

Gartner Magic Quadrant Sources and Disclaimer

1. Gartner Magic Quadrant for Network Access Control; by Lawrence Orans, John Pescatore, Mark Nicolett; March 27, 2009
2. Gartner Magic Quadrant for Endpoint Protection Platforms; by Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald; May 4, 2009
3. Gartner Magic Quadrant for Security Information and Event Management; by Mark Nicolett, Kelly M. Kavanagh; May 29, 2009
4. Gartner Magic Quadrant for Content-Aware Data Loss Prevention; by Eric Ouellet, Paul E. Proctor; June 22, 2009
5. Gartner Magic Quadrant for PC Life Cycle Configuration Management; by Terrence Cosgrove, Ronni J. Colville; December 29, 2008

The Magic Quadrants are copyrighted by Gartner, Inc. and are reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Appendix

Full slide deck (all questions)

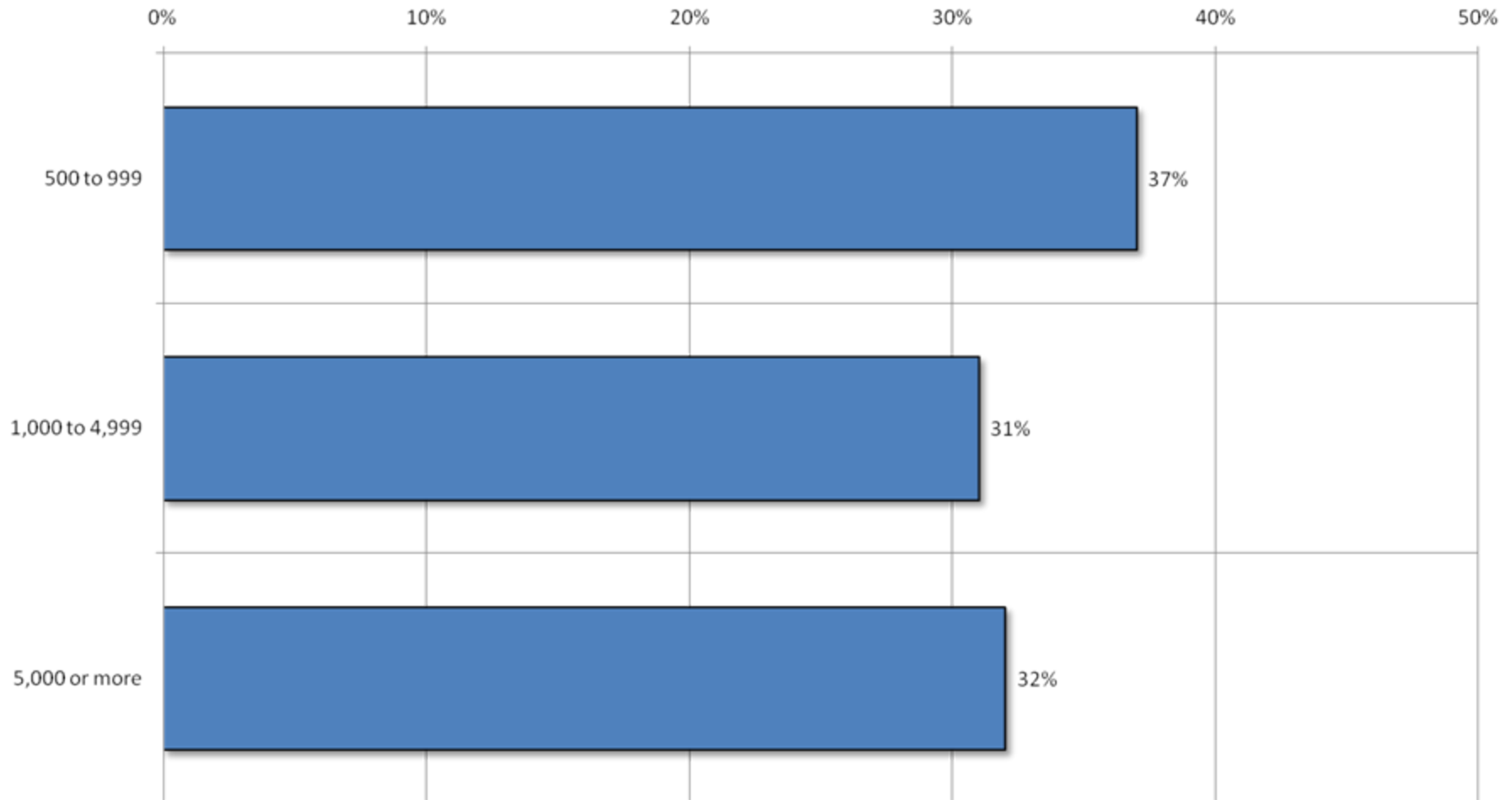
Methodology

- Applied Research performed survey
- January 2010
- 2,100 worldwide responses
- Small enterprise (500 – 999 employees)
- Medium enterprise (1,000 – 4,999 employees)
- Large enterprise (5,000 or more employees)

Demographics

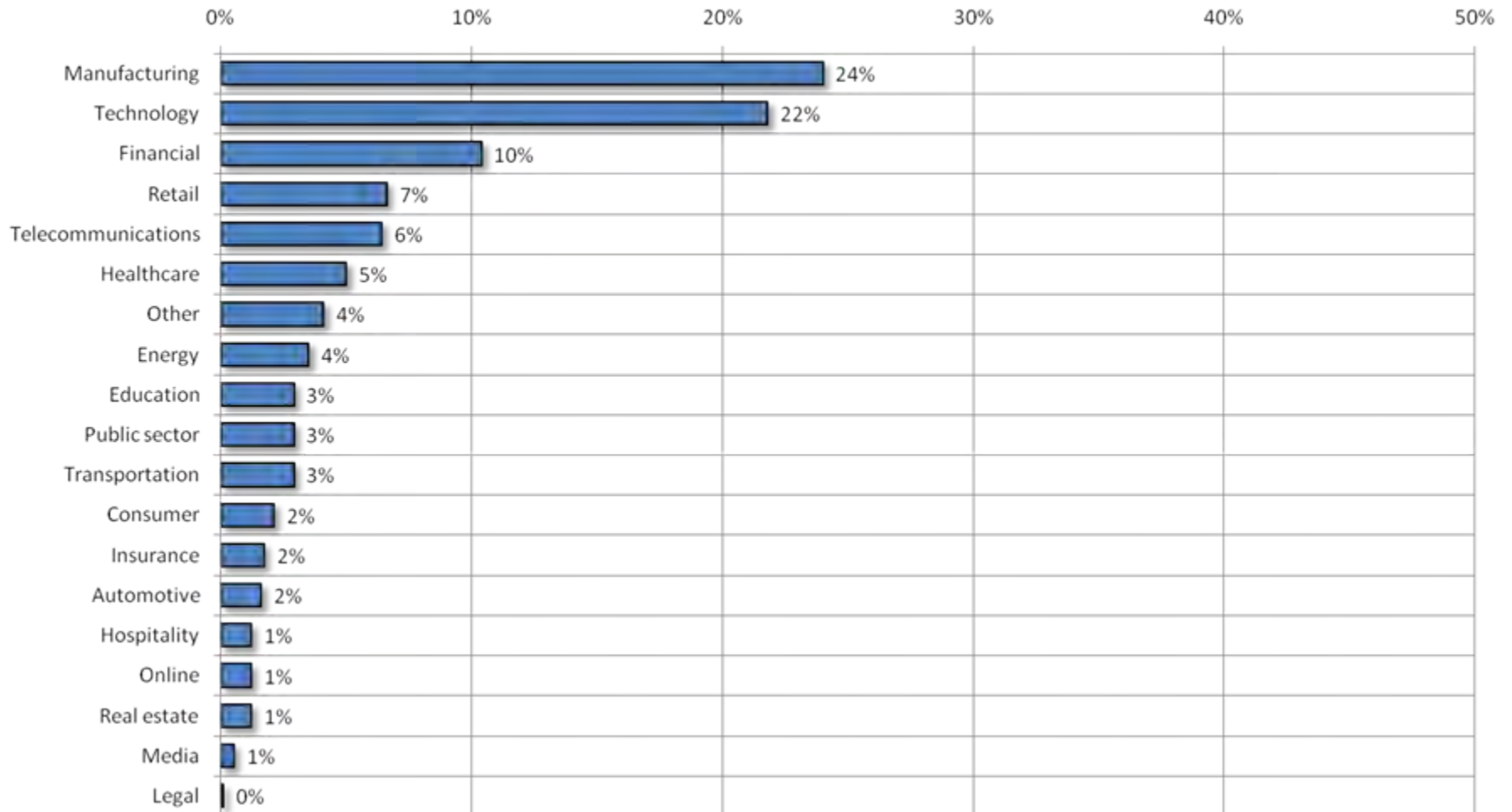
Company size

Q1: How many employees are in your company worldwide?



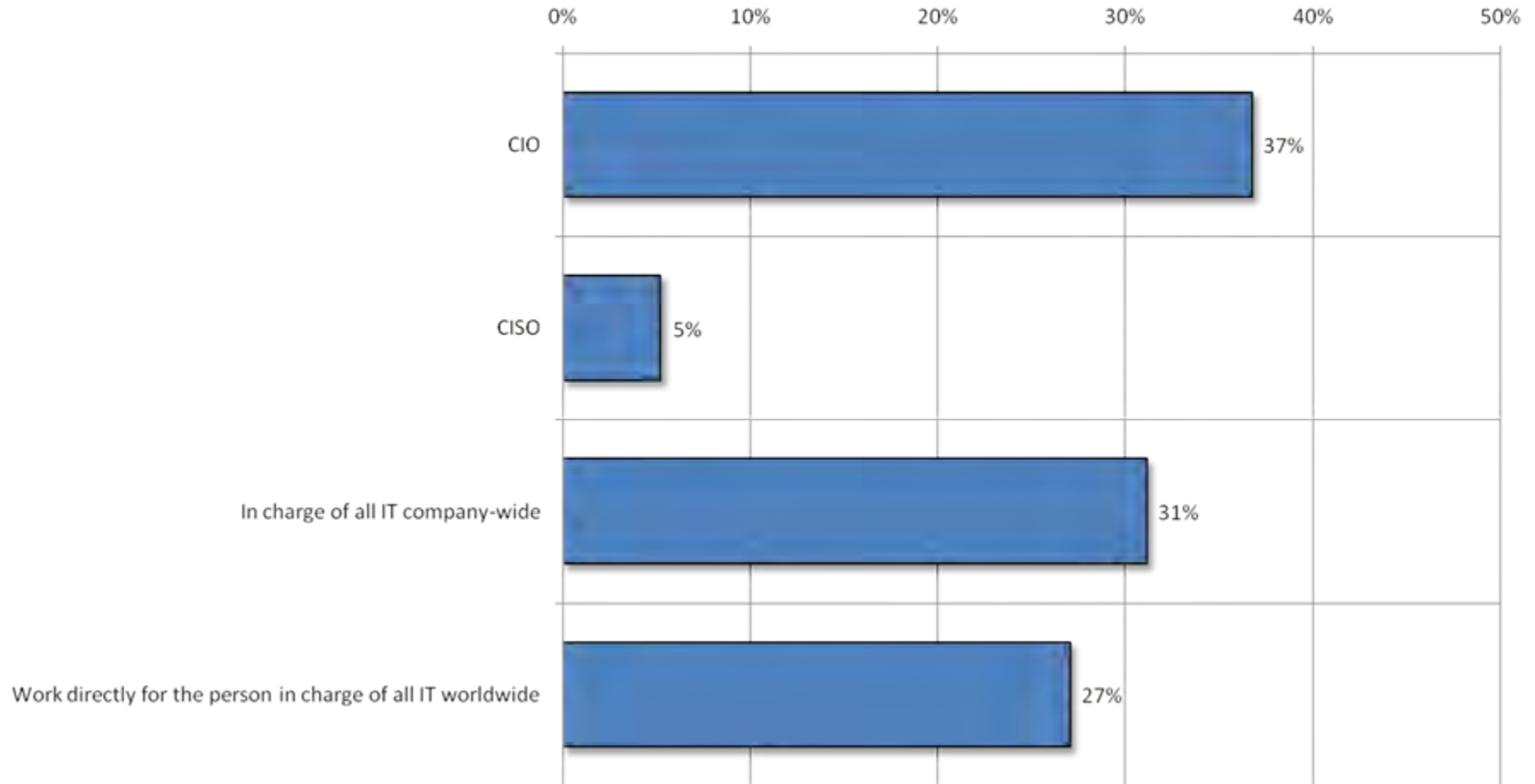
Industries

Q2: In which industry do you work?



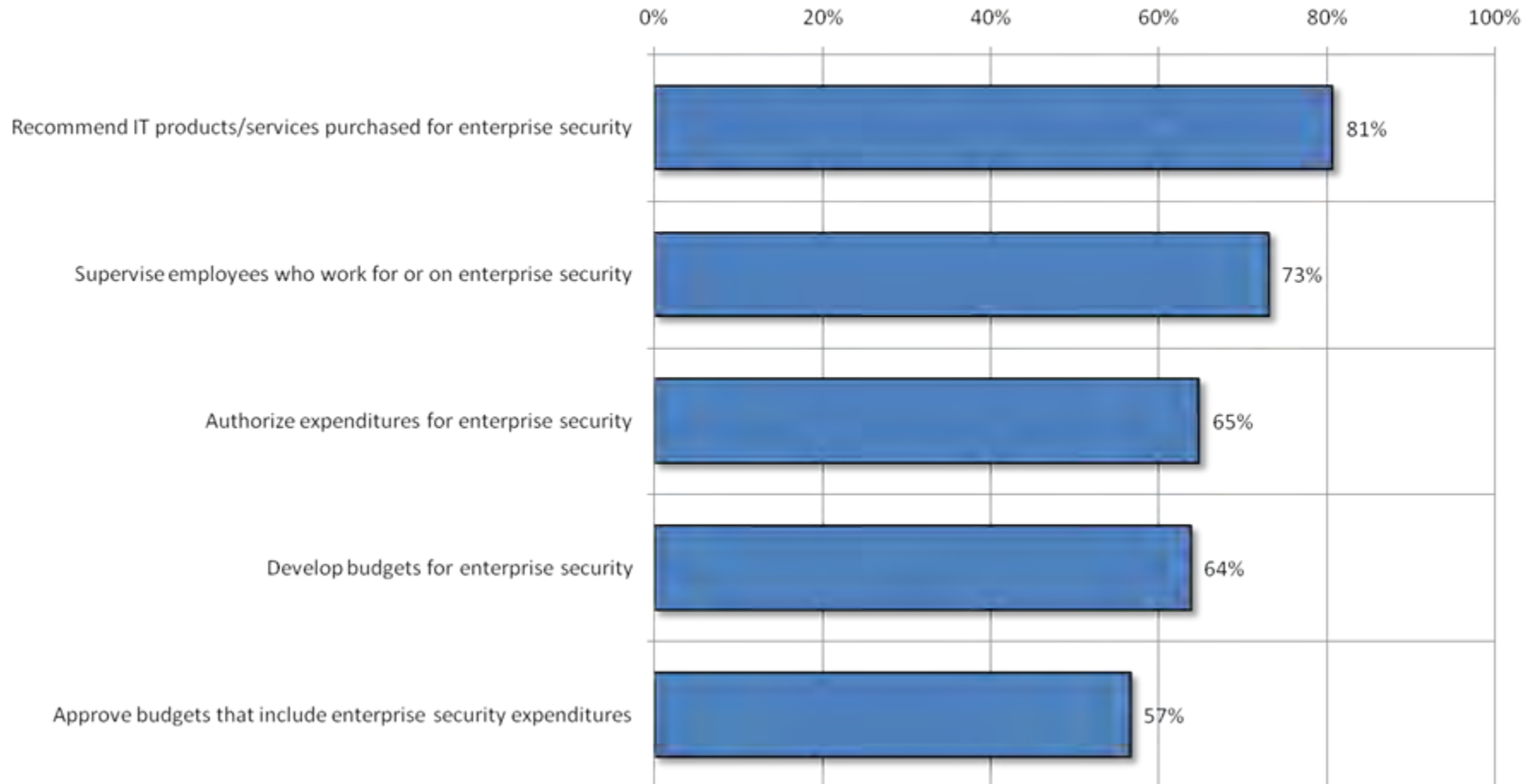
Medium enterprise

Q5: What is your role within your company?
(Only asked of Medium Enterprise)



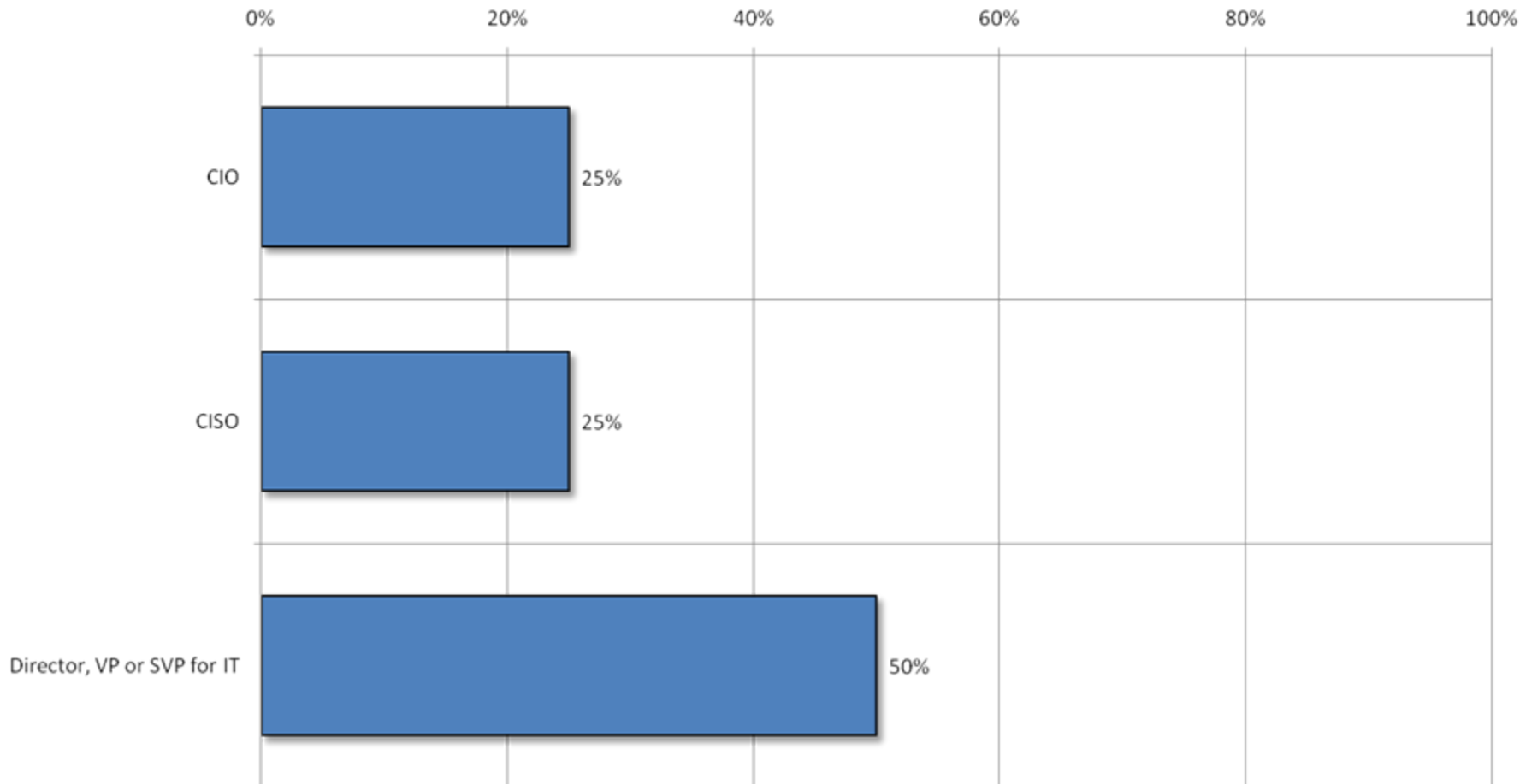
Medium enterprise

Q6: Which of the following, if any, do you do?
(Only asked of Medium Enterprise)



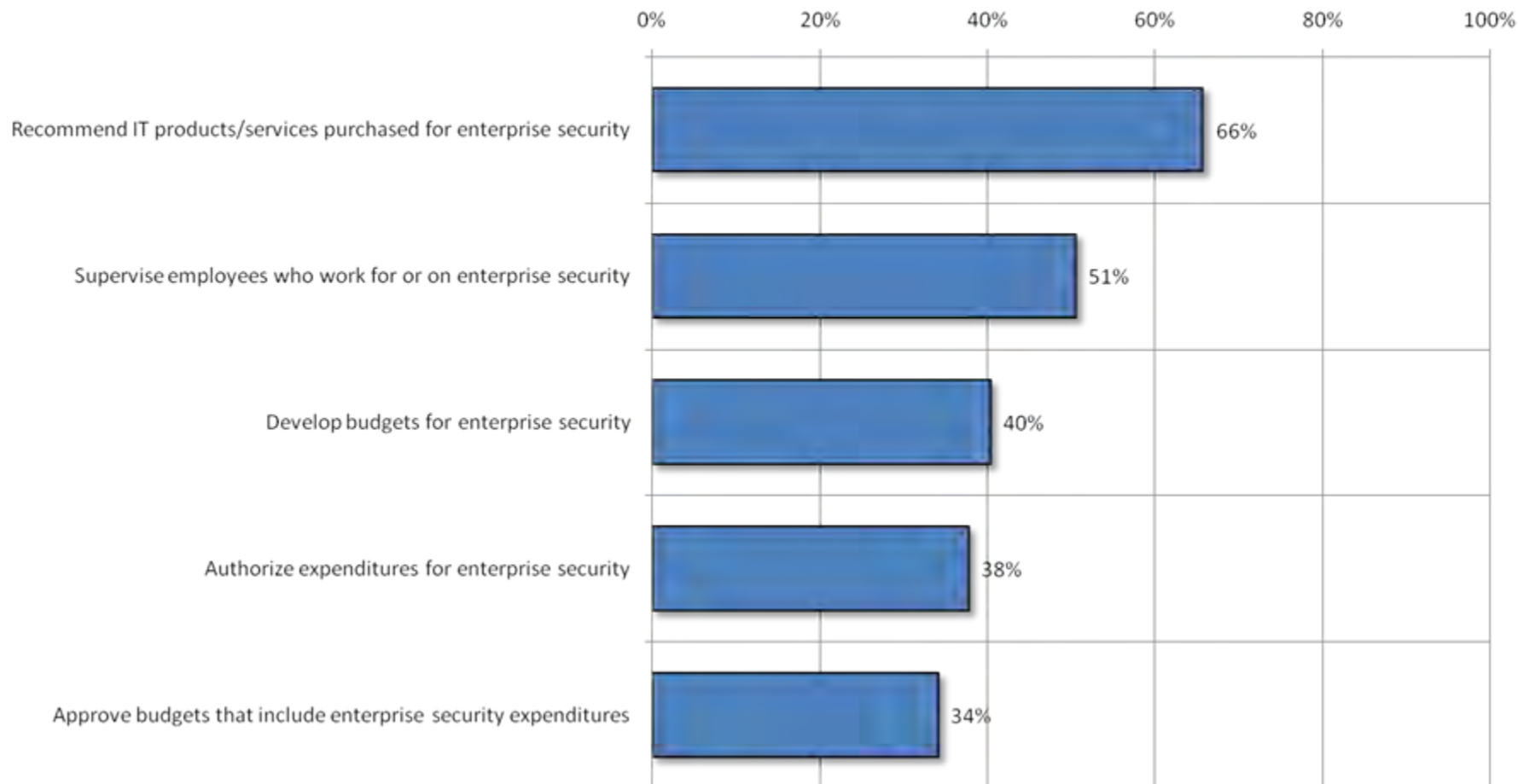
Large enterprise

Q7: What is your role within your company?
(Only asked of Large Enterprise)



Large enterprise

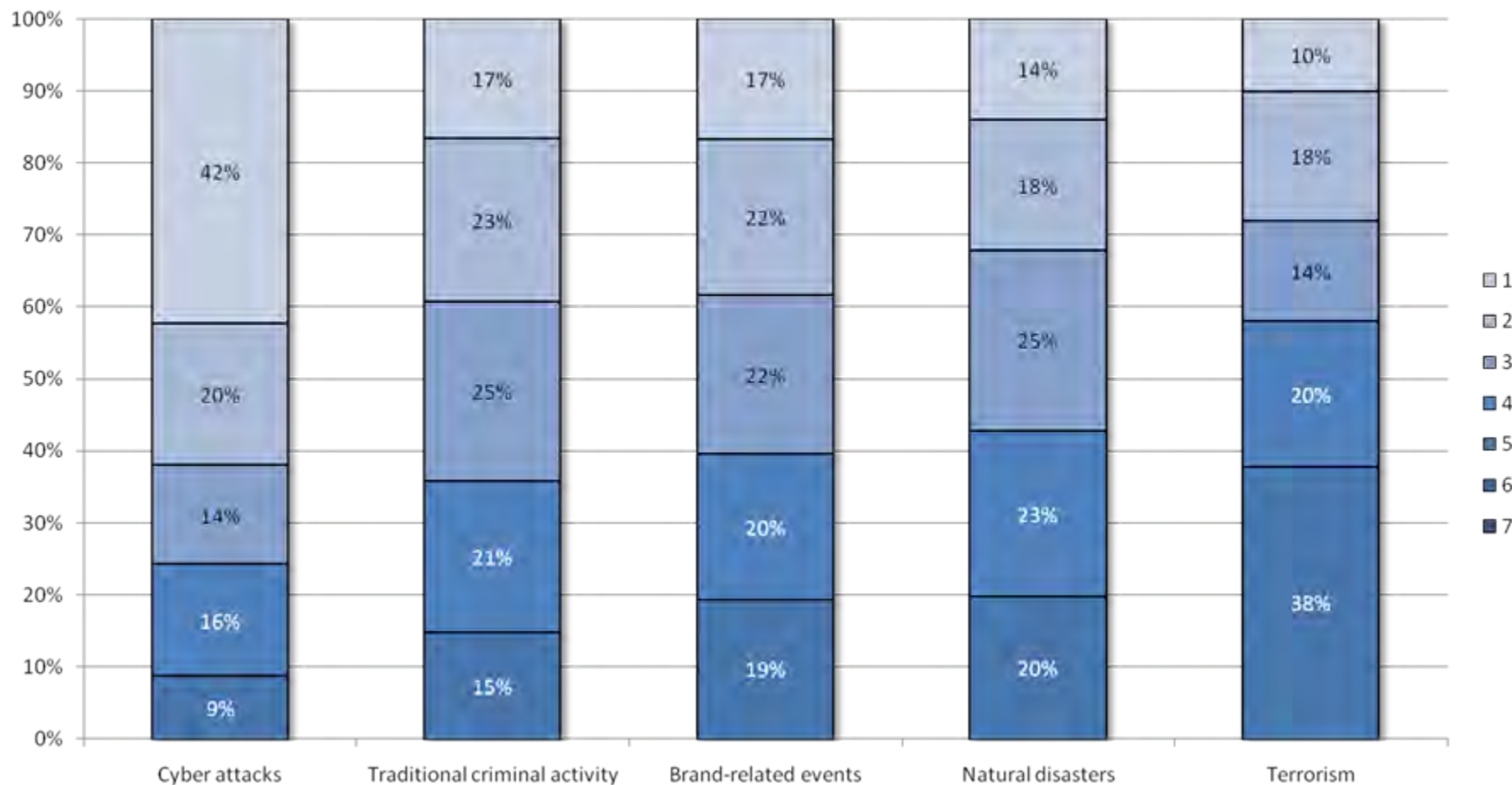
Q8: Which of the following, if any, do you do?
(Only asked of Large Enterprise)



Objectives

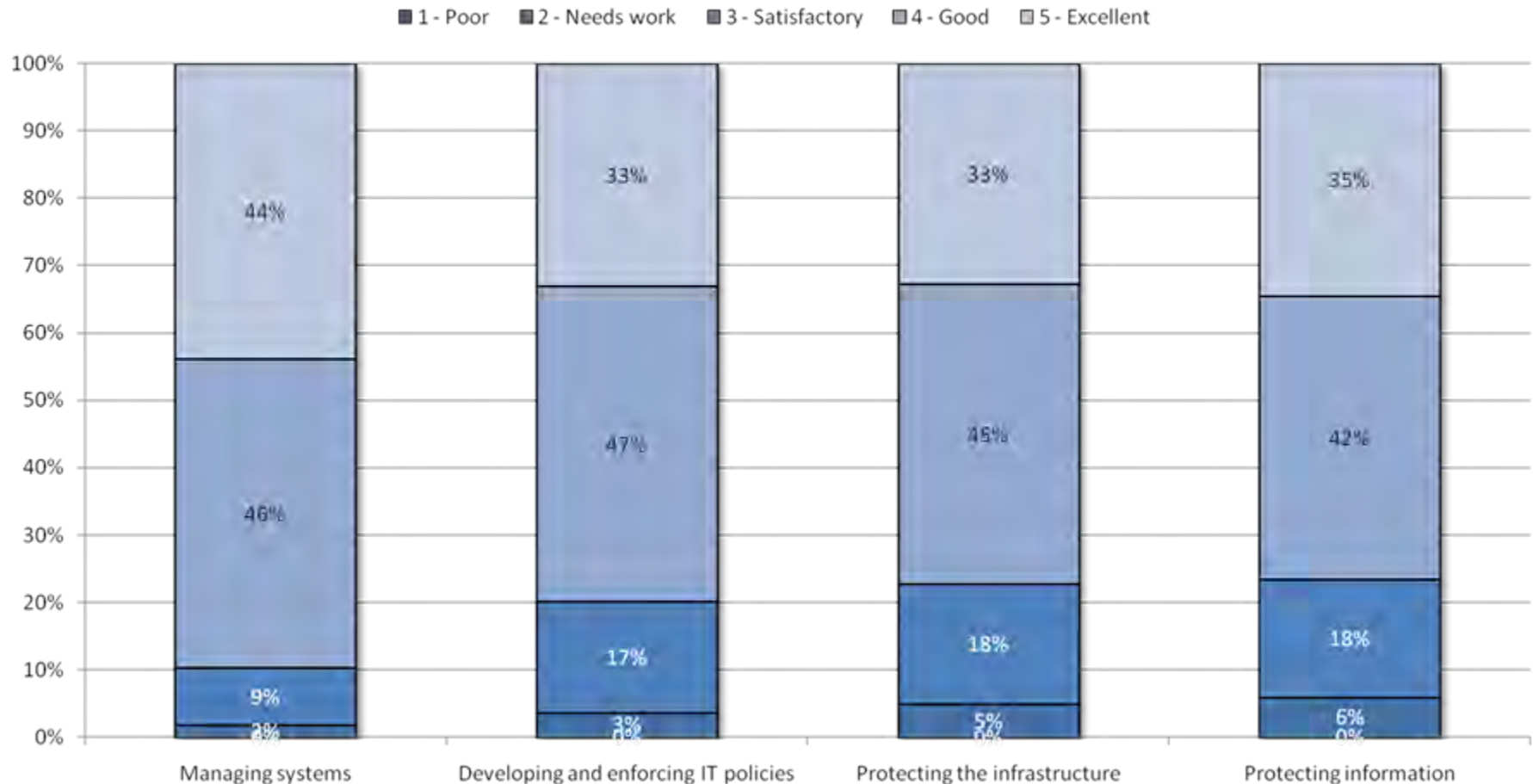
Security risks

Q9: Please rank the following risks in order of significance to your organization.



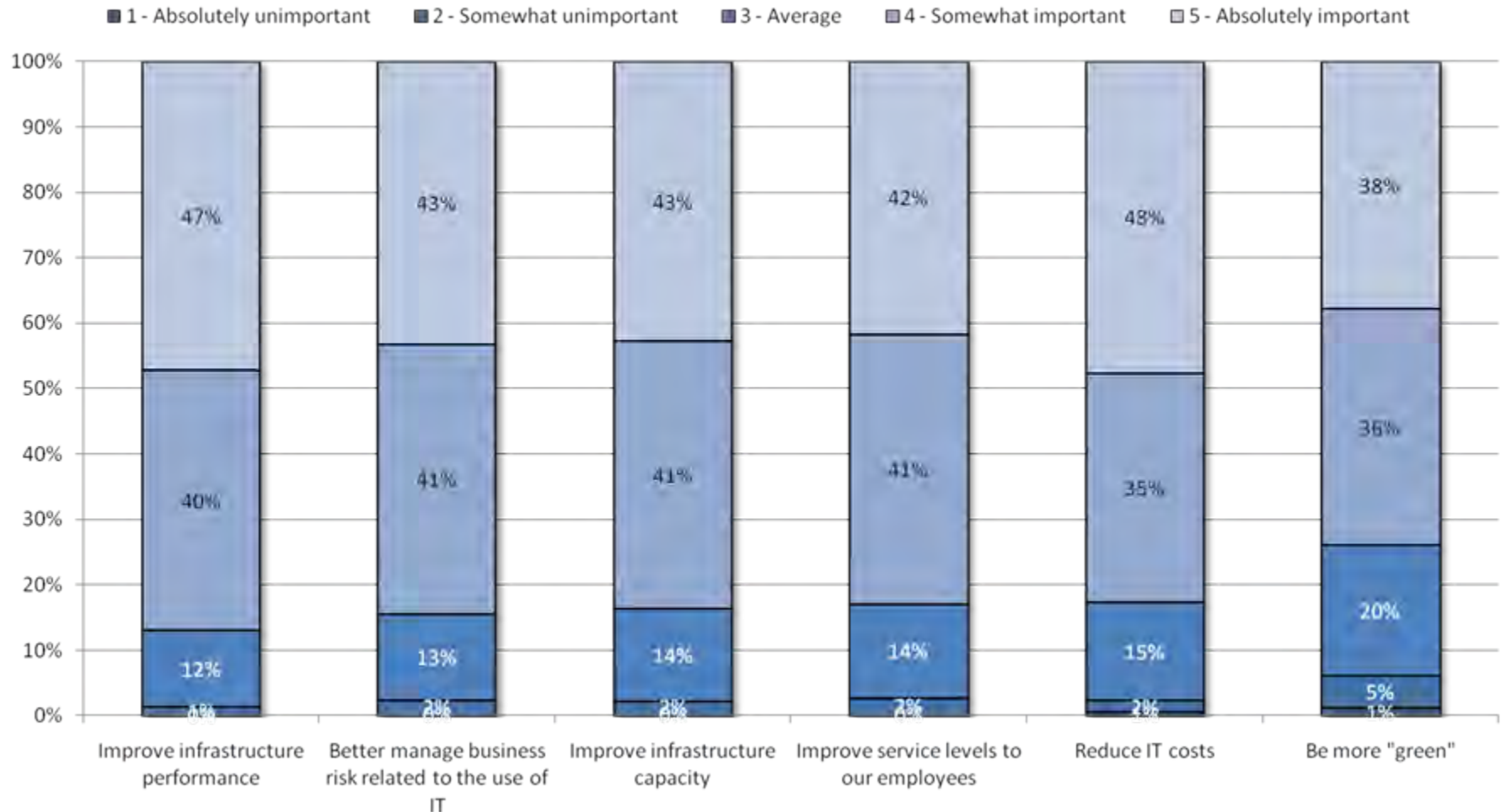
Enterprise security status

Q10: How would you rate your organization's current state in each of these areas of Enterprise Security?



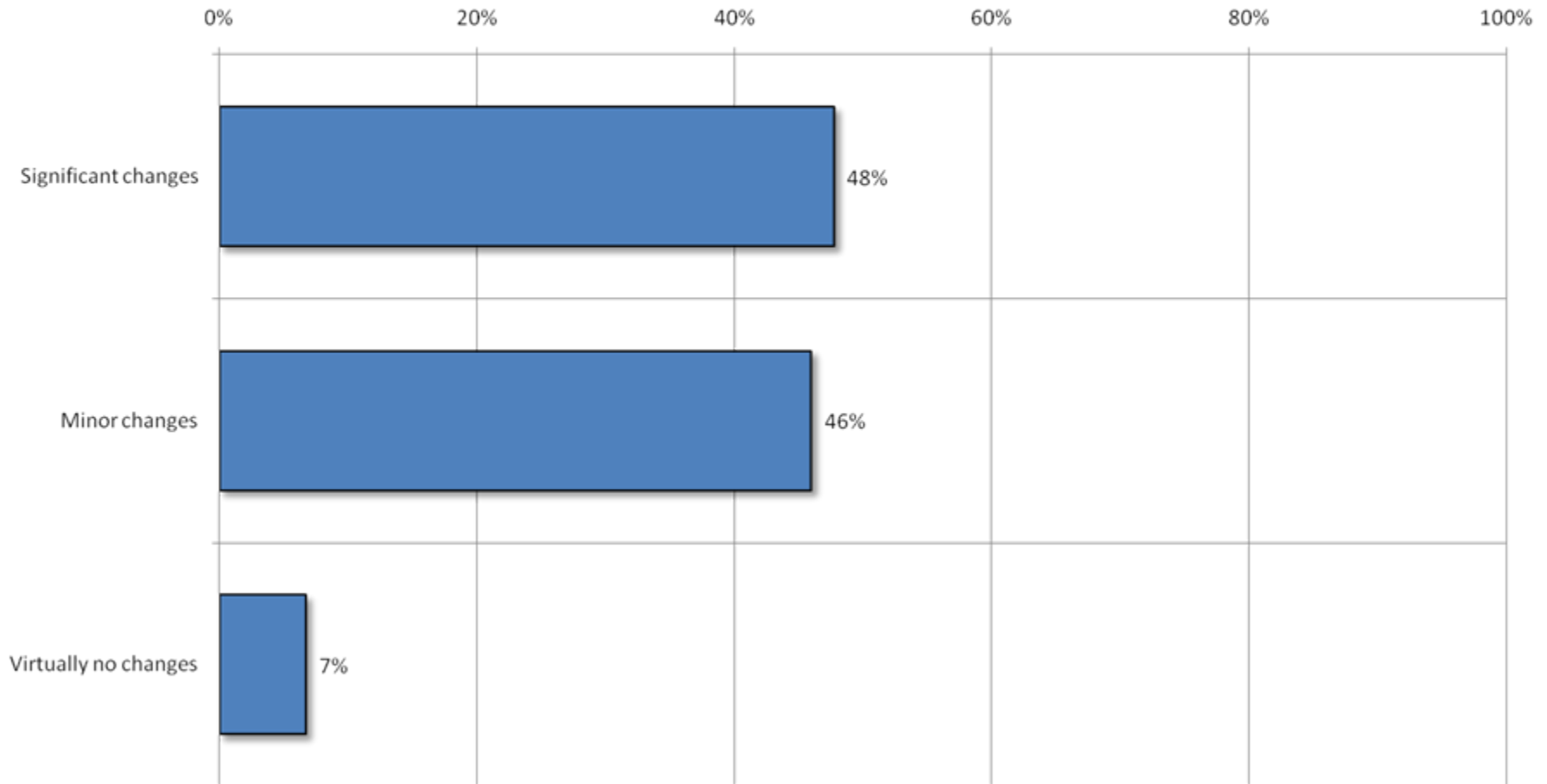
IT improvements

Q11: Please rate the following IT improvement areas for 2010.



