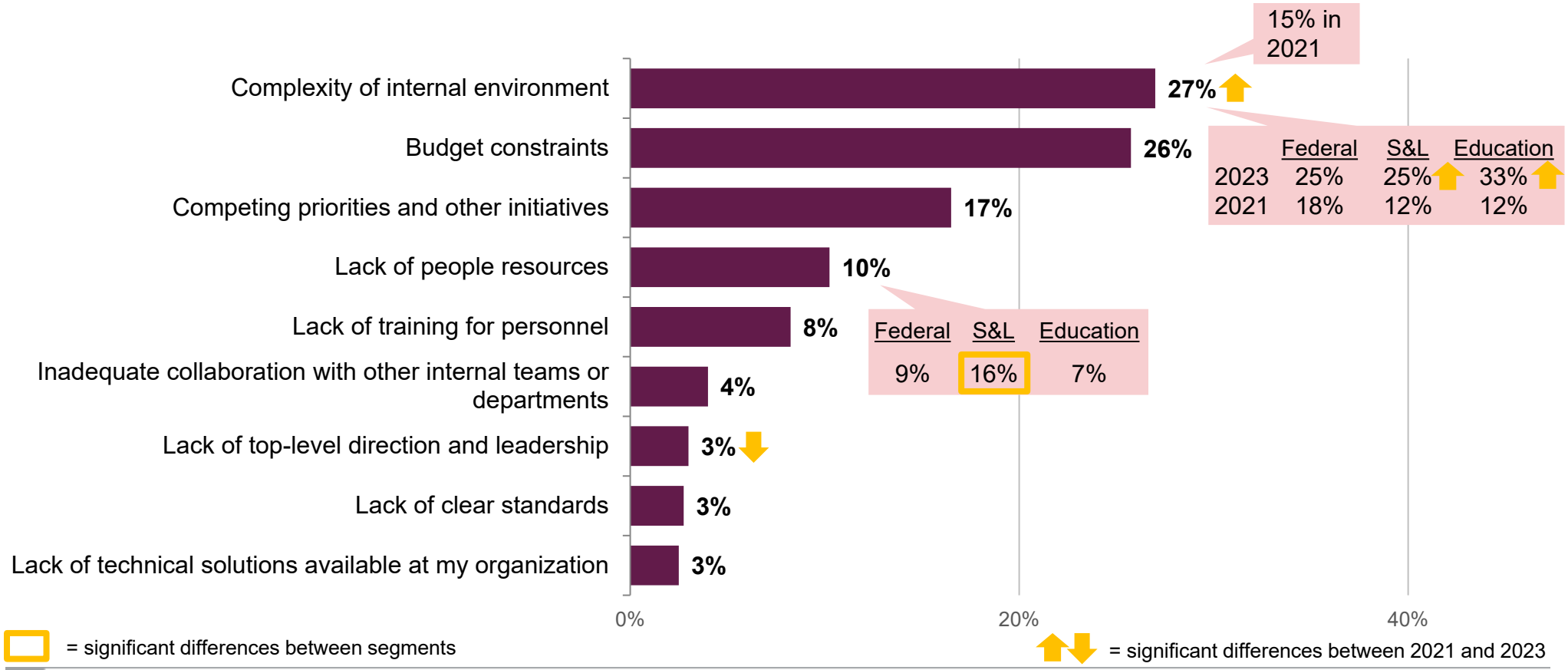




Which of the following best describes your current job title/function? How long have you worked at your current organization?

IT Security Obstacles

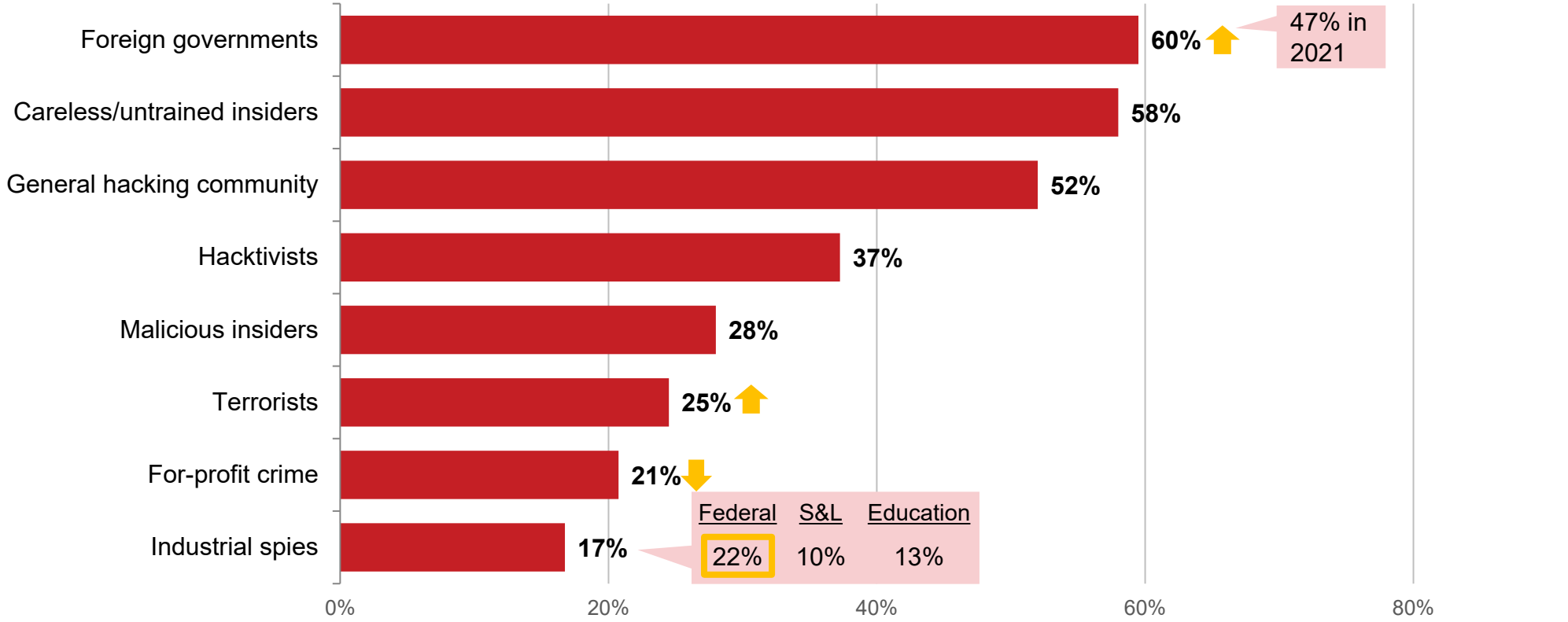
- Complexity of the internal environment rises to the top of the list of significant obstacles to maintaining or improving organization IT security. Budget constraints are a close second.



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

Sources of Security Threats

- With a significant increase from 2021, foreign governments rise to the top as the greatest source of IT security threats to organizations. Careless/untrained insiders fall in a close second. In 2021, the general hacking community ranked first.



= significant differences between segments

Note: Multiple responses allowed

= significant differences between 2021 and 2023

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

Sources of Security Threats - Federal Trend

- The top three sources of security threats have remained the same for the federal respondents since 2014. Foreign governments have become a greater source of IT security threats over time with reports nearly doubling from 2014 to 2023.
- There are no significant changes from 2021 to 2023 for any sources of threats.

Federal	2014	2015	2016	2017	2018	2019	2021	2023
Foreign governments	34%	38%	48%	48%	52%	48%	59%	63%
Careless/untrained insiders	42%	53%	48%	54%	56%	52%	52%	58%
General hacking community	47%	46%	46%	38%	48%	40%	56%	53%
Hacktivists	26%	30%	38%	34%	31%	26%	42%	38%
Malicious insiders	17%	23%	22%	29%	36%	29%	30%	30%
Terrorists	21%	18%	24%	20%	25%	22%	23%	27%
For-profit crime	11%	14%	18%	17%	15%	20%	27%	22%
Industrial spies	6%	10%	16%	12%	19%	16%	23%	22%

Note: Multiple responses allowed = top three sources

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

Sources of Security Threats - State/Local + Education Trend

- Since 2019, the top three sources of security threats for SLED respondents have remained the same. For state/local governments, the threat of the general hacking community has decreased. The threat of foreign governments increased in the education sector.

