Market Connections
Research you can act on.

Federal Network Security Survey Report

April 20, 2015

About the Study

As networks become increasingly complex—and more data moves across the network—vulnerability to security breaches can increase. Despite the volume of unencrypted inter- and intra-agency data traversing most enterprises, many federal agencies are not implementing procedures to protect the network because it is expensive and degrades performance. The right tools can help agencies overcome these network security obstacles, and provide end-to-end protection of data within the data center and in transit—without adding complexity to the network.

Government market research firm Market Connections, Inc. conducted this study to learn to what extent agencies feel their data is protected in transit, the challenges they face in addressing data protection proactively and any gaps between priorities and actions.

Key Research Findings

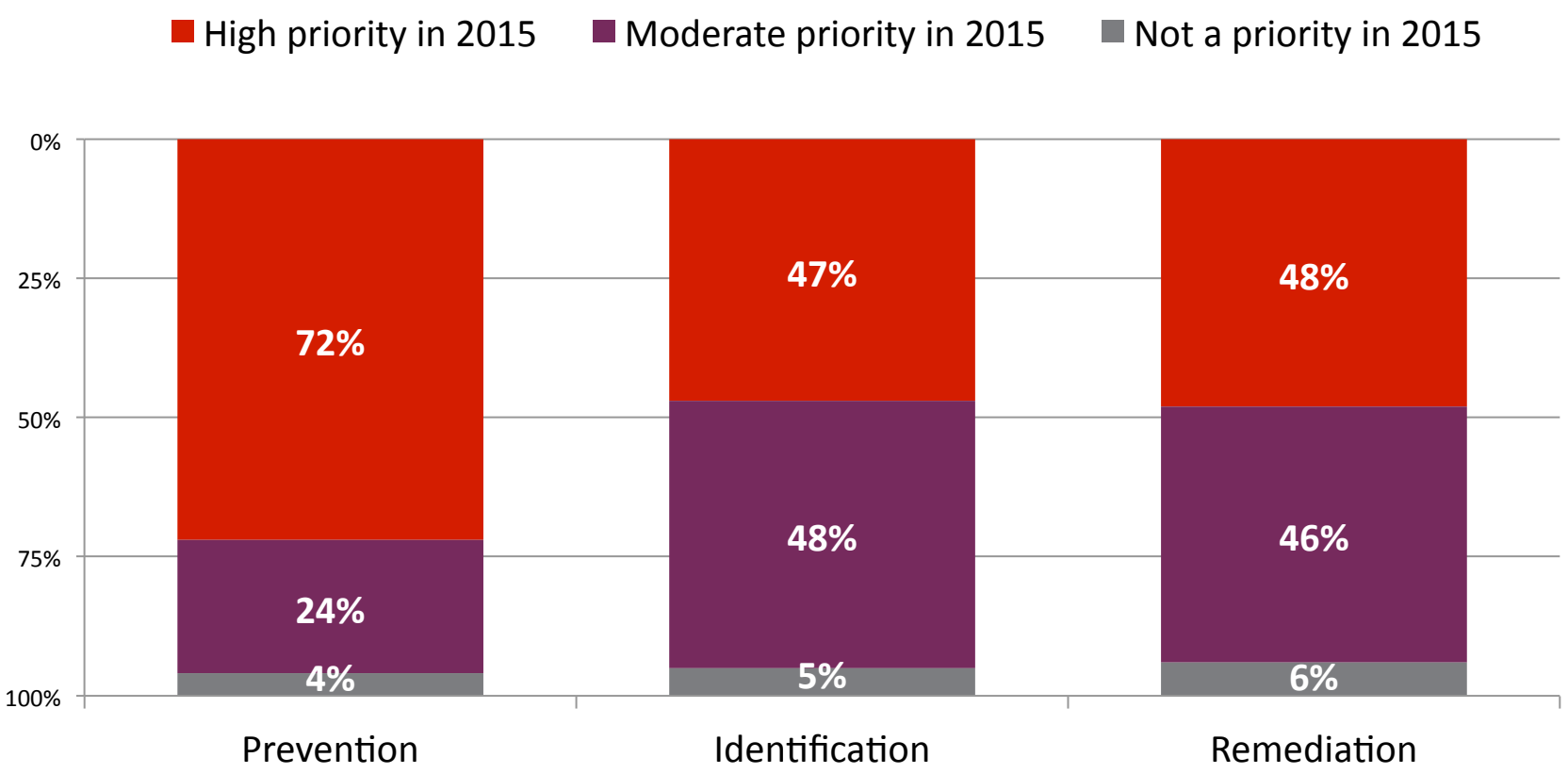
- **Prevention is the highest priority within an agency's cybersecurity strategy.**
- **Only 26% of agencies feel their data on the network is fully protected.**
  - The ability to protect data on the network diminishes the further the data travels.
  - Budget constraints, limited resources, complexity and impact on the network performance are top challenges for agencies when protecting the data on the network.
- **Encrypting the data on the network is important to 95% of respondents.**
- **Seventy-six percent of agencies encrypt their data. A majority (62%) focus on SSL.**
  - In most cases, agencies are are focused on SSL encryption to secure web-based applications. Yet there are many other applications that need to be encrypted in transit. What encryption is used in those cases?

Key Research Findings (continued)

- **Those who are not encrypting their data are not doing so because of budget constraints and the impact on network performance.**
- **Eighty-seven percent believe it is important to base their network protection strategy on the Suite B encryption algorithm.**

Cybersecurity Priorities

- Agencies' cybersecurity priorities for 2015 include a widespread focus on prevention (72%), although identification (47%) and remediation (48%) are also high priorities.