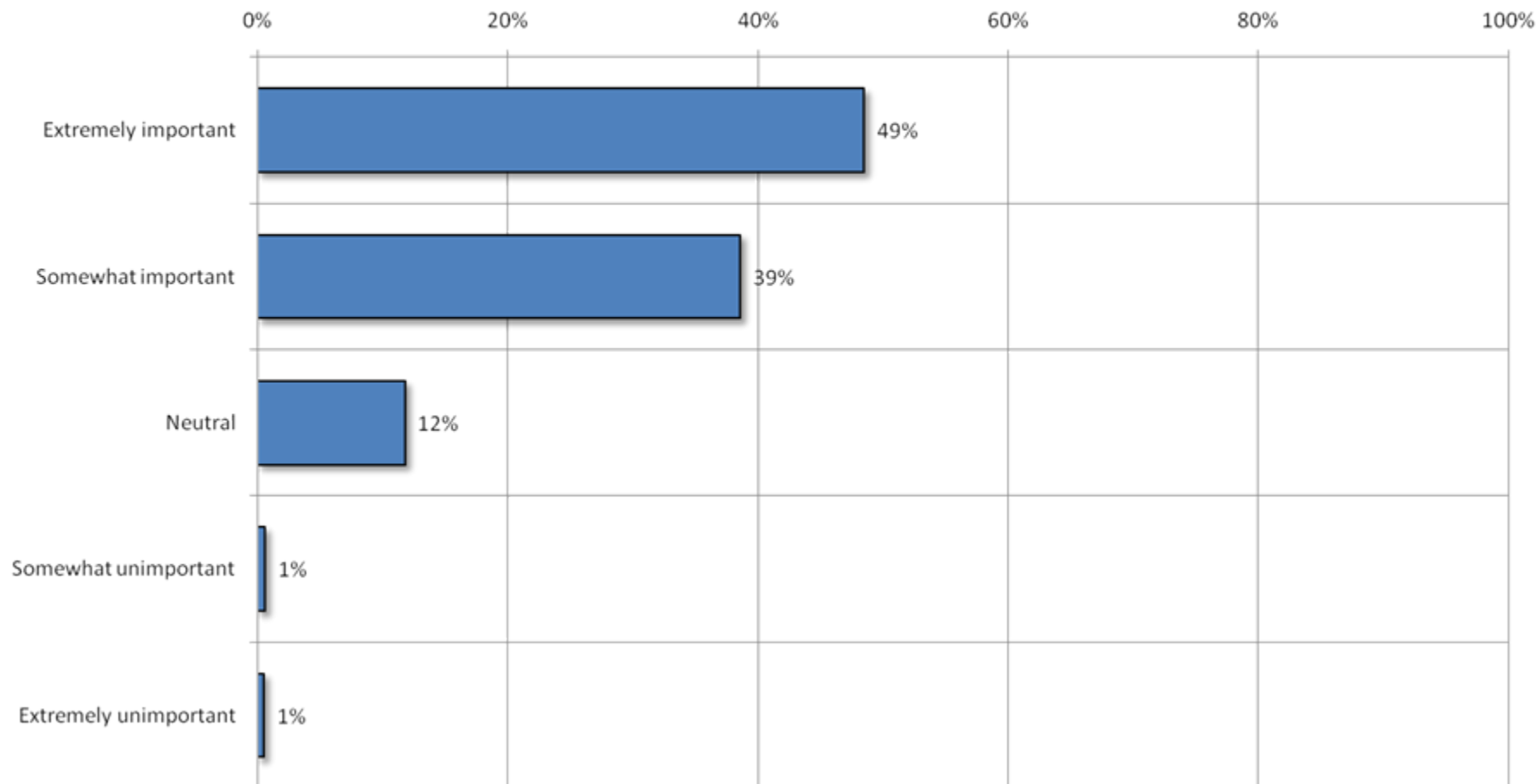
Planned change for enterprise security

Q12: How would you characterize the level of change to the enterprise security you are planning for 2010?



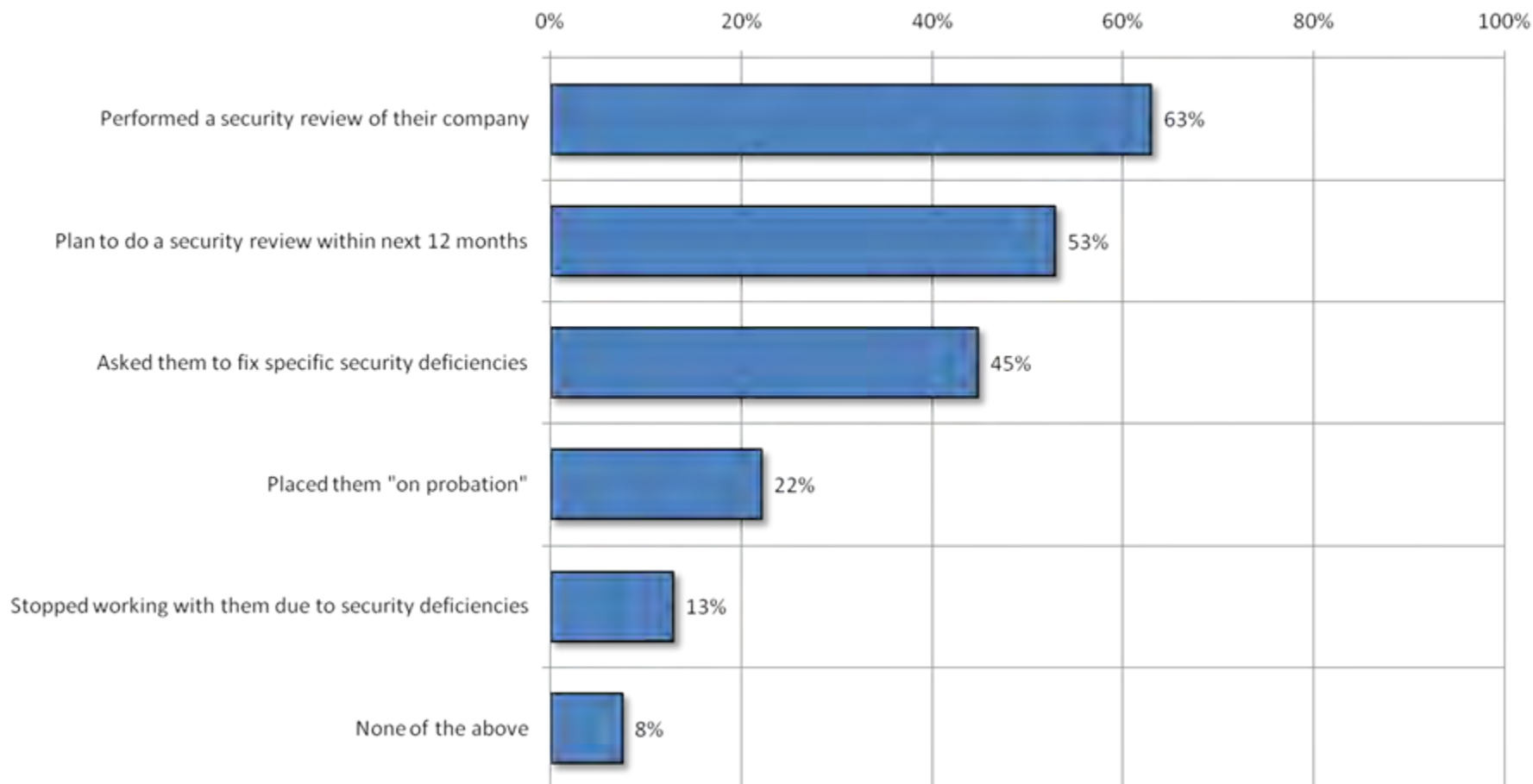
Vendor security protection

**Q13: How important is the security protection level of your vendors
(companies you buy goods or services from)?**



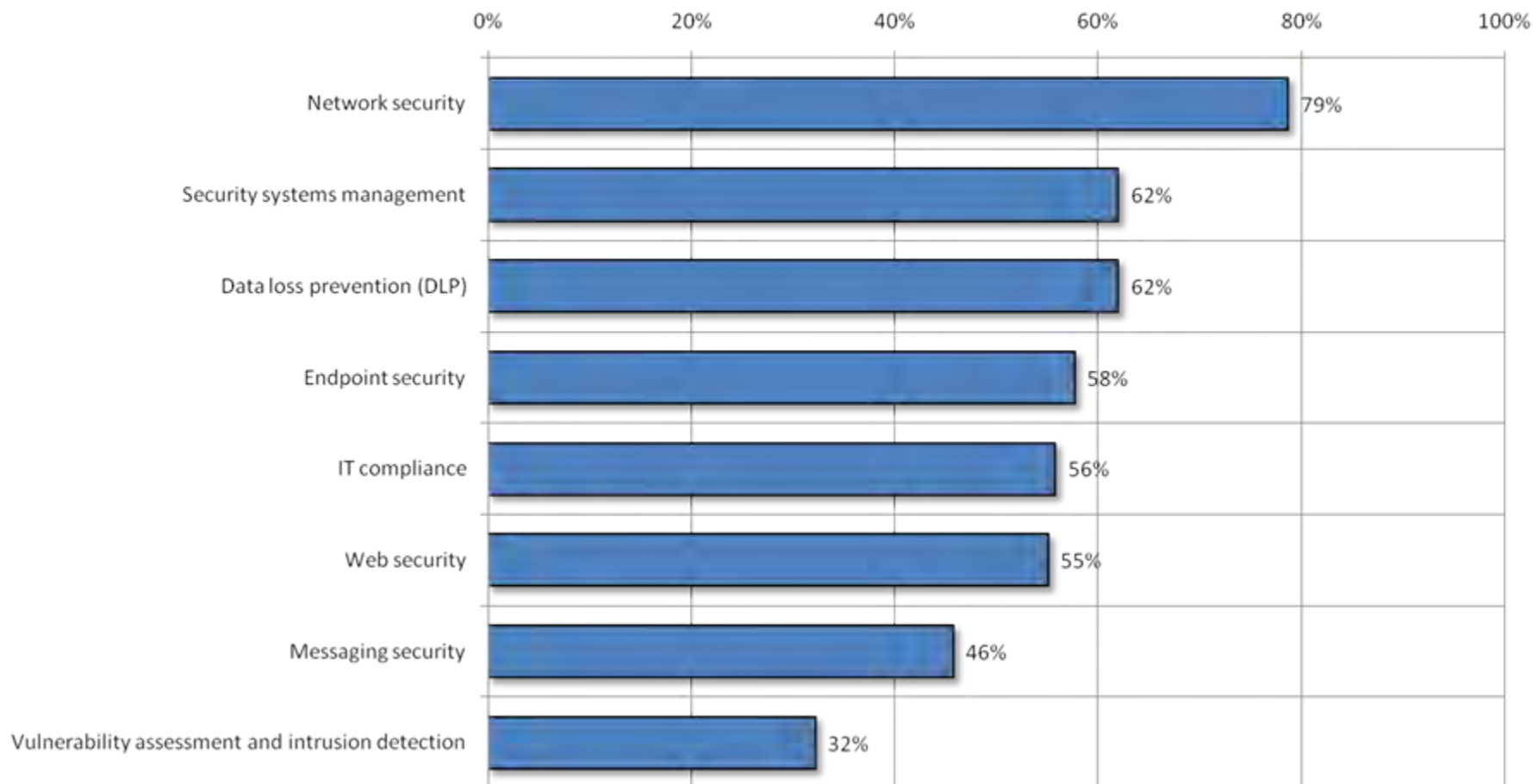
Vendor security

Q14: Which of the following statements is true for your organization with regards to vendors?



Vendor security

Q15: If you answered yes to any statements in Q14, indicate which security areas were involved. Mark all that apply.



Staffing & Budget

Enterprise security staff

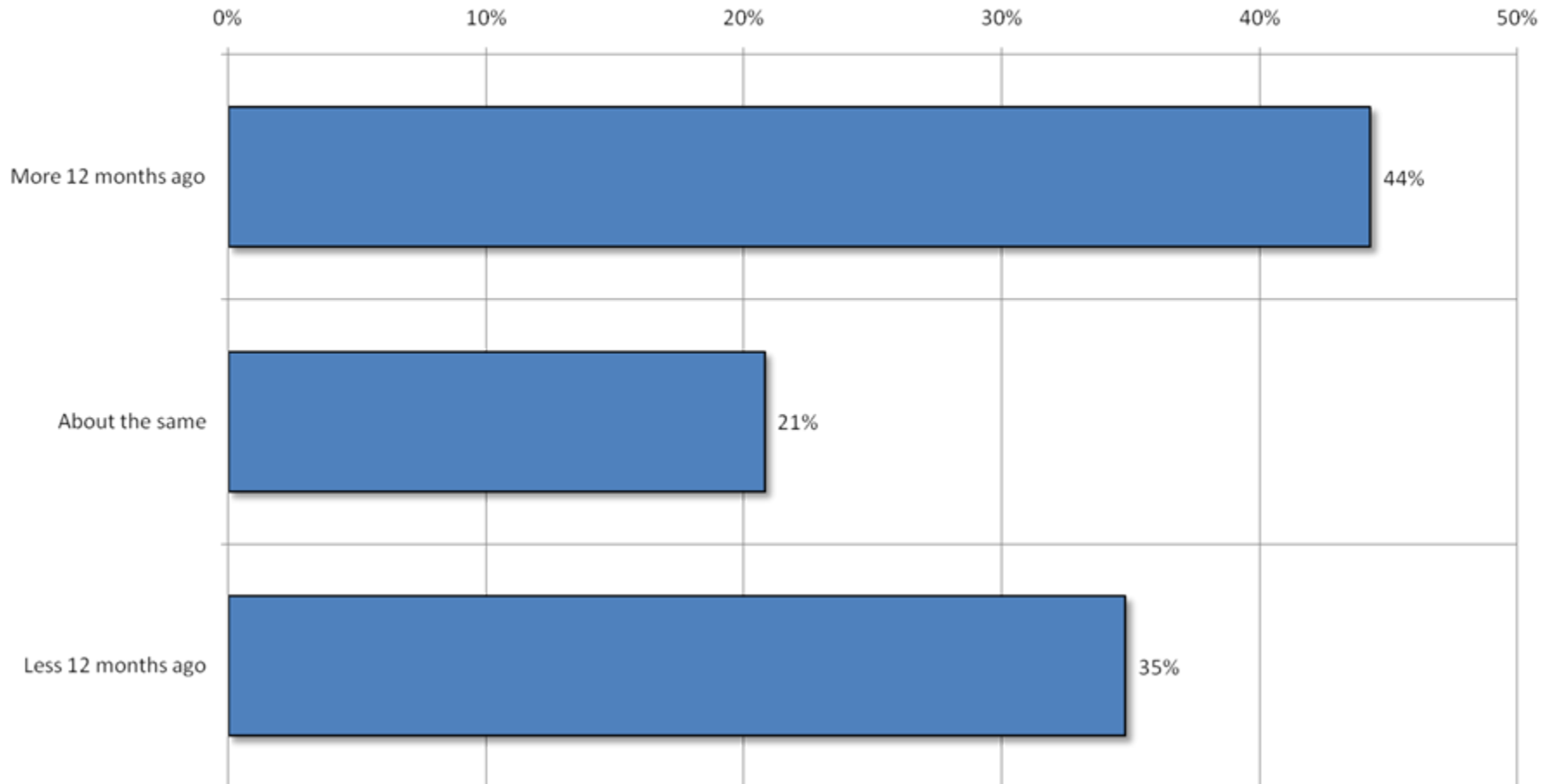
Q16: Roughly how many people work on enterprise security or IT compliance in your organization worldwide?

Median

120 people

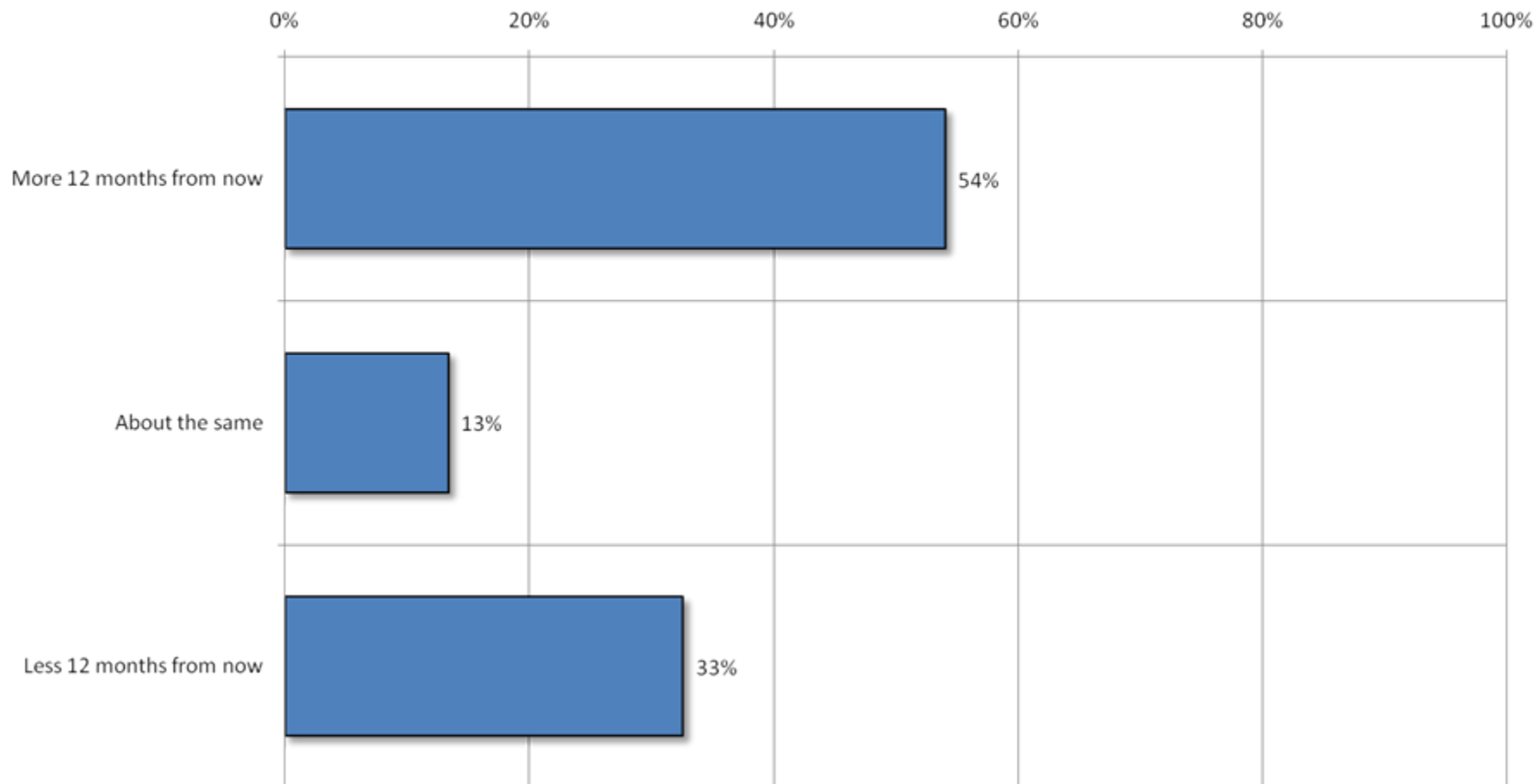
Enterprise security staff

Q17: How does the size of your enterprise security and IT compliance staff compare to 12 months ago?



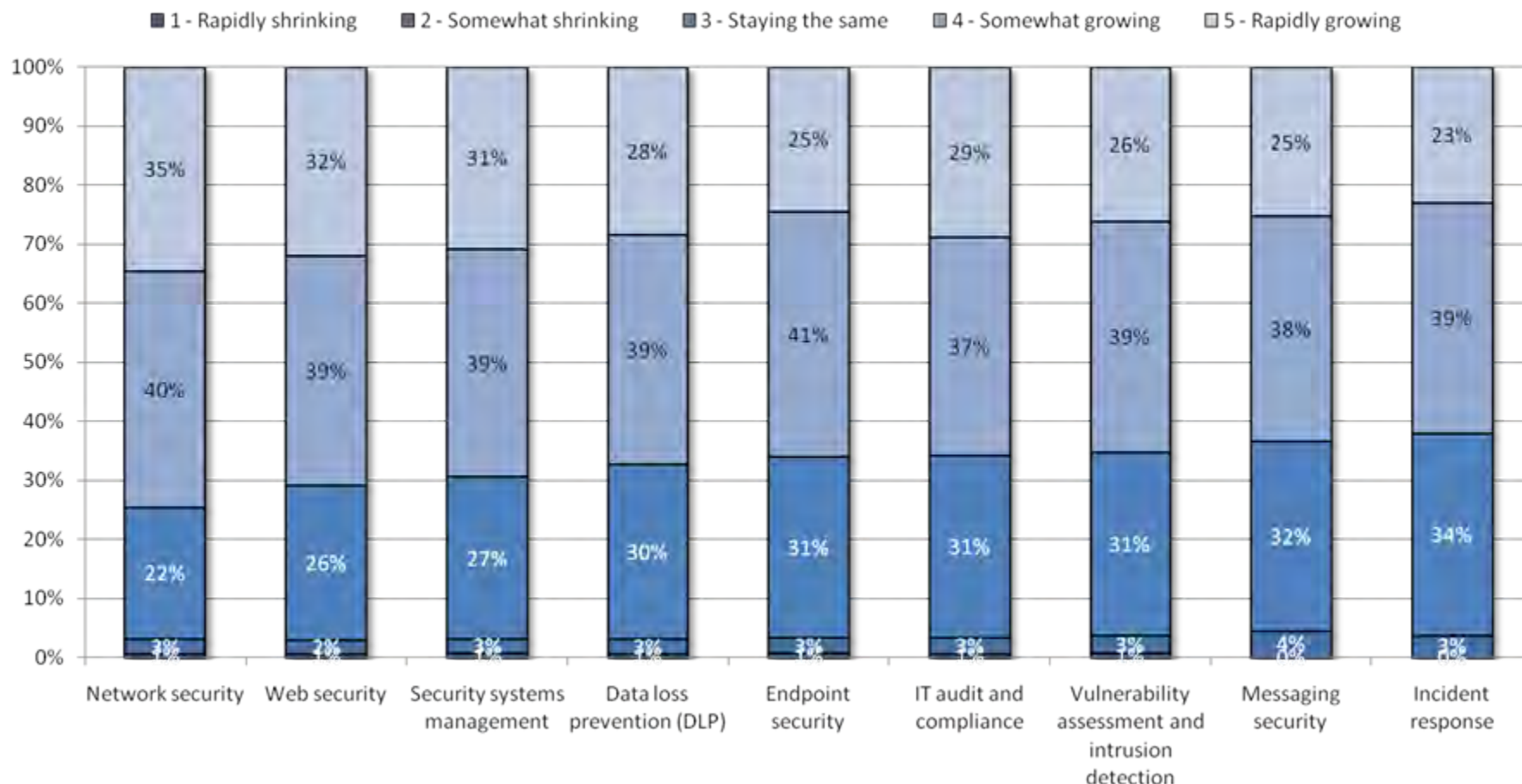
Enterprise security staff

Q18: How will the size of your enterprise security and IT compliance staff change over the next 12 months?



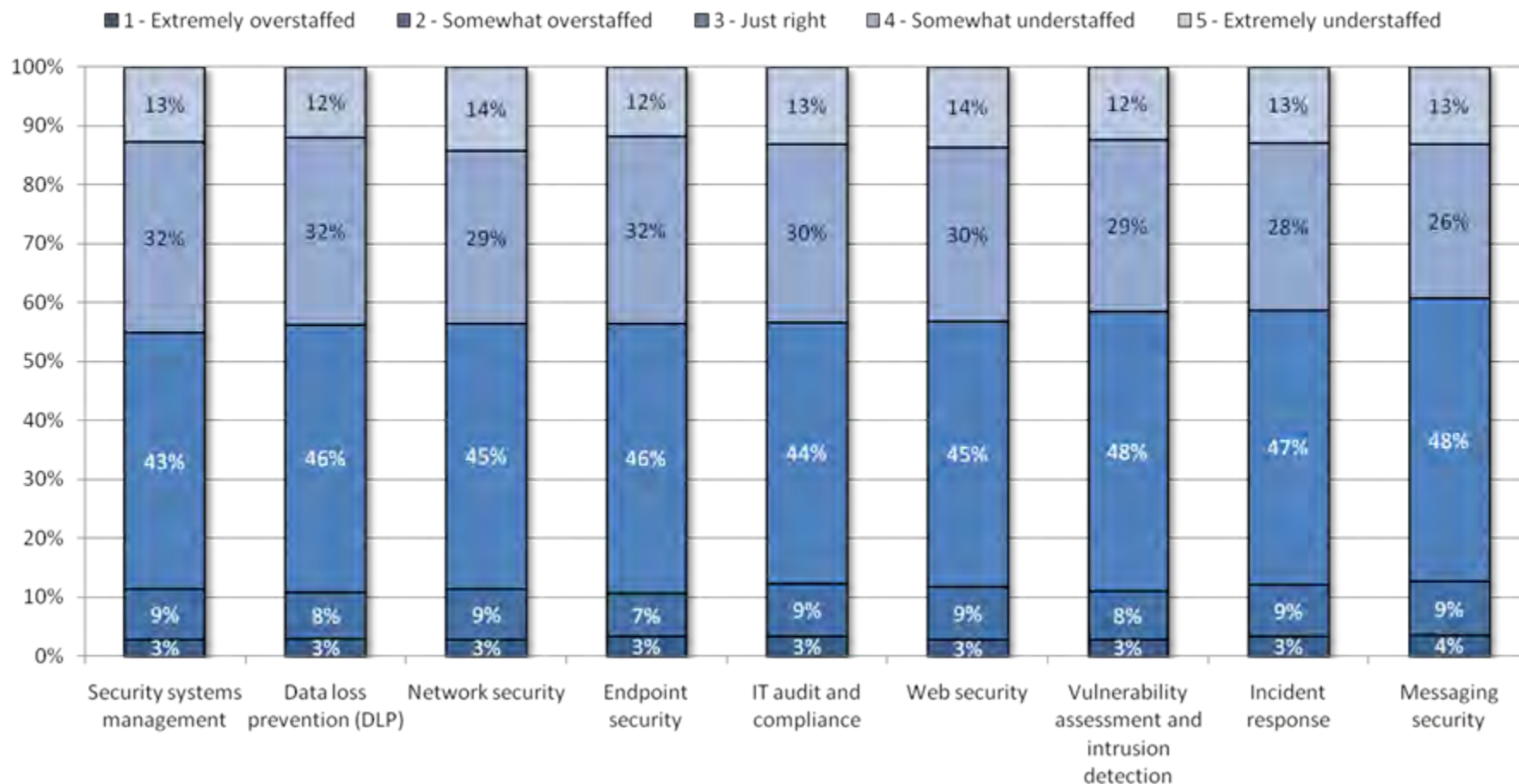
Manpower capacity change

Q19a: How would you characterize your manpower capacity for each of the following enterprise security skill sets?



Manpower capacity staffing

Q19b: How would you characterize your manpower capacity for each of the following enterprise security skill sets?



Enterprise security job requisitions

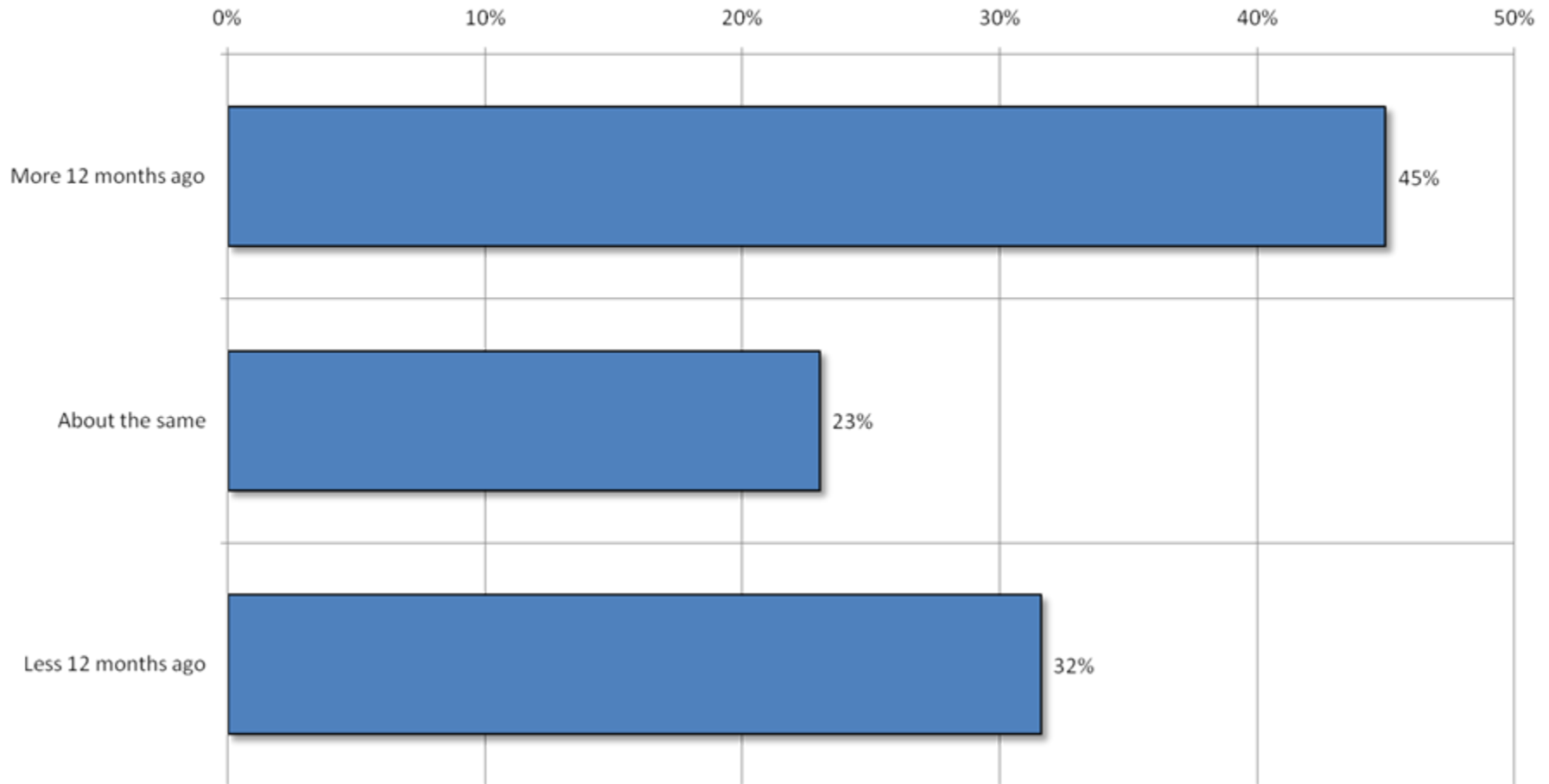
Q20: How many requisitions for enterprise security jobs does your company have open worldwide at the moment?

Median

20 requisitions

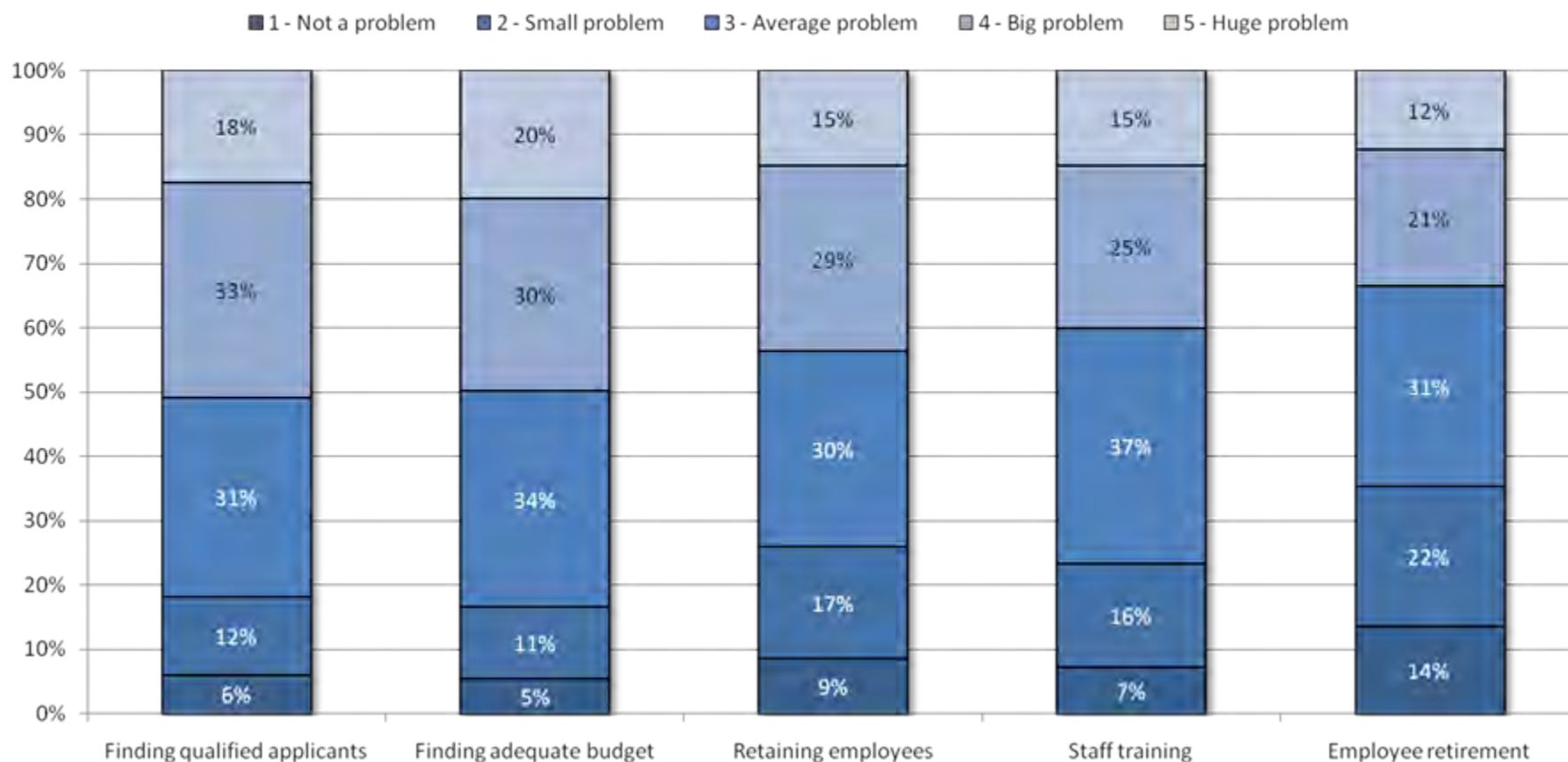
Enterprise security job requisitions

Q21: How does the number of enterprise security jobs your company currently has open compare to 12 months ago?



Staff recruiting

Q22: How big or small is each of the following problems when your organization is trying to recruit or retain enterprise security staff appropriately?



Enterprise security budget

Q23: What will your annual budget for all of your enterprise security worldwide be in 2010?

Median

\$600,000

Enterprise security budget

Q24: What is the percentage change for your enterprise security budgets over 2009?

Median

11%

Enterprise security budget

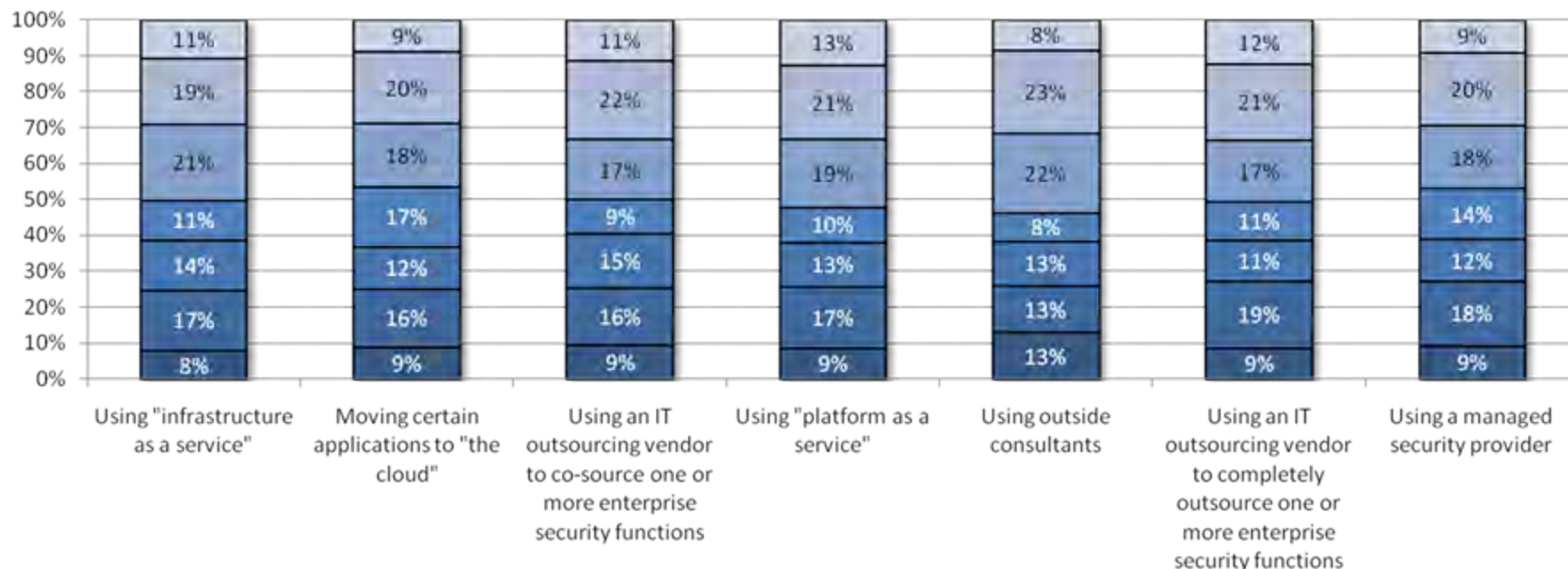
Q25: Looking ahead, what do you anticipate the percentage change for your enterprise security budgets will be in 2011 when compared to 2010?

Median	11%
--------	-----

Outsourcing

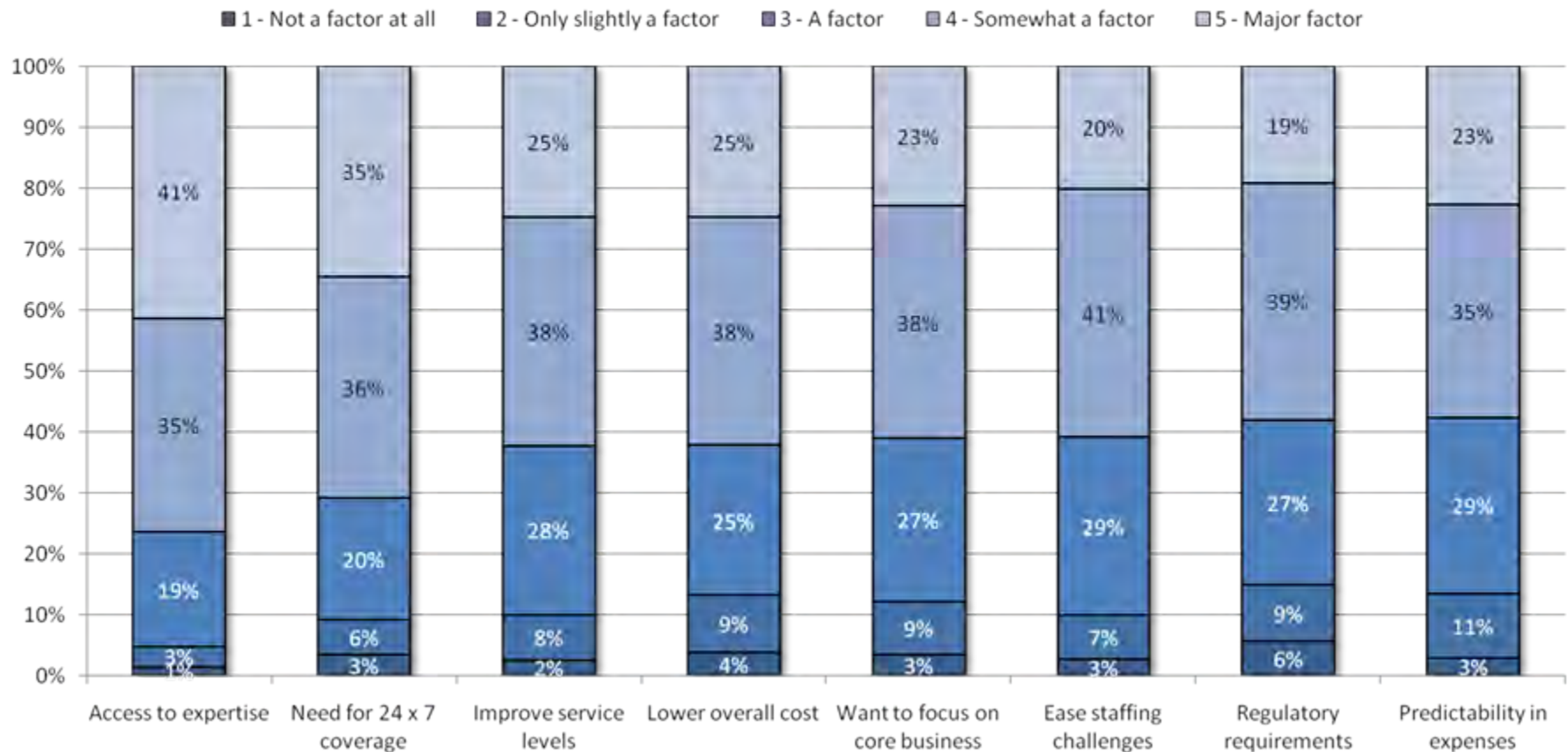
Q27: What methods -- if any -- do you use (or plan to use) to augment your internal staff's capacity in order to accomplish more than you could on your own?