State/Local	2019	2021	2023
Careless/untrained insiders	52%	51%	58%
Foreign governments	48%	46%	56%
General hacking community	40%	63%	47% ↓
Hacktivists	26%	43%	35%
Malicious insiders	29%	36%	28%
Terrorists	22%	18%	23%
For-profit crime	20%	29%	18%
Industrial spies	16%	21%	10% ↓

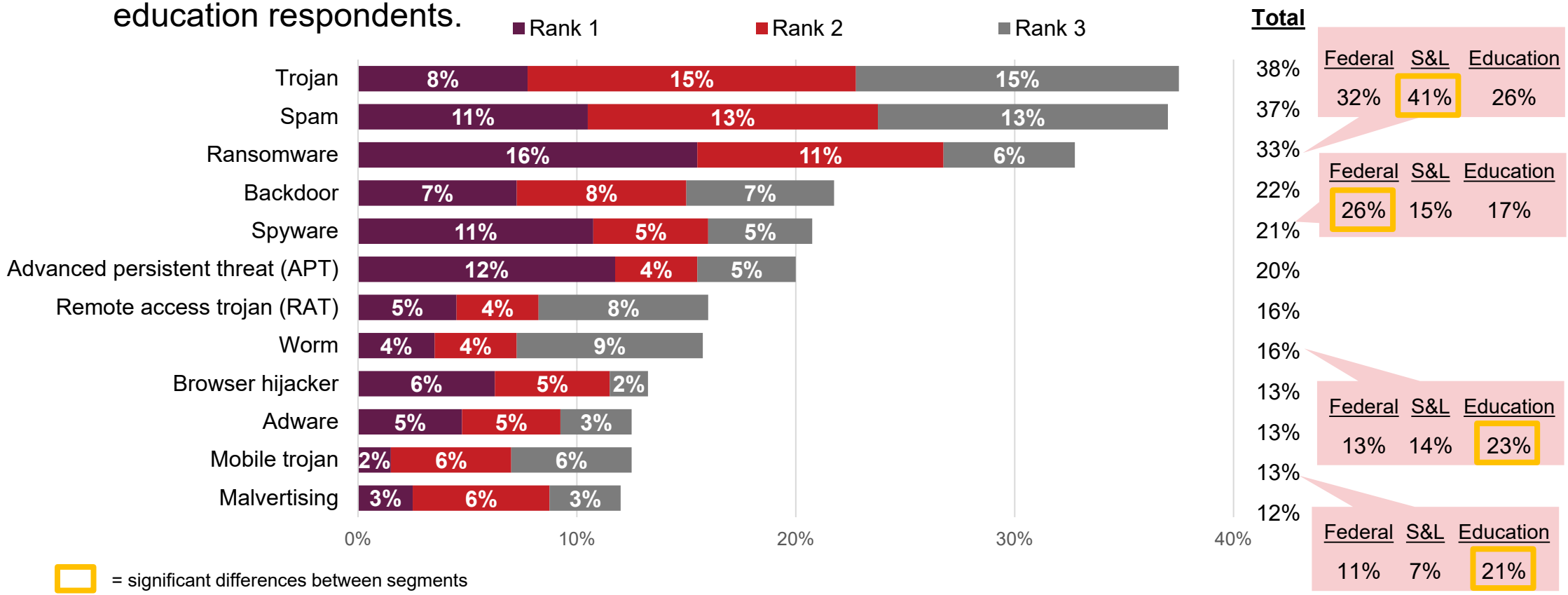
Education	2019	2021	2023
Careless/untrained insiders	52%	53%	58%
Foreign governments	48%	25%	56% ↑
General hacking community	40%	49%	55%
Hacktivists	26%	32%	38%
Malicious insiders	29%	33%	25%
For-profit crime	20%	25%	22%
Terrorists	22%	11%	22% ↑
Industrial spies	16%	14%	13%

Note: Multiple responses allowed ↑↓ = significant differences between 2021 and 2023 ■ = top three sources

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

Biggest IT Security Threats

- The three biggest IT security threats to organizations are believed to be trojans, spam, and ransomware.
- State/local respondents rank ransomware as a threat significantly more often than education respondents.

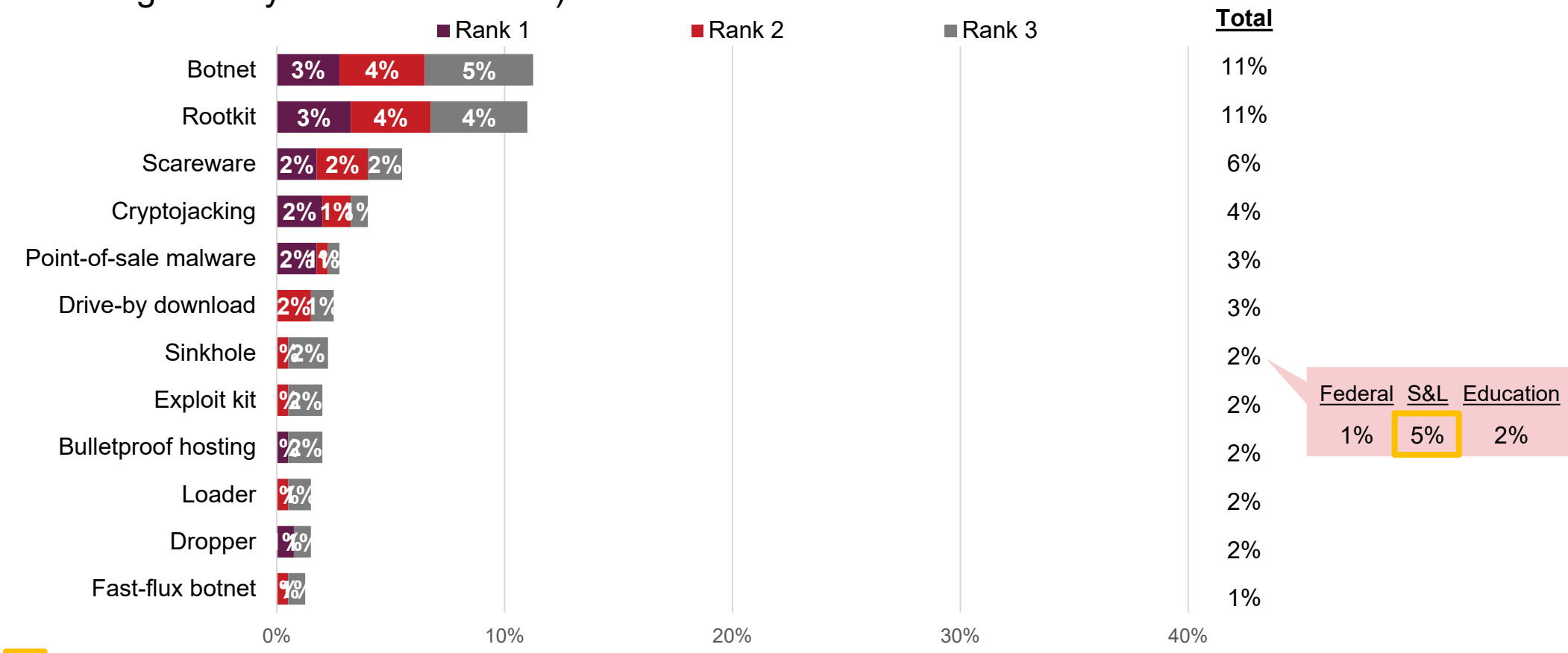


= significant differences between segments

Which of the following do you believe are the biggest IT security threats to your organization? (rank top 3)

Other IT Security Threats

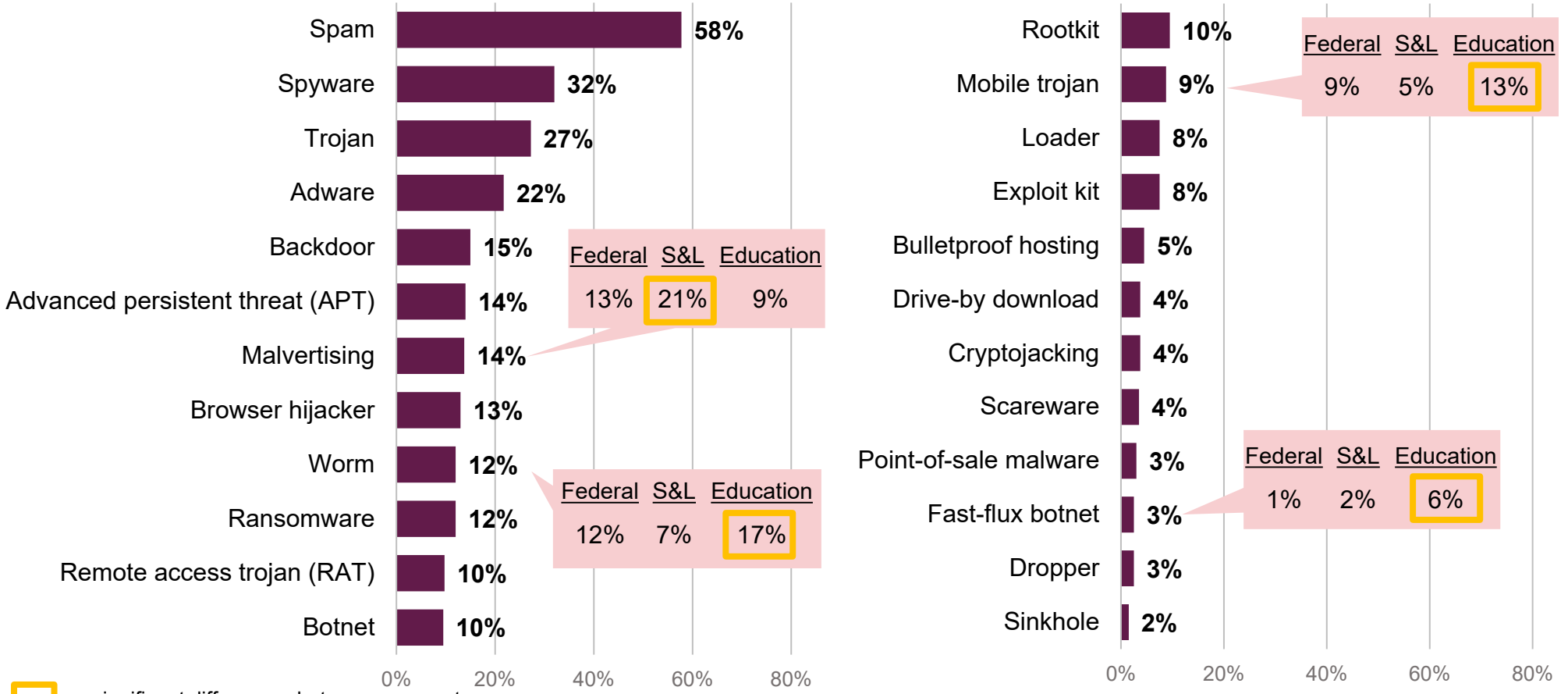
- The threats of least concern are fast-flux botnets, droppers, and loaders (which respondents are generally less familiar with).