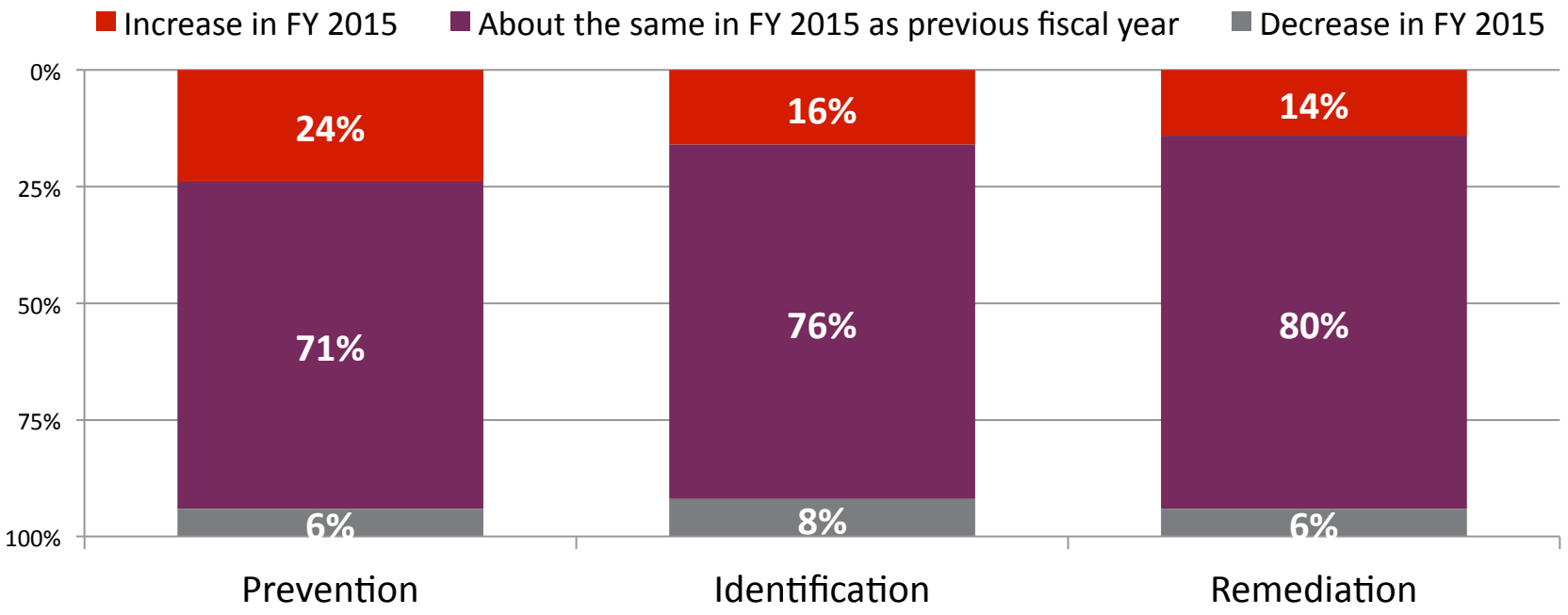


N=200

Q *What are your agency's cybersecurity priorities for 2015 with regard to prevention, identification, and remediation?*

Cybersecurity Budget

- In most instances, agencies' cybersecurity budgets are estimated to remain unchanged from the previous fiscal year. In line with its relatively higher priority, 24% of respondents anticipate budgets for prevention to rise in FY 2015.

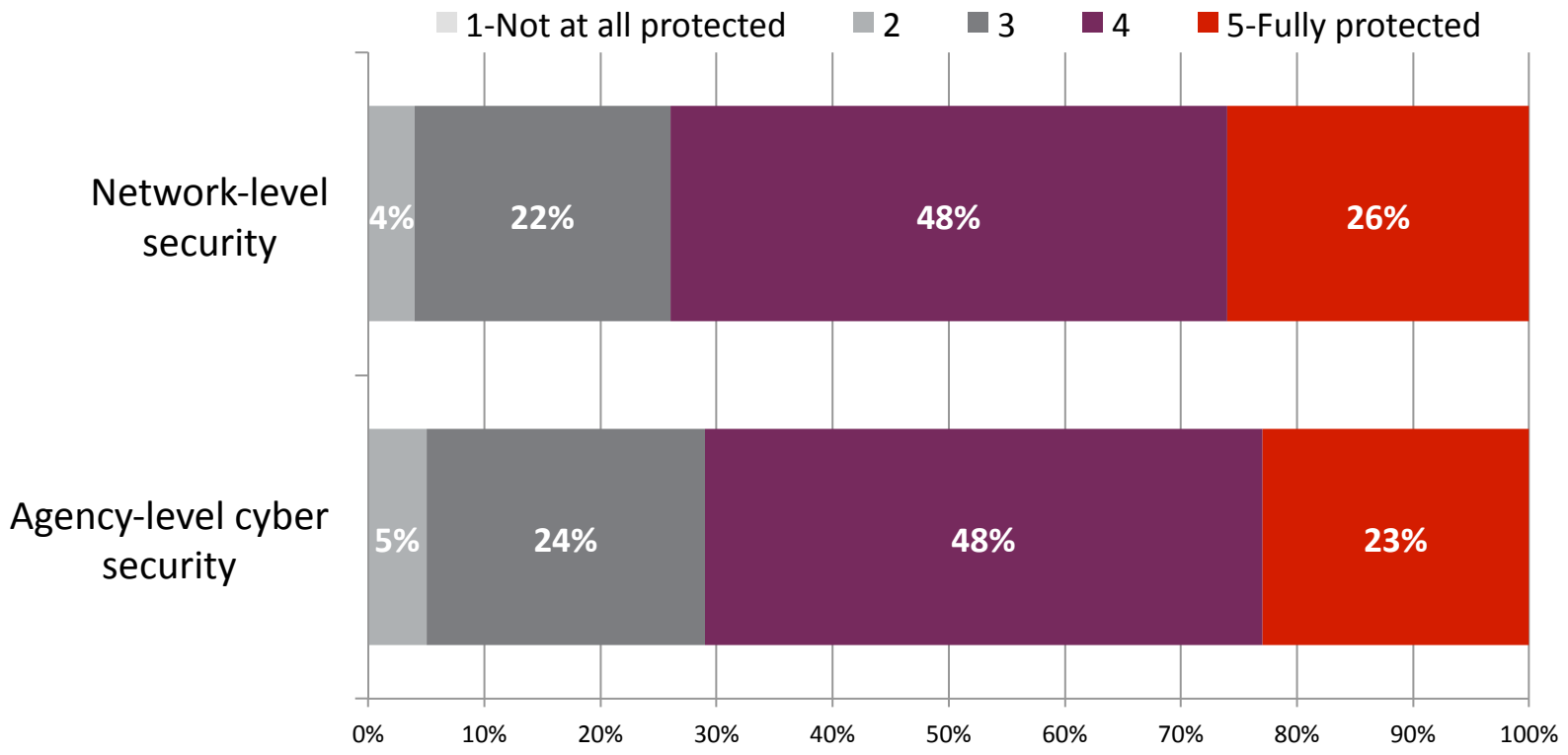


N=200

Q *To the best of your knowledge, in each of the following areas did your agency's cyber security budget increase, decrease, or stay about the same as the previous fiscal year?*

Cyber and Network Security

- Only one-quarter of agencies feel their data on the network is fully protected. Similarly, just 23% rate their agency as fully cyber-secure.