- 1 - We do not think of this activity as being "outsourcing" per se
- 2 - Do not employ, no plans to do so
- 3 - Do not use, but are exploring
- 4 - Do not use, but plan to in the future
- 5 - Currently using in a minor way
- 6 - Currently using in a moderate way
- 7 - Currently using in a major way



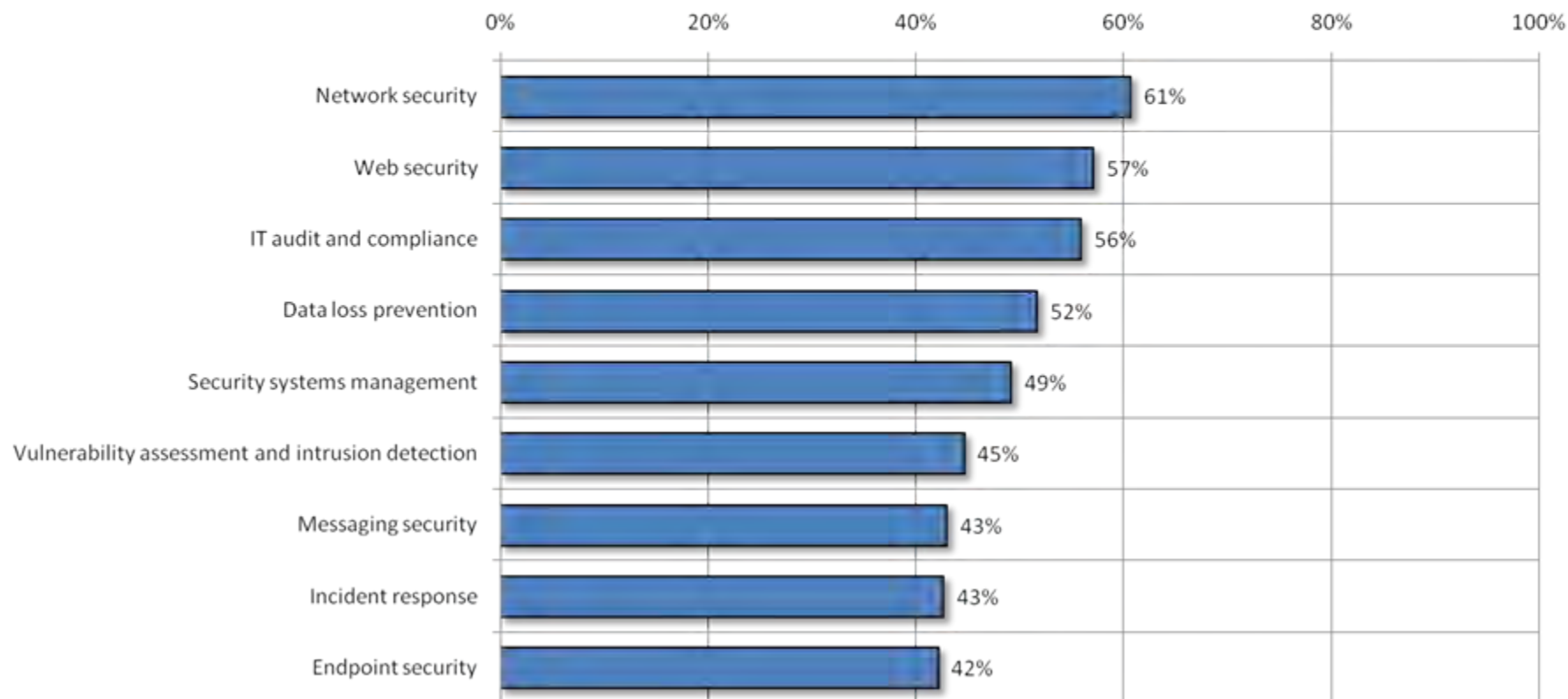
Outsourcing

Q28: What factors influenced your decision to consider these methods?
(Only asked of those who indicated that they are at least considering at least one of the tactics in previous question)



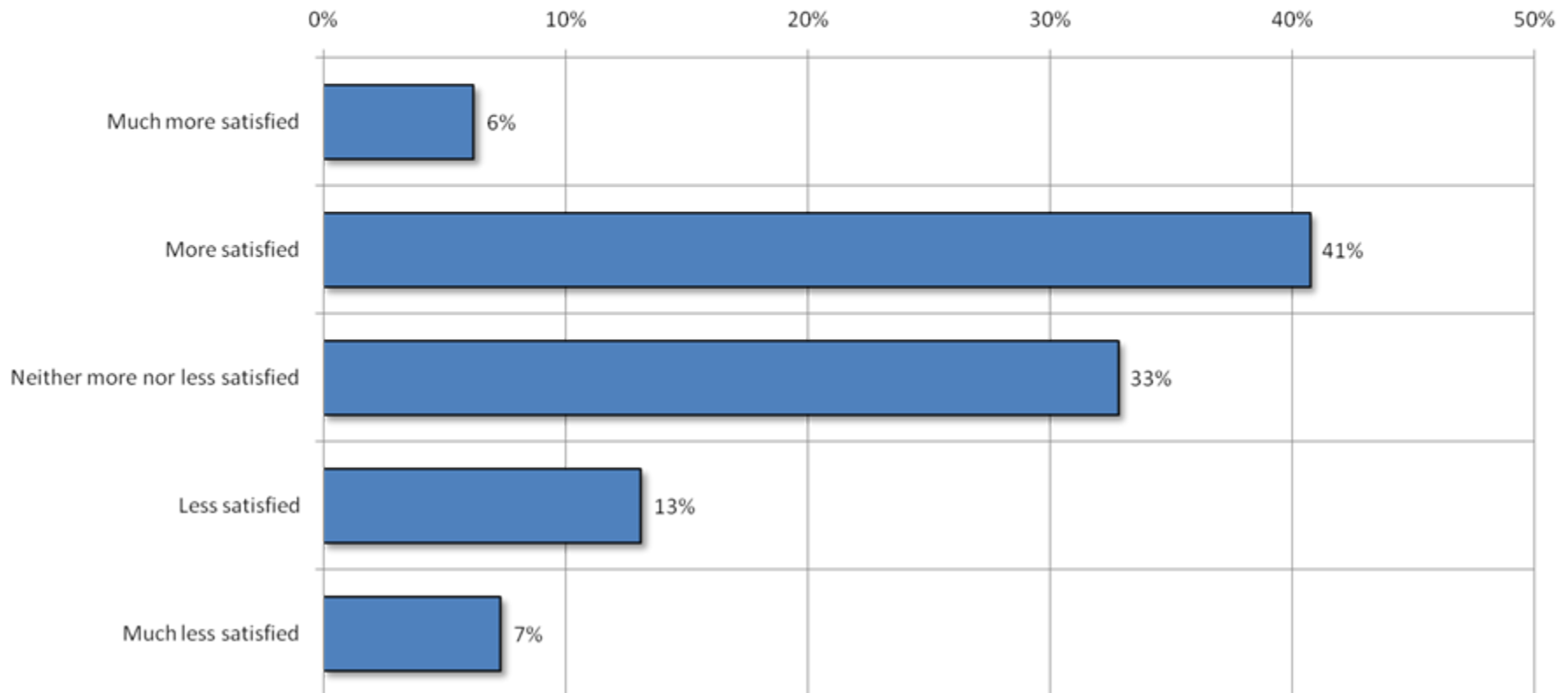
Outsourcing

Q29: What kinds of tasks are you considering (or will you consider) using these outsourcing methods for? (Only asked of those who indicated that they are at least considering at least one of the tactics in Q31)



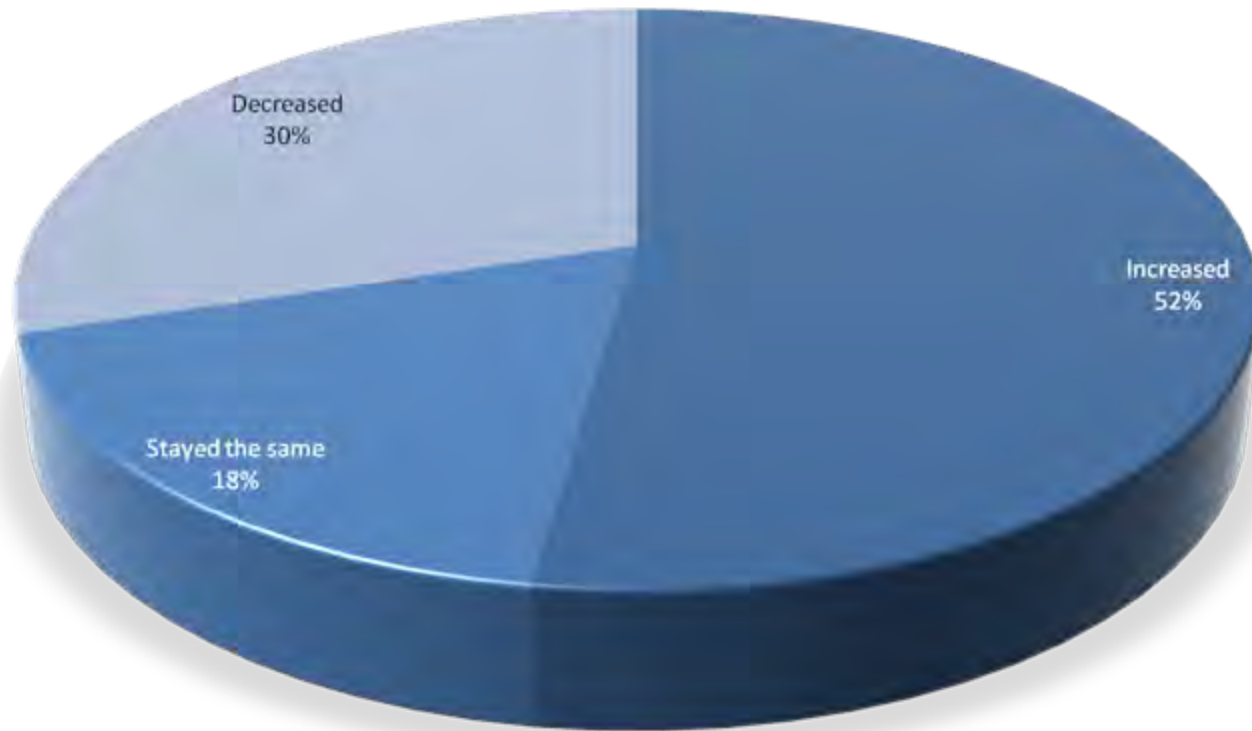
Outsourcing impact

Q30: Over the past 12 months, how do you think the use of outsourcing has impacted internal users' satisfaction with the organization's enterprise security? (Only asked of those who indicated that they are at least considering at least one of the tactics)



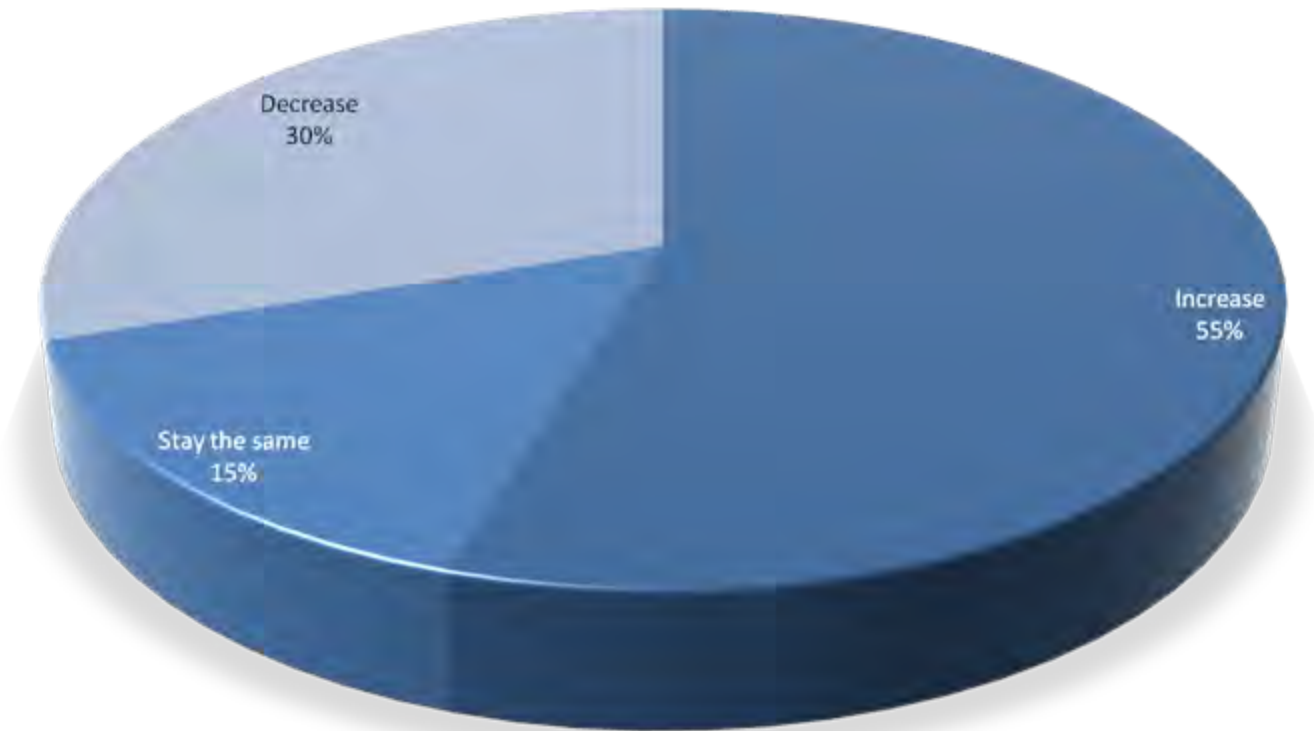
Training budget

Q31: Has your budget for staff training (in the area of enterprise security) in the past 12 months...?



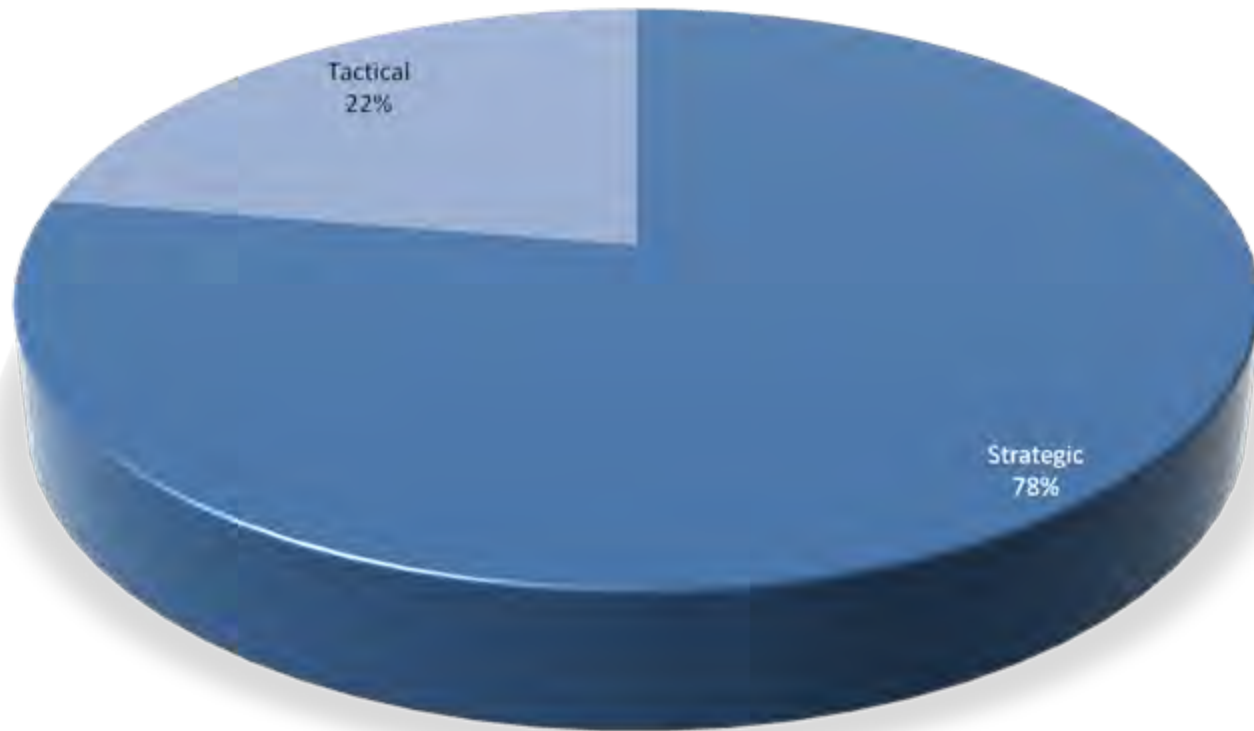
Training budget

Q32: Related to budget for staff training (in the area of enterprise security), in the next 12 months, do you expect it to...?



Training

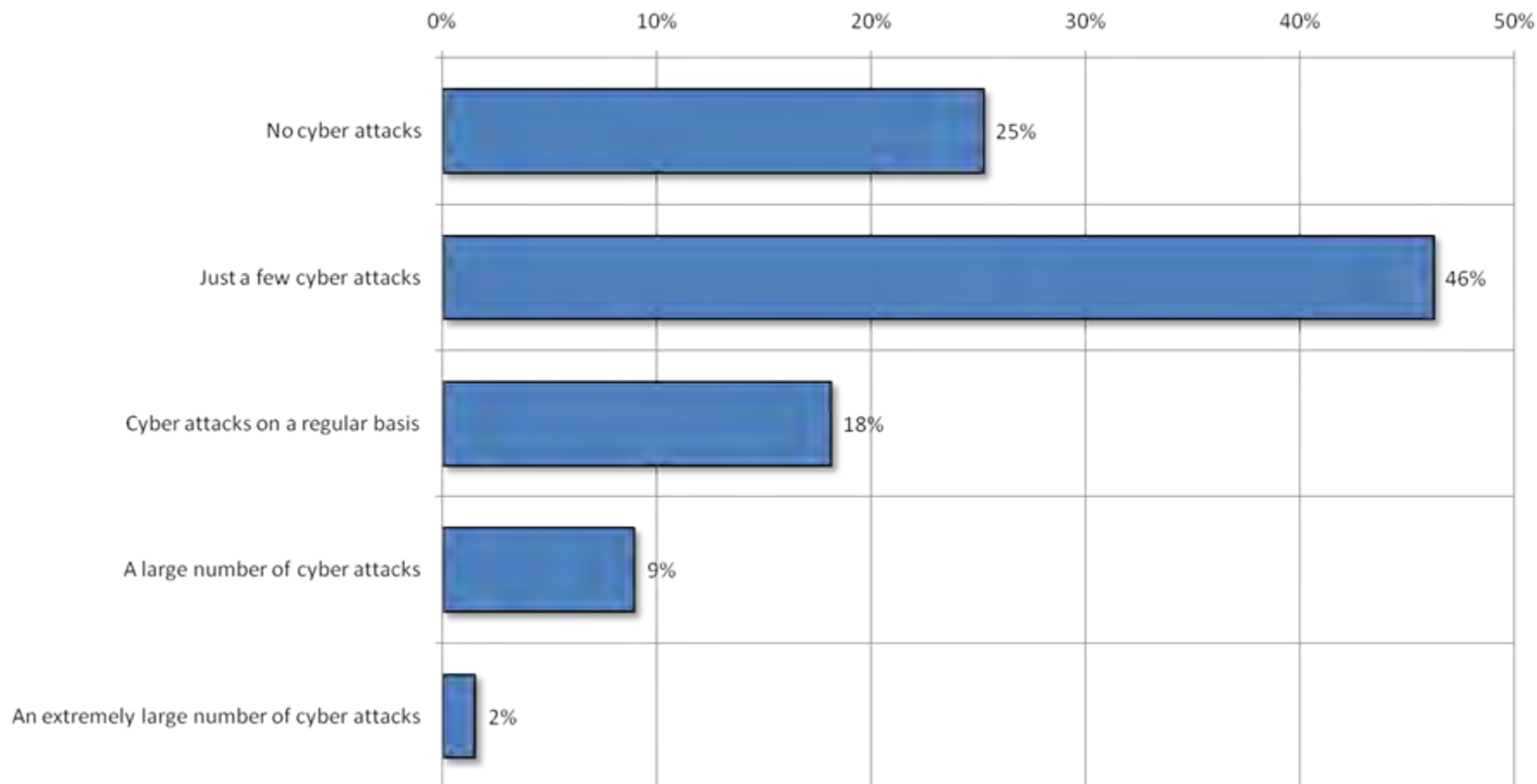
Q33: Is the training and development of your staff (in the area of enterprise security) viewed as...?



Attacks & Remediation

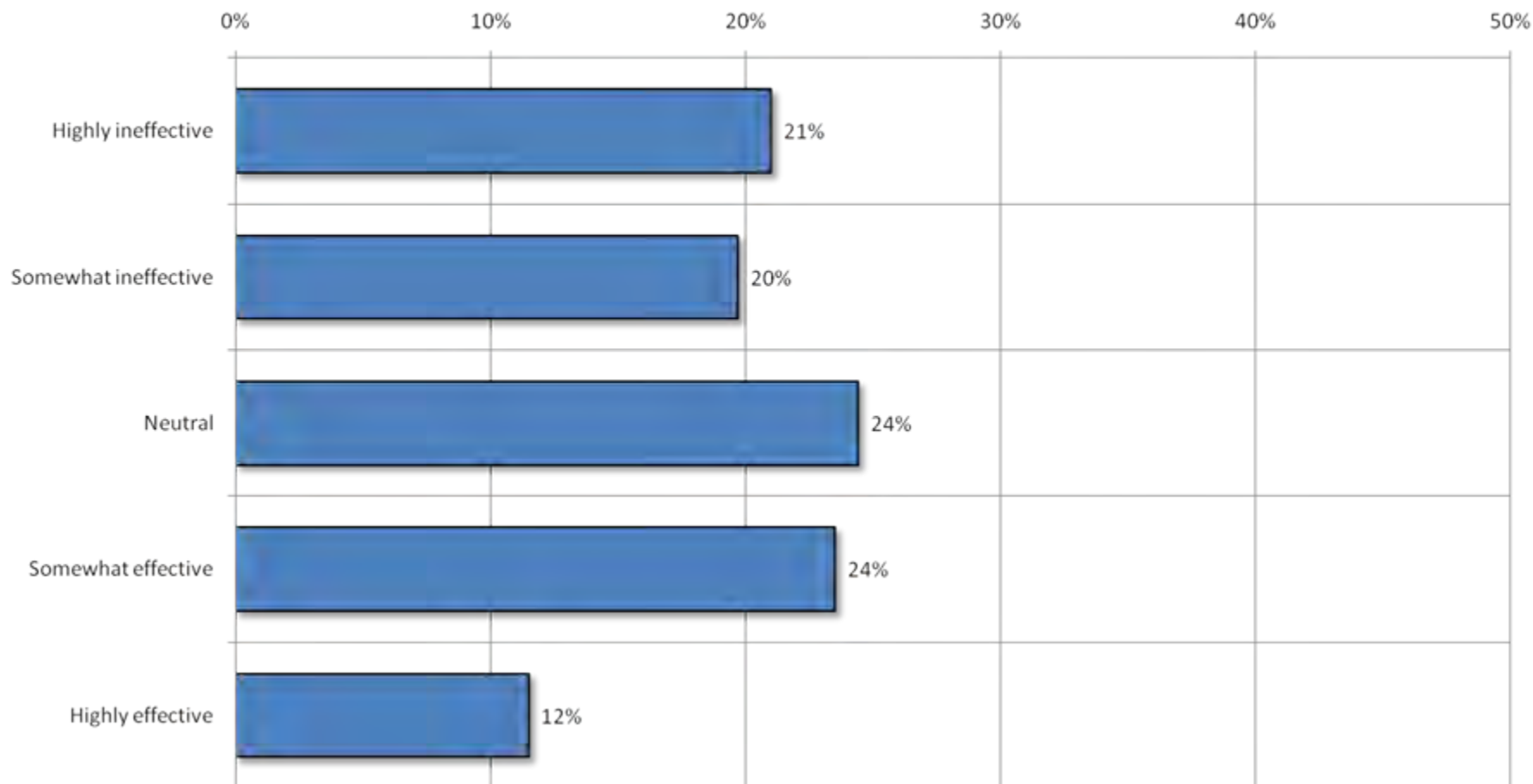
Cyber attacks

Q34: Characterize the quantity of cyber attacks against your organization over the past 12 months.



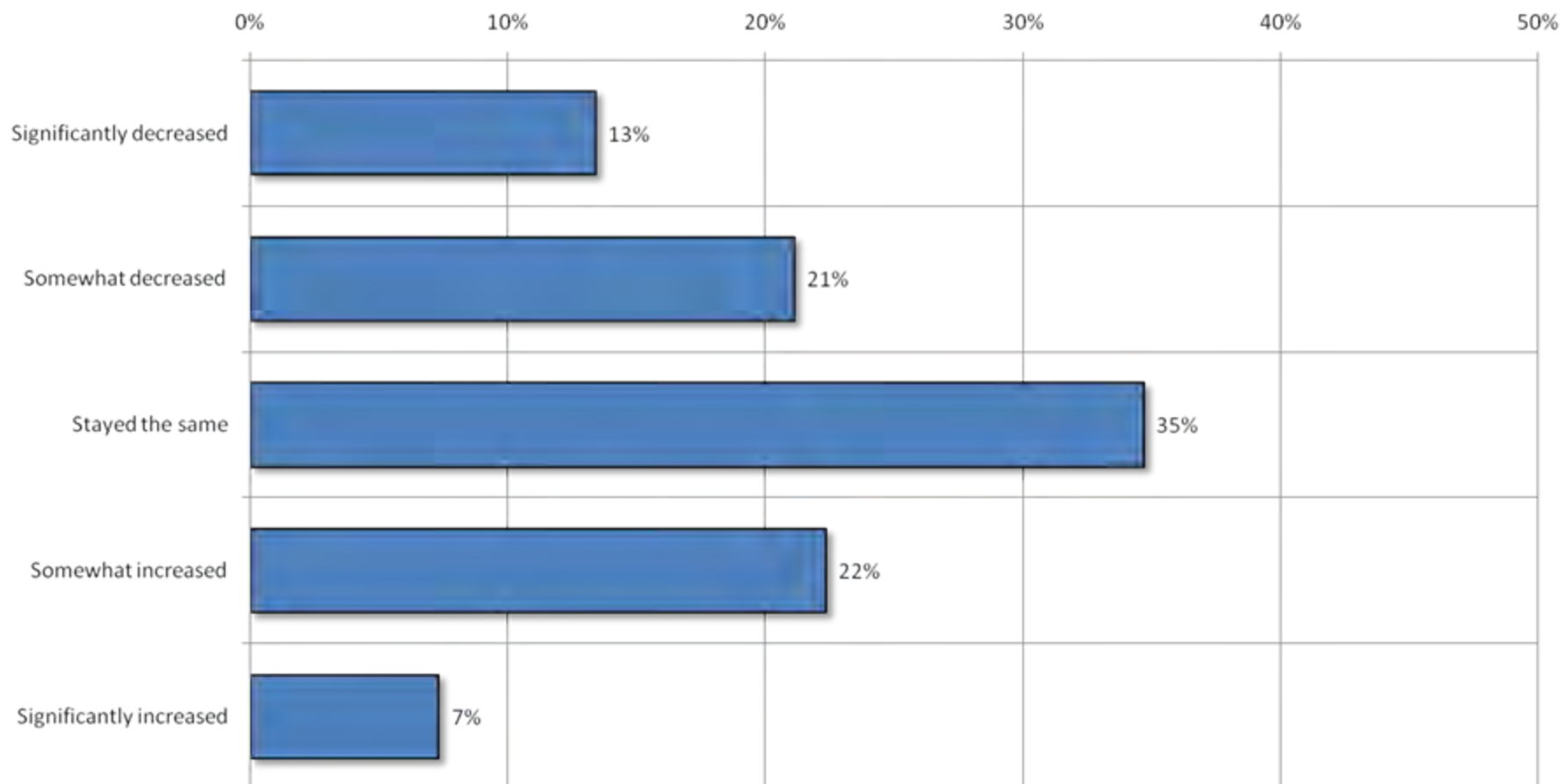
Cyber attacks

Q35: Rate the effectiveness of cyber attacks against your organization over the past 12 months.



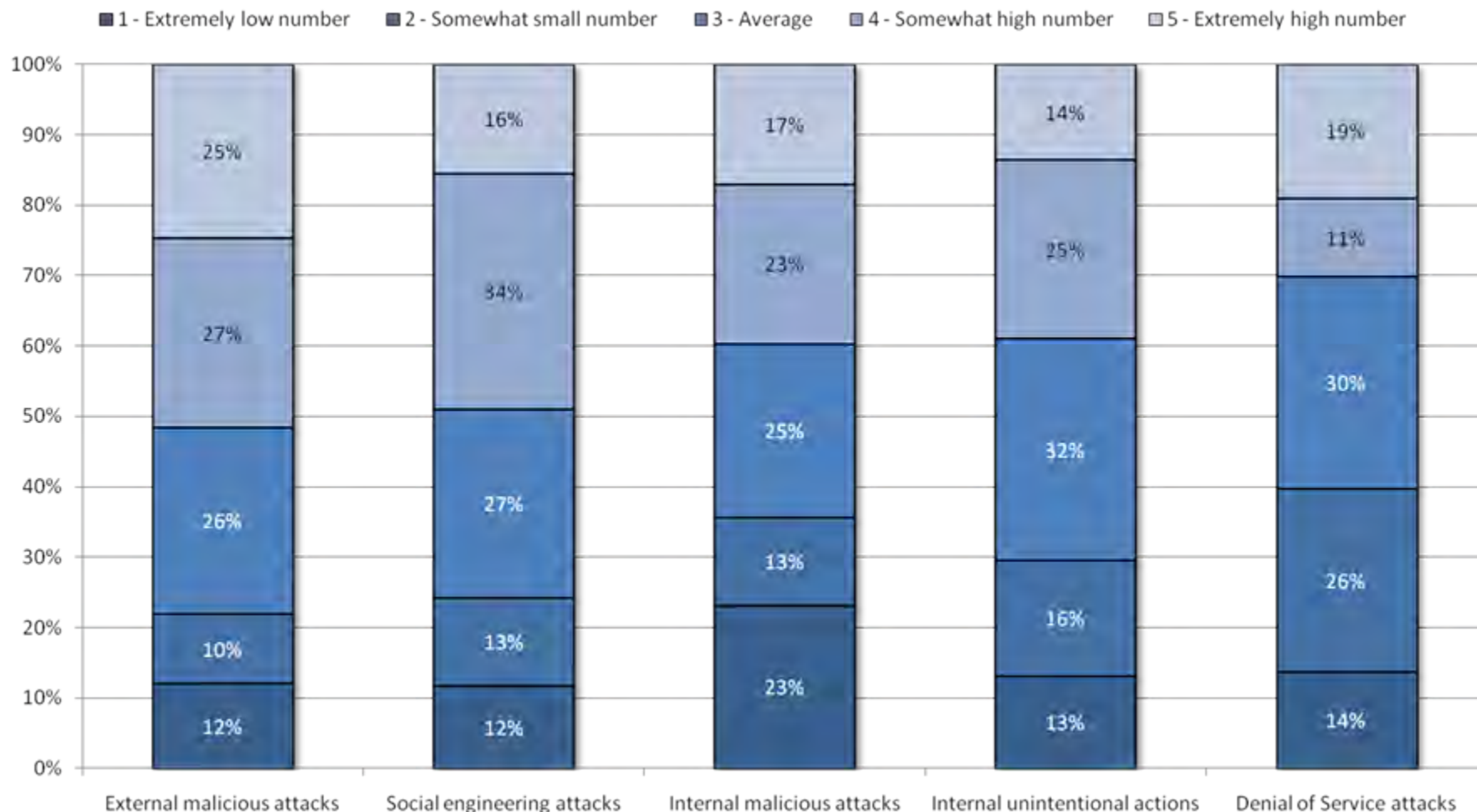
Cyber attacks

Q36: Characterize the growth of cyber attacks against your organization over the past 12 months.



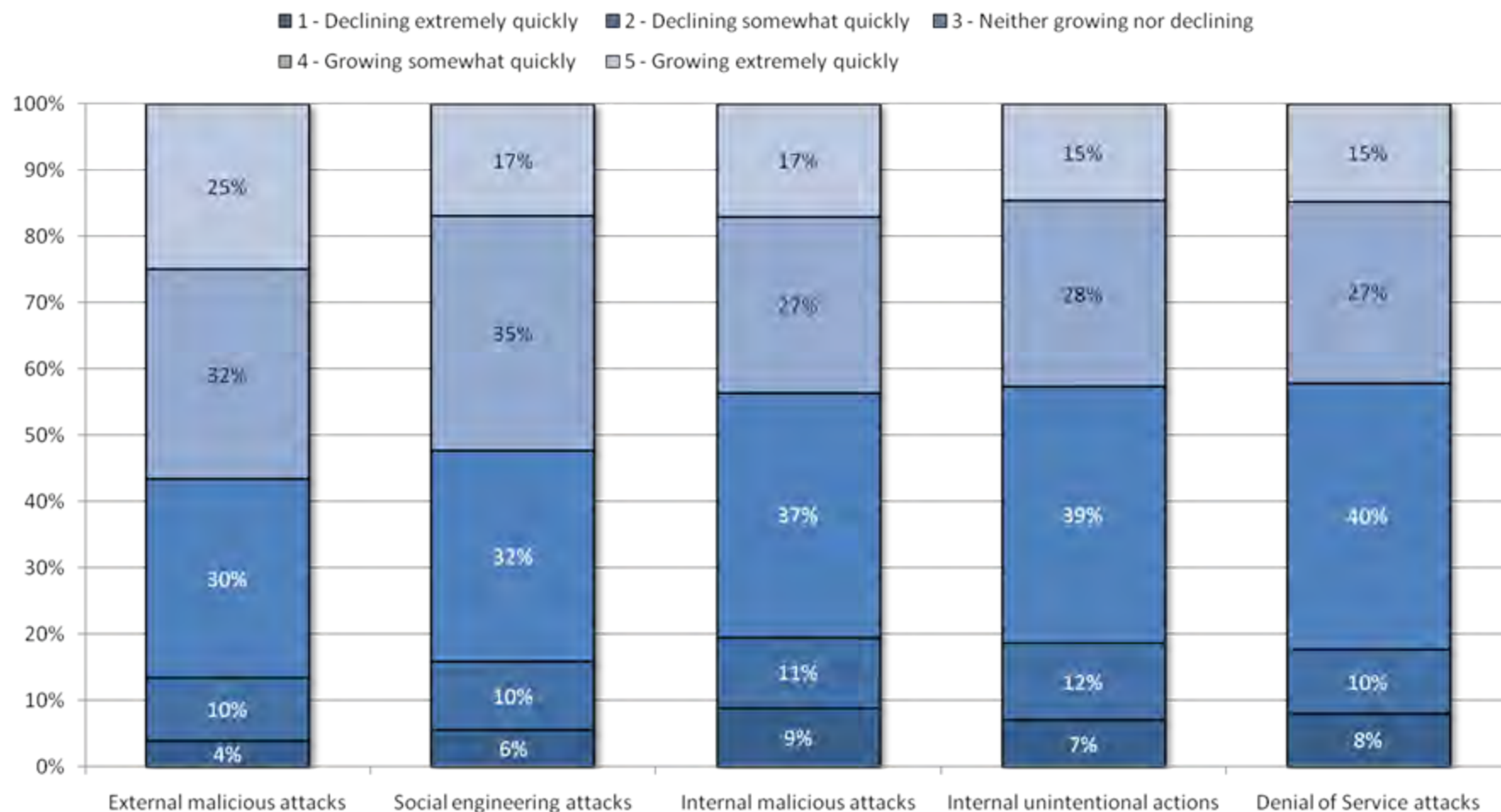
Cyber attacks

Q37: Which of the following cyber attacks did you experience in 2009?



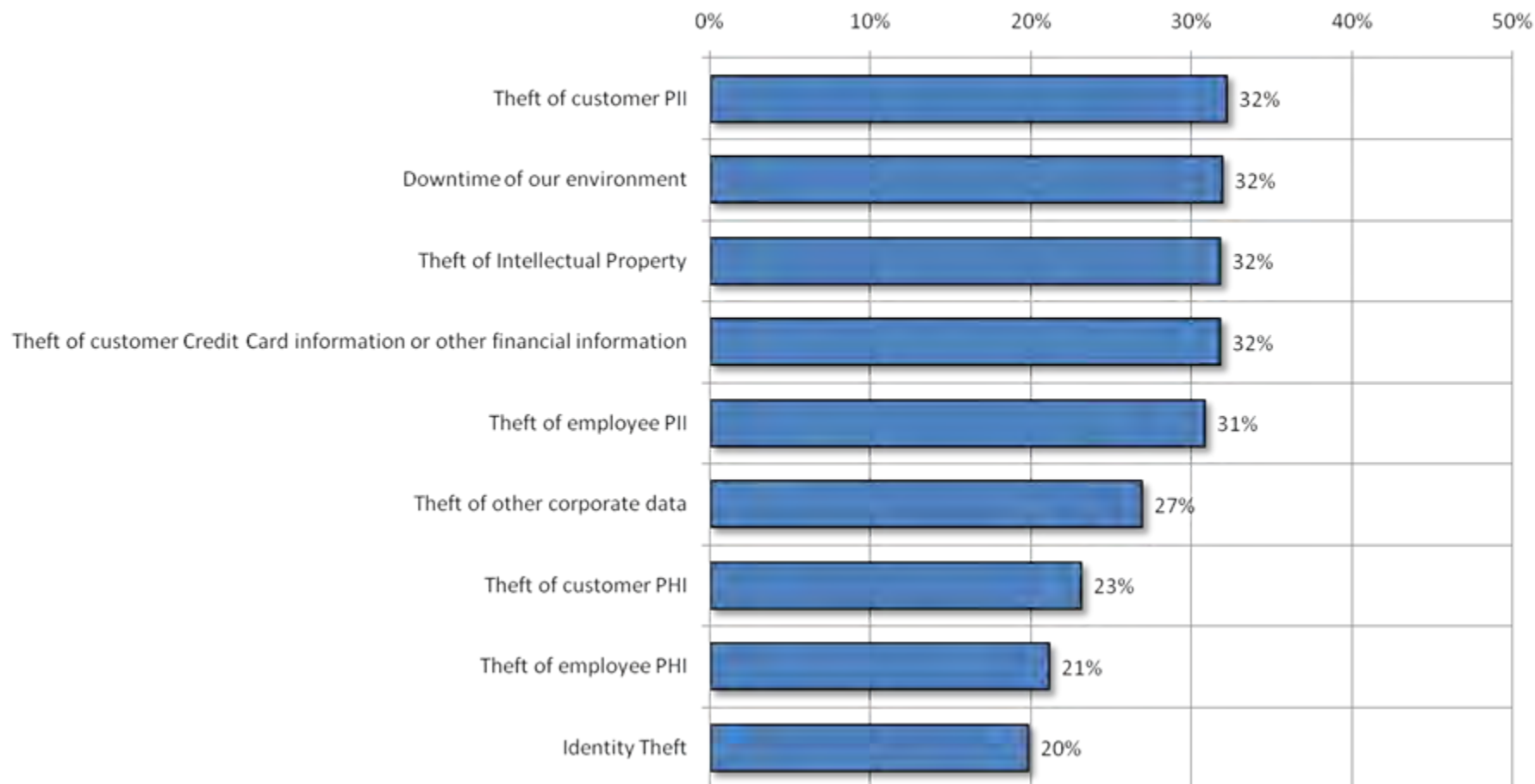
Cyber attacks

Q38: How is the quantity of these types of attacks changing over time?