Which of the following do you believe are the biggest IT security threats to your organization? (rank top 3)

IT Threats in the Last 12 Months

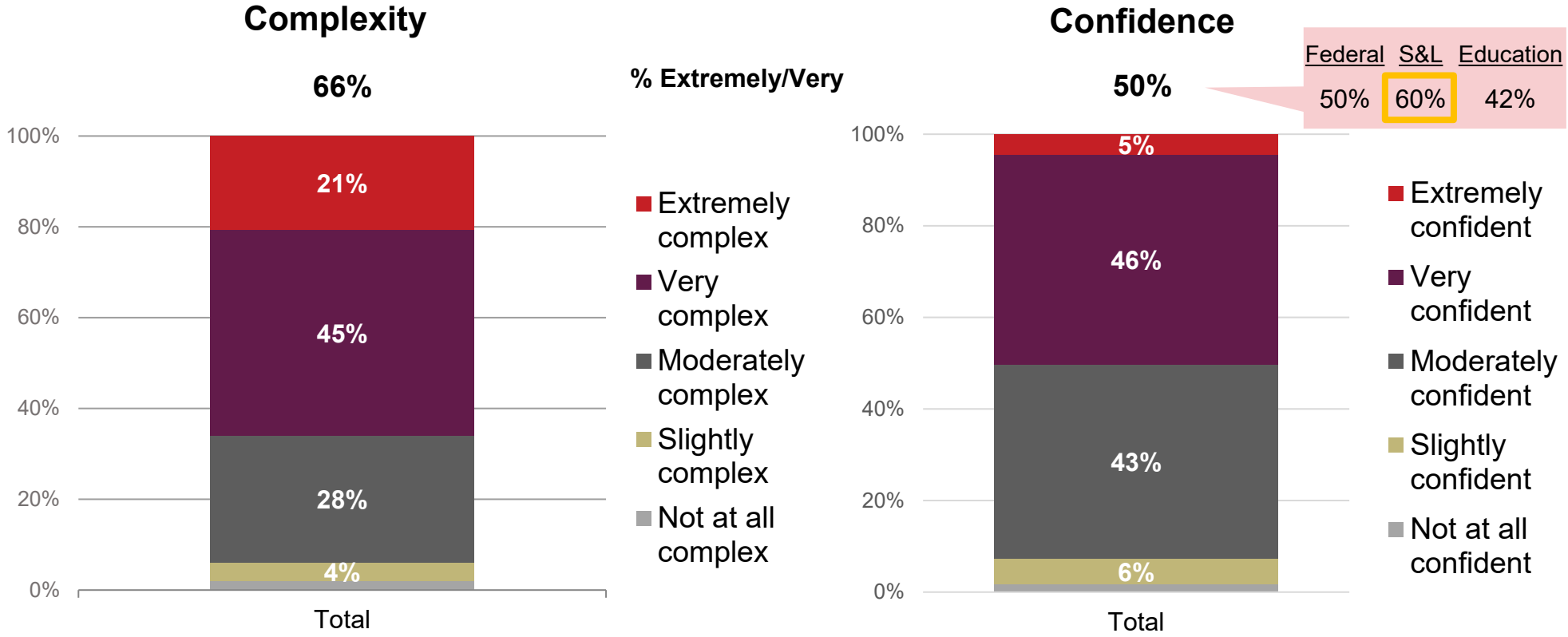
- Spam is the most common threat organizations have been impacted by in the last 12 months.



Over the past 12 months, has your organization been impacted by any of the following types of IT security threats? (select all that apply)

IT Environment Management Complexity and Confidence

- Two-thirds of respondents feel their IT environment is extremely or very complex to manage. Yet, half are extremely/very confident in their ability to manage their environment. State/local respondents are more confident than those in the education sector.

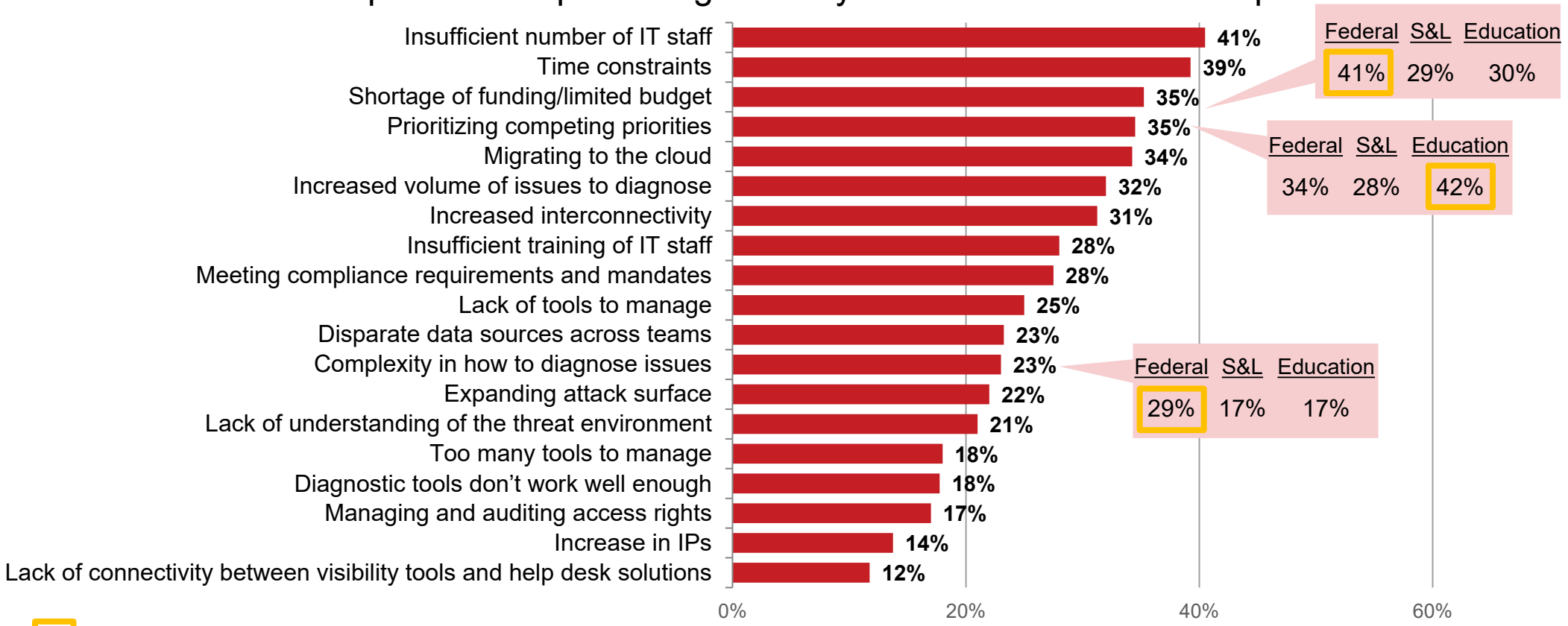


= significant differences between segments

How complex is your organization's IT environment to manage? How confident are you in your organization's ability to manage its IT environment?

Challenges in Managing the IT Environment

- Respondents have indicated that their top challenge in managing their IT environment is an insufficient number of IT staff. Time constraints are second, followed by budget issues which federal respondents reported significantly more than state/local respondents.



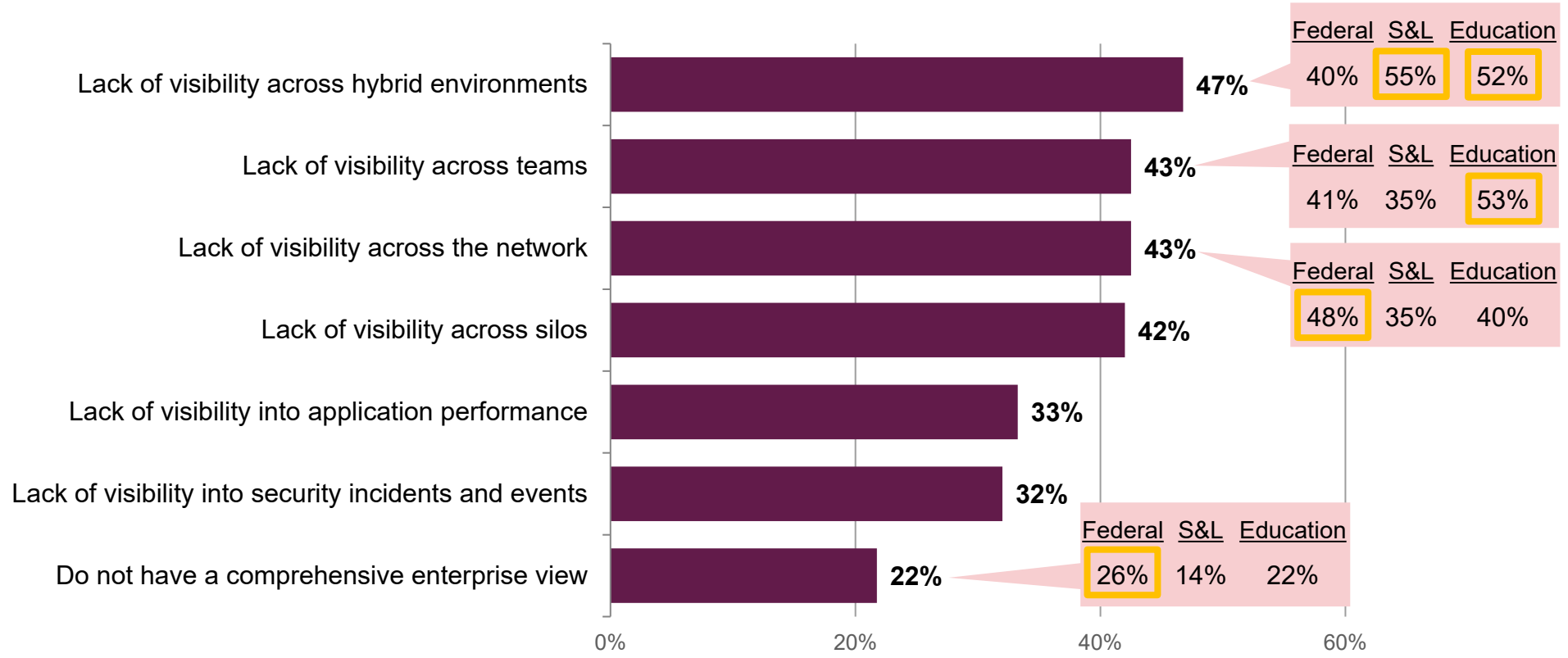
= significant differences between segments