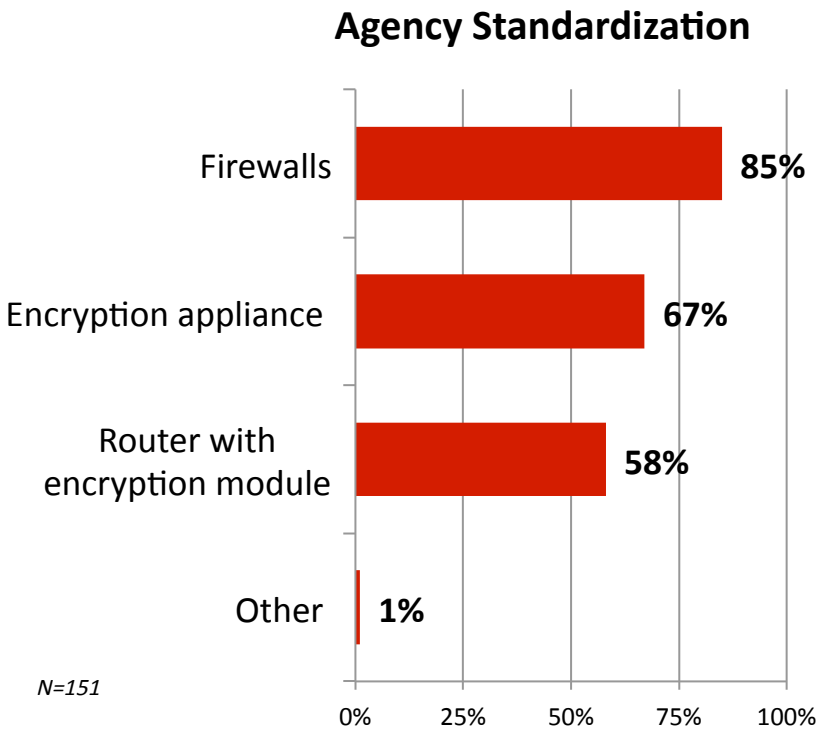


N=200

Q *In your opinion, how would you best rate your agency's overall cyber security protection, and your agency's level of network security?*

Agency Standardization

- Historically, agencies have used firewalls, encryption appliances and routers with encryption modules. Some of these tools can impact performance and do not sufficiently protect data on the network.

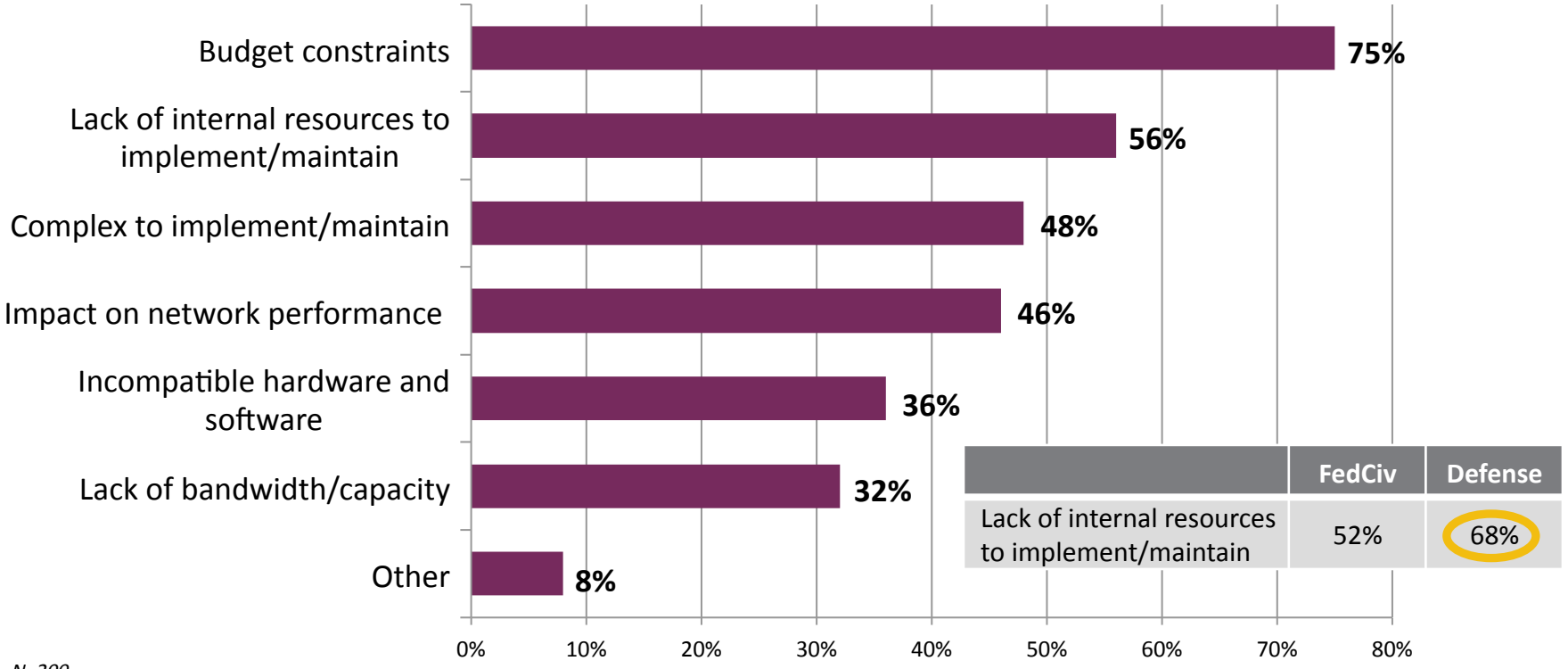


Note: Multiple responses allowed

Q *For the traffic on your network today, what has your agency standardized on to perform encryption/decryption? (select all that apply)*

Top Challenges Protecting Data

- Budget constraints, limited resources, complexity and impact on network performance are top challenges for agencies when protecting the data on the network.