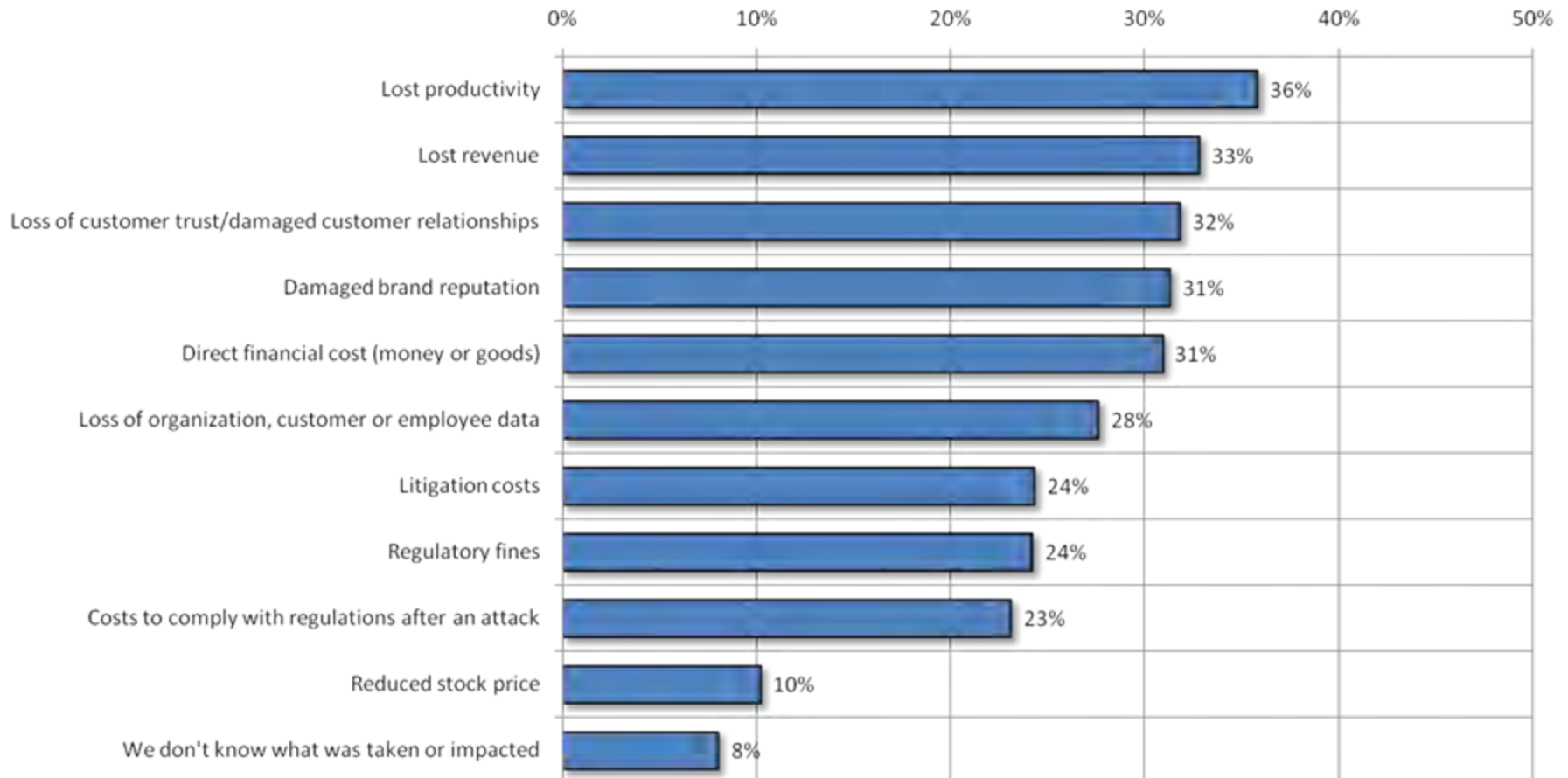
Cyber losses

Q39: Indicate which kinds of cyber losses you have experienced in the past. Mark all that apply.



Cyber attack costs

Q40: Please indicate which costs your organization experienced as a result of cyber attacks in the past. Mark all that apply.

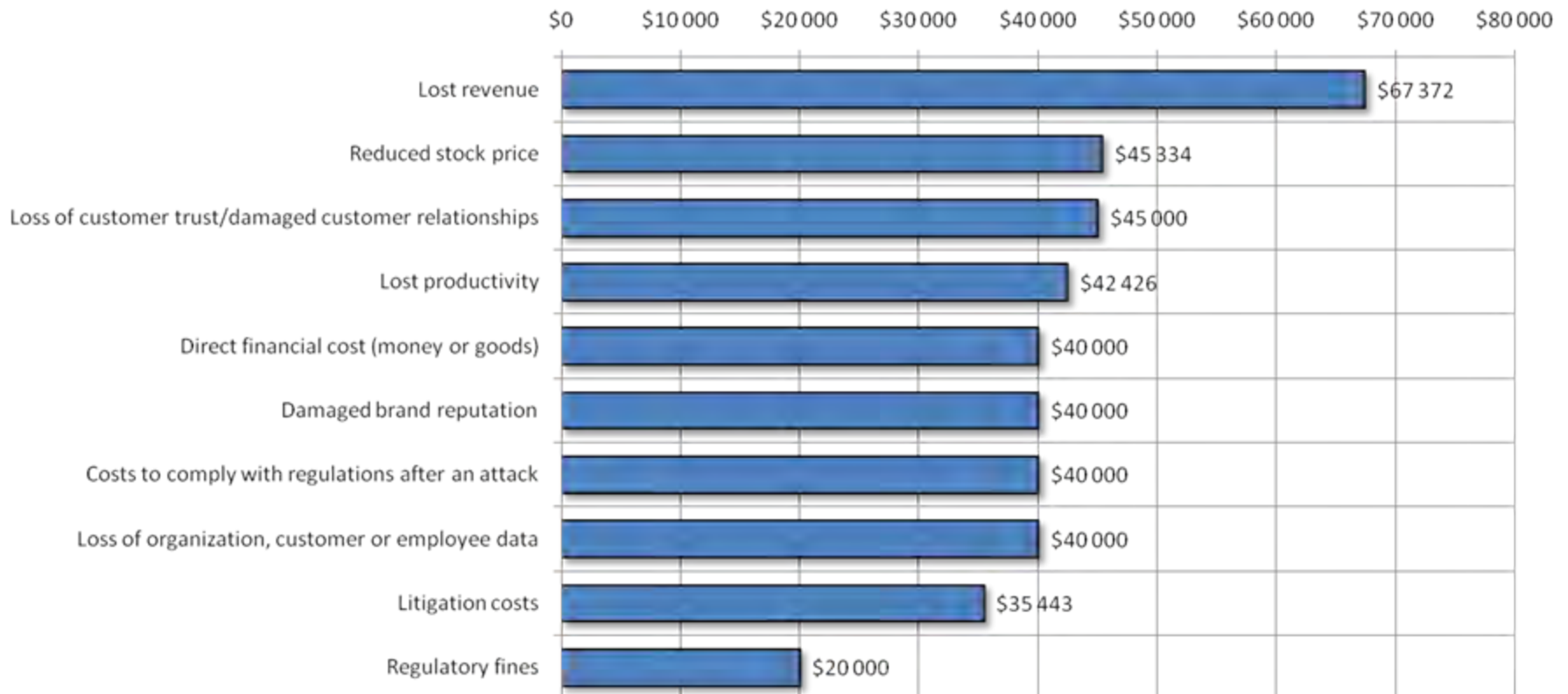


Cyber attack costs

Q41: Please assign a total value, in monetary terms, of each of these losses in 2009.

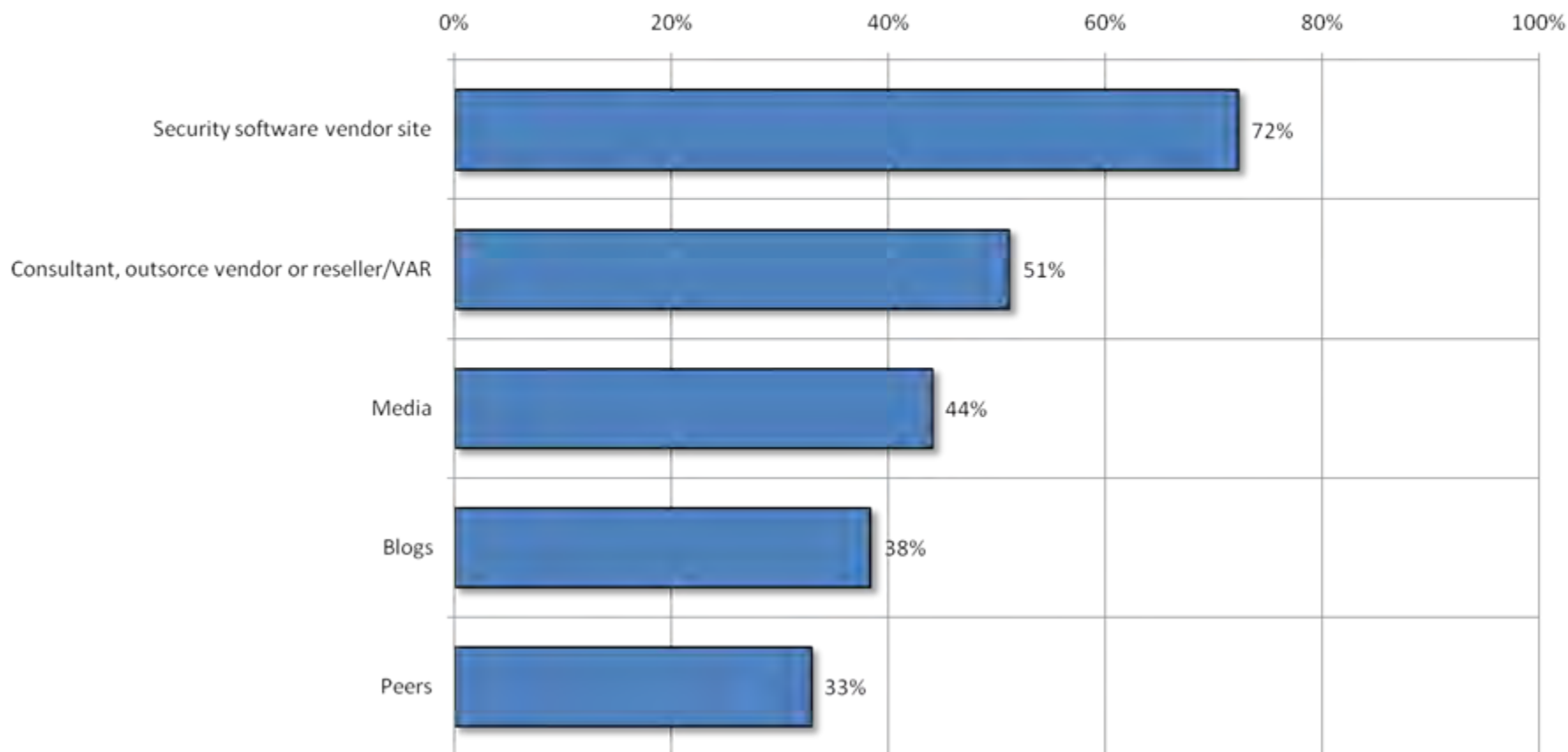
(Only asked of those who indicated each cost in Q40)

(Medians shown)



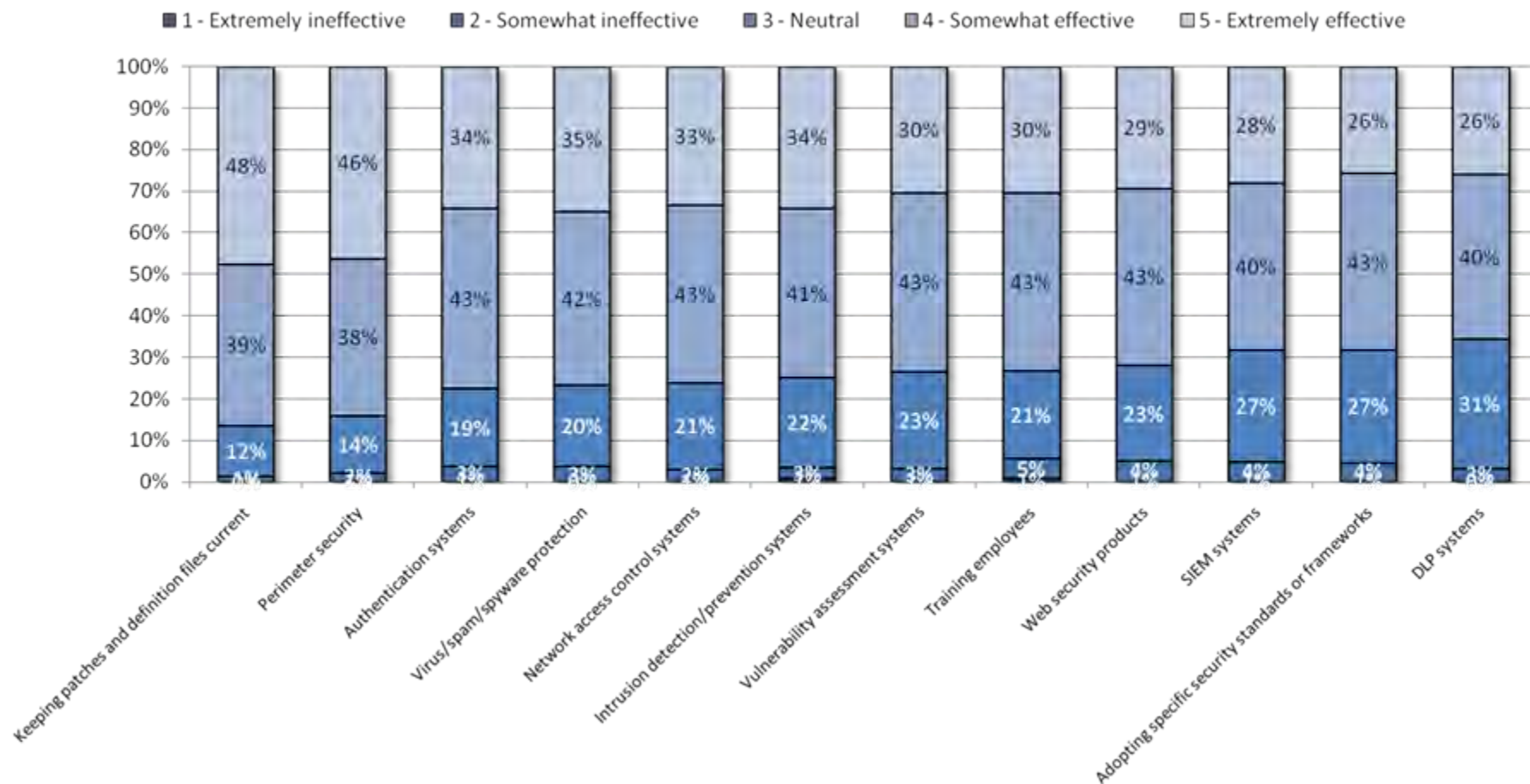
Cyber attack info

Q42: When you have sustained a cyber attack, where do you go to find information about that type of attack and how to respond? Mark all that apply.



Safeguards

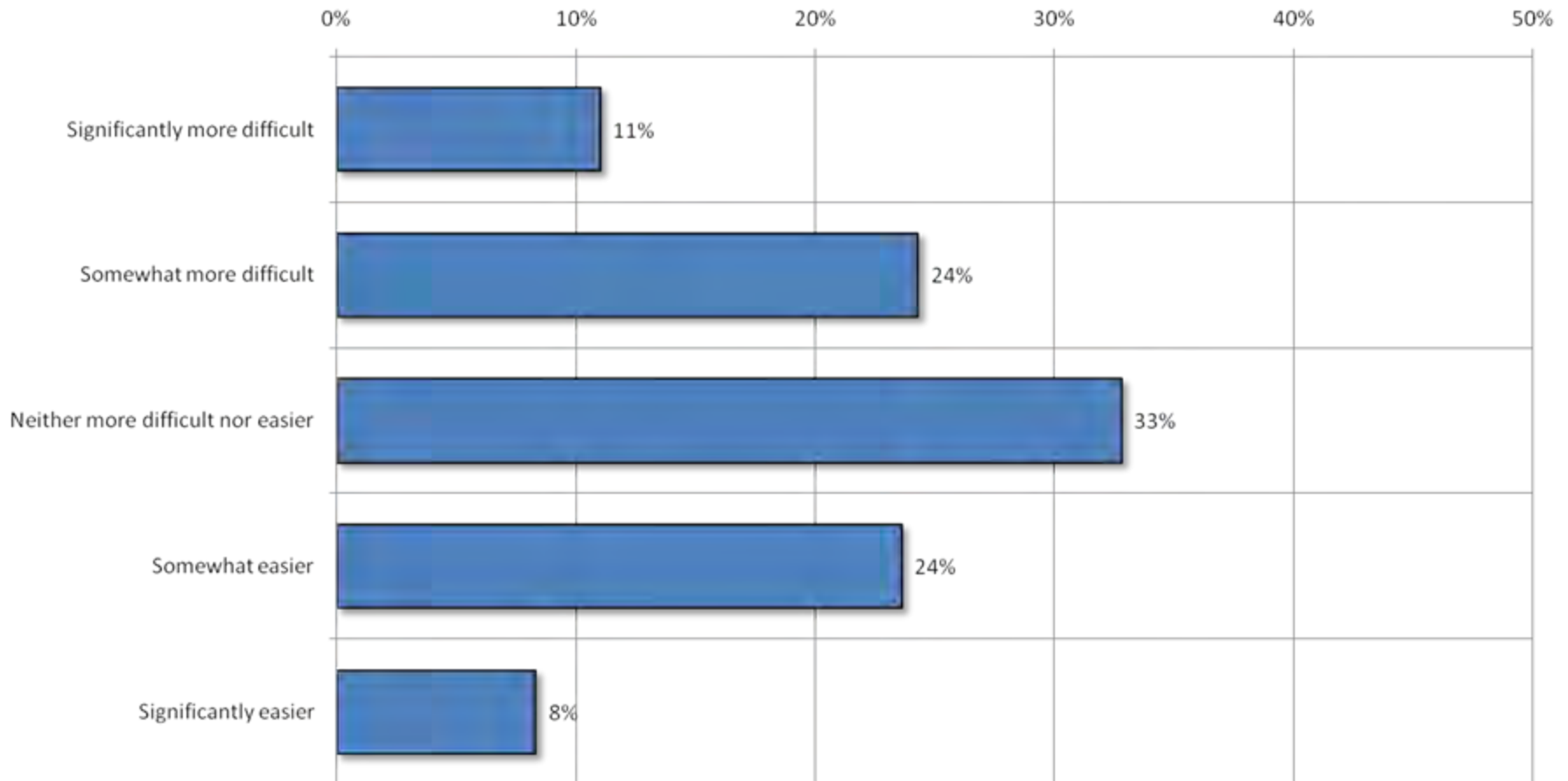
Q43: Please rate the following safeguards in terms of their effectiveness in curbing cyber attacks against your organization.



Network Security

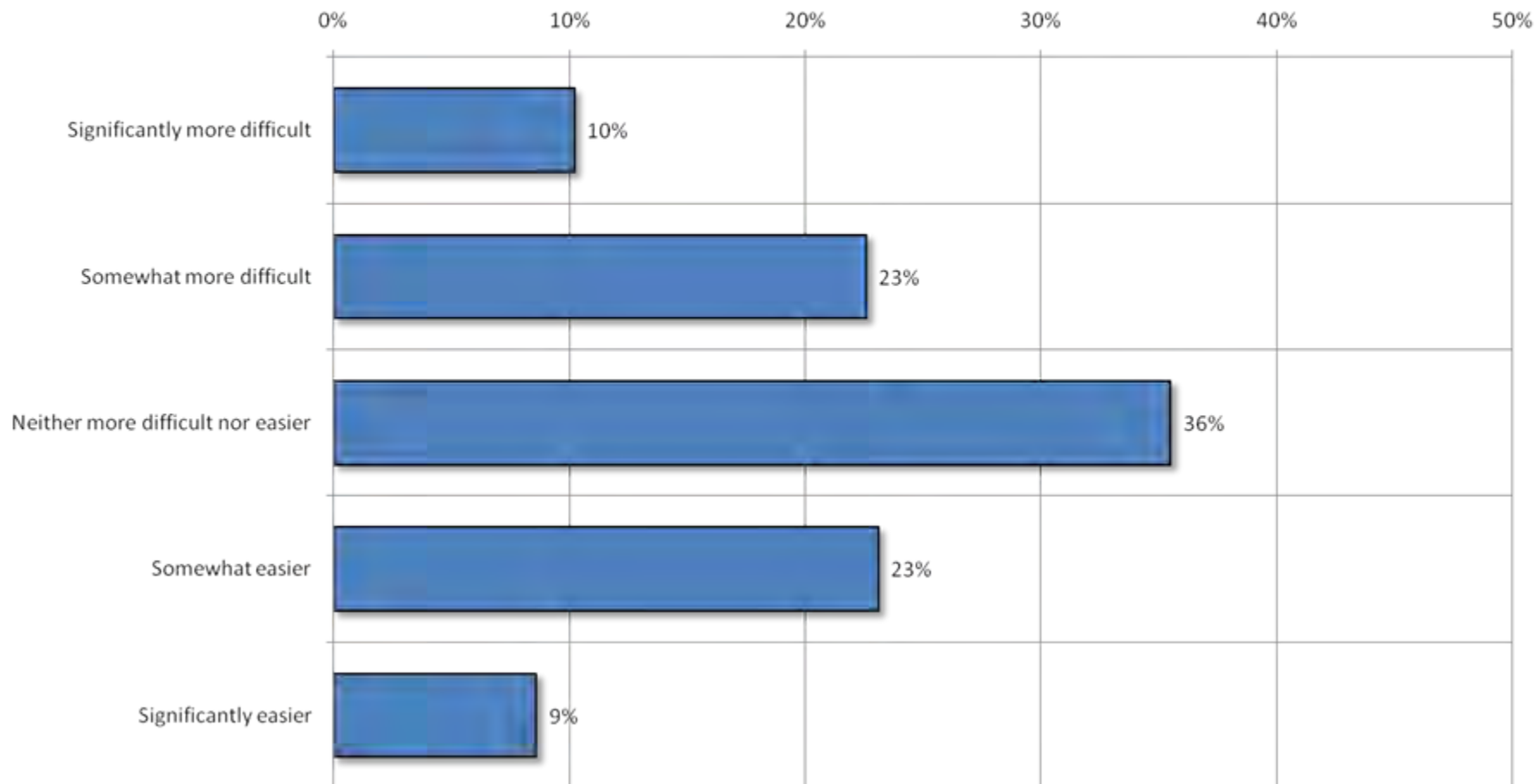
IaaS and network security

Q44: Does "Infrastructure-as-a-Service" make it easier or harder to do your job with regards to network security?



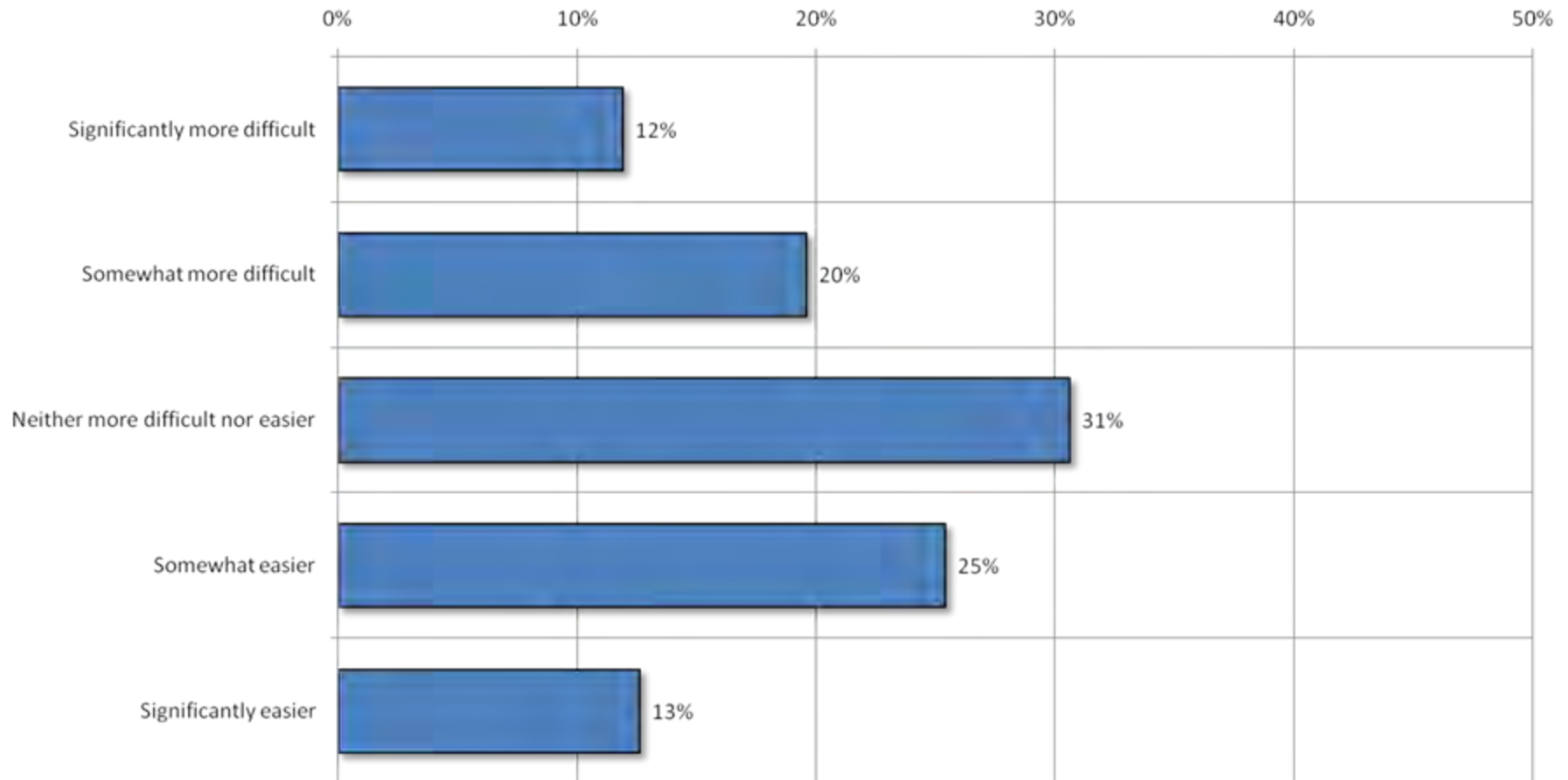
PaaS and network security

Q45: Does "Platform-as-a-Service" make it easier or harder to do your job with regards to network security?



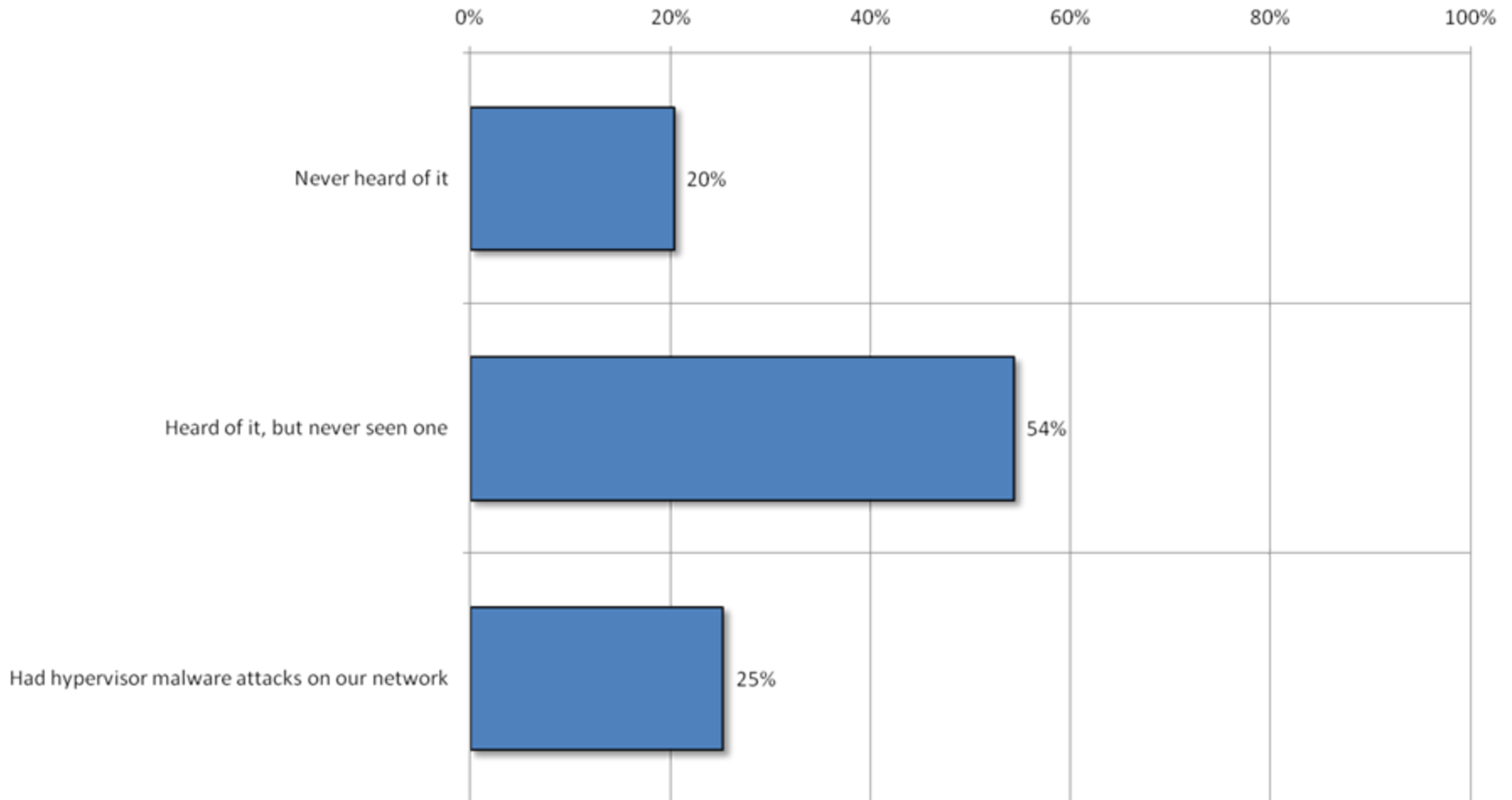
Server virtualization and network security

Q46: Does server virtualization make it easier or harder to do your job with regards to network security?



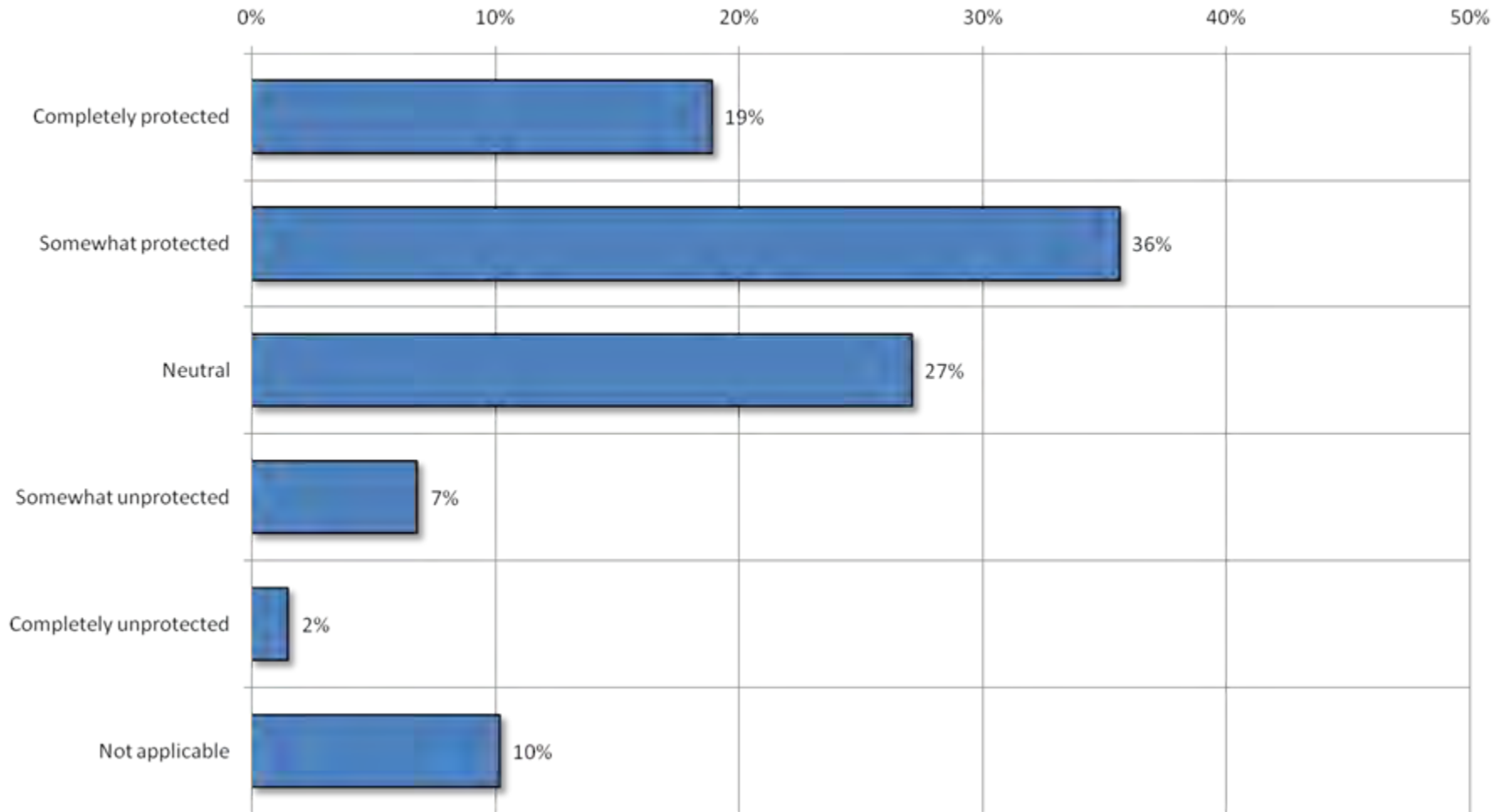
Hypervisor malware

Q47: What is your experience with hypervisor malware?



Hypervisor malware

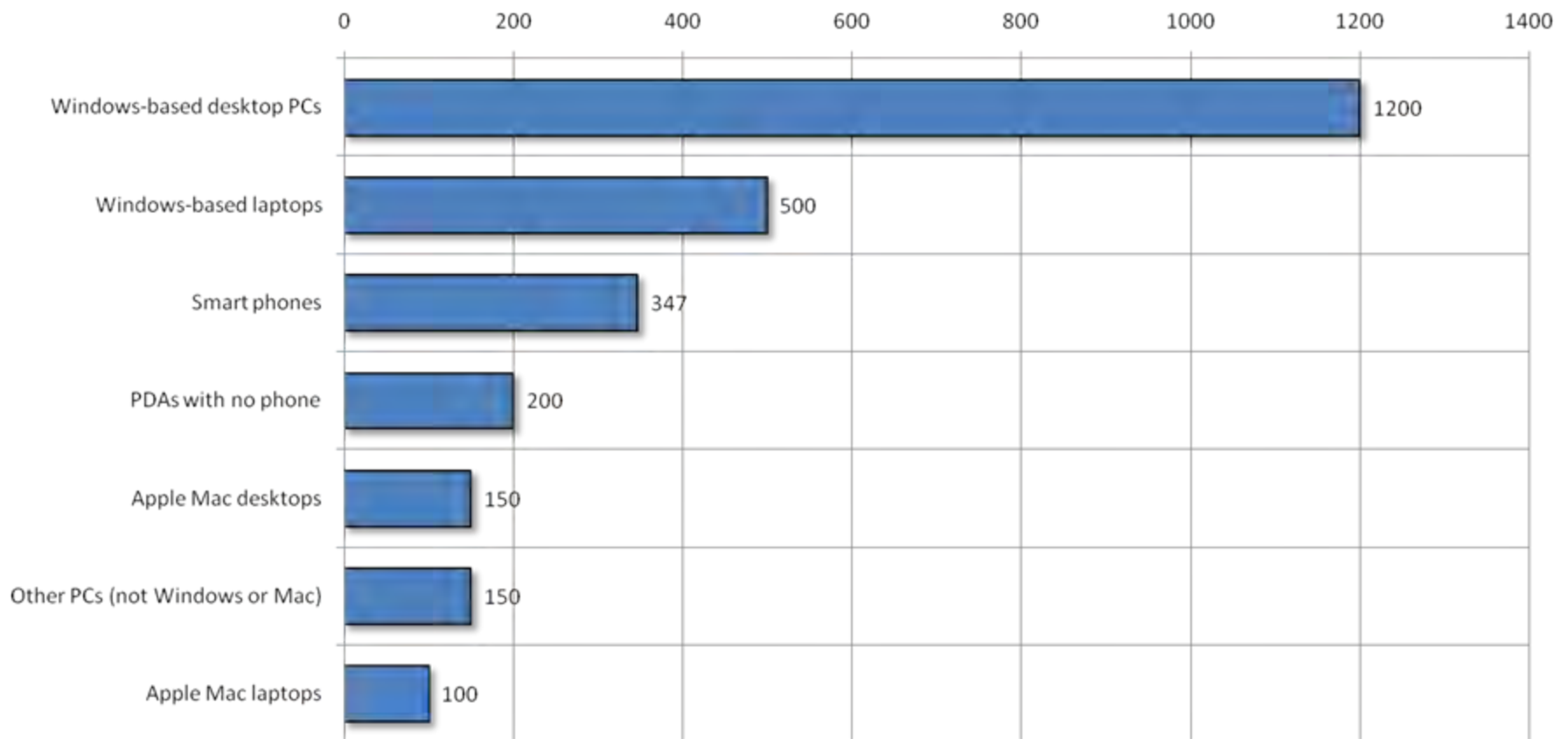
Q48: How protected are you against hypervisor malware?