Note: Multiple responses allowed

Which of the following are challenges to managing the IT environment in your organization? (select all that apply)

Visibility Challenges

- The top visibility challenge is a lack of visibility across hybrid environments. This issue is significantly more common with state/local and education respondents.



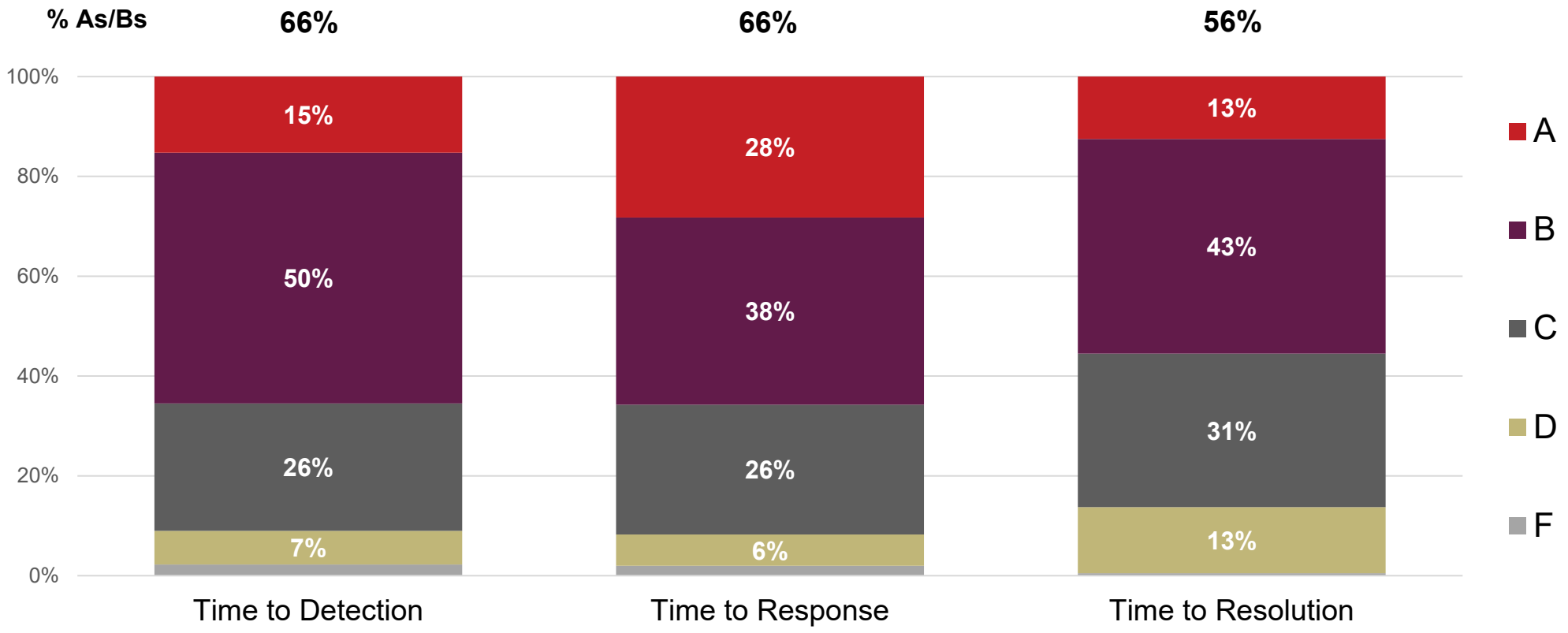
= significant differences between segments

Note: Multiple responses allowed

Which of the following visibility challenges does your organization face in its IT environment? (select all that apply)

Ability Timeline Report Cards

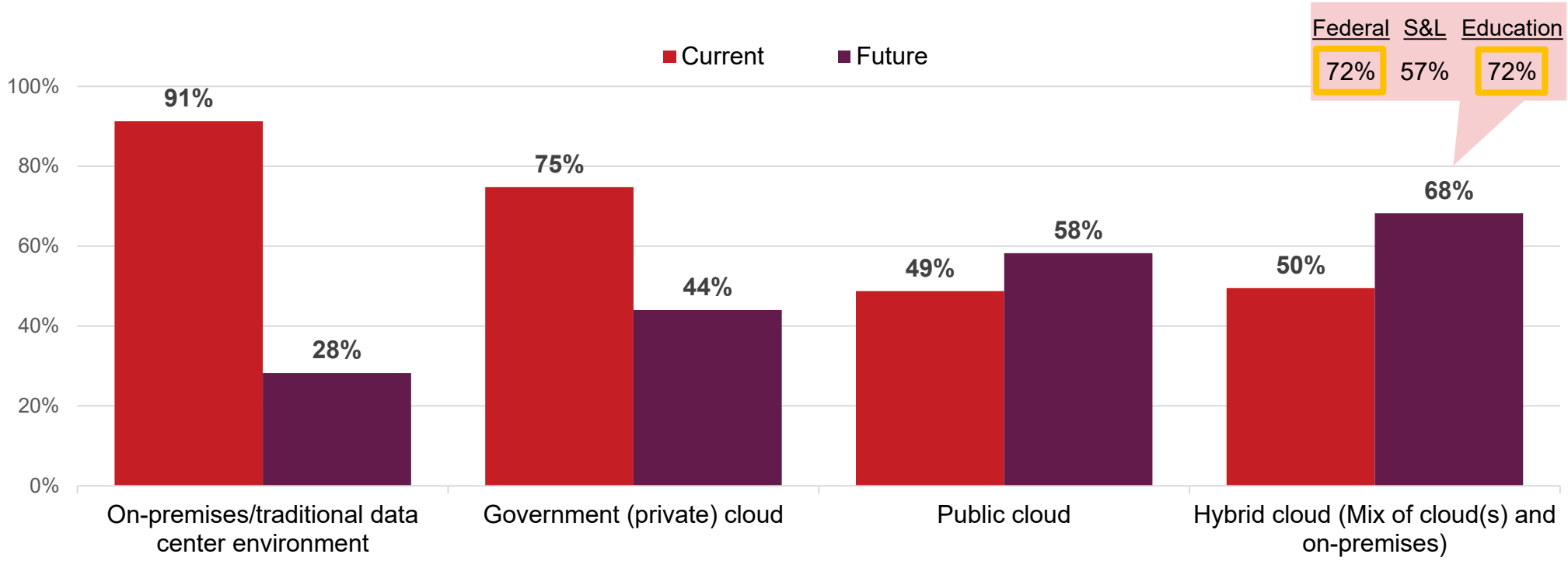
- Respondents most often grade their organization as a “B” for time to detection, response, and resolution.



How would you grade your organization’s ability to detect, respond to, and resolve security incidents and events?

Current and Future IT Environment

- Currently, on-premises/traditional data center environments are the most prevalent.
- In the future, respondents believe that hybrid cloud environments will be the most common. Federal and education respondents indicate this more than state/local respondents.