N=200

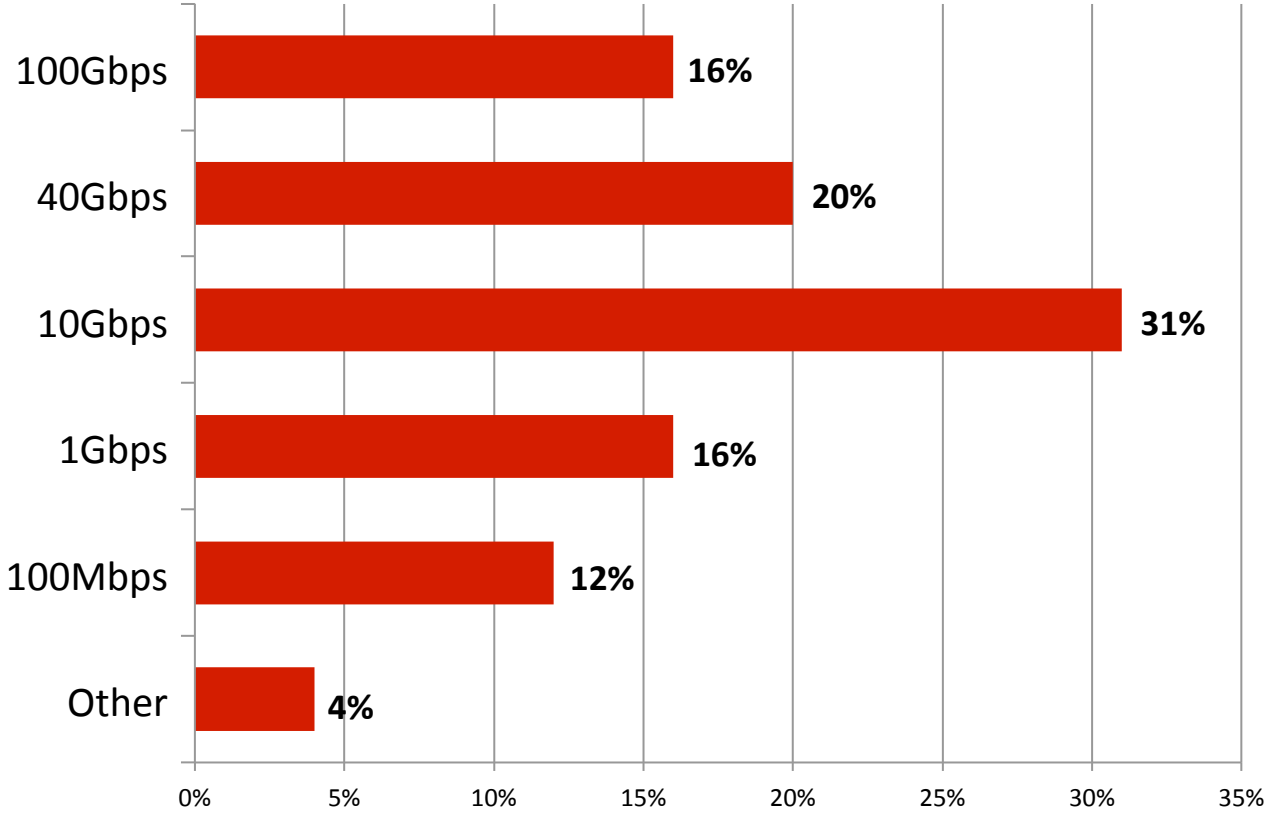
Note: Multiple responses allowed

= statistically significant difference

Q *What are the top challenges you face with regard to protecting your data on the network? (select top 3)*

Network Connection Speed

- Typical connection speeds between data centers or remote offices vary widely. Sixty-seven percent run at 10Gbps or faster. At these speeds, the encryption method can become more of a hindrance than a help.