Endpoint Security

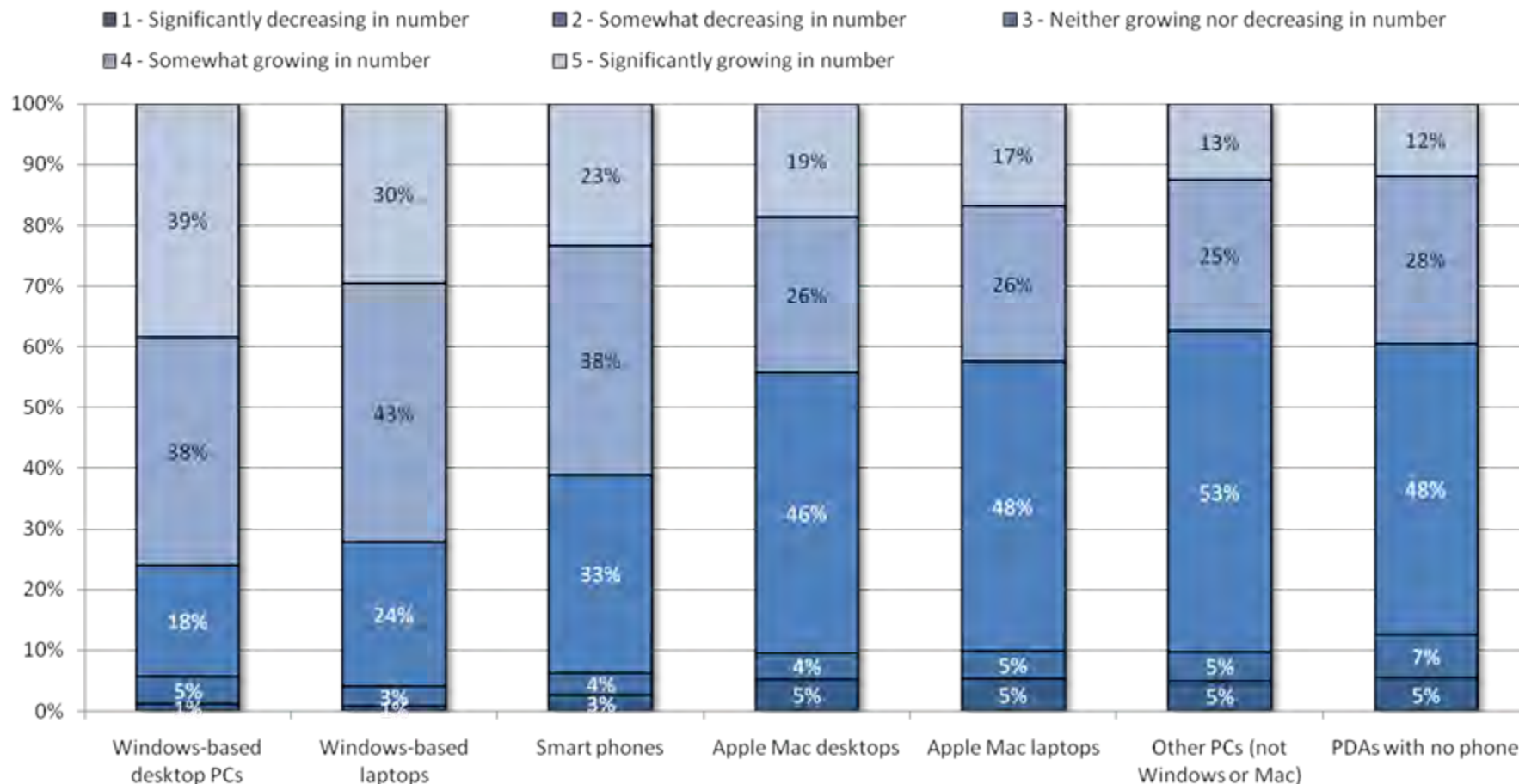
Endpoint types

**Q49: How many of the following endpoints are in use throughout your organization worldwide?
(Medians shown)**



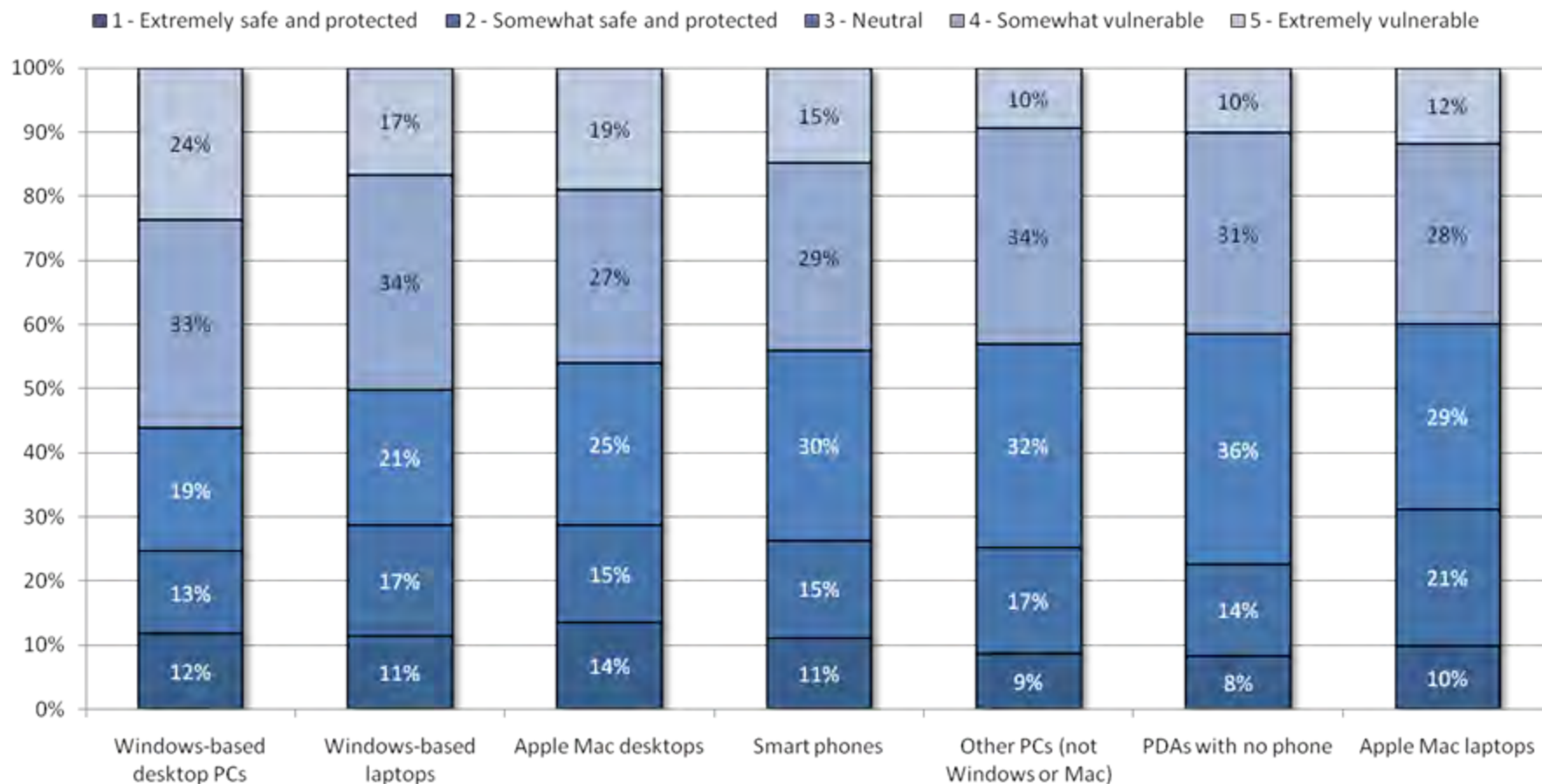
Endpoint types

Q50: How is the number of each of the following endpoints changing throughout your organization worldwide?



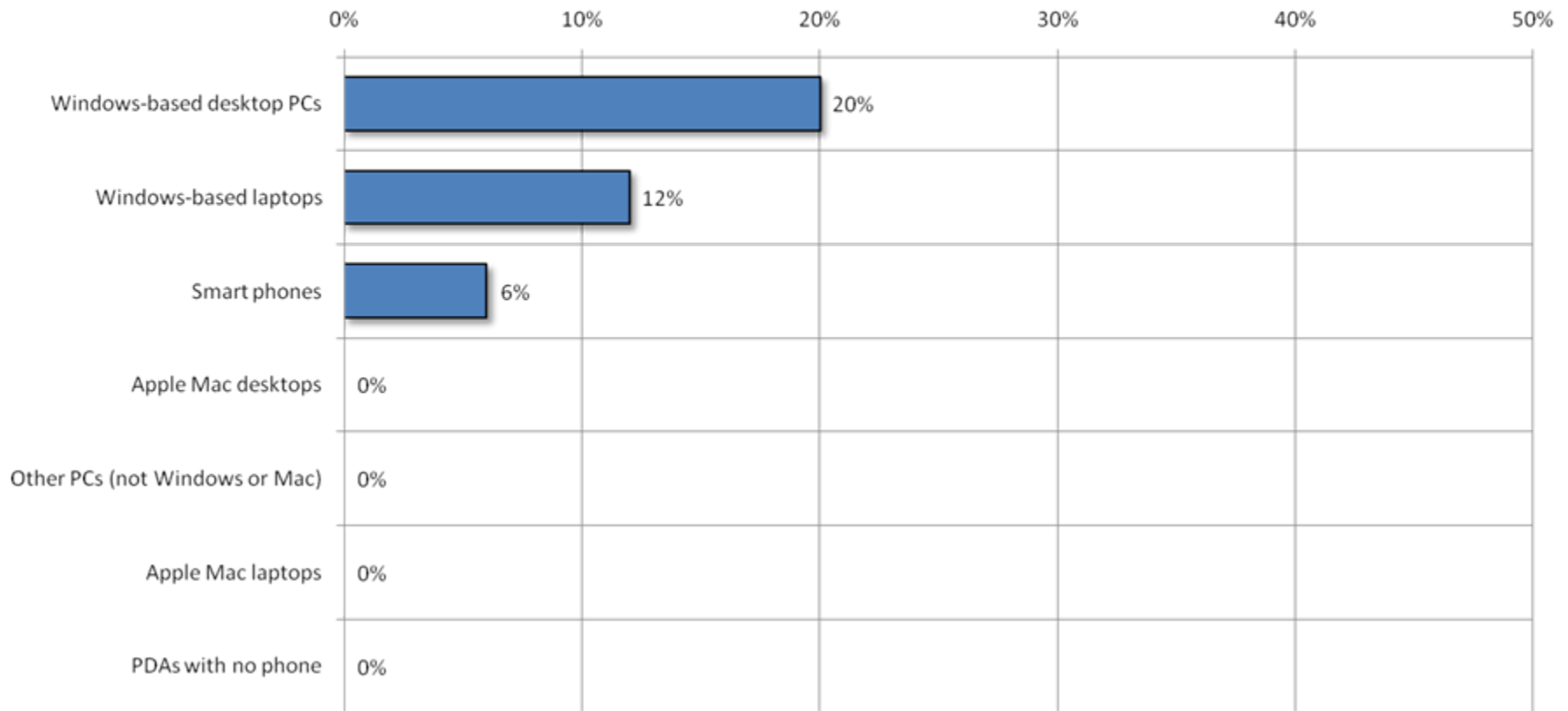
Endpoint vulnerability

Q51: How vulnerable are each of these endpoints? (Asked only for those endpoints used)



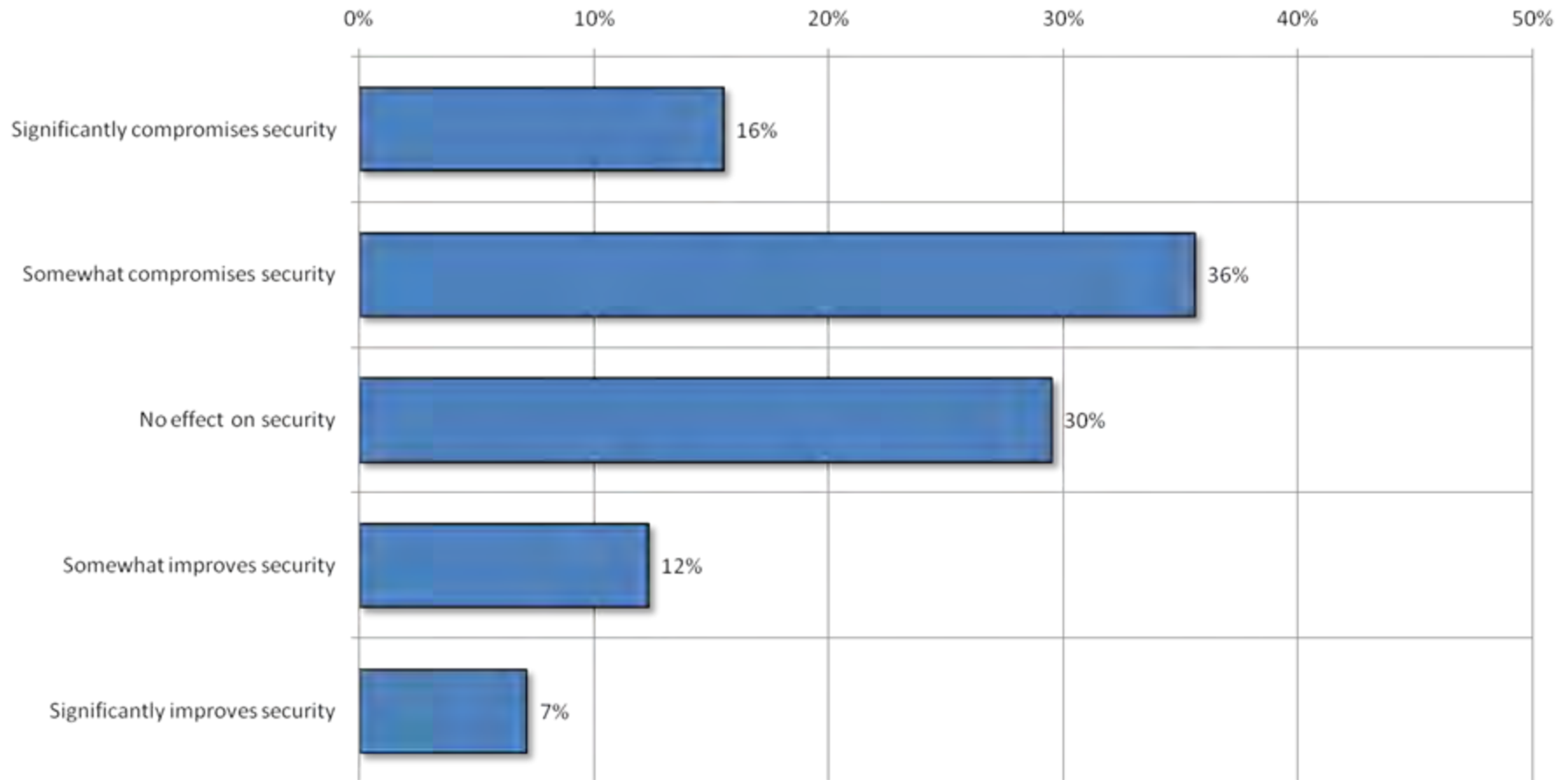
Employee-owned endpoints

**Q52: What percentage of your endpoints was selected, purchased, and is owned by your employees?
(Medians shown)**



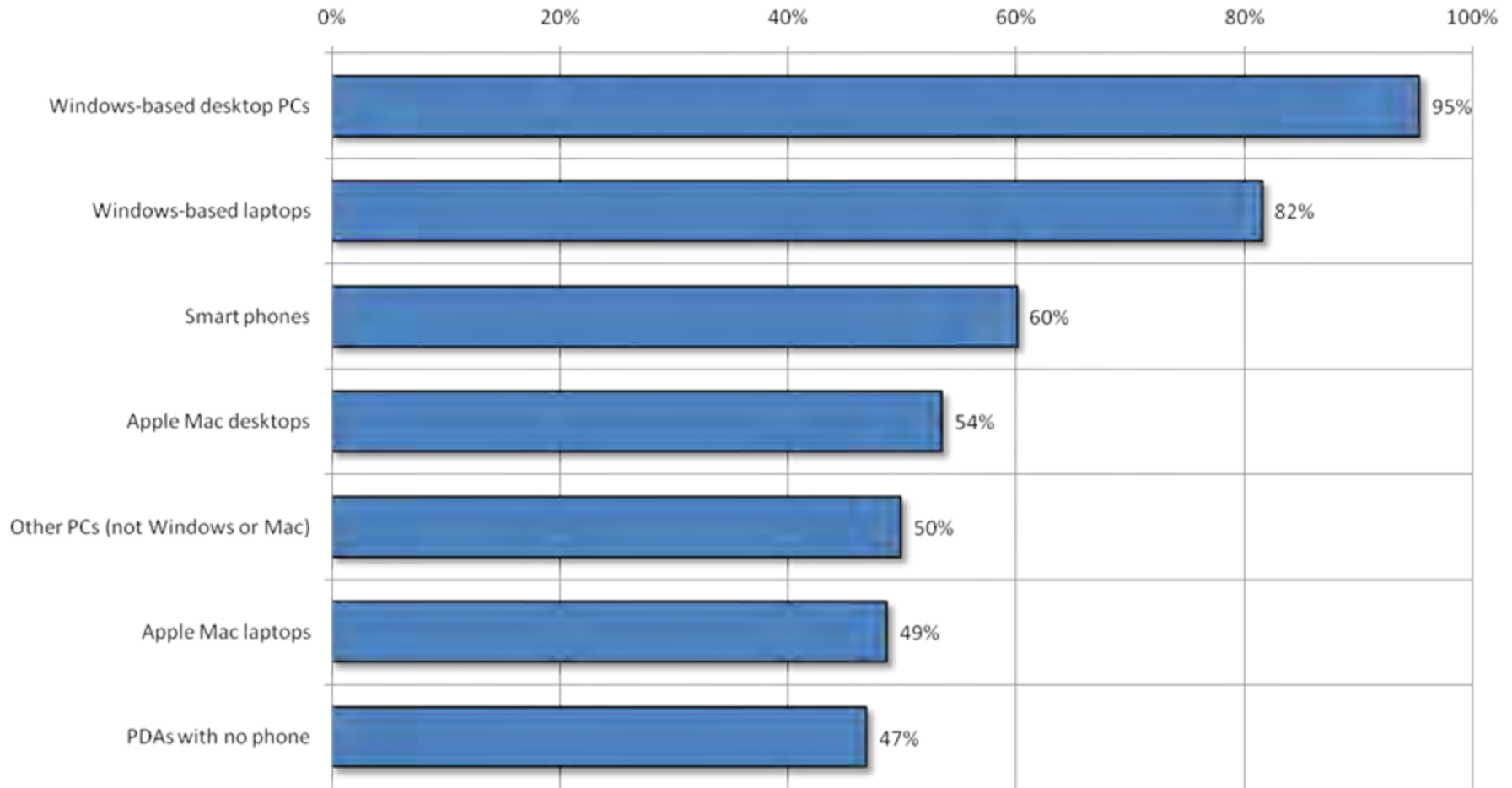
Employee-owned endpoints

Q53: What is the impact to your organization's IT security from employee-owned endpoints?



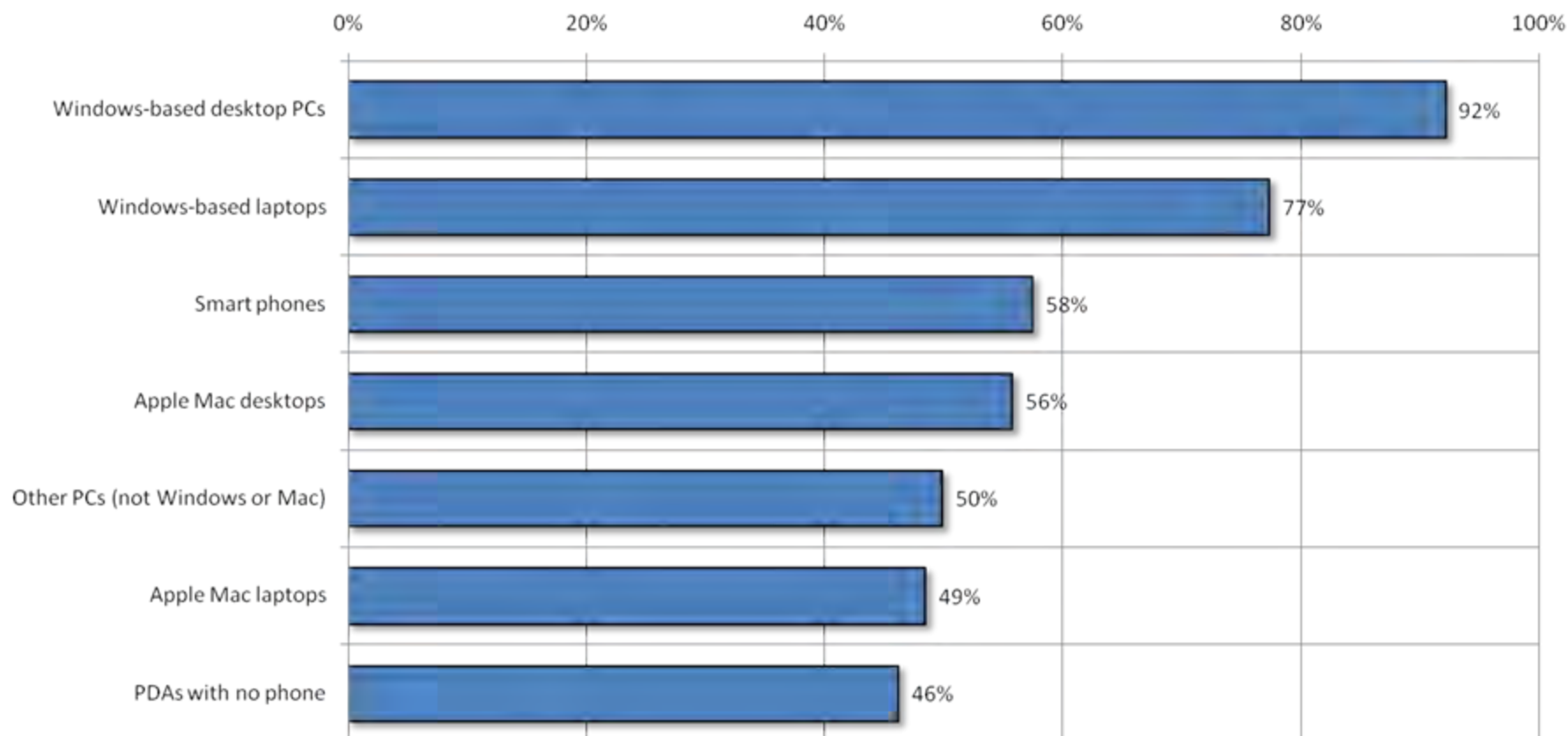
Endpoint standardization

Q54: Do you standardize your endpoint configurations?



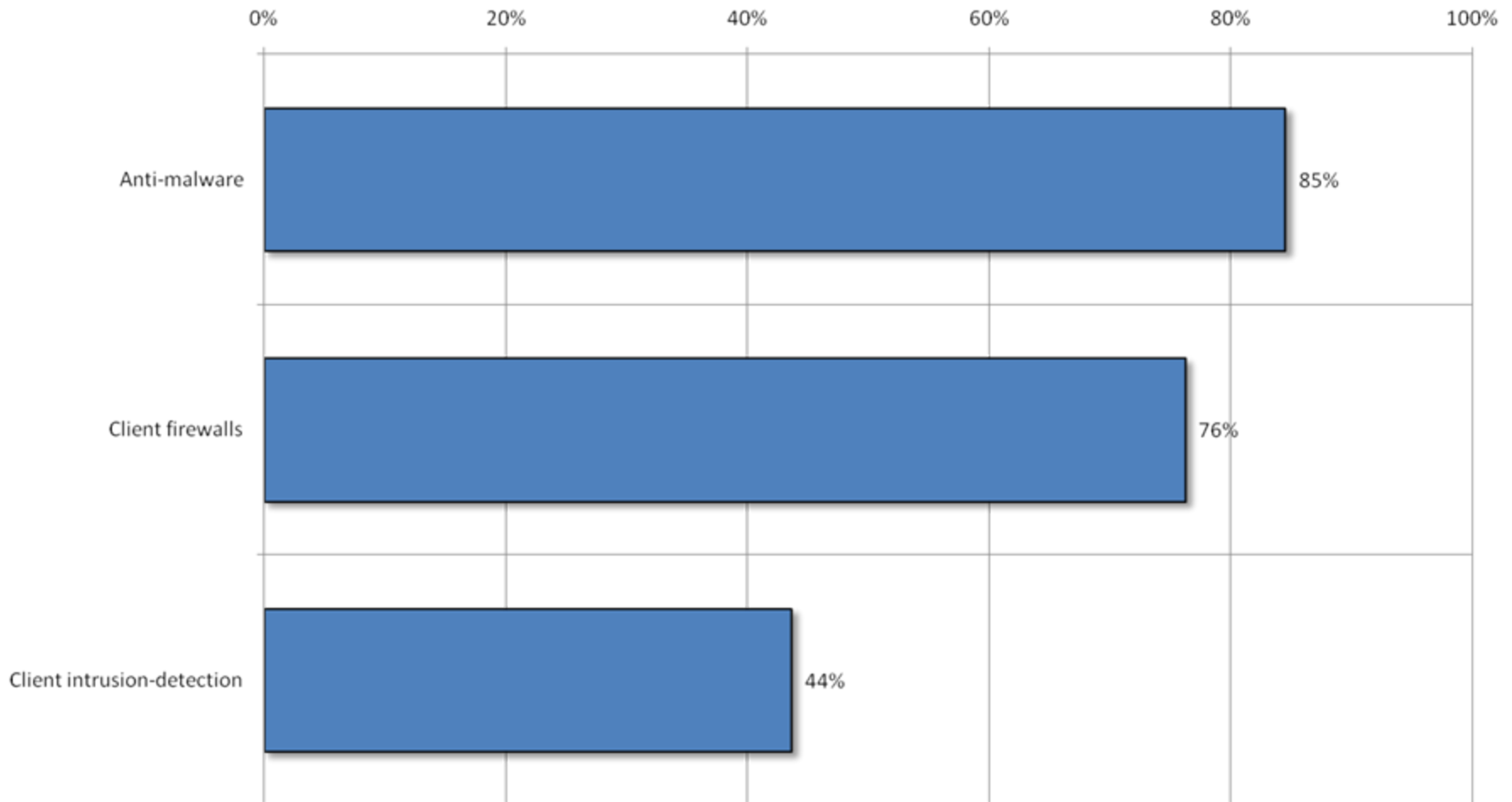
Endpoint control

Q55: Do you employ a network access control system that checks to make sure endpoints meet corporate standards and block and/or bring them up to standard before granting access to the network?



Endpoint safeguards

Q56: Which of the following endpoint security safeguards do you use?

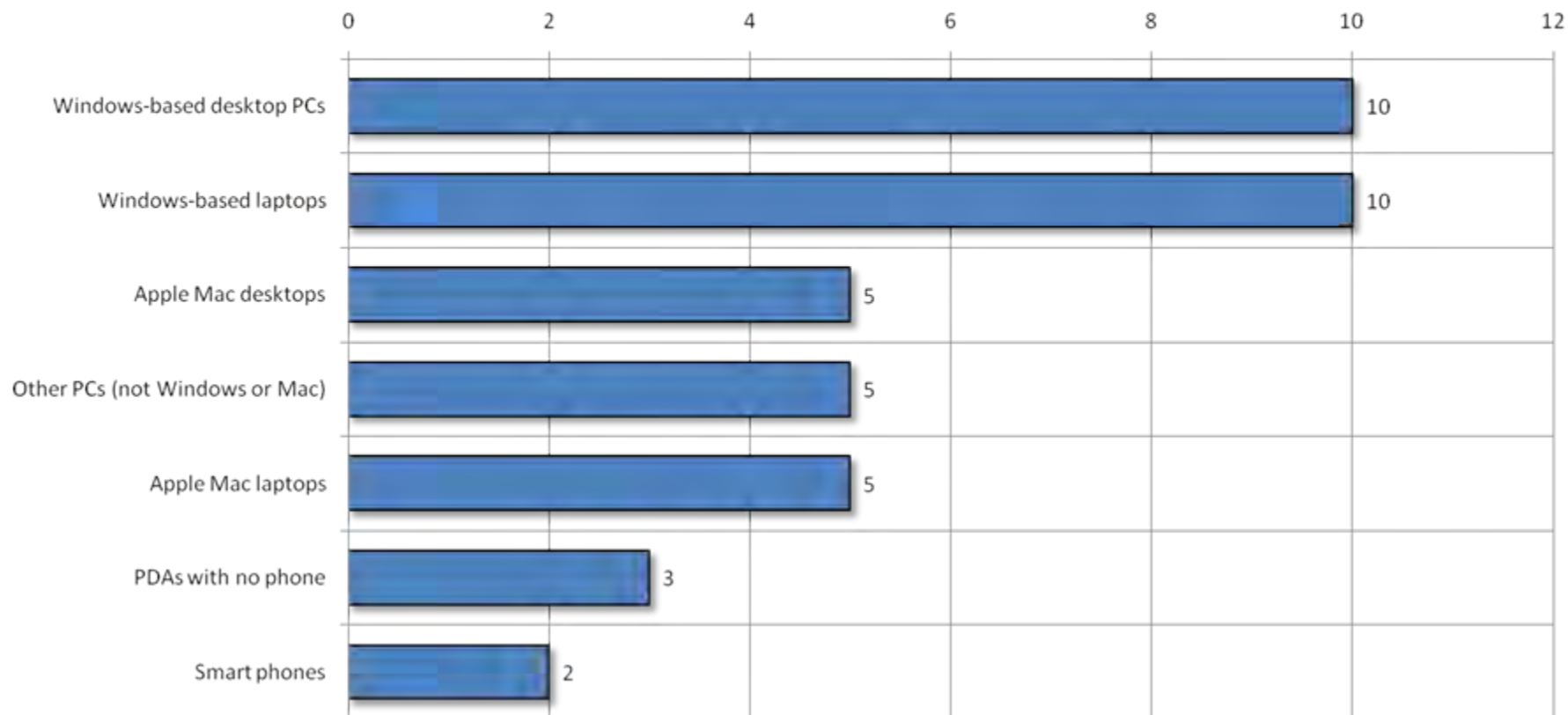


Endpoint attacks

Q57: Worldwide, how many incidents/attacks have you sustained against each of these endpoints in the past 12 months?

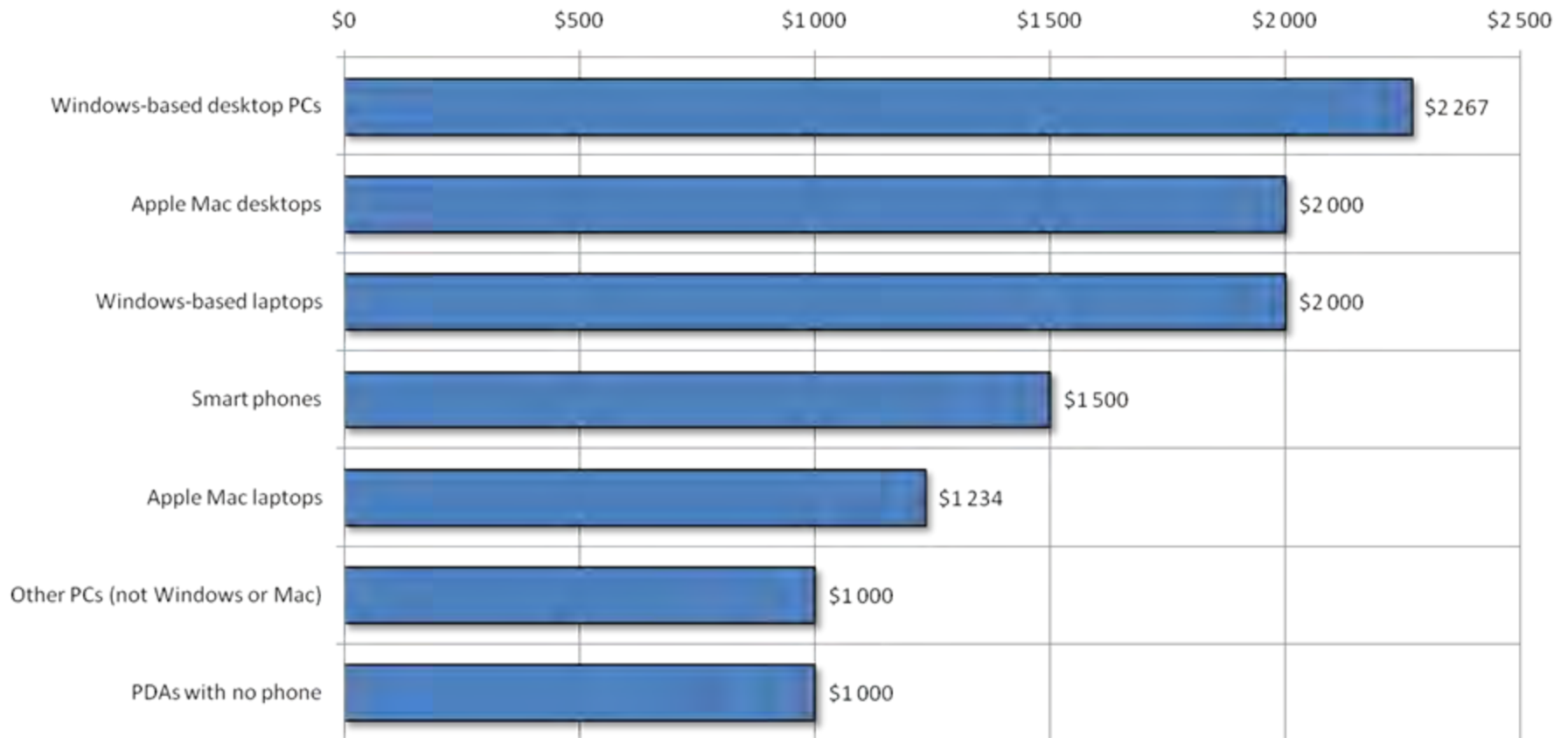
(Asked only for those endpoints used)

(Medians shown)



Attack remediation costs

**Q58: What is the average cost (in US \$) spent by IT remediating attacks on each of these endpoints for a single attack?
(Medians shown)**



Endpoint attack causes

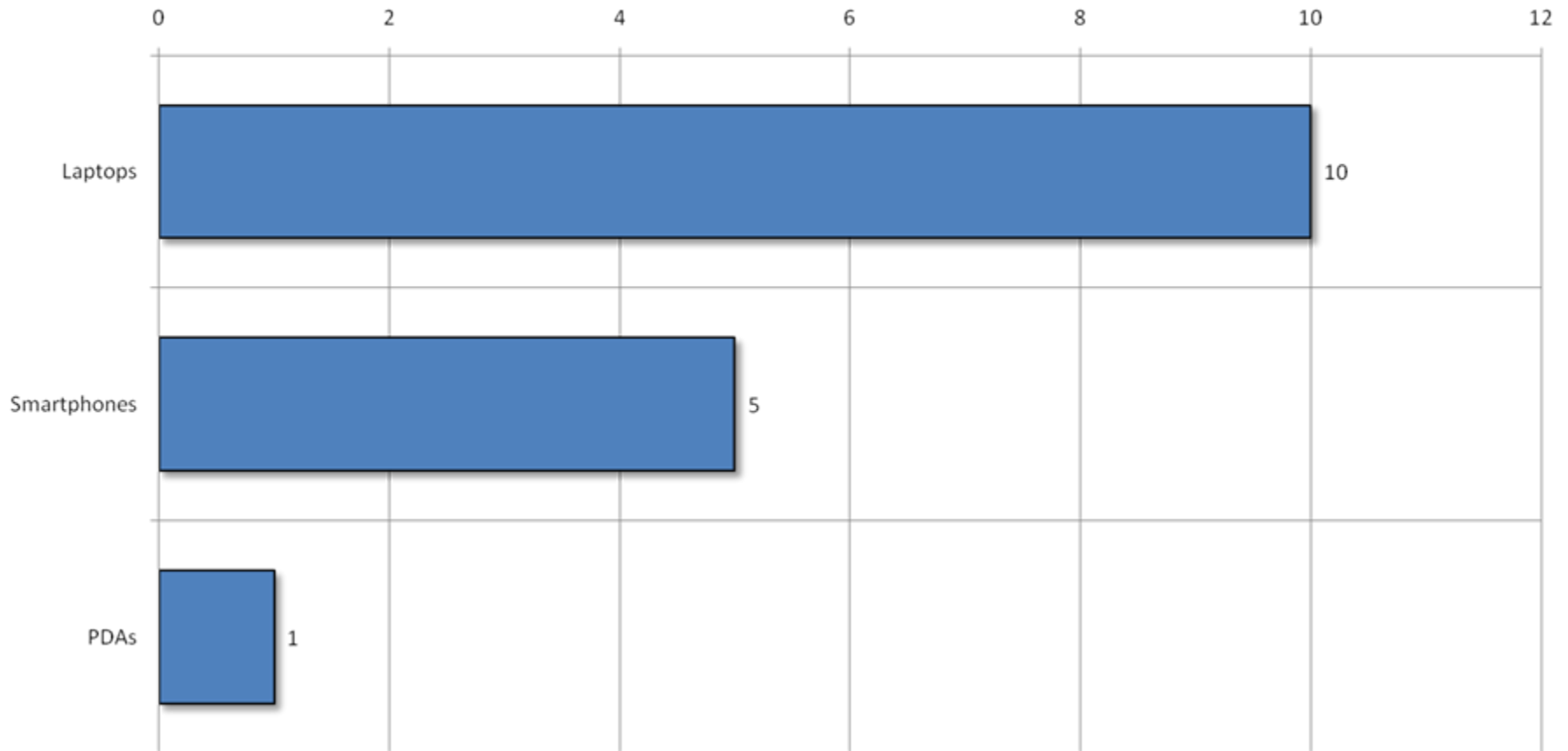
Q59: What percentage of the aforementioned attacks were the results of improper configurations such as missed OS patches, incorrect security settings, out of date virus profiles, etc?