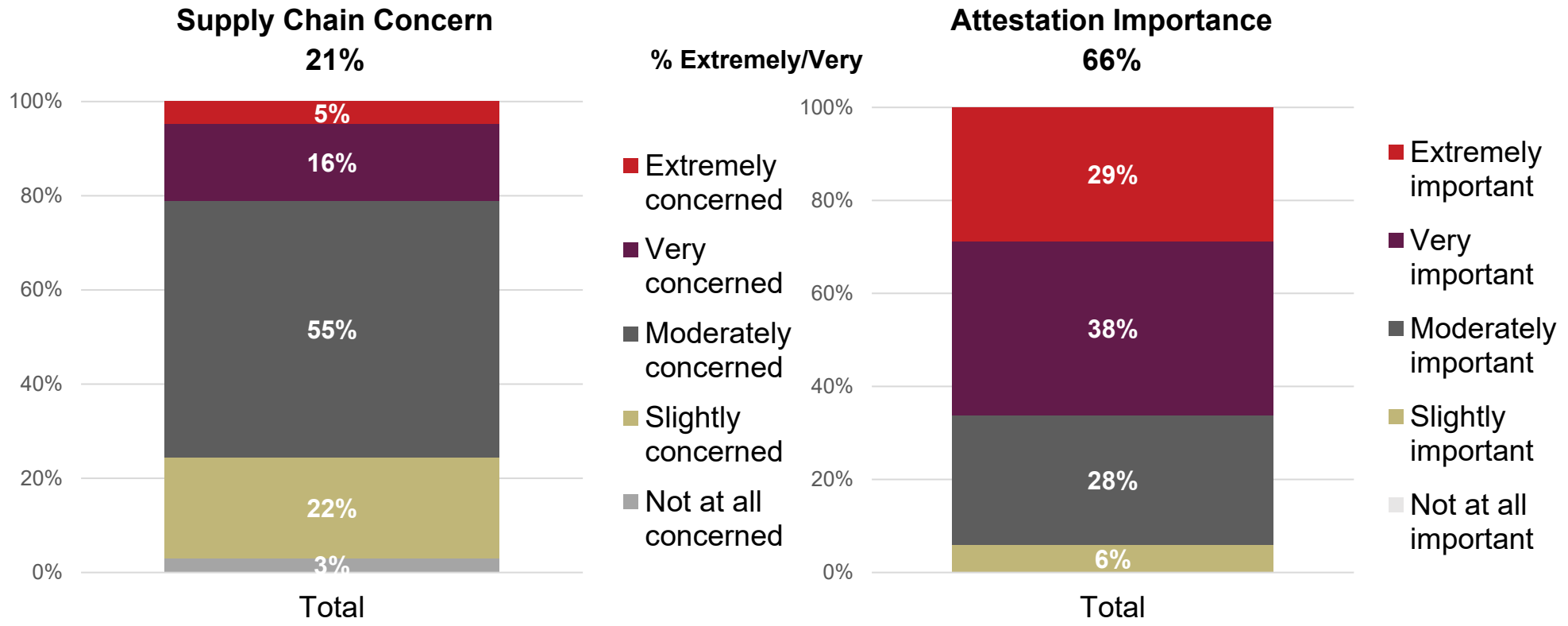
= significant differences between segments

Note: Multiple responses allowed

Which of the following comprise your organization's IT environment? And which do you anticipate will comprise your organization's environment three years from now?

Supply Chain Security Concerns and Attestation

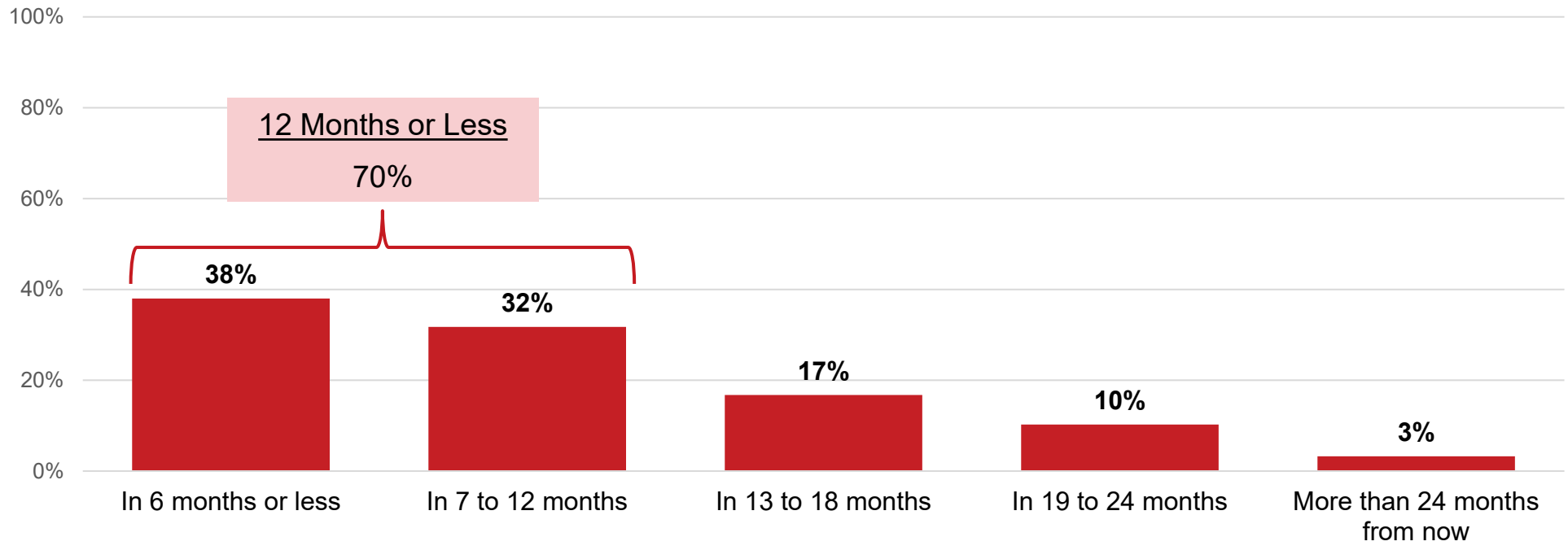
- Two in ten are extremely/very concerned with software supply chain security. Over half are moderately concerned.
- Two thirds indicate that vendor attestations are extremely/very important.



How would you describe your level of concern with your organization's software supply chain security for its IT products? How important is it to you that your organization's vendors attest to complying with the government-specified secure software development practices, as described in the NIST Guidance?

Attestation Timelines

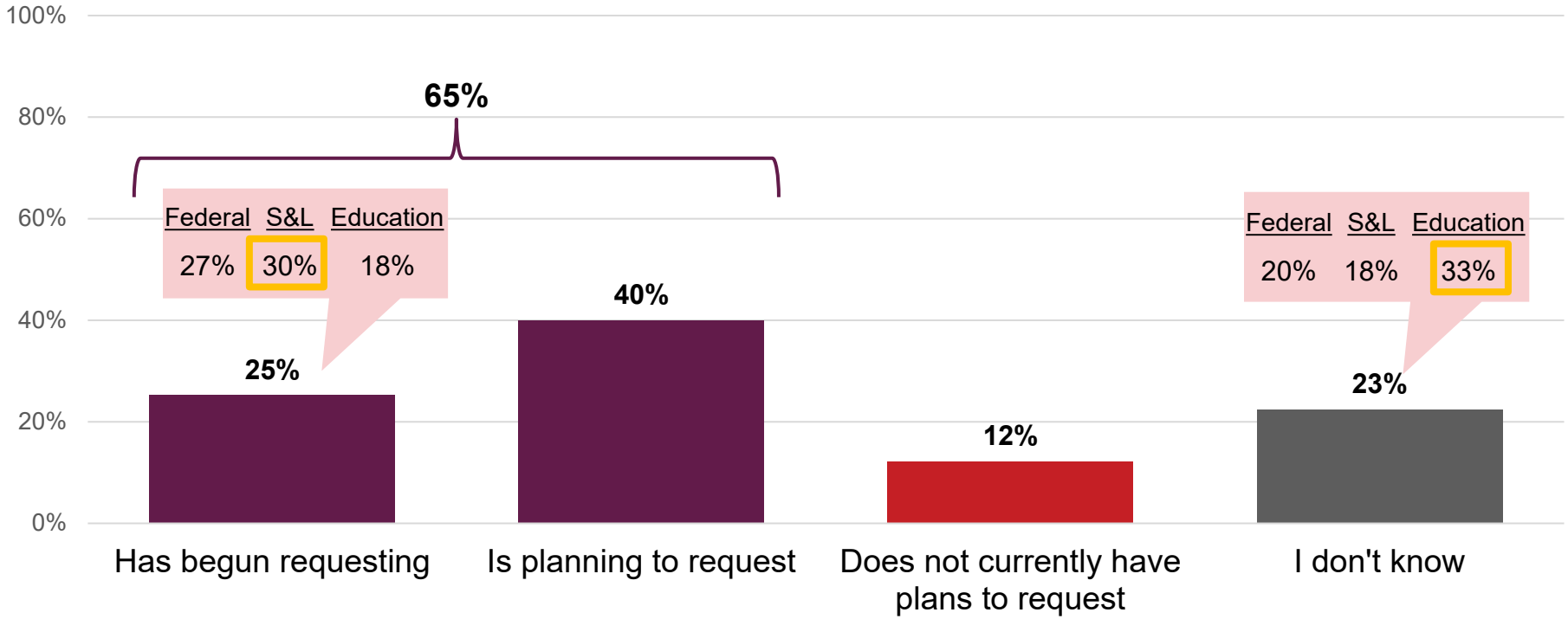
- Seven in ten want attestations provided within 12 months, with over half of that population wanting it within six months (38%).



How soon would you like your organization's vendors to provide an attestation for its software?

Software Bill of Materials (SBOMs)

- Respondents most often report that their organization is planning to request SBOMs from vendors but has not done so yet.
- Only one quarter have begun requesting. More state/local than education respondents have requested SBOMs.