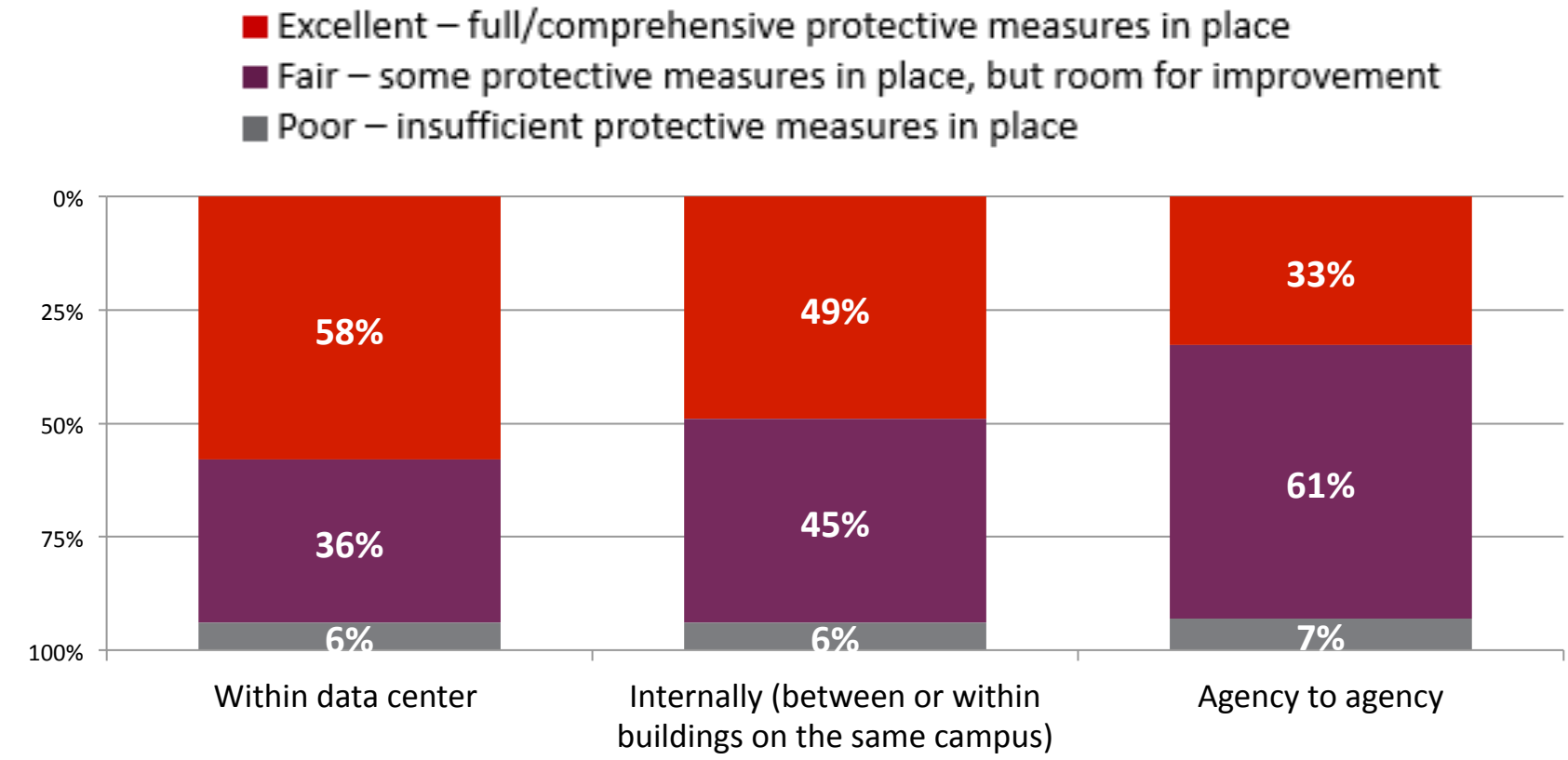


N=200

Q *What is your agency's typical network connection speed between data centers or remote offices?*

Ability to Protect Data in Transit/ Over the Network

- The ability to protect data on the network diminishes the further the data travels.

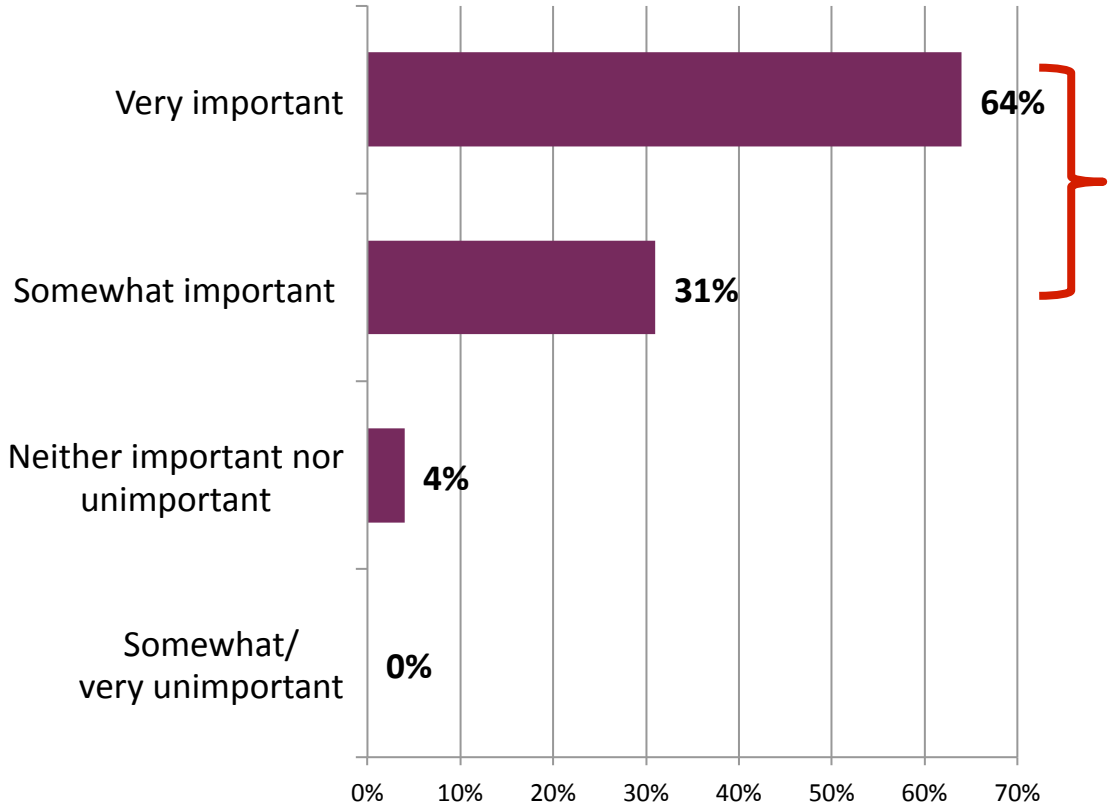


N=198

Q *How would you rate your agency's ability to protect the following aspects of data in transit/ over the network?*

Data Encryption Importance

- Encryption of data on the network is considered important by 95% of respondents.