Median

20%

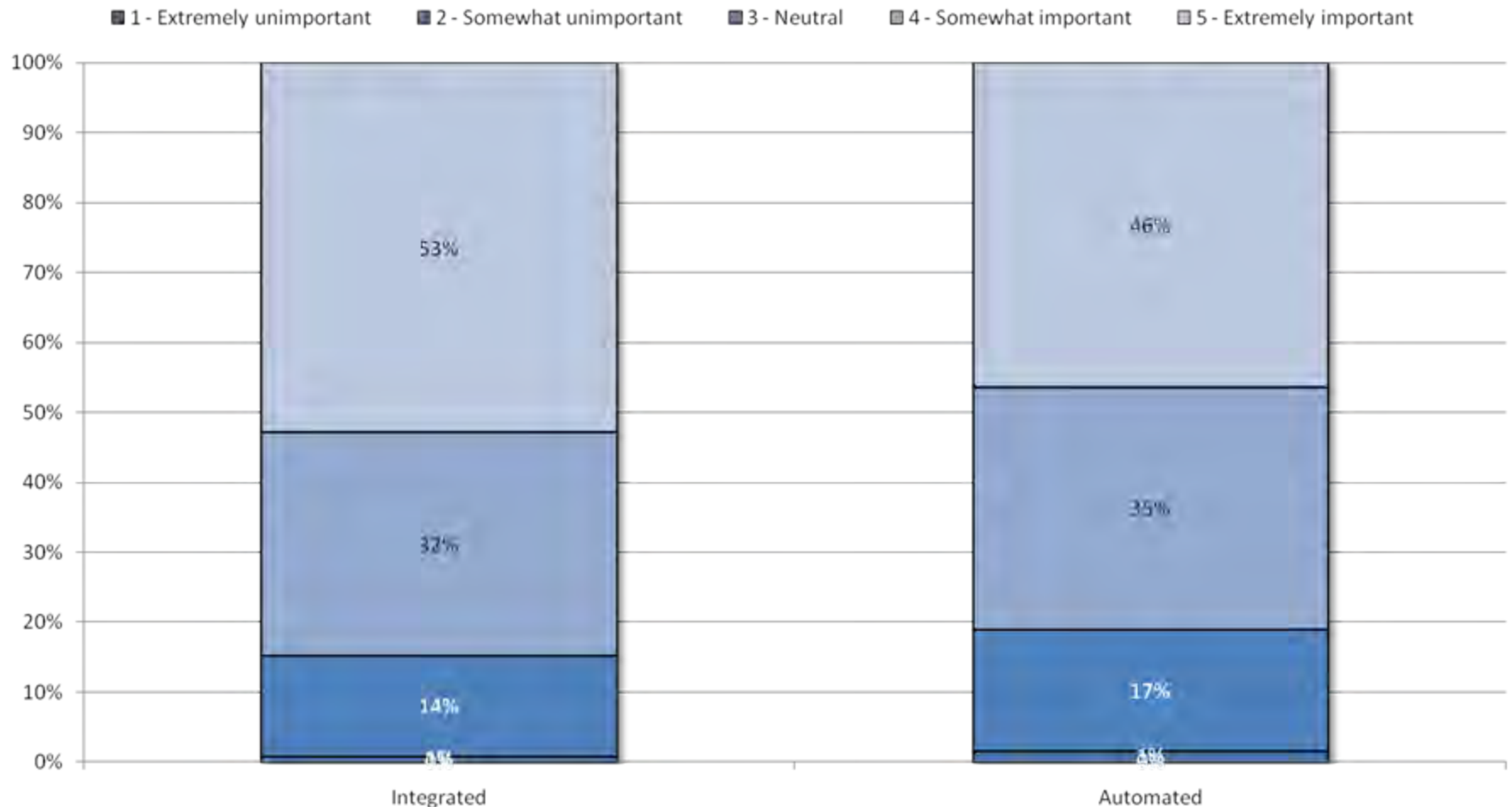
Lost devices

Q60: How many of each of these mobile devices are lost or stolen worldwide within your organization annually?
(Medians shown)



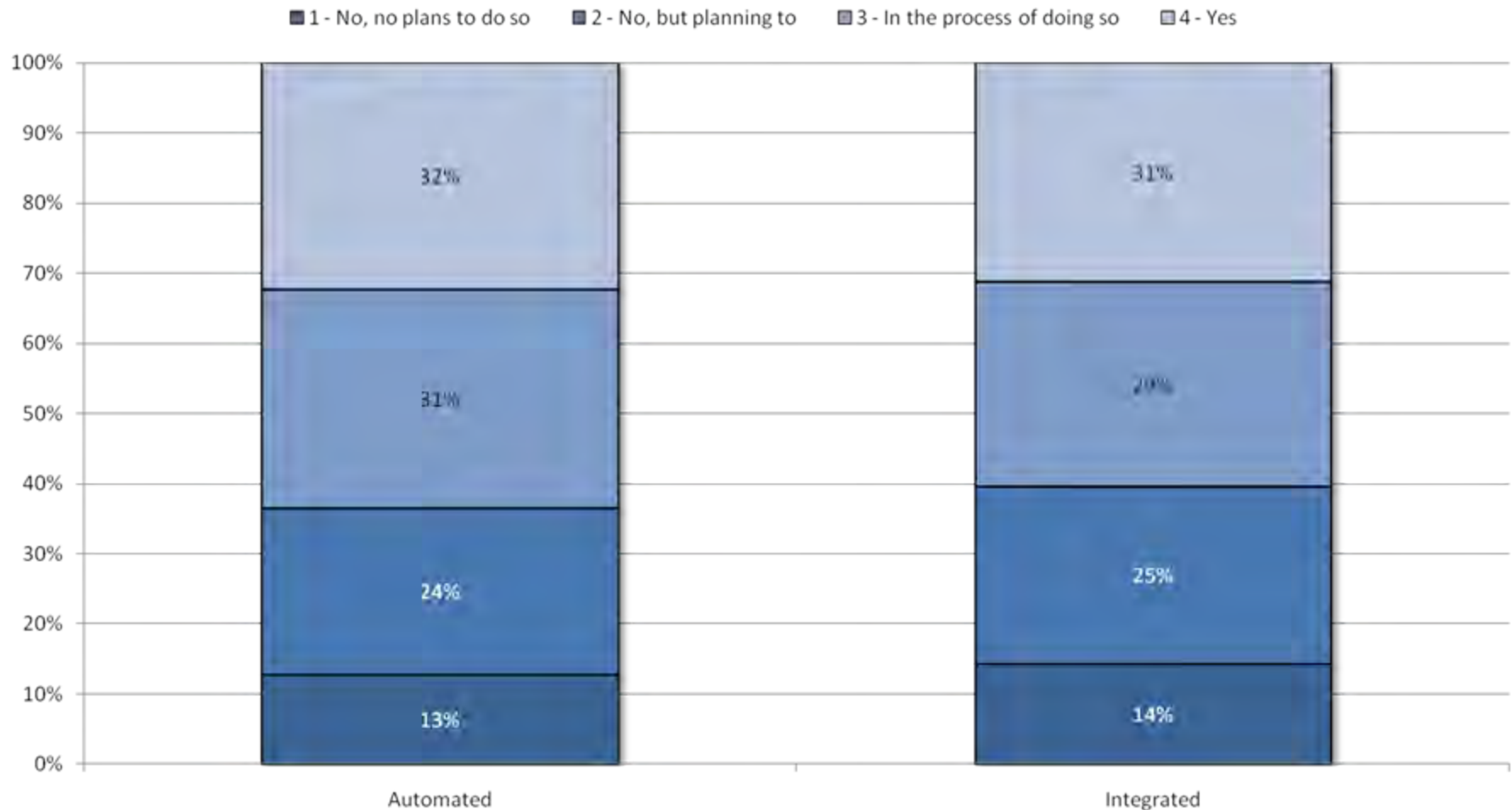
Endpoint security processes

Q61: How important is it to have your endpoint security process...?



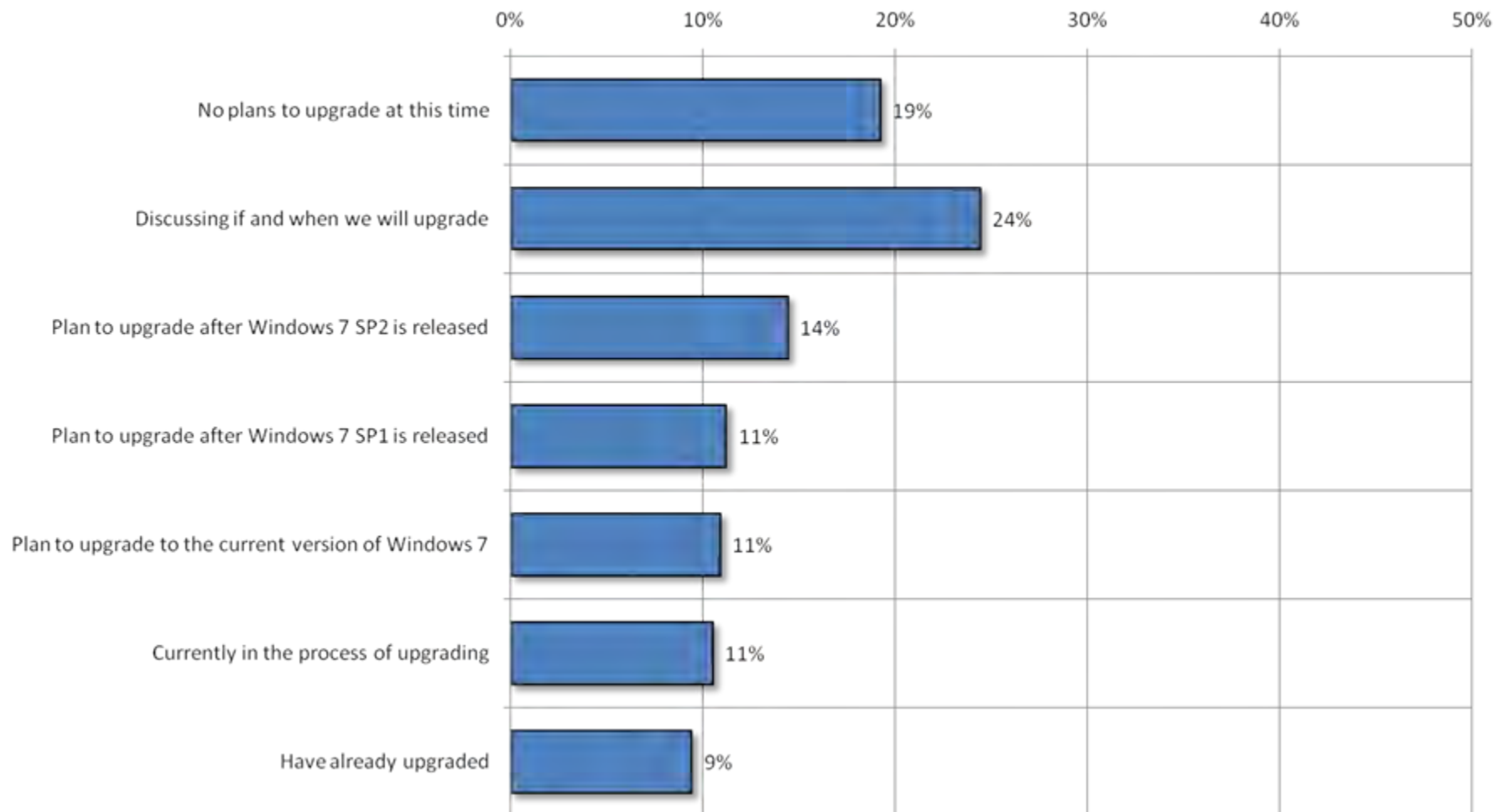
Endpoint security processes

Q62: Are your endpoint security processes...?



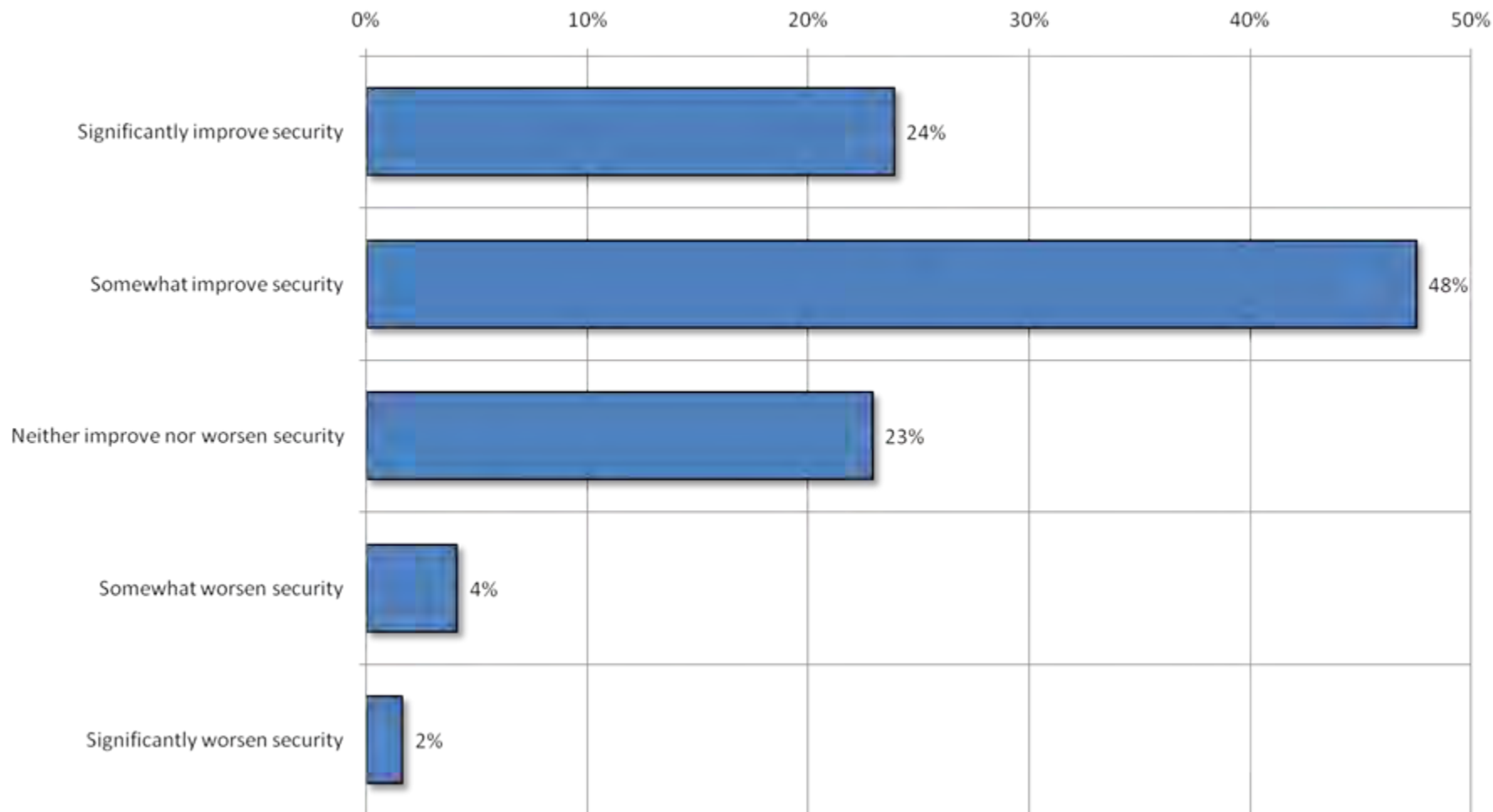
Windows 7

Q63: What are your plans for Windows 7?



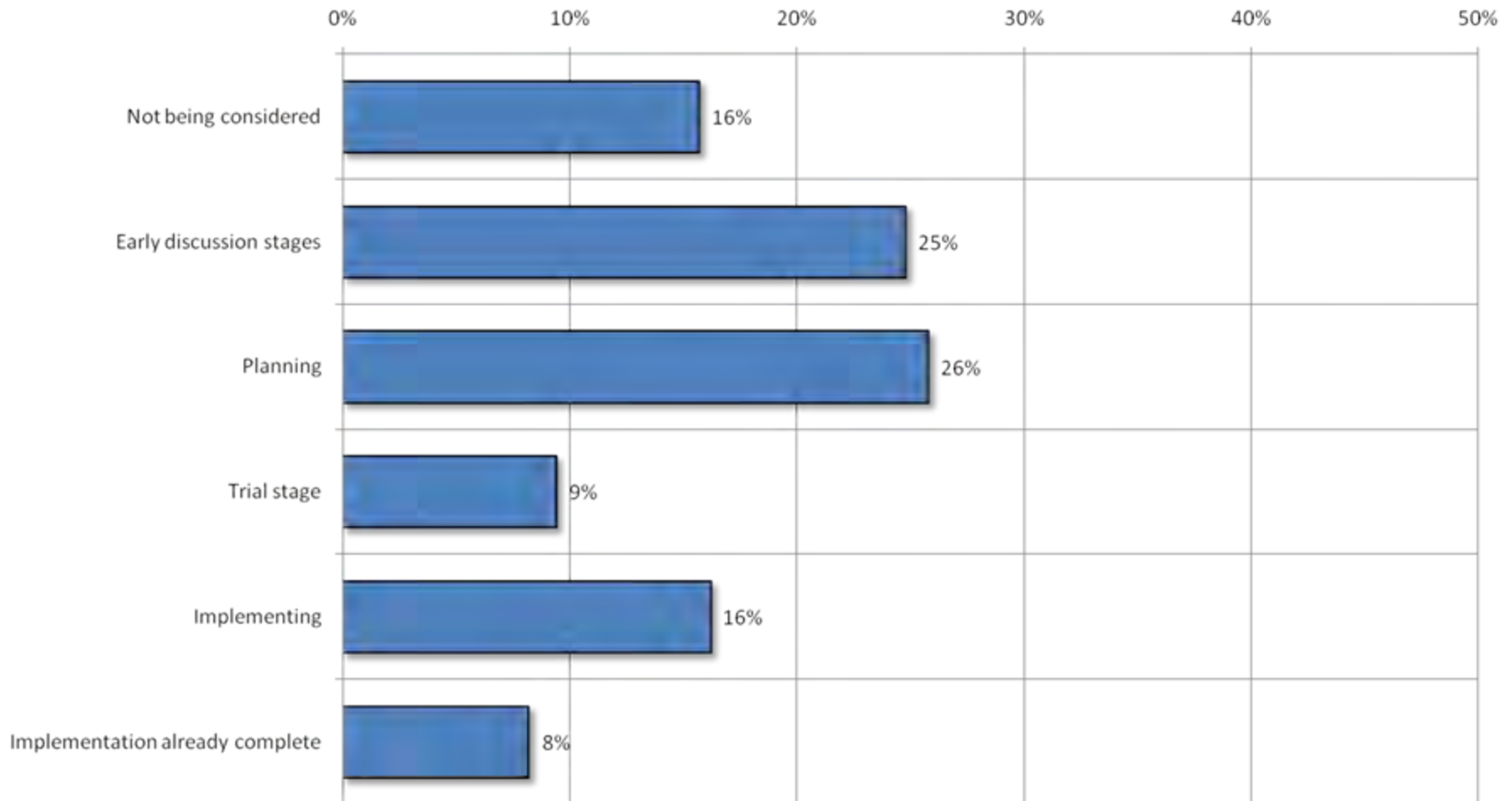
Windows 7

Q64: How do you think Windows 7 will affect endpoint security?



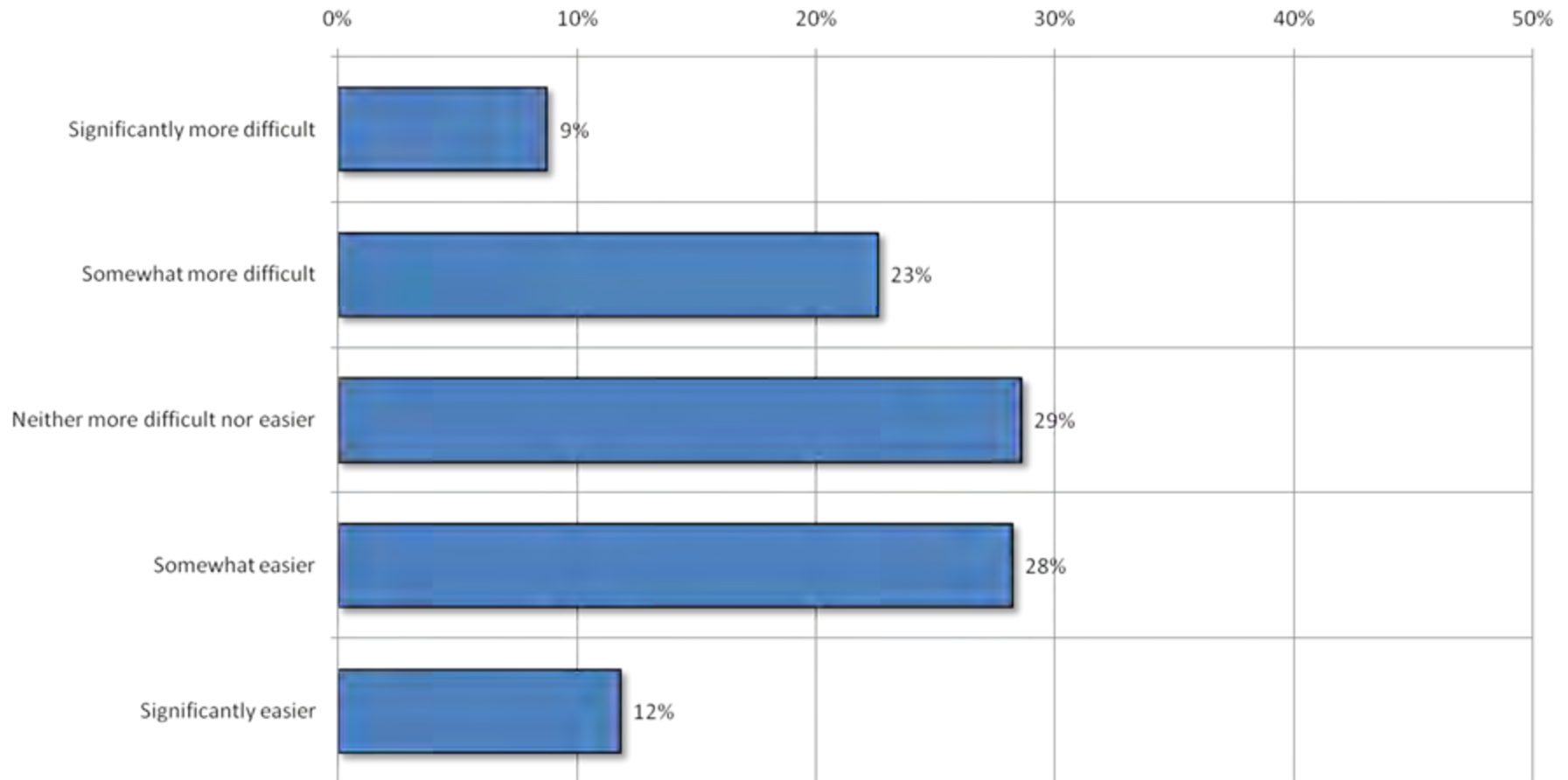
Endpoint virtualization

Q65: What are your plans for endpoint virtualization?



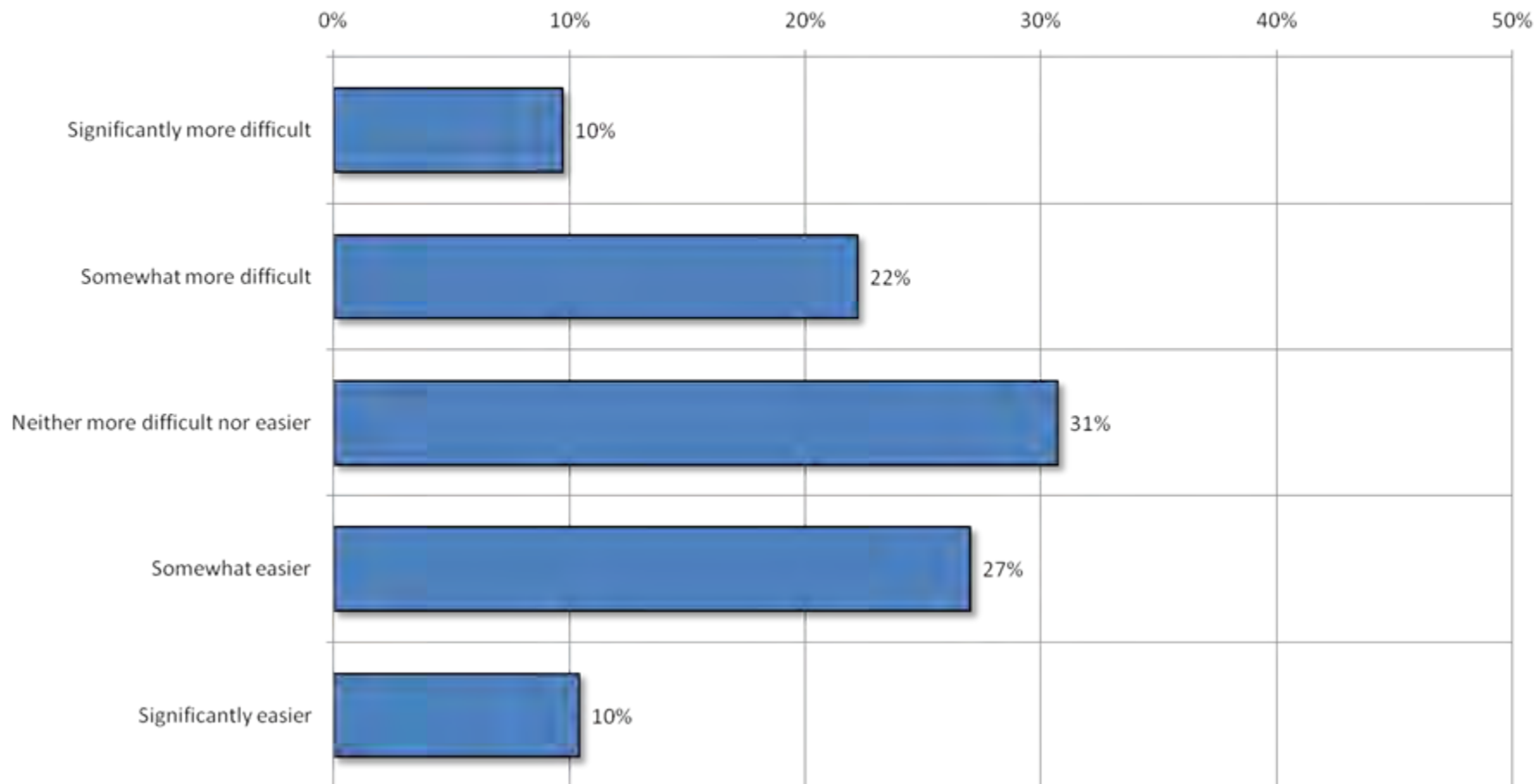
Endpoint virtualization

Q66: Does endpoint virtualization make it easier or harder to do your job with regards to network security?



Software-as-a-Service

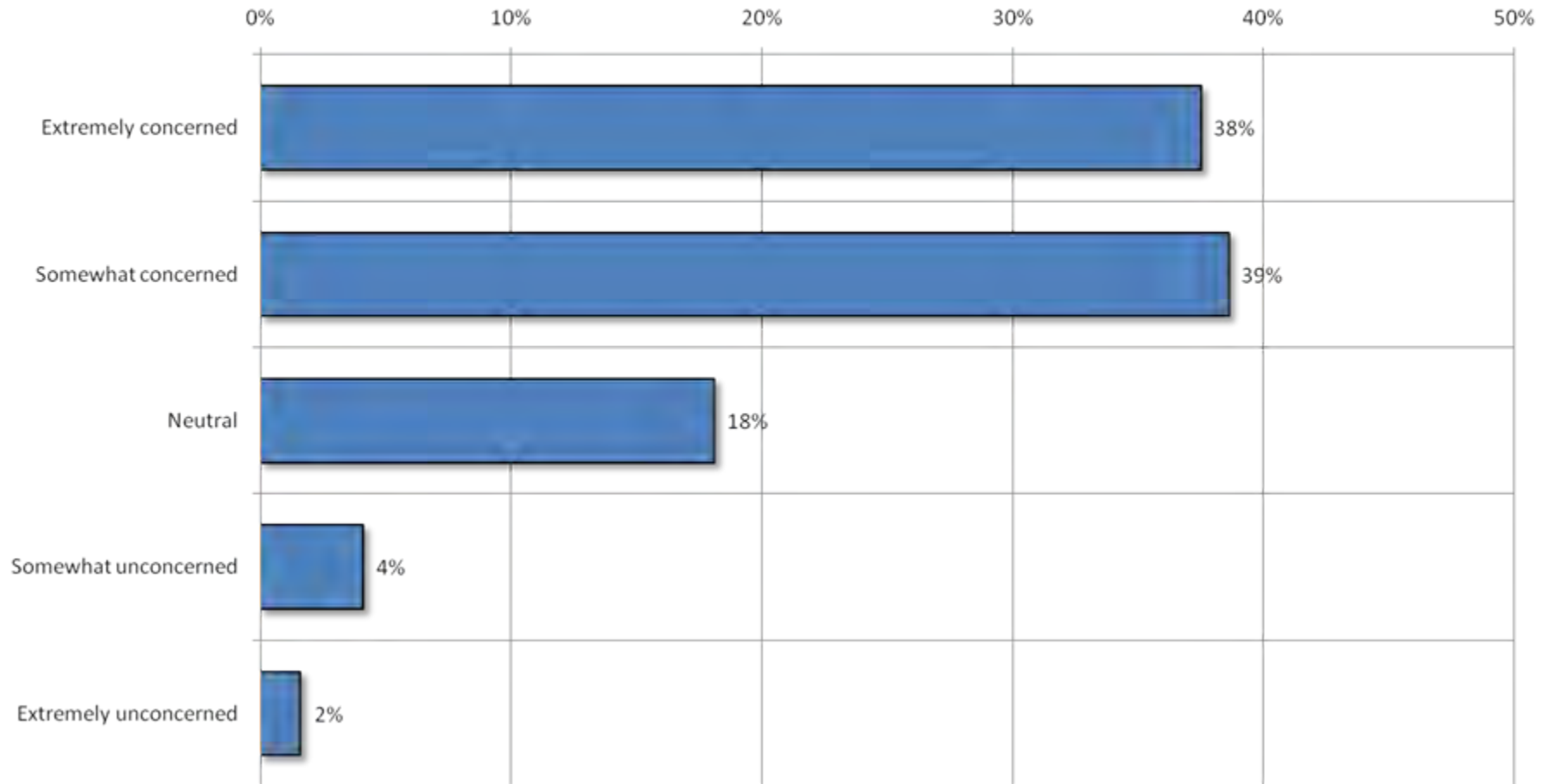
Q67: Does Software-as-a-Service (SaaS) make it easier or harder to do your job with regards to network security?



Data Loss Prevention

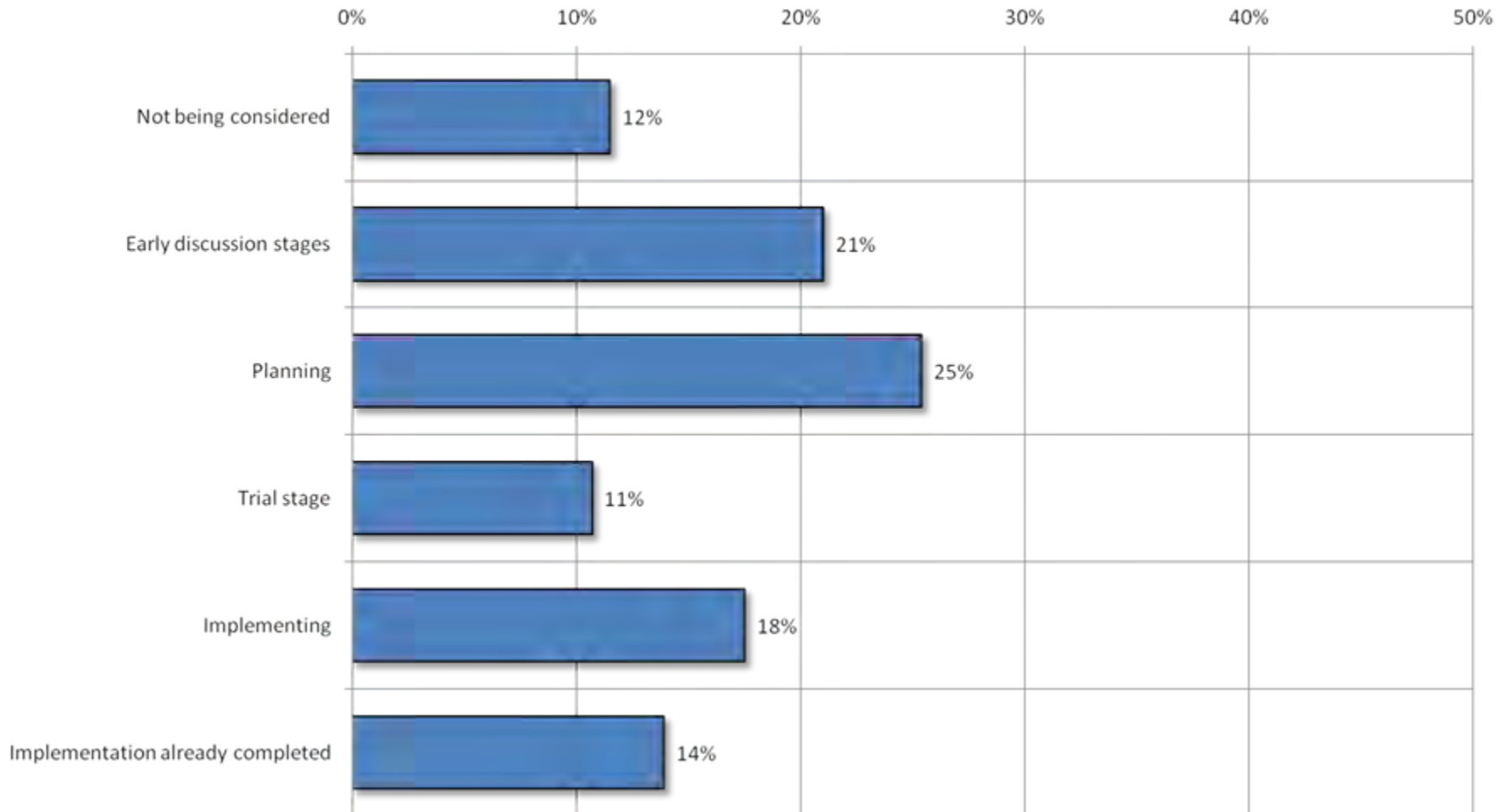
Data loss concern

Q68: How concerned are you regarding loss of confidential/proprietary data?



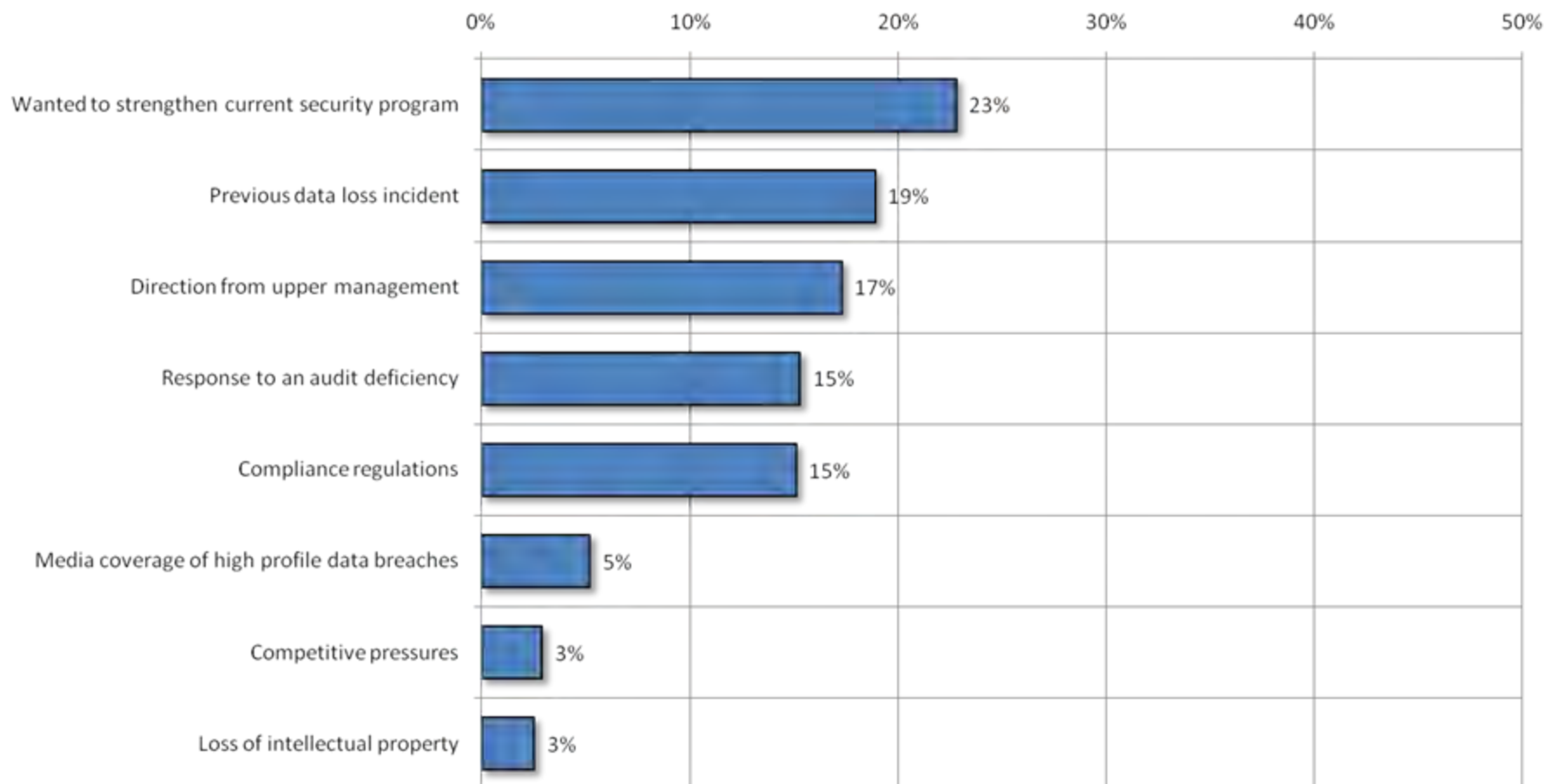
Data loss prevention

Q69: What is your organization's involvement with a DLP system?



Data loss prevention

Q70: What drove you to consider/implement a DLP program/solution?
(Only asked of those who are at least discussing DLP)

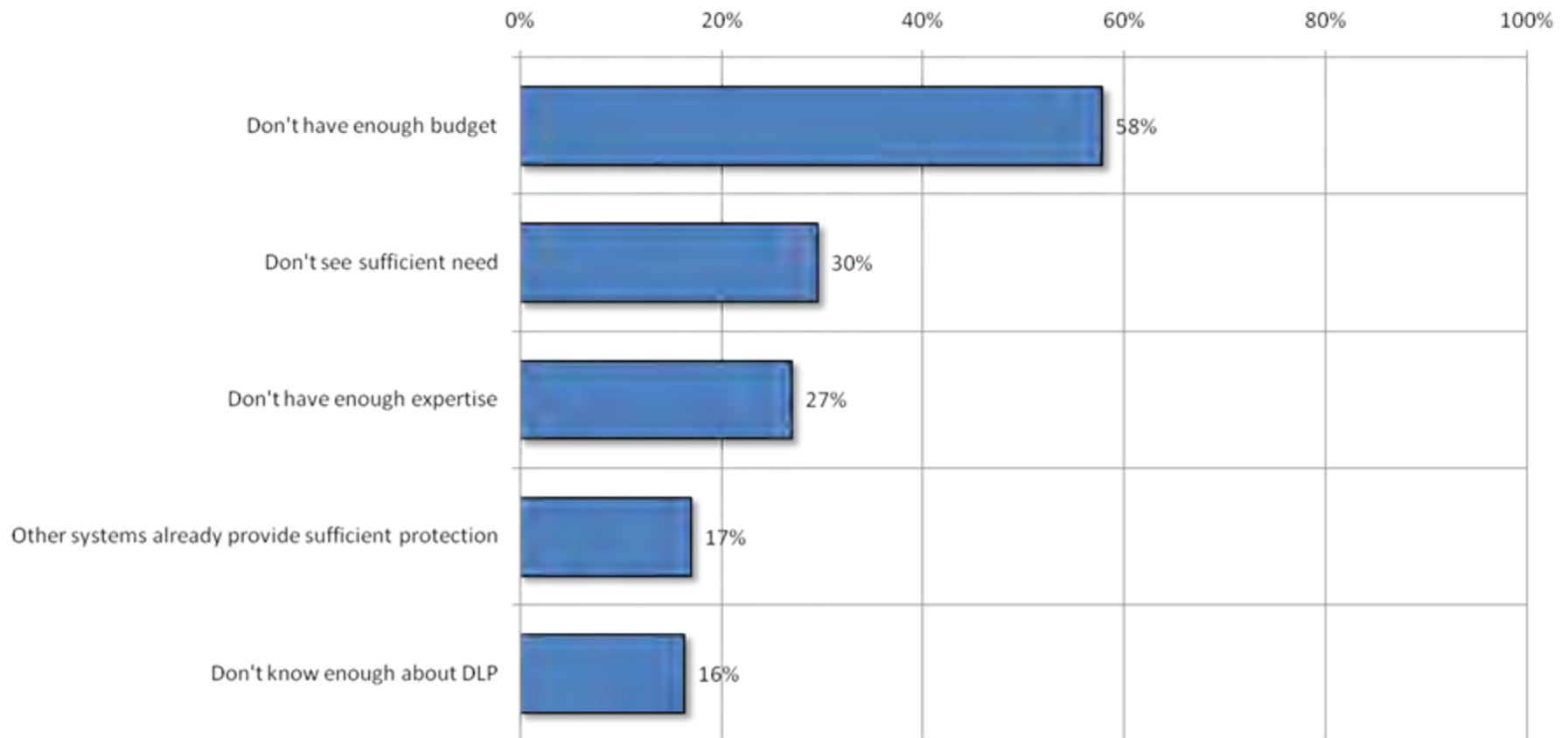


Data loss prevention

Q71: Why has your organization chosen to NOT have a DLP solution?