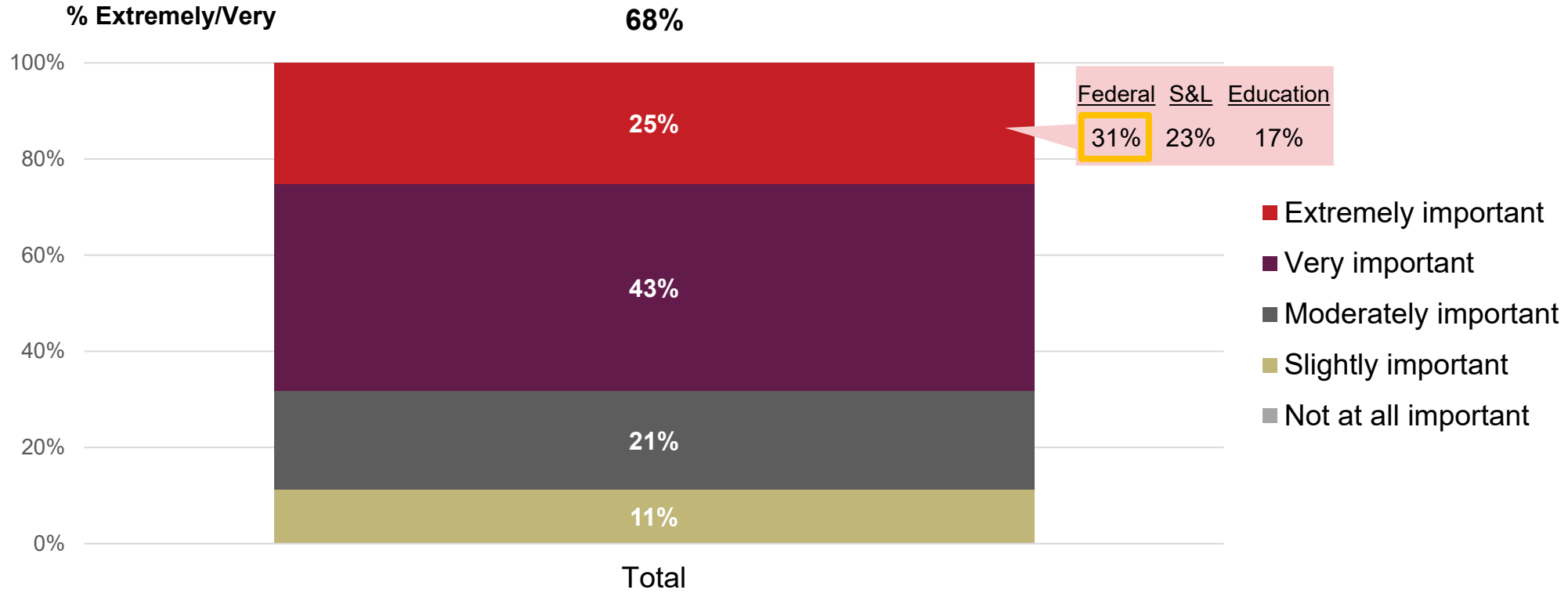


= significant differences between segments

Is your organization requesting or planning to request Software Bill of Materials (SBOMs) from your vendors?

Vendor Transparency

- Two thirds report that it is extremely/very important that vendors provide information on how they develop and secure their software. Significantly more federal than education respondents find it extremely important.

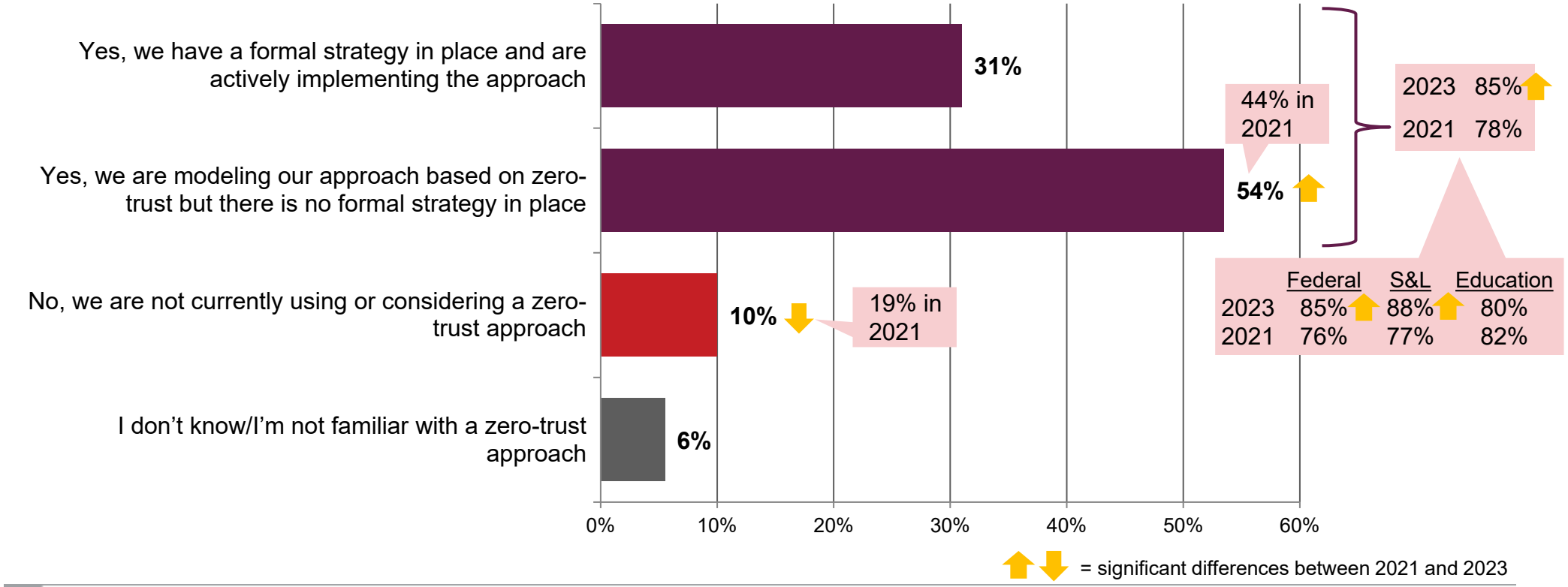


= significant differences between segments

How important is it to you in the next 12 months that your organization's vendors provide information on how they develop and secure their software?

Using a Zero-Trust Approach to IT Security

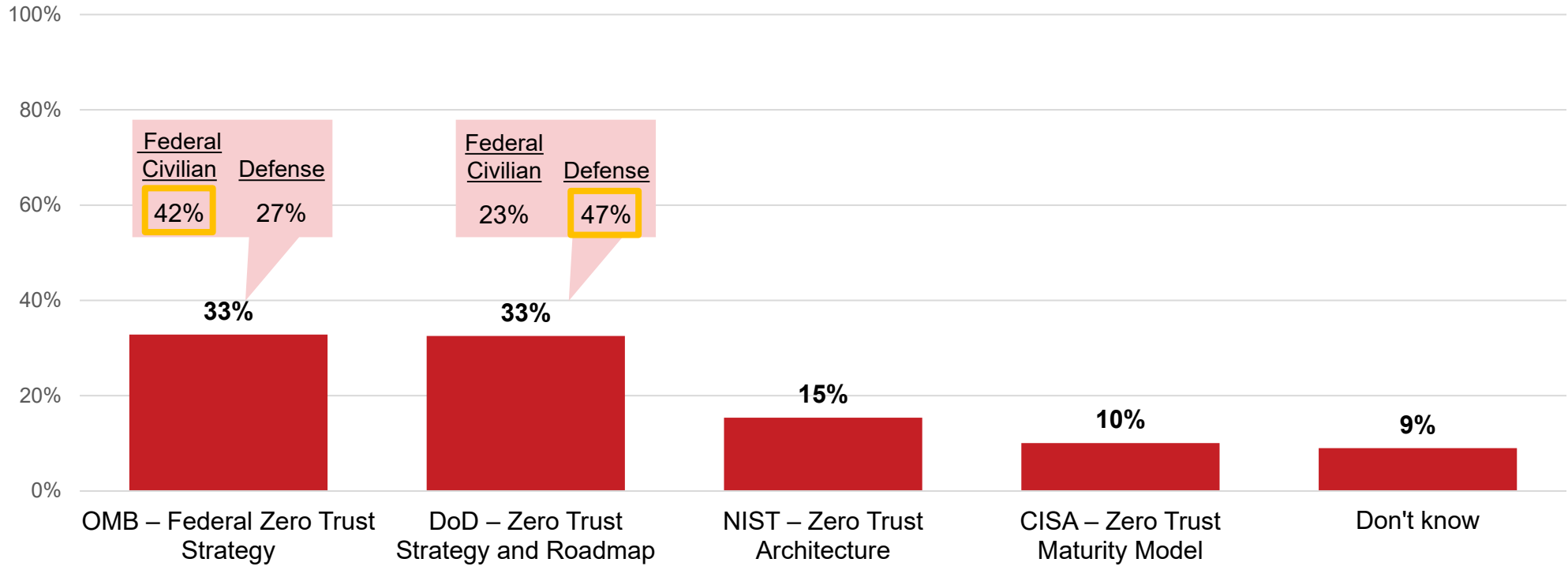
- Three in ten have a formal strategy in place and are actively implementing the zero-trust approach. A significant shift is seen from respondents not using/considering a zero-trust approach to now modeling their approach based on zero-trust.



Is your organization currently using or considering a zero-trust approach to IT security?

Zero-Trust Approach Used

- OMB and DoD strategies are tied for the most used zero-trust approaches.