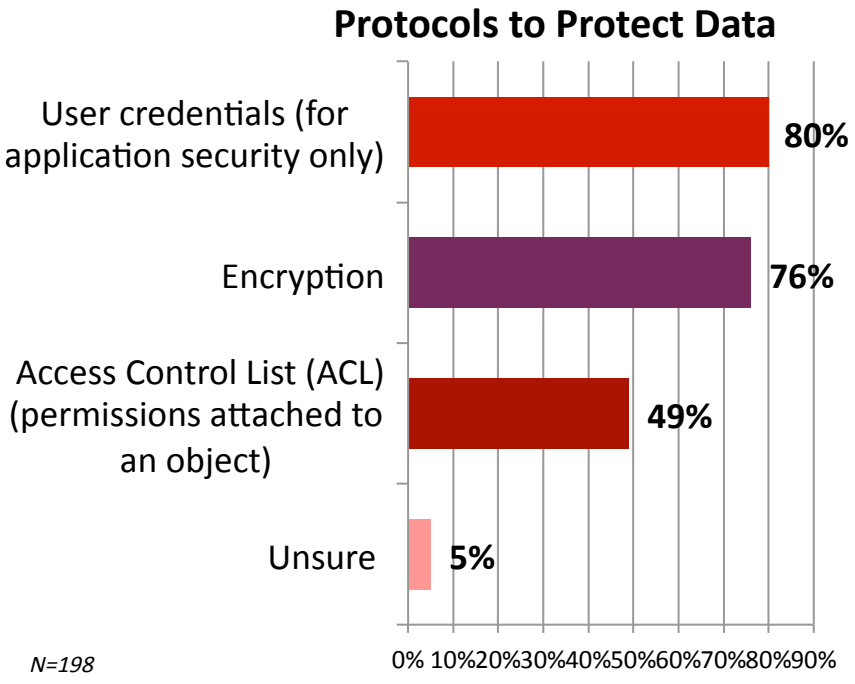
95% IMPORTANT

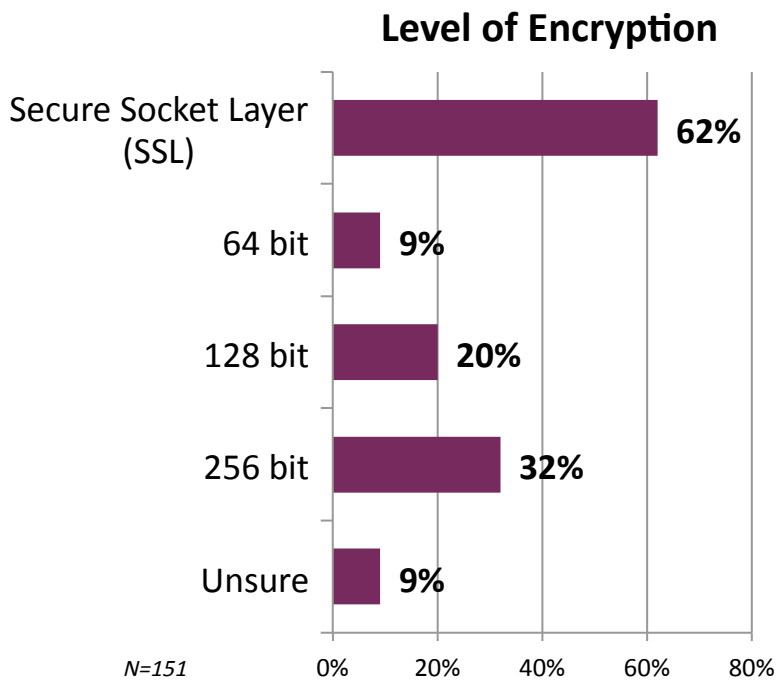
N=200

Q *How important is encryption of data on the network, relative to the overall security of your agency's data?*

Protecting Data

- Although agencies may think they are protecting their data at sufficient levels, a majority are focused on SSL encryption to secure web-based applications. This does not address other inflight traffic types that require a minimum of 128 bit solutions for Secret and 256 bit encryption solutions for Top Secret inflight data sets.



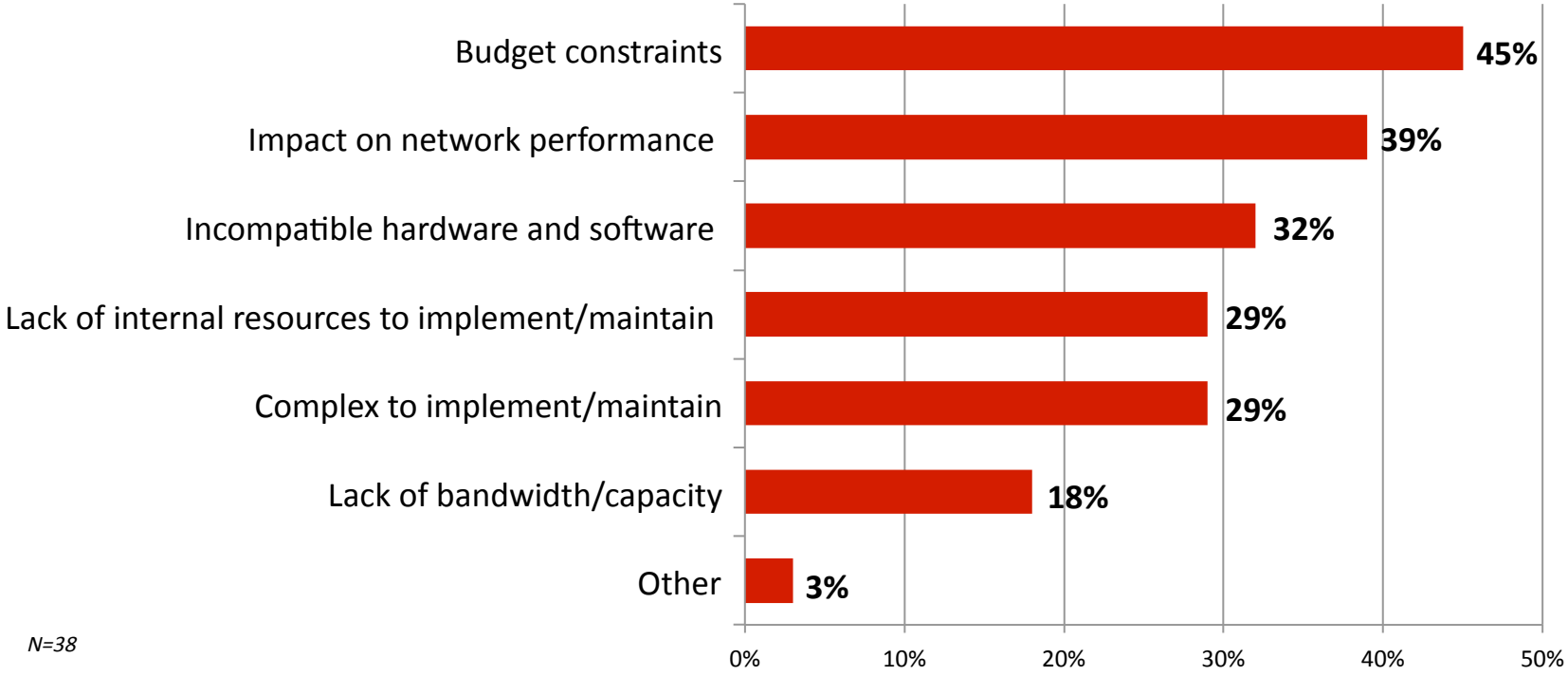


Note: Multiple responses allowed

Q *What protocols do you require to protect your network's data when in transit? (select all that apply)*

Reasons for Not Encrypting Data

- Those who are not encrypting their data are not because of budget constraints and the impact on the network performance.