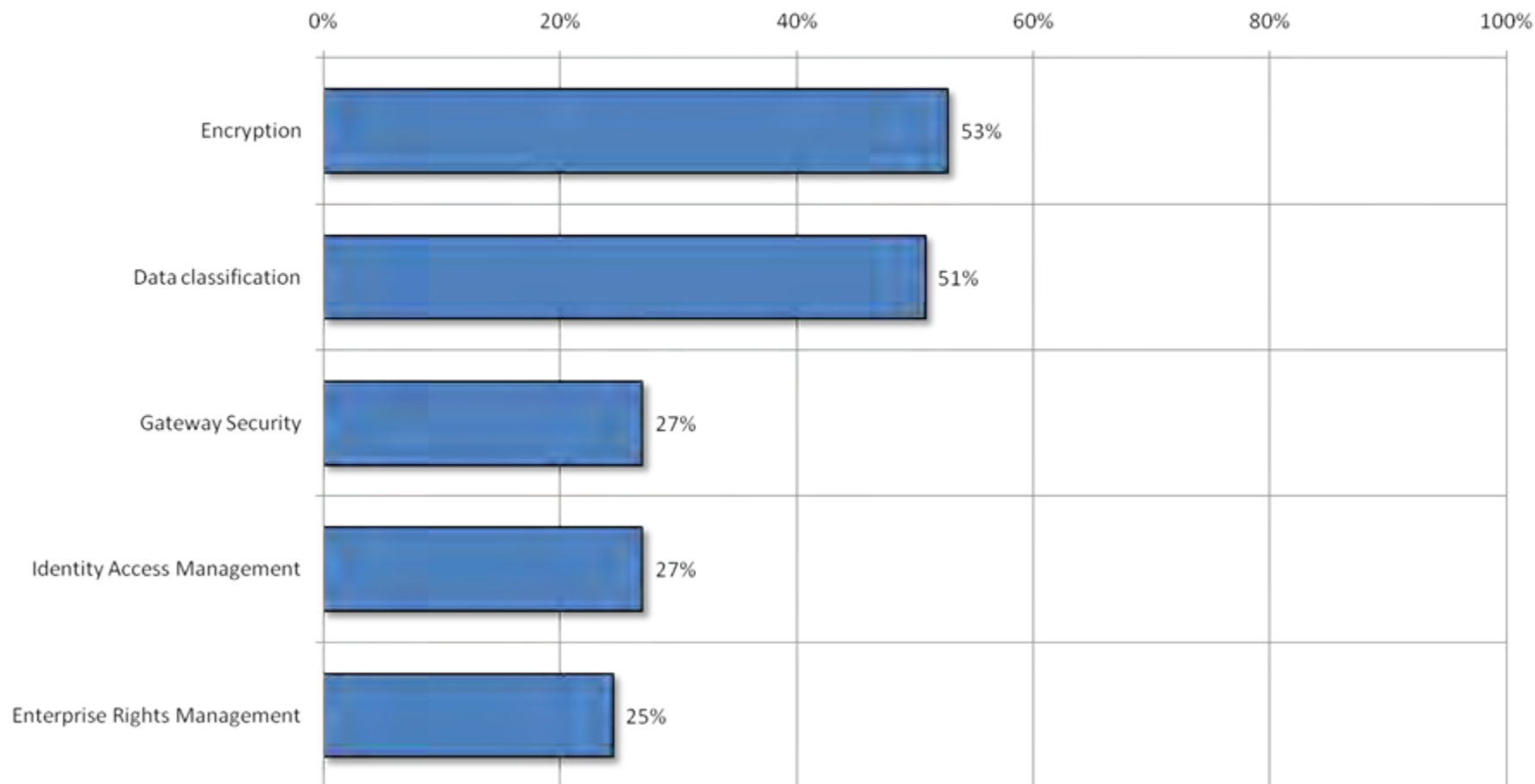
Mark all that apply.

(Asked only of those who are not considering DLP)



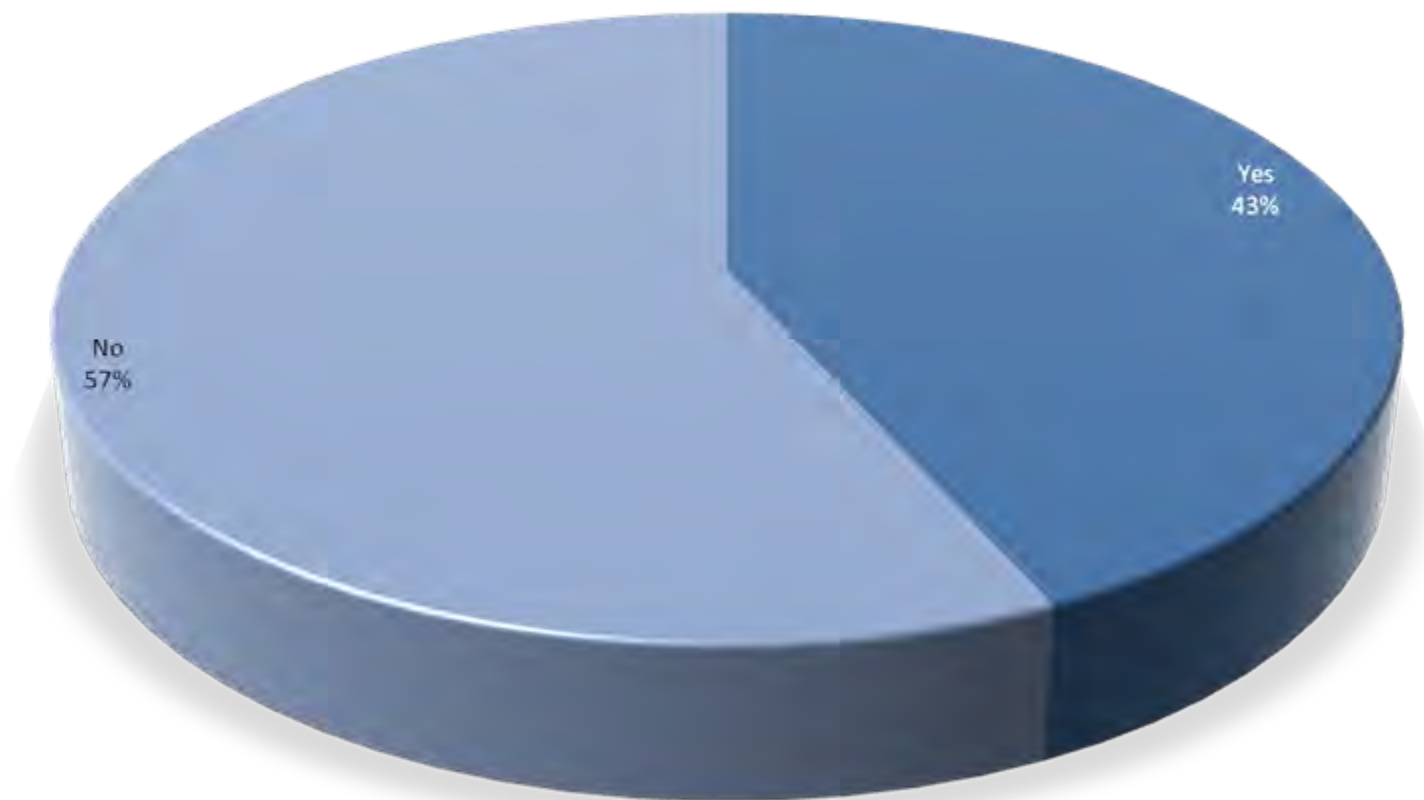
Other information security systems

Q72: What other information security systems or technologies do you use in your organization? Mark all that apply.



Previous data loss

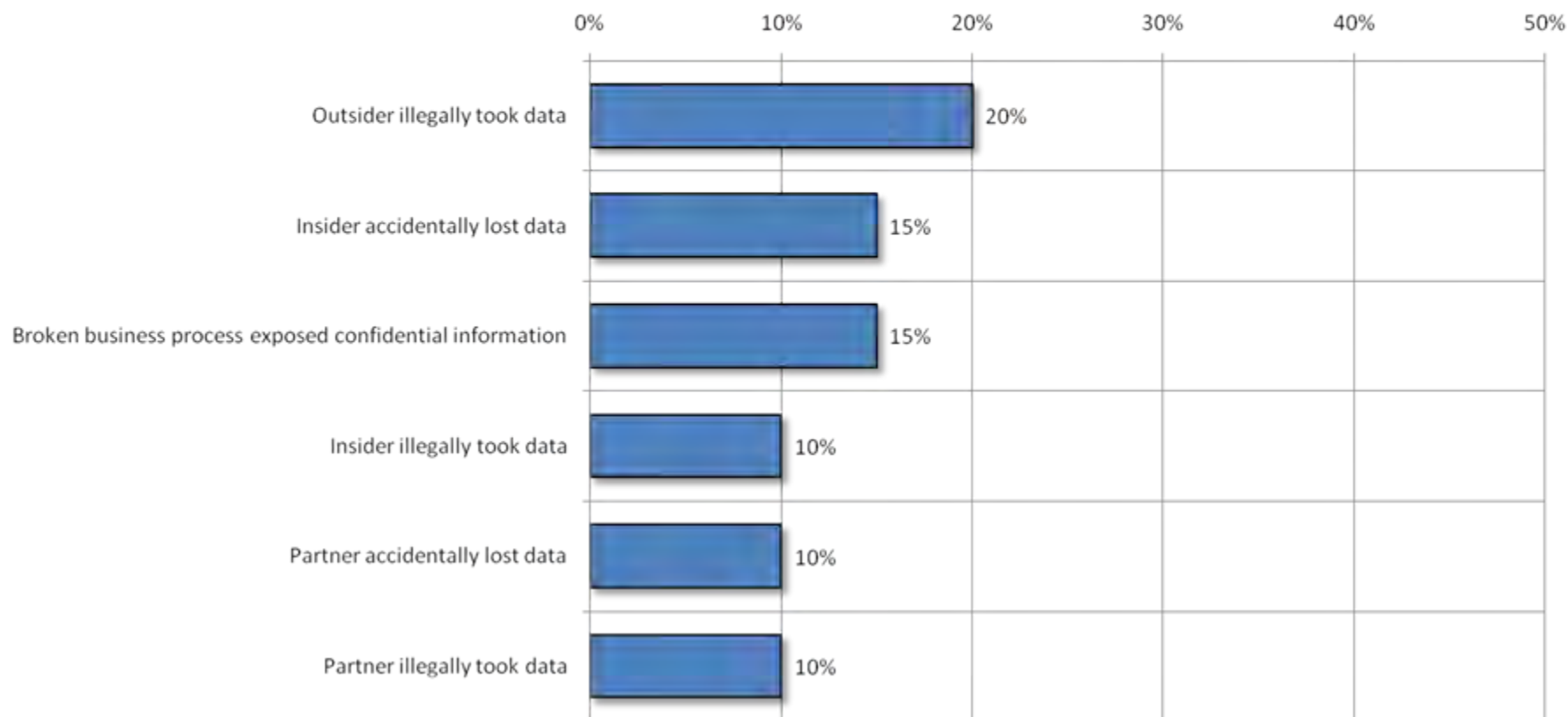
Q73: Have you lost confidential/proprietary data in the past?



Previous data loss

Q74: What percentage of your past data losses have come from each of the following areas?

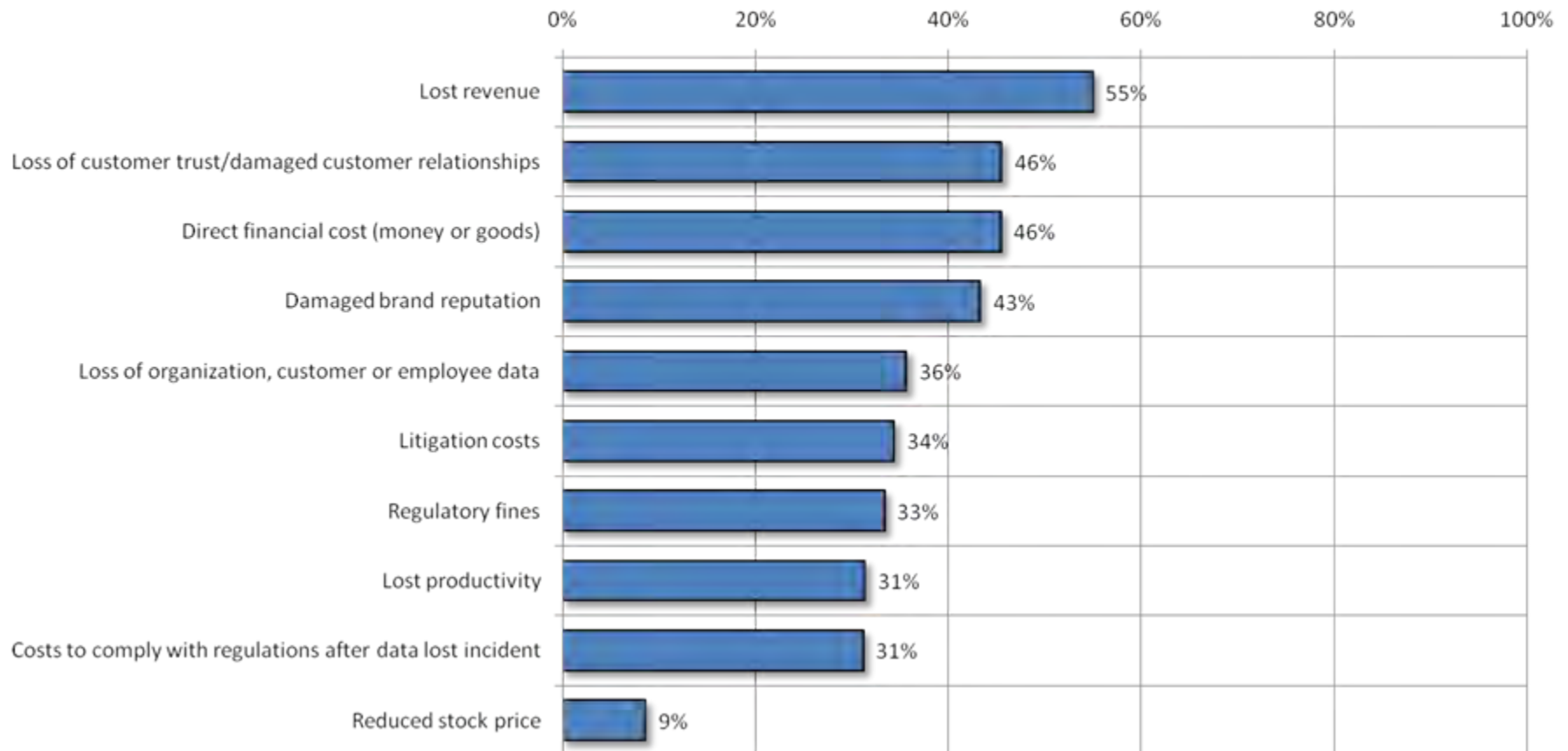
**(Asked only of those who have lost confidential/proprietary data in the past)
(Means shown)**



Data loss consequences

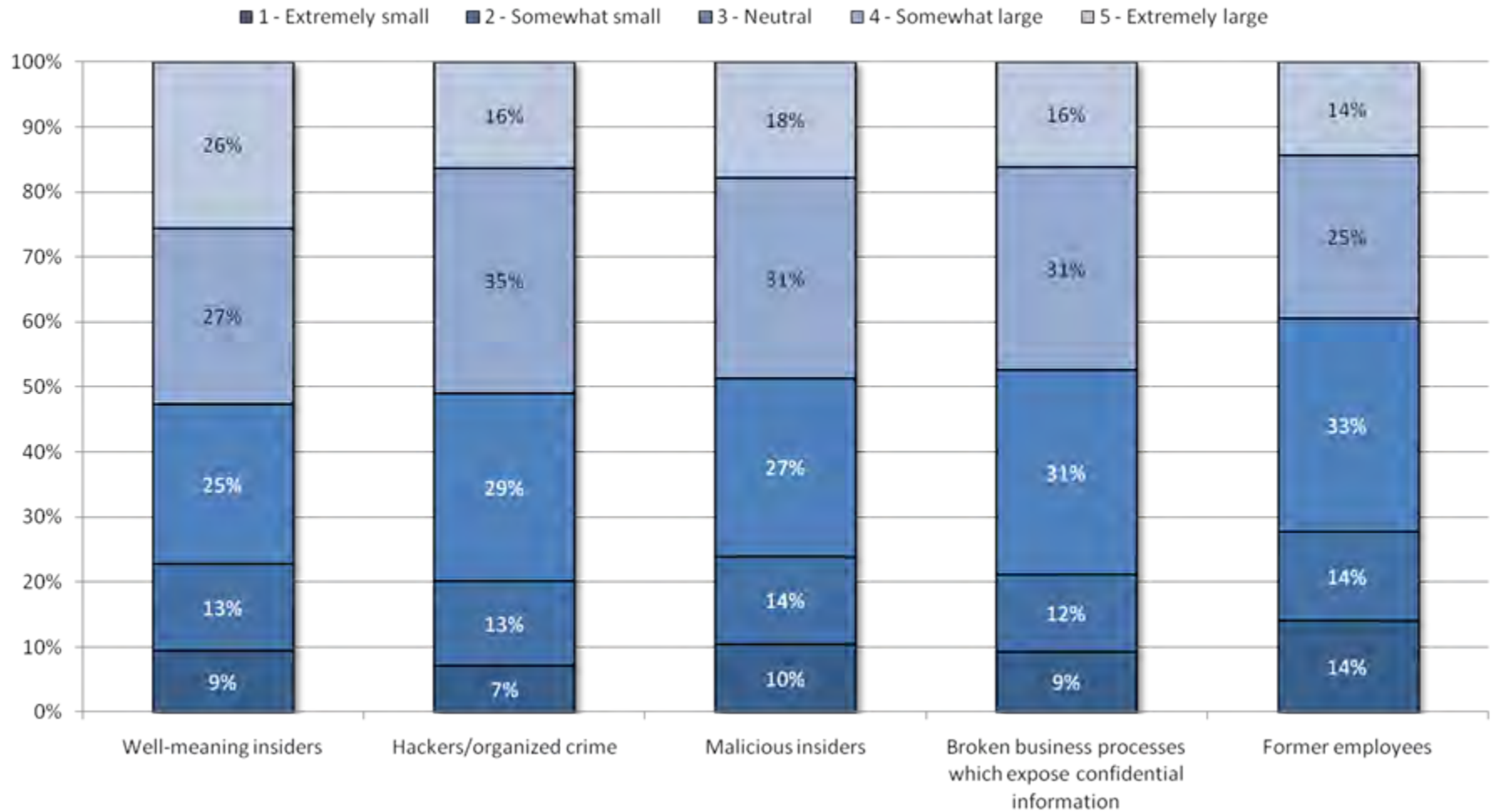
Q75: What have been the consequences of data loss to your organization? Mark all that apply.

(Asked only of those who have lost confidential/proprietary data in the past)



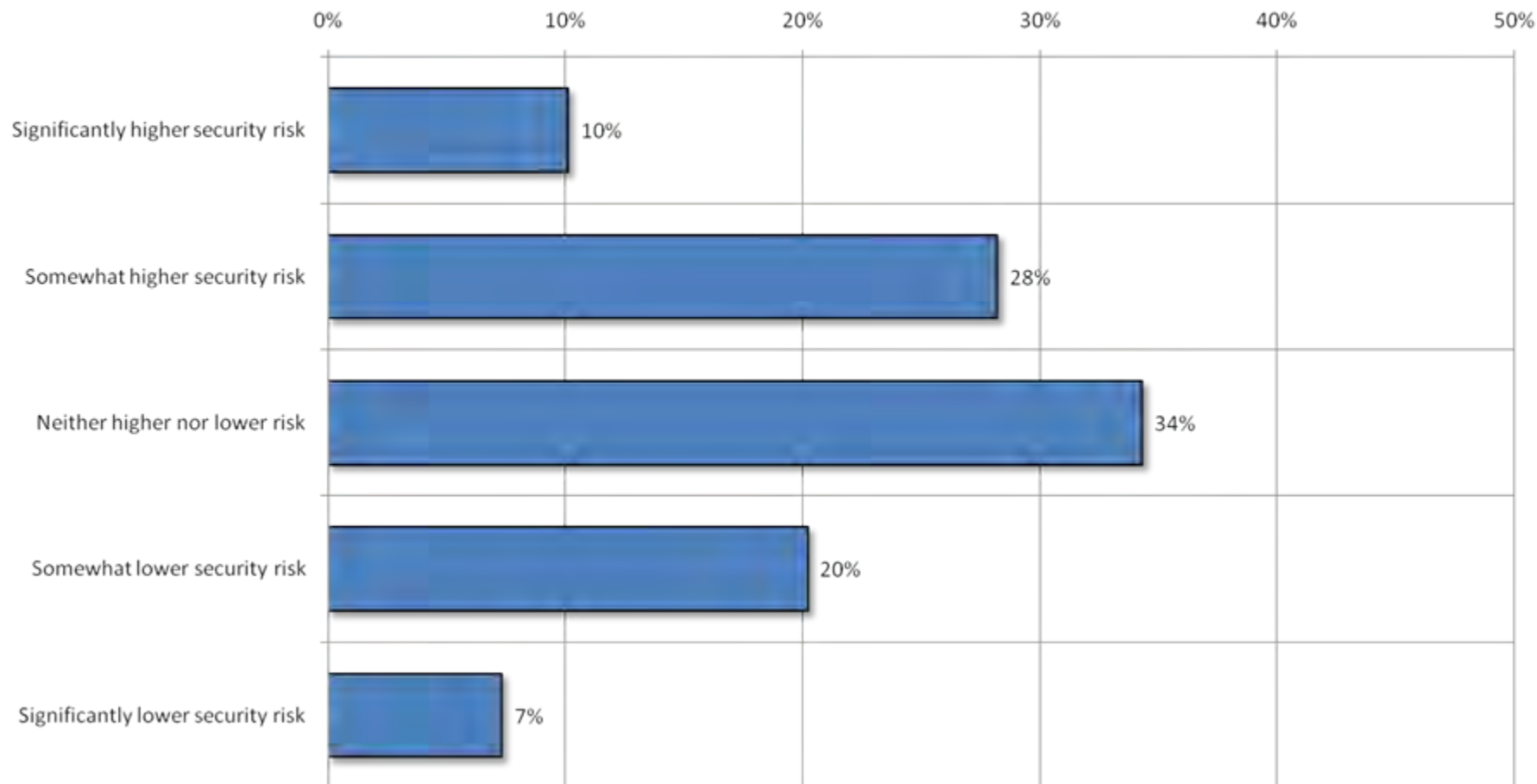
Data loss threats

Q76: How big is the threat of data loss from the following?



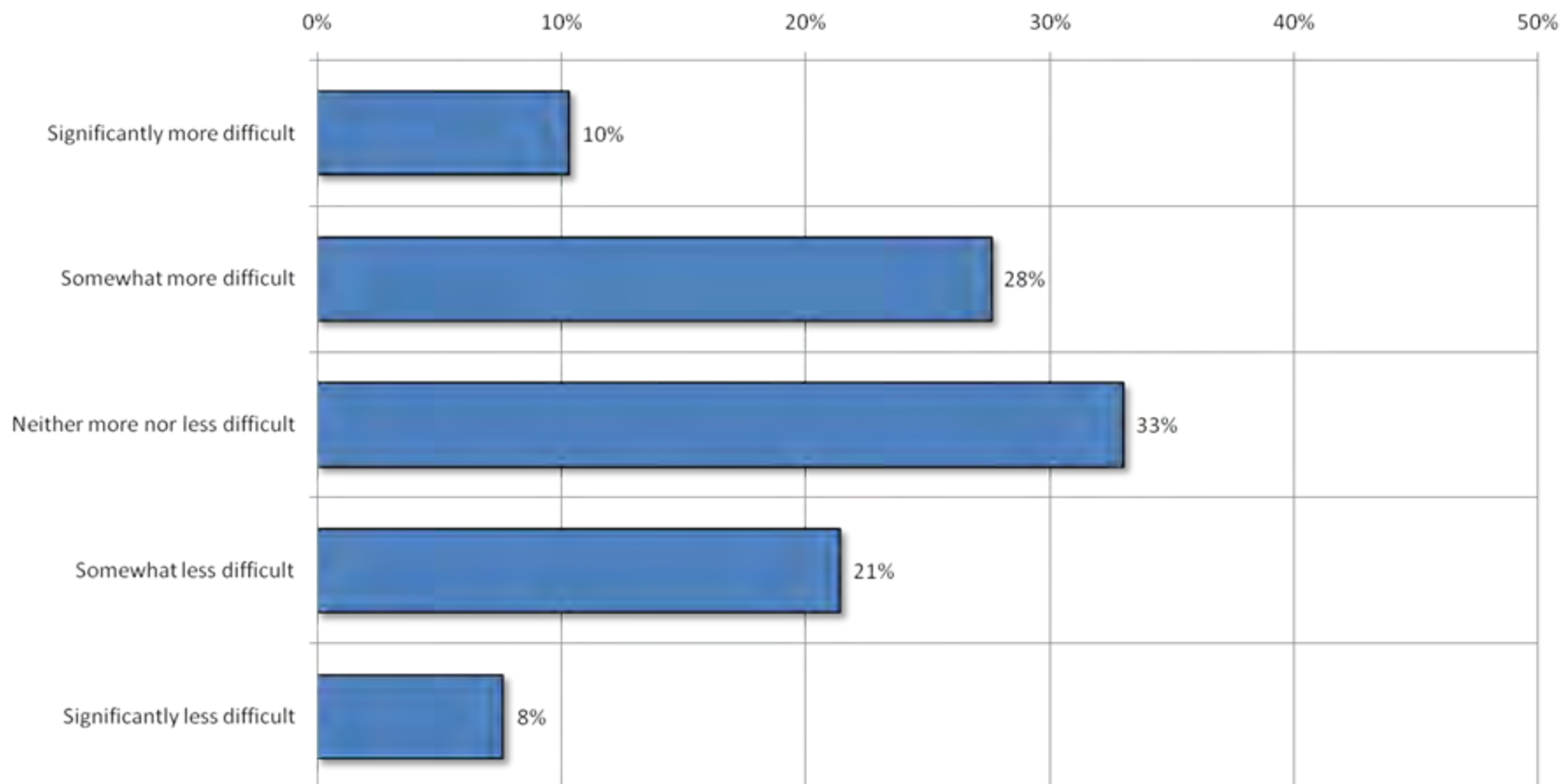
Virtualization strategy

Q77: Does your virtualization strategy make the risk of losing data bigger or smaller?



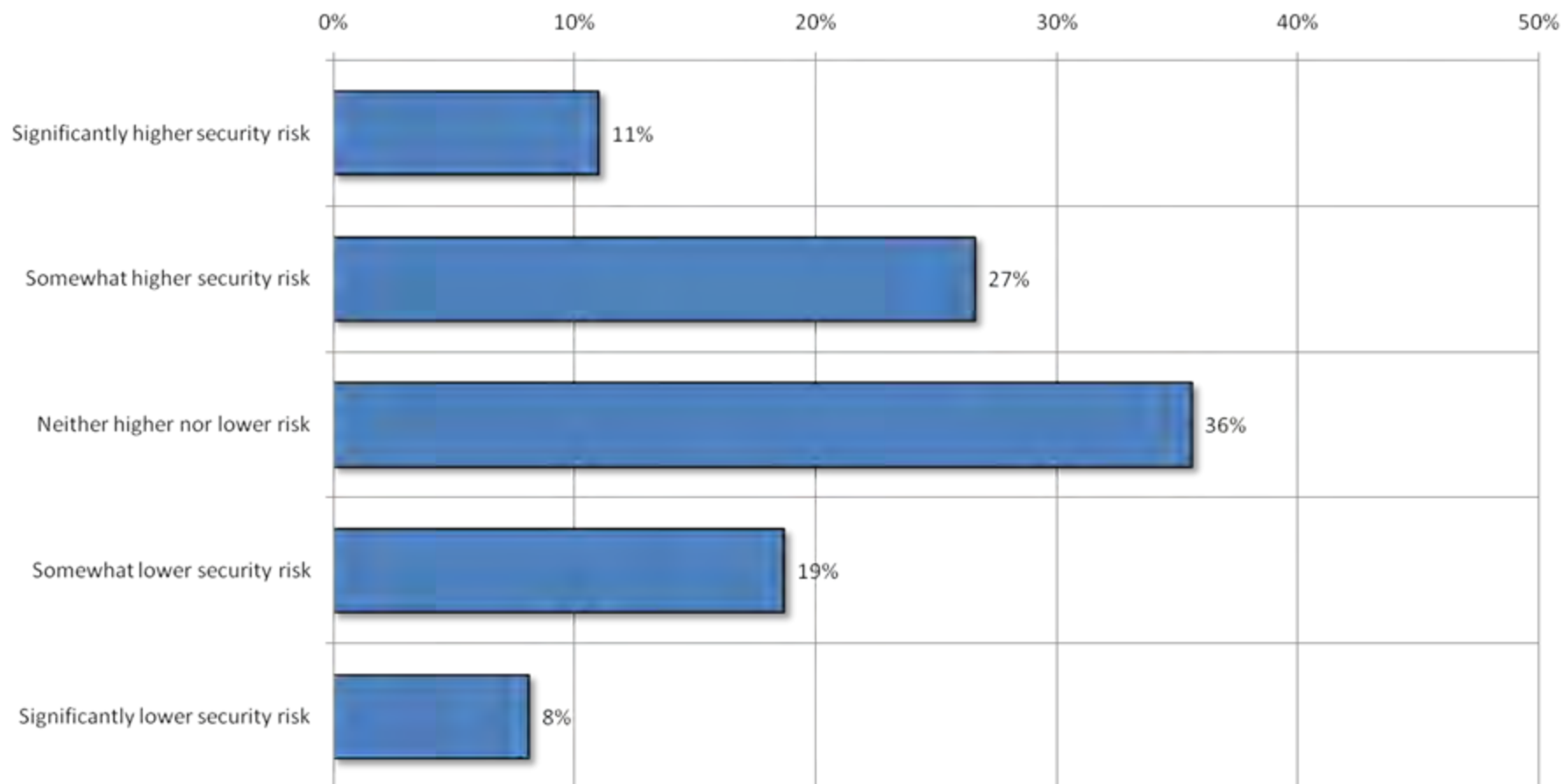
Virtualization strategy

Q78: Does your virtualization strategy make it easier or harder to prevent and/or react to data loss?



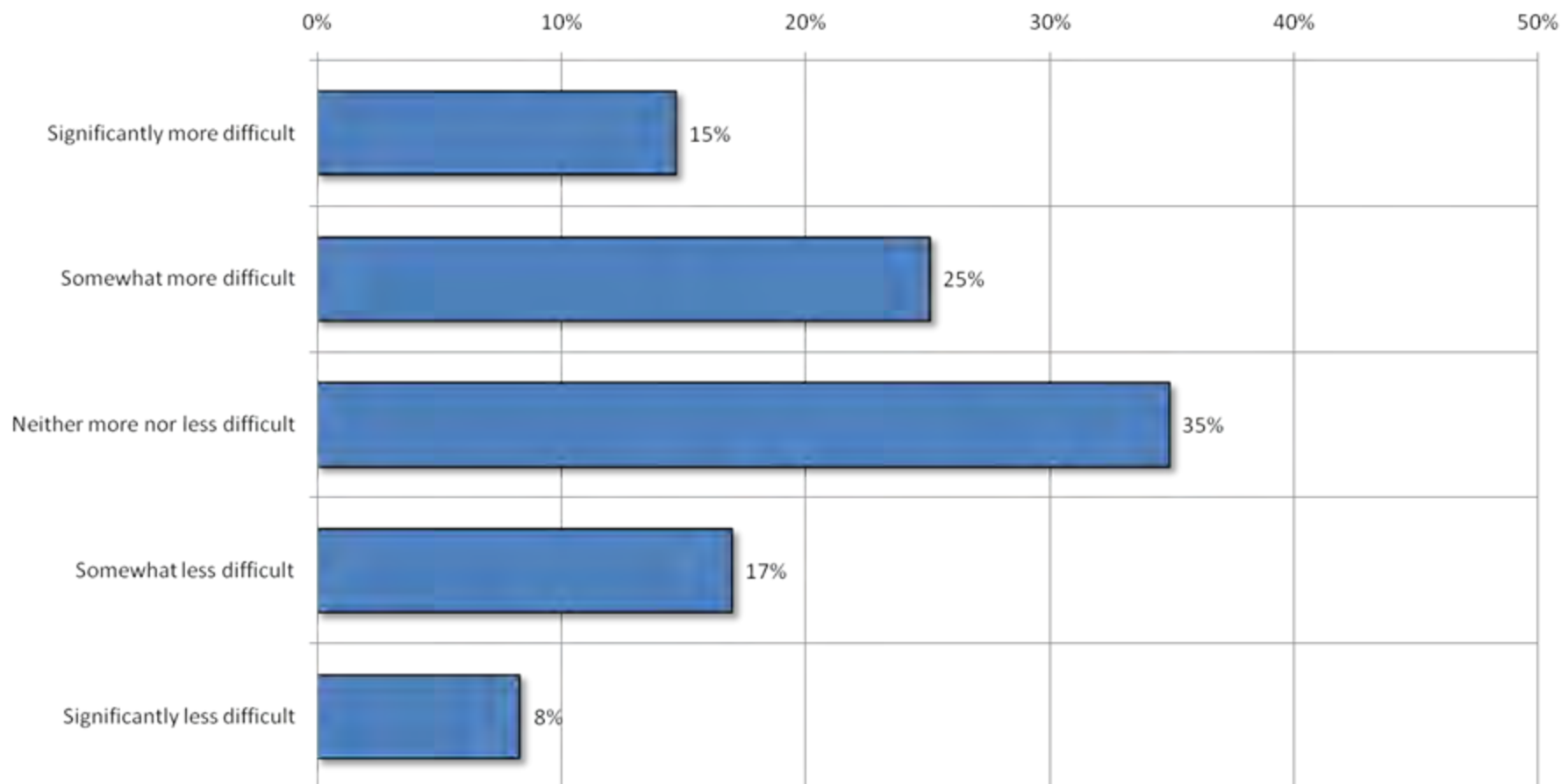
Cloud computing strategy

Q79: Does your cloud computing strategy make the risk of losing data bigger or smaller?



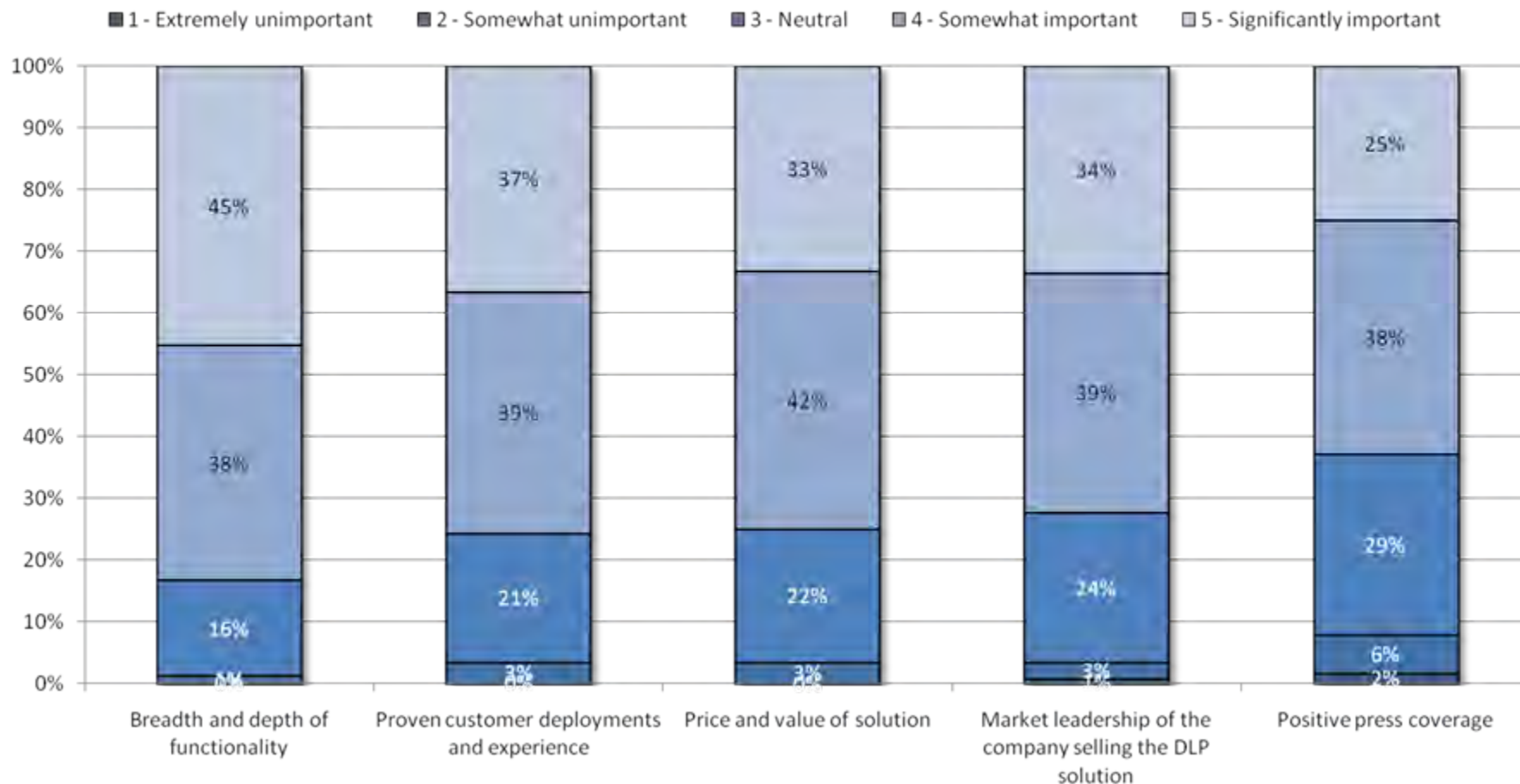
Cloud computing strategy

Q80: Does your cloud computing strategy make it easier or harder to prevent and/or react to data loss?



DLP selection

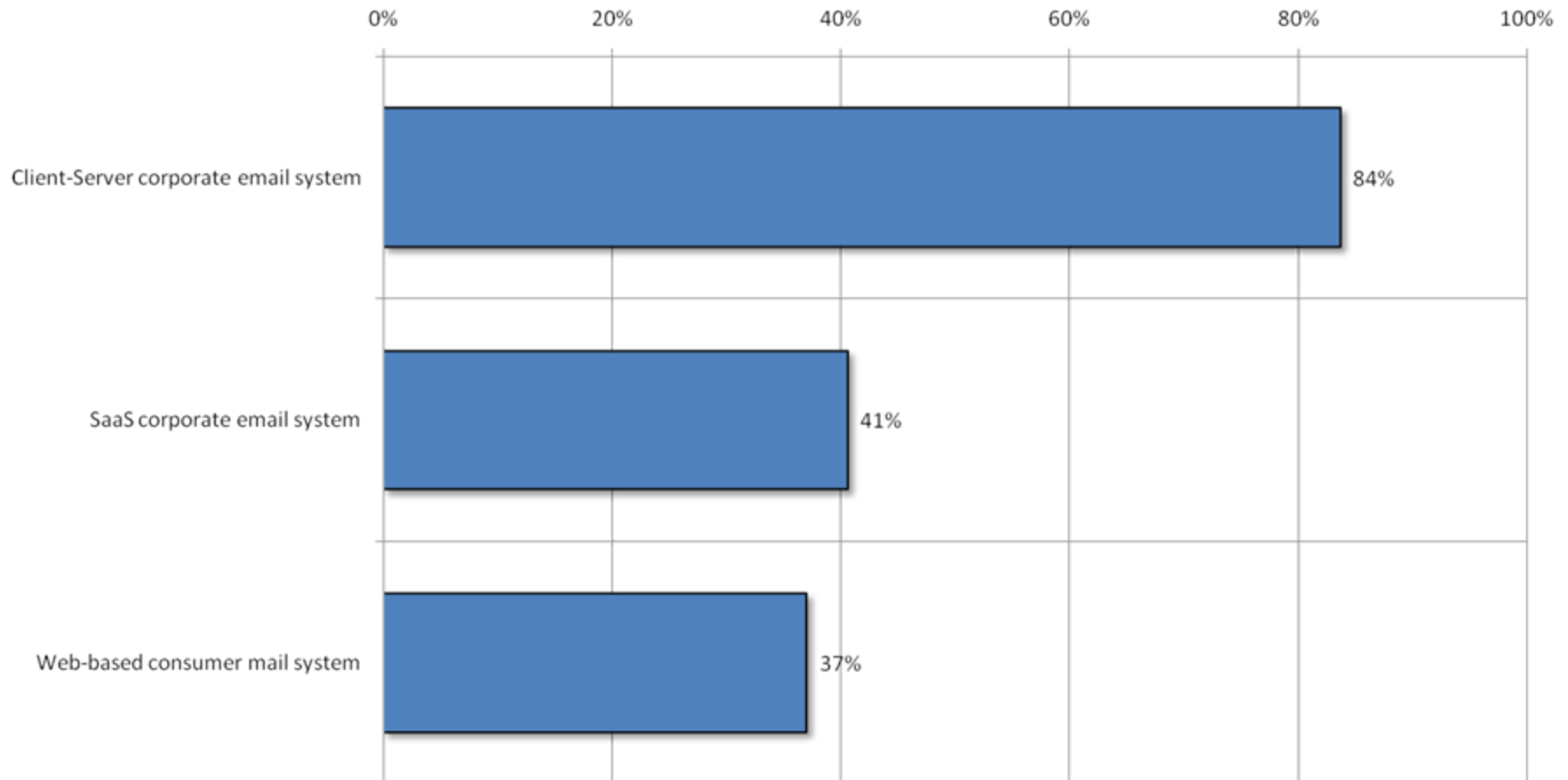
Q81: How important are the following factors when selecting a DLP product/solution?