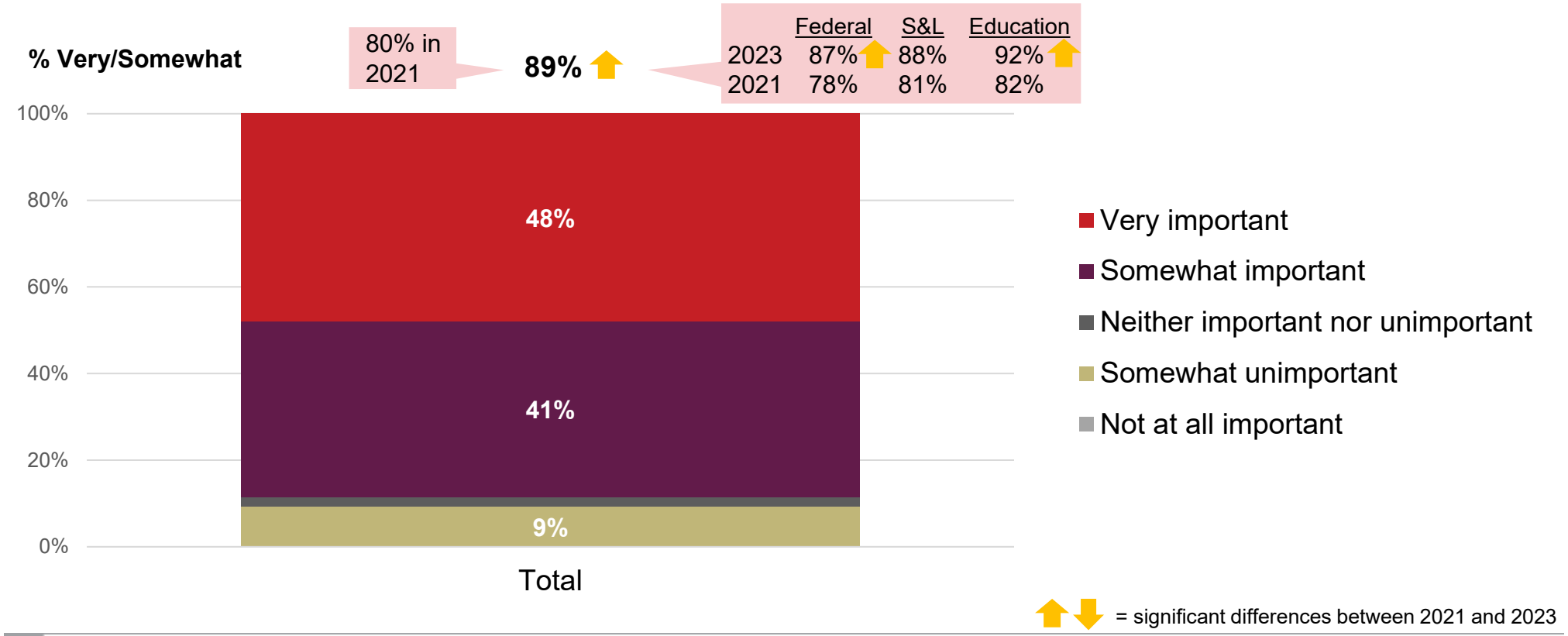


= significant differences between segments

[IF FORMAL STRATEGY IN PLACE] Which zero-trust approach is your organization focusing on most?

Importance of a Zero-Trust Approach

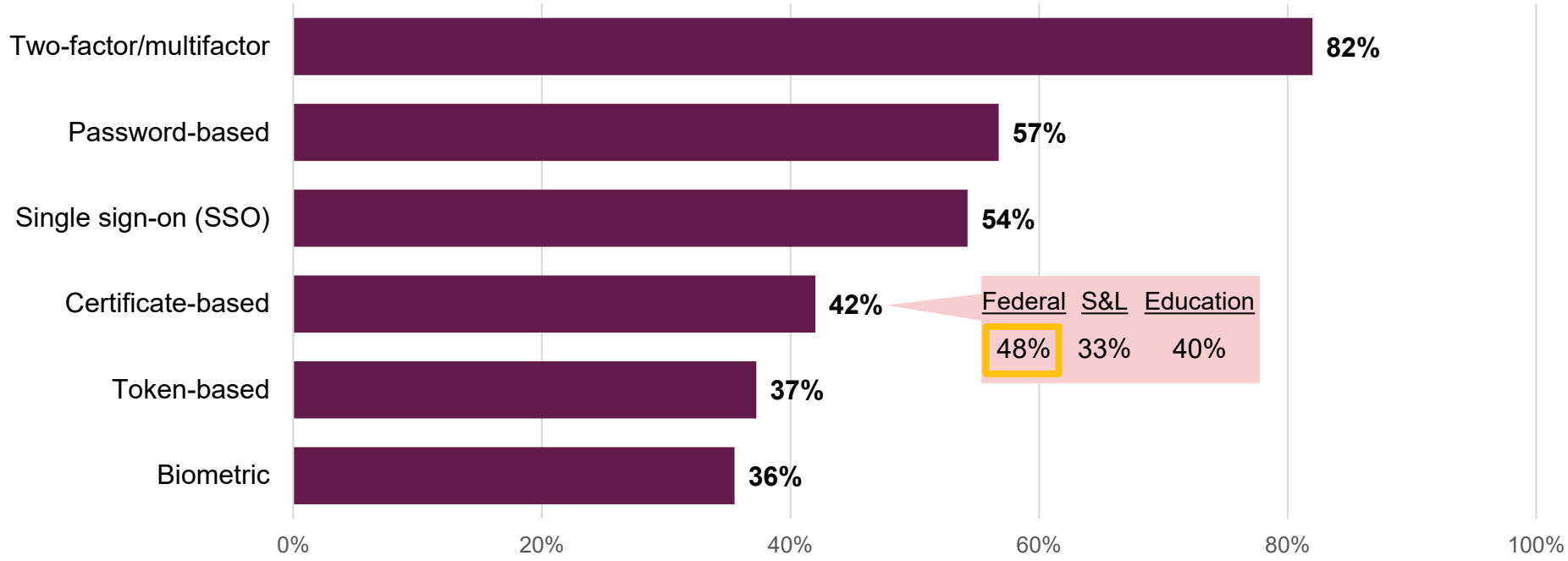
- The importance of implementing a zero-trust approach is high among all public sector organizations. Nearly nine out of ten report it to be very/somewhat important, which is a significant increase from 2021.



Regardless of whether you're implementing a zero-trust approach or not, how important is it for [GOVERNMENT AGENICES, EDUCATIONAL INSTITUTIONS, STATE AND LOCAL GOVERNMENTS] to adopt a zero-trust approach?

Authentication Methods

- The most common authentication method used is two-factor/multifactor.
- Federal respondents report using certificate-based authentication more than state/local respondents.



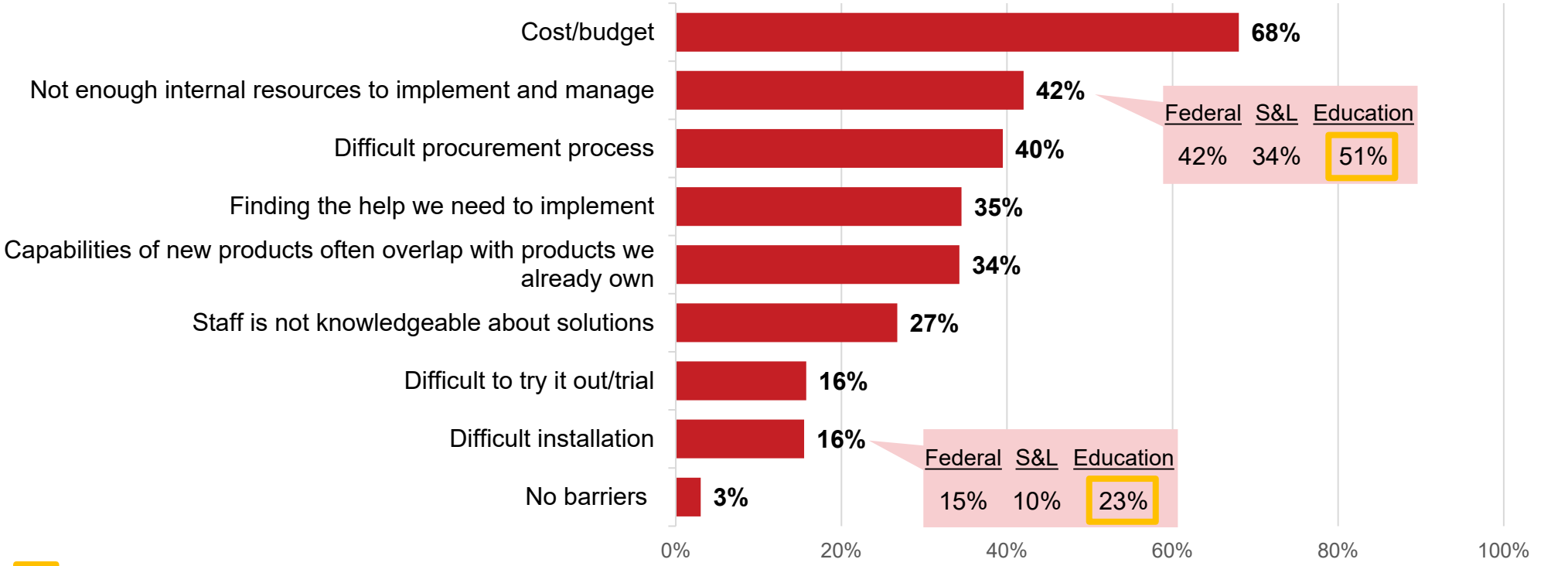
= significant differences between segments

Note: Multiple responses allowed

What types of authentication methods does your organization use? (select all that apply)

Barriers to Implementation

- The most common barrier to implementing a new IT security solution is cost/budget.
- Insufficient internal resources come in second, which are noted by more education than state/local respondents.