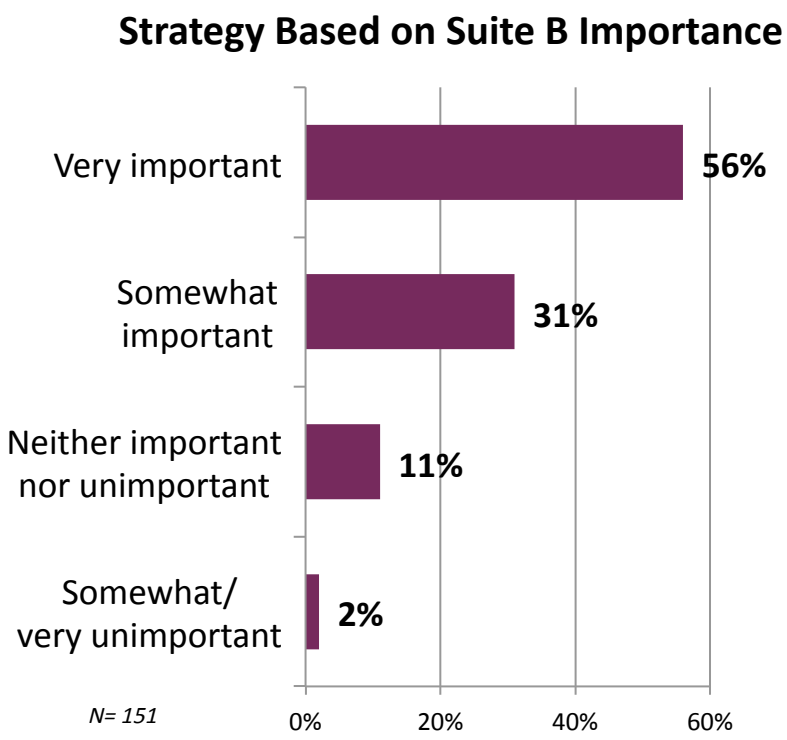
N=38

Note: Multiple responses allowed

Q *For what reason(s) are you not encrypting the data on your network? (select all that apply)*

Importance of Suite B

- Eighty-seven percent of respondents believe it is important to base their network protection strategy on the Suite B encryption algorithm.



Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It is to serve as an interoperable cryptographic base for both unclassified information and most classified information.

Note: Multiple responses allowed

Q *How important is it that your network data security strategy is based on Suite B (a government certified solution) versus some other standard approach?*

Recommendations

Despite the priority agencies place on security and prevention, the study results show there is no place within the enterprise where data is fully protected to prevent cyber-attacks. It is critical to ensure your encryption strategy expands as your enterprise grows to accommodate additional users and networking services.

Checklist for selecting a data protection solution for your network…

- ✓ Simple to implement and maintain
- ✓ Does not impact your network or increase network costs due to complexity and management overhead
- ✓ Protects the different types of data on your network and is Suite B compliant if you have Secret and Top Secret data
- ✓ Can handle your data connection speed today as well as into the future

About the Survey

Market Connections designed and conducted a blind online survey among 200 federal government IT decision makers and influencers in February 2015.

- Two hundred completed interviews yields a +/-6.9% margin of error.
- Sixty different agencies participated in the survey.

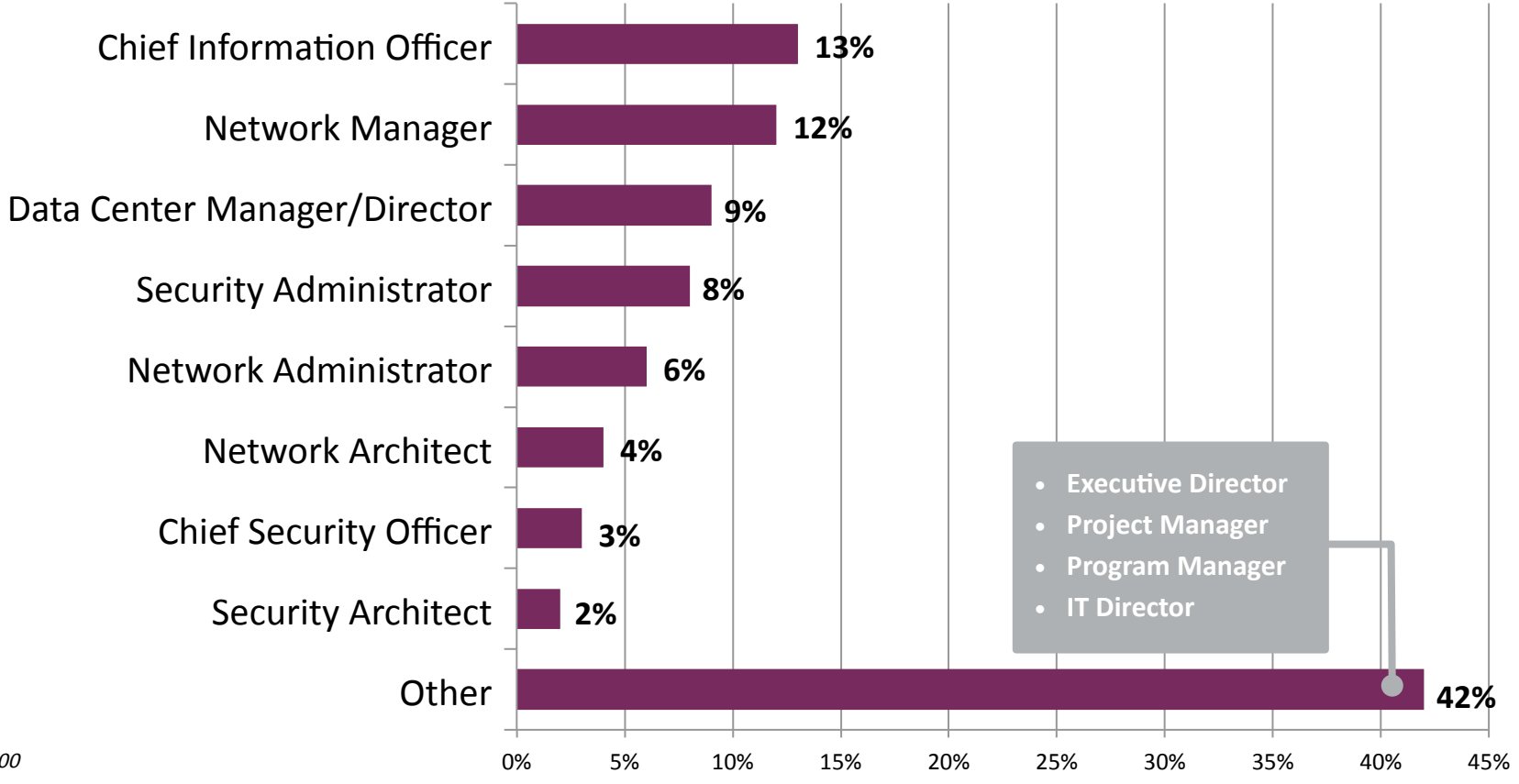
Throughout the report, notable significant differences are reported. Statistical analyses were conducted for agency type (federal civilian vs. defense).