Messaging/Collaboration Security

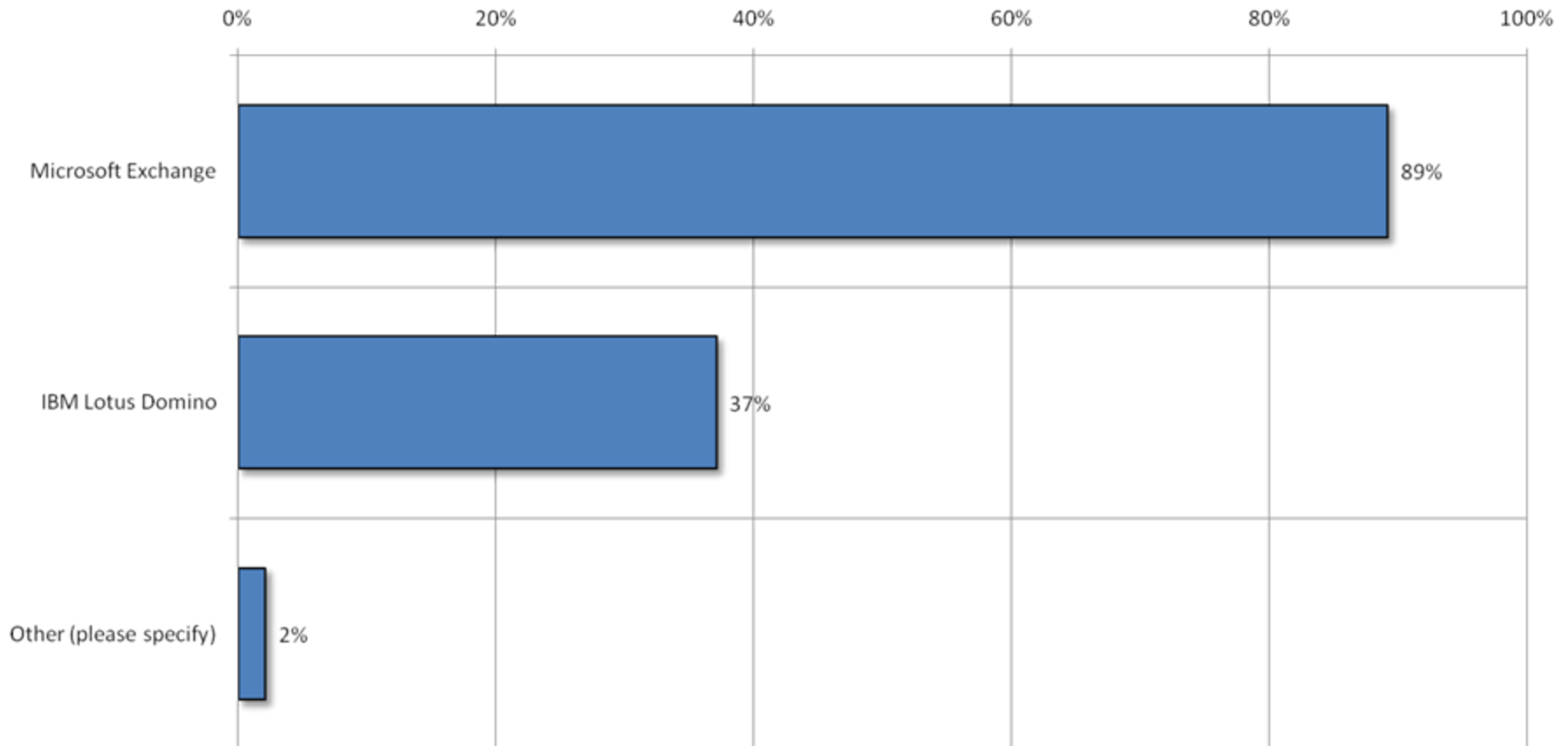
Email systems

**Q82: What kind of email systems are used within your organization?
Mark all that apply.**



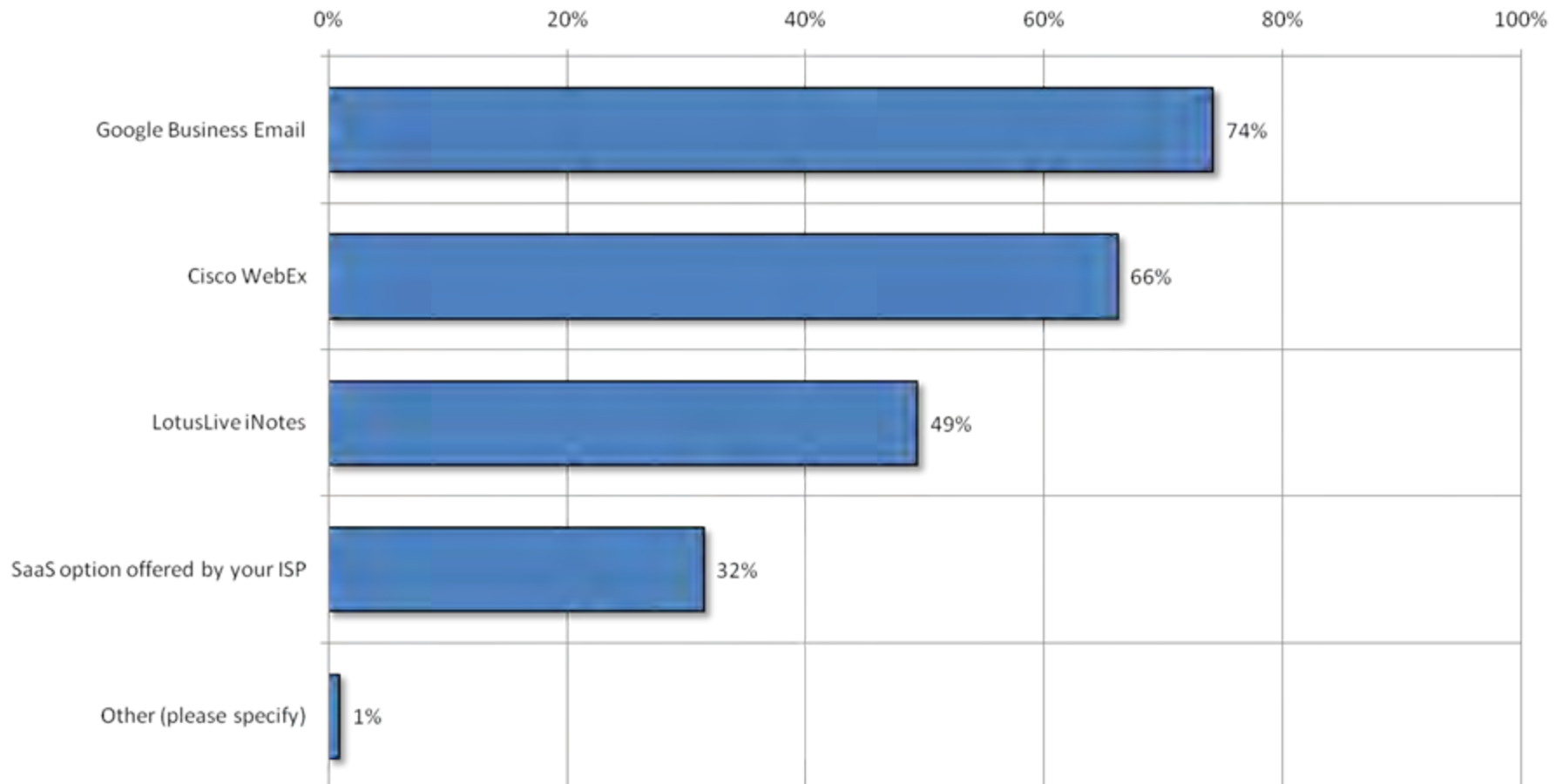
Email systems

Q83: Which client-server corporate email system(s) do you use?
(Asked only of those who indicated that they use a client-server corporate email system)



Email systems

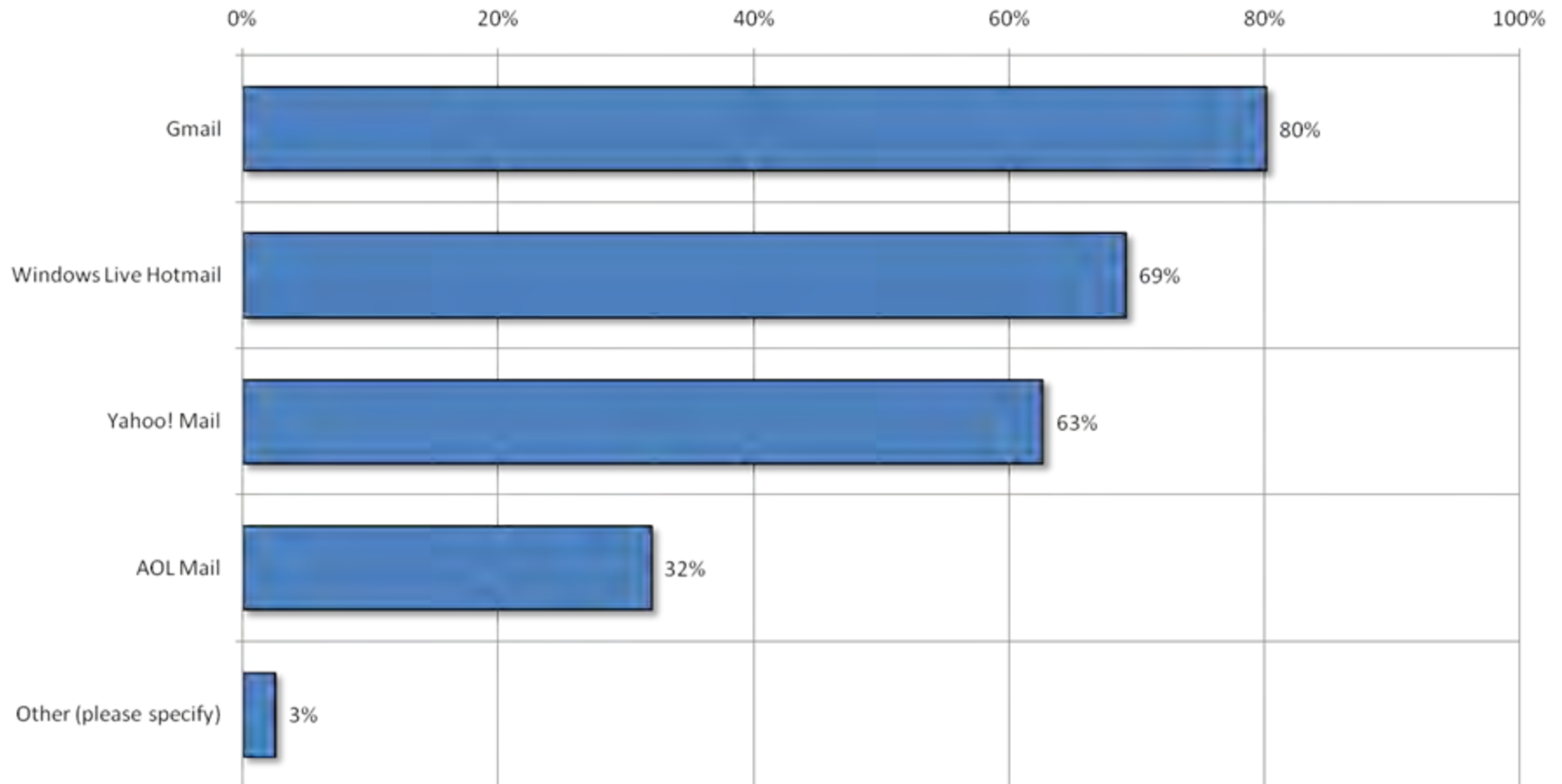
Q84: Which SaaS corporate email system(s) do you use?
(Asked only of those who indicated that they use a SaaS corporate email system)



Email systems

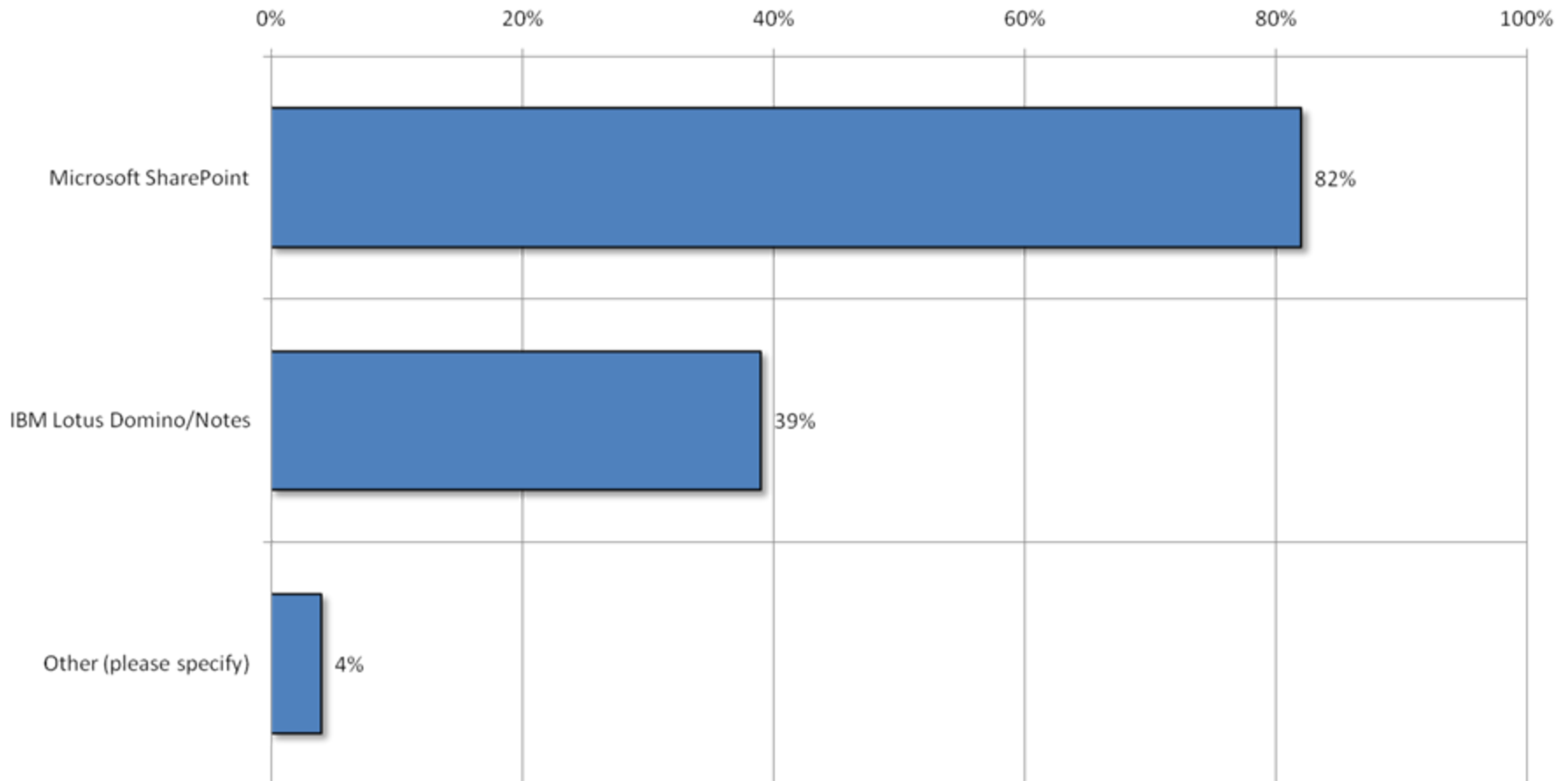
Q85: Which web mail email system(s) do you use?

(Asked only of those who indicated that they use a web-based consumer mail system)



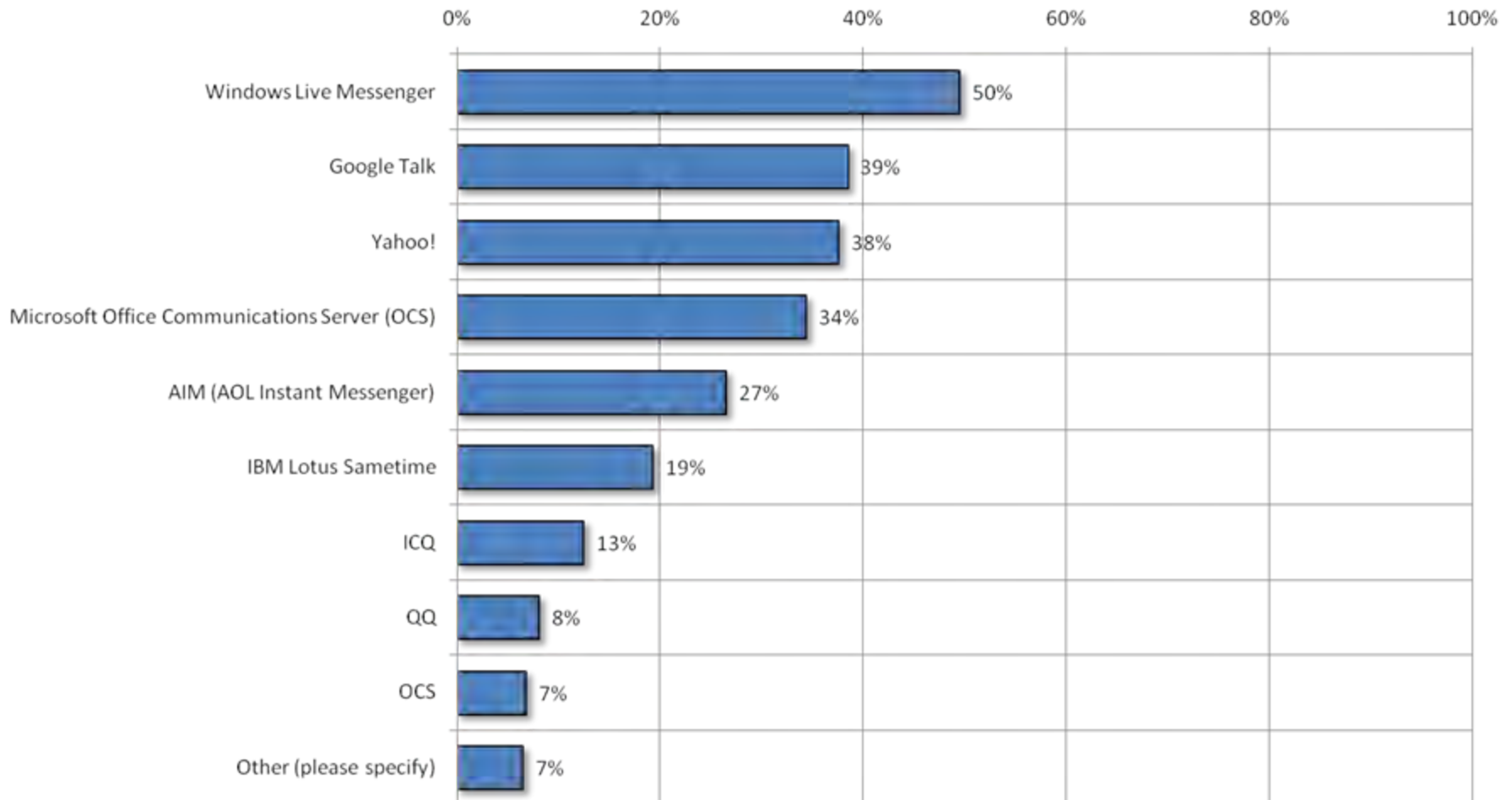
Collaboration systems

Q86: What kind of collaboration systems are used within your organization? Mark all that apply.



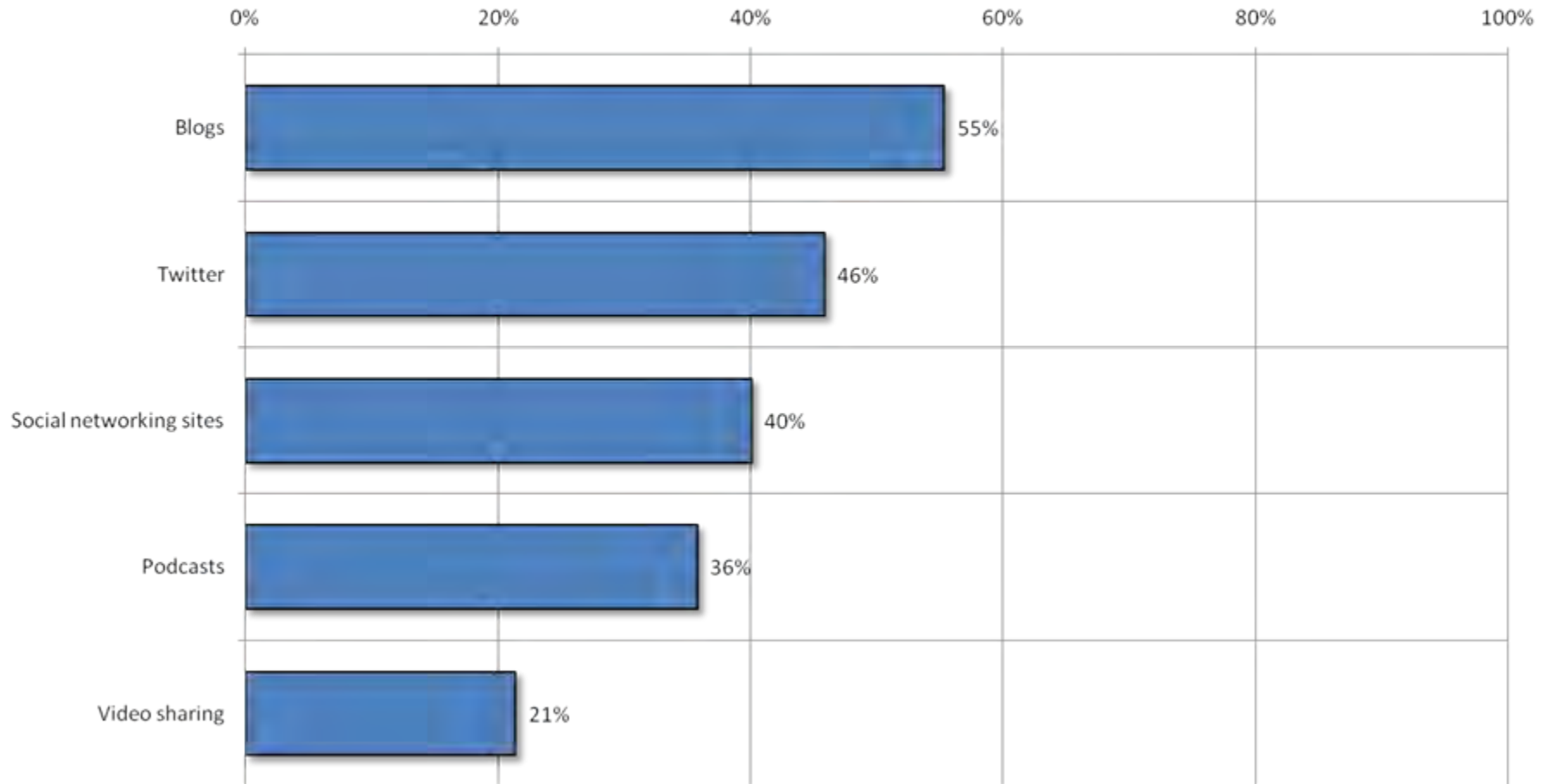
Instant messaging

Q87: What IM systems are used officially within your organization?



Social media tools

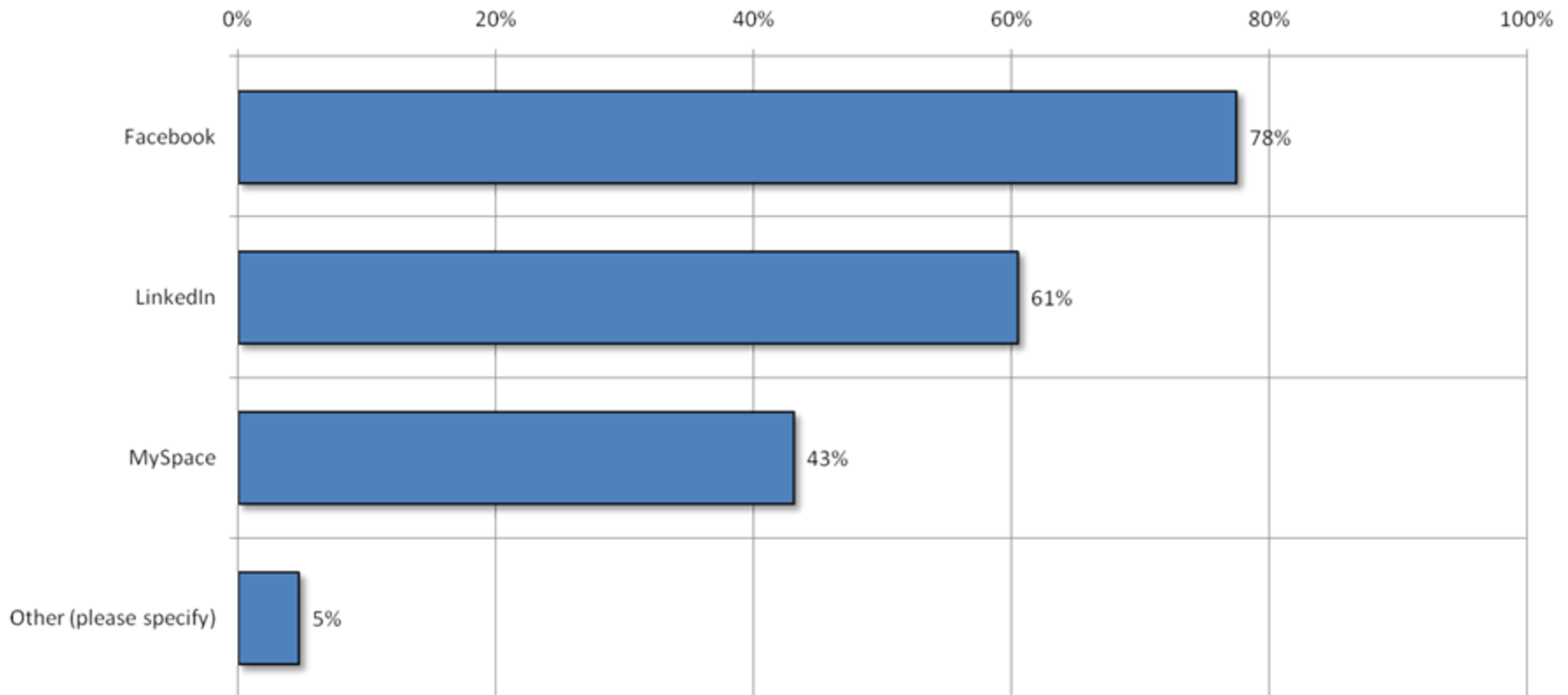
Q88: Which of the following social media tools are used officially within your organization?



Social networking sites

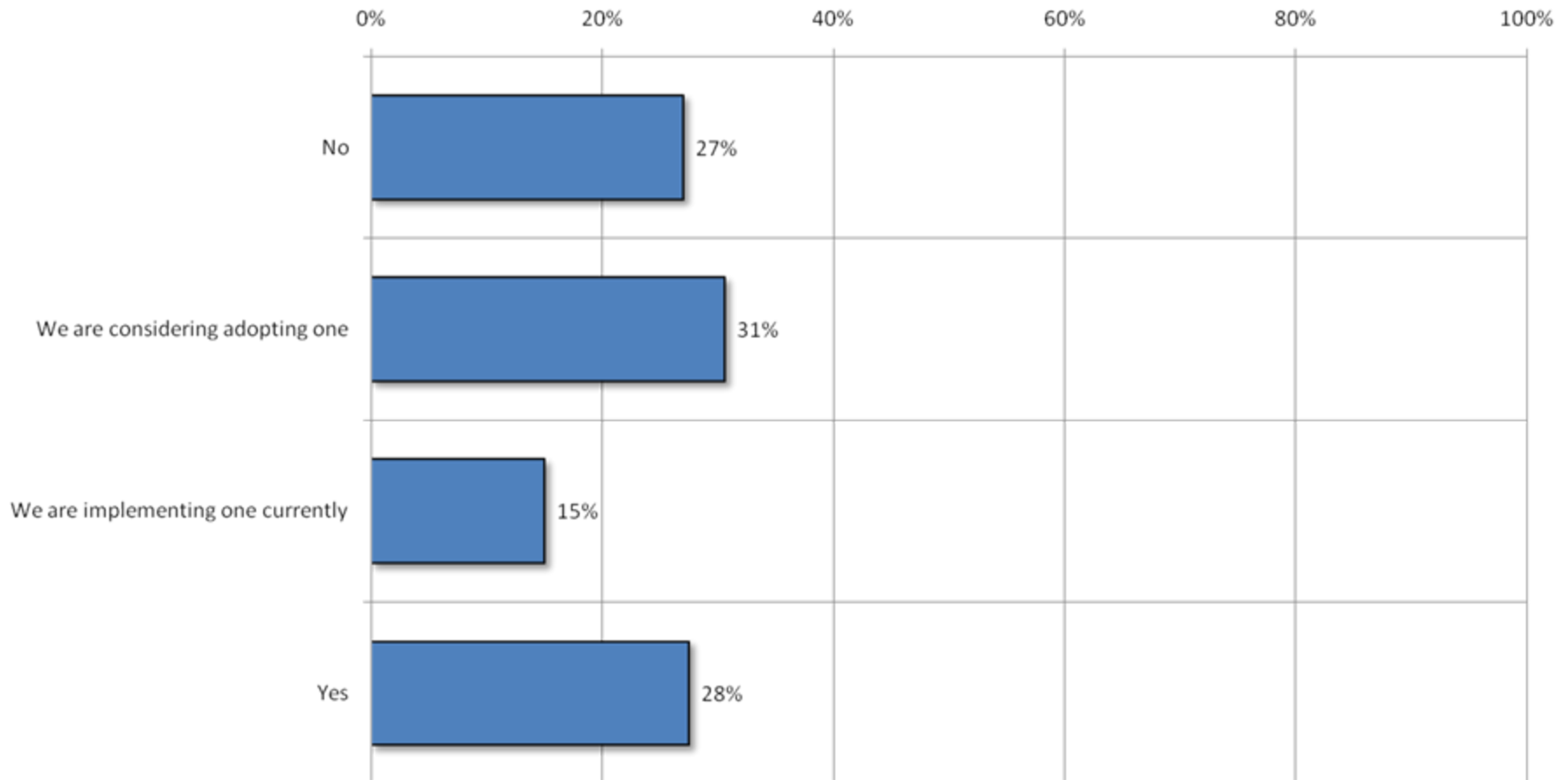
Q89: Which social networking sites are used officially within your organization?

(Asked only of those who indicated that they officially use social networking sites within their organizations)



Employee access to social media

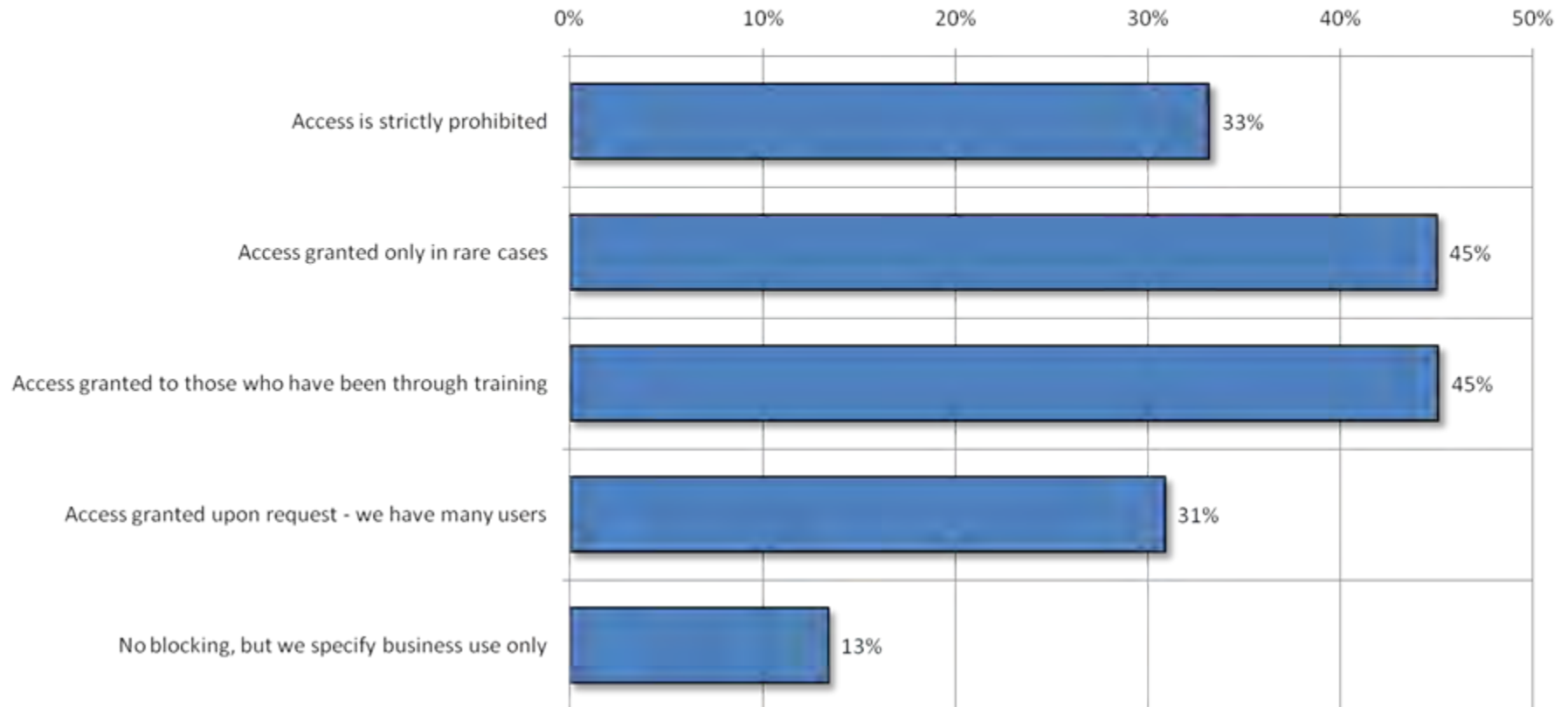
Q90: Do you have an organization-wide policy on employee access to/use of social media sites?



Employee access to social media

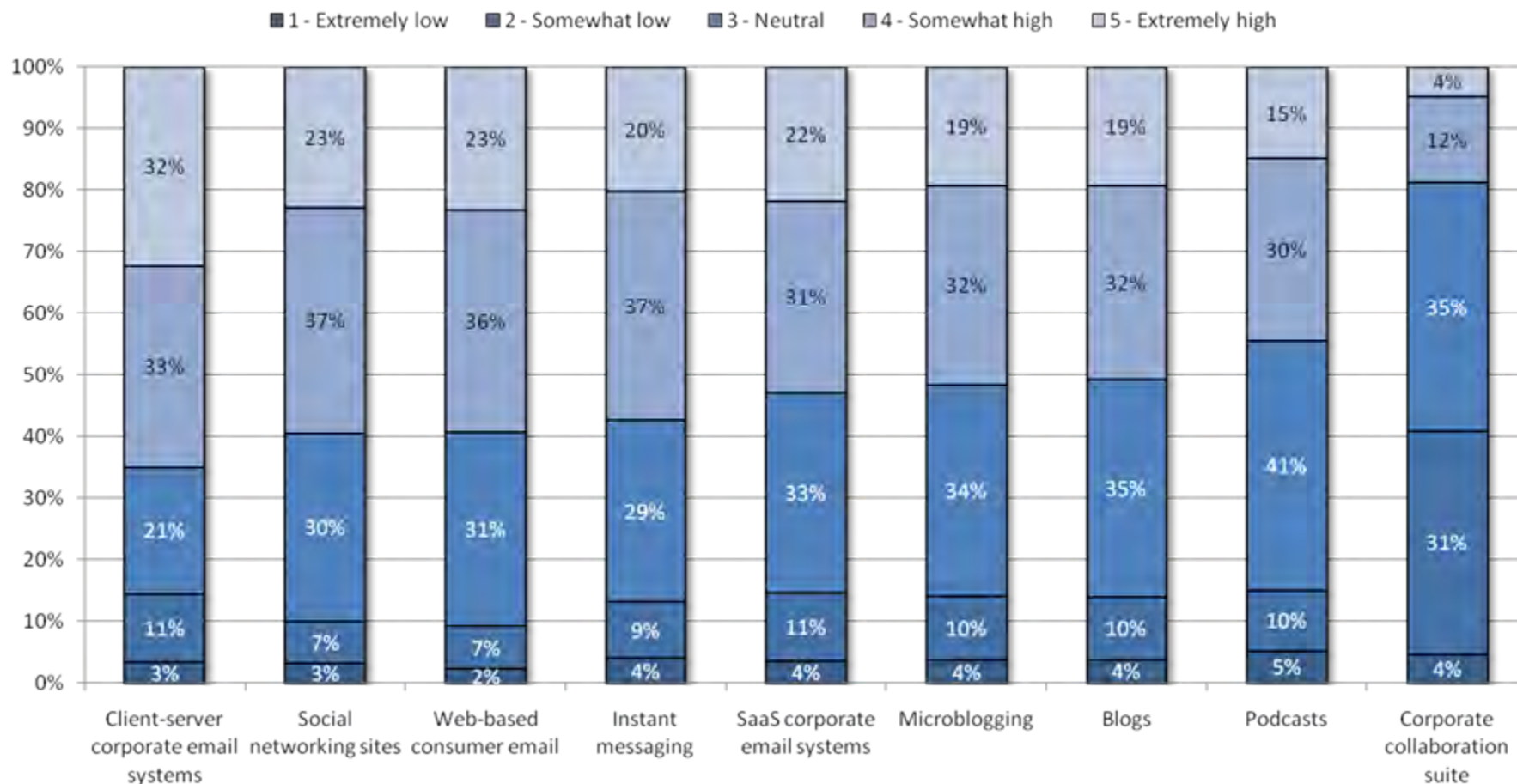
Q91: What policy are you considering or will you/have you implemented for the aforementioned sites? Mark all that apply.

(Asked only of those who are at least considering adopting a policy for one of the sites mentioned in Q103)



Messaging/Collaboration threats