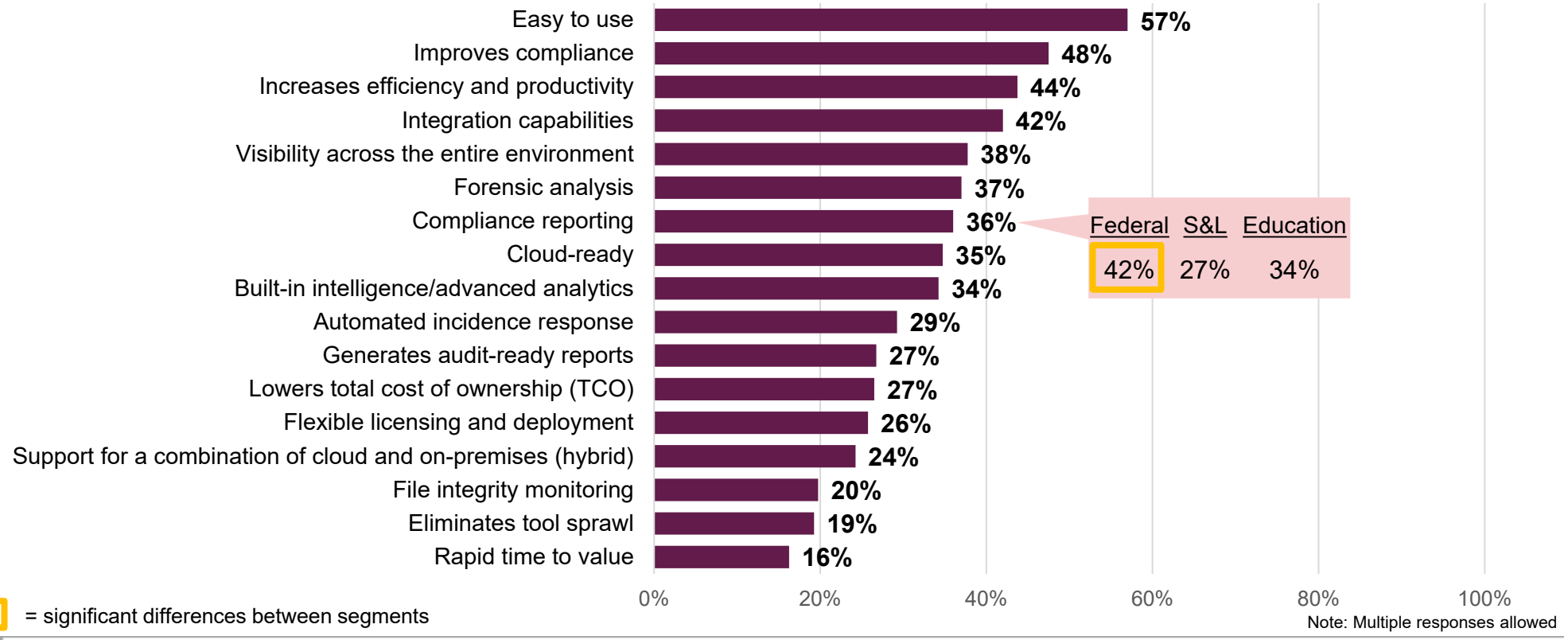
= significant differences between segments

Note: Multiple responses allowed

Which of the following are barriers to implementing a new IT security solution in your organization? (select all that apply)

Important Features

- The most important feature in IT security products is ease of use.
- Improving compliance and efficiency/productivity follow.



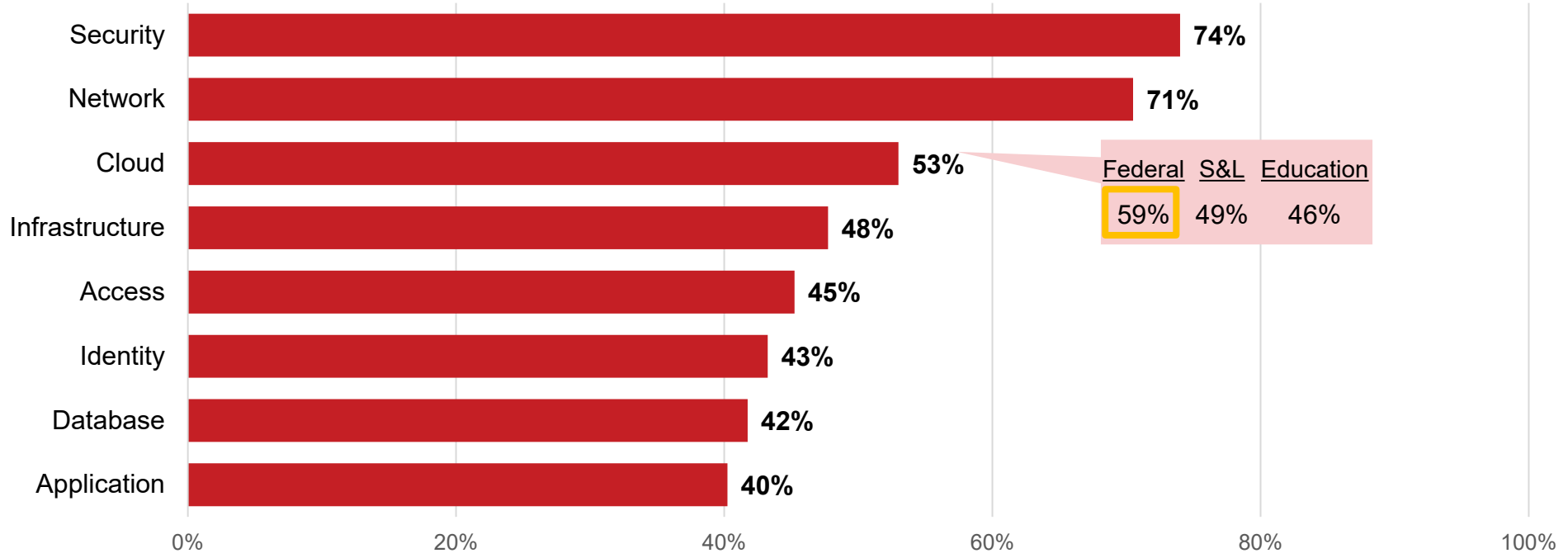
= significant differences between segments

Note: Multiple responses allowed

What features are important to you and/or your organization in IT security products? (select all that apply)

Visibility Preferences

- Security and network information are most preferred to have visibility into within a single IT security platform. Cloud is a distant third with federal respondents more likely to prefer this than education respondents.



= significant differences between segments

Note: Multiple responses allowed

What data sources/information would you prefer your organization have visibility to within a single IT security platform? (select all that apply)

Representative Comments

We have reduced data security breaches and increased efficiency by adopting ZTA.

COUNTY GOVERNMENT

Data leaks and cyberattacks are growing alarmingly and need to be checked.

DEFENSE / MILITARY

Staff need to understand more about the global threat landscape.

FEDERAL CIVILIAN

Proficiency lies in crafting powerful technology to counter cybersecurity threats.

EDUCATION: K-12

Each day brings in a new challenge and every problem needs a unique solution.

FEDERAL CIVILIAN

Finding good security talent is a big challenge.

FEDERAL JUDICIAL BRANCH

Our leadership spends more time making decisions based on cost versus threat. As a result, we end up spending more money because of security incidents.

DEFENSE / MILITARY

The daily threats of compromised security are a growing problem, and it's extremely important to stay ahead of the game and combat any potential attacks.

DEFENSE / MILITARY

Lack of zero-trust implementation on the part of workers will open a wide space for hackers to compromise the data security and use them for malicious purposes.

EDUCATION: K-12

The greatest challenge we face is that we have 27 different organizations and each one has its own IT budget. The centralized IT organization under the Agency CIO has very little authority to mandate policy. Policy is a key to success, but ours is unenforceable.

FEDERAL CIVILIAN

Please feel free to share any other comments or concerns regarding your organization's unique security challenges and/or success stories.

Key Takeaways

The complexity of the internal environment is the most significant obstacle to maintaining or improving IT security for public sector organizations.

- Mentions of the complexity of the internal environment rose significantly in 2023, pushing it to the top obstacle organizations face, surpassing budget concerns.
- Concerns with complexity rose across all organization types, with significant increases seen among state/local government and education respondents.
- Two-thirds feel their IT environment is extremely/very complex to manage.

Key Takeaways

Overall, foreign governments are the greatest source of IT security threats to public sector organizations.

- With a significant increase from 2021, foreign governments rose to the top as the greatest overall source of IT security threats, surpassing both the general hacking community and careless/untrained insiders.
- Concerns with foreign governments rose across all organization types to the highest point to date, with a significant increase seen among education respondents.
- For federal respondents, foreign governments have become a significantly greater source of IT security threats over time, with reports nearly doubling from 2014 (34%) to 2023 (63%).

Key Takeaways

Most public sector respondents are moderately concerned with their organization's software supply chain security and feel vendor attestations and SBOMs are important.

- Two in ten are extremely/very concerned with software supply chain security. Over half are moderately concerned.
- Two-thirds indicate that vendor attestations are extremely/very important, and seven in ten want them provided within 12 months.
- Two-thirds have either begun requesting or are planning to request SBOMs from vendors and say it is extremely/very important that vendors provide information on how they develop and secure their software.

Key Takeaways

The adoption and perceived importance of zero-trust approaches have continued to increase.

- Up significantly from 2021, 85% of public sector organizations now use a formal or informal zero-trust approach to IT security. This increase is driven by federal and state/local government respondents.
- The reported importance of implementing a zero-trust approach is high among all public sector organizations. Nine out of ten report it to be very/somewhat important, which is a significant increase from eight out of ten in 2021.

Elizabeth Lowery, Director of Research Services

elowery@govexec.com

Julia Hagen, Research Analyst

jhagen@govexec.com