Due to rounding, graphs may not add up to 100%.

Sample Agencies Represented (In Alphabetical Order)	
Air Force	Department of State (DOS)
Army	Department of the Interior (DOI)
Congress	Department of Transportation (DOT)
Department of Agriculture (USDA)	Department of Treasury (TREAS)
Department of Commerce (DOC)	Department of Veteran Affairs (VA)
Department of Defense (DOD)	Federal Aviation Administration (FAA)
Department of Energy (DOE)	Judicial/Courts
Department of Homeland Security (DHS)	National Institutes of Health (NIH)
Department of Housing and Urban Development (HUD)	Navy
Department of Justice (DOJ)	US Postal Service (USPS)

Job Role

- A wide variety of agency roles are represented, the most common of which are Chief Information Officer, Network Manager, Data Center Manager/Director and Security Administrator.

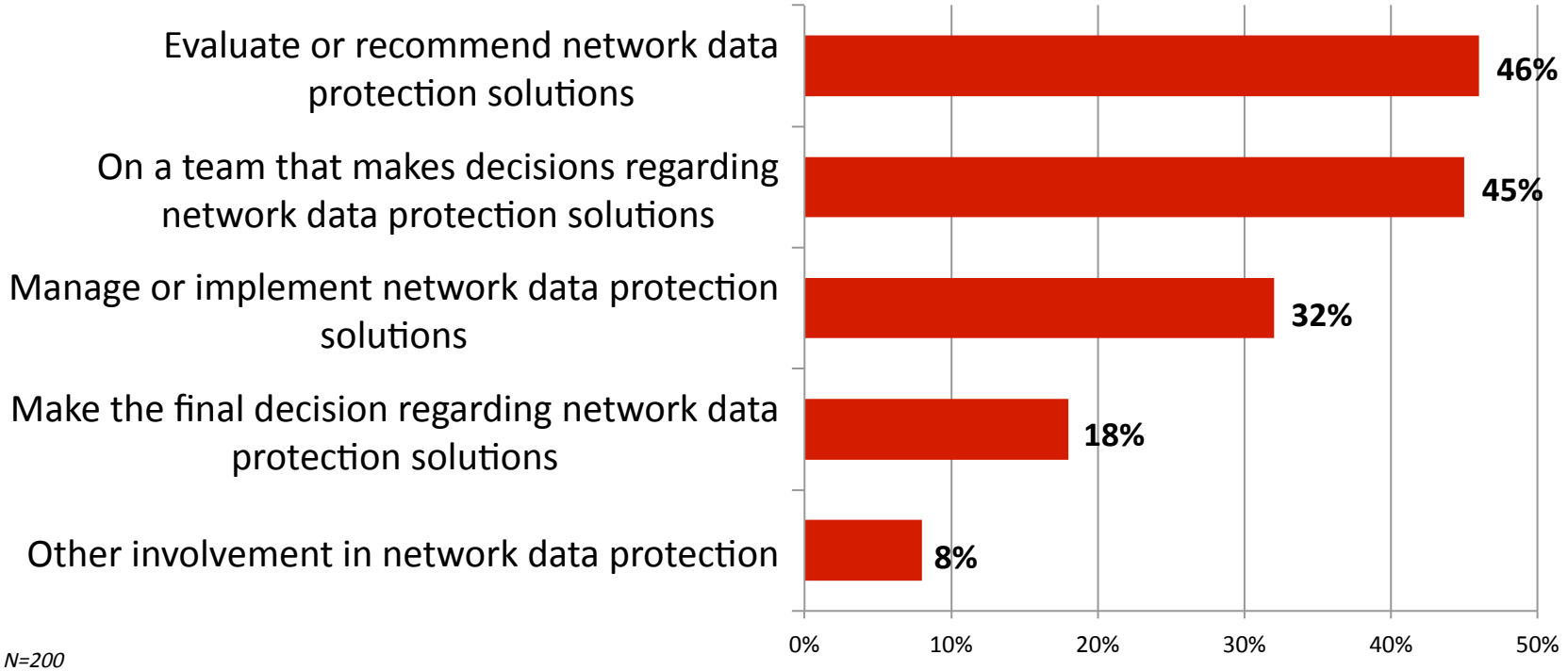


N=200

Q *What is your role at your agency?*

Decision Making Involvement

- Nearly half of respondents mention they evaluate or recommend network data protection solutions (46%), or are part of a team that does so (45%). Thirty-two percent also describe their role as managing or implementing network data protection solutions. And 18% make the final decision regarding network data solutions.



N=200

Note: Multiple responses allowed

Q *How are you involved in decisions or recommendations regarding your agency's network data protection? (select all that apply)*

Contact Information

Market Connections
Research you can act on.

Dave Glantz, Director of Research Services
DaveG@marketconnectionsinc.com | 703.378.2025, ext. 104

Monica Mayk, Marketing Director
MonicaM@marketconnectionsinc.com | 703.378.2025, ext. 107

Susan Rose, Thought Leadership Content Lead
SusanR@marketconnectionsinc.com | 703-944-7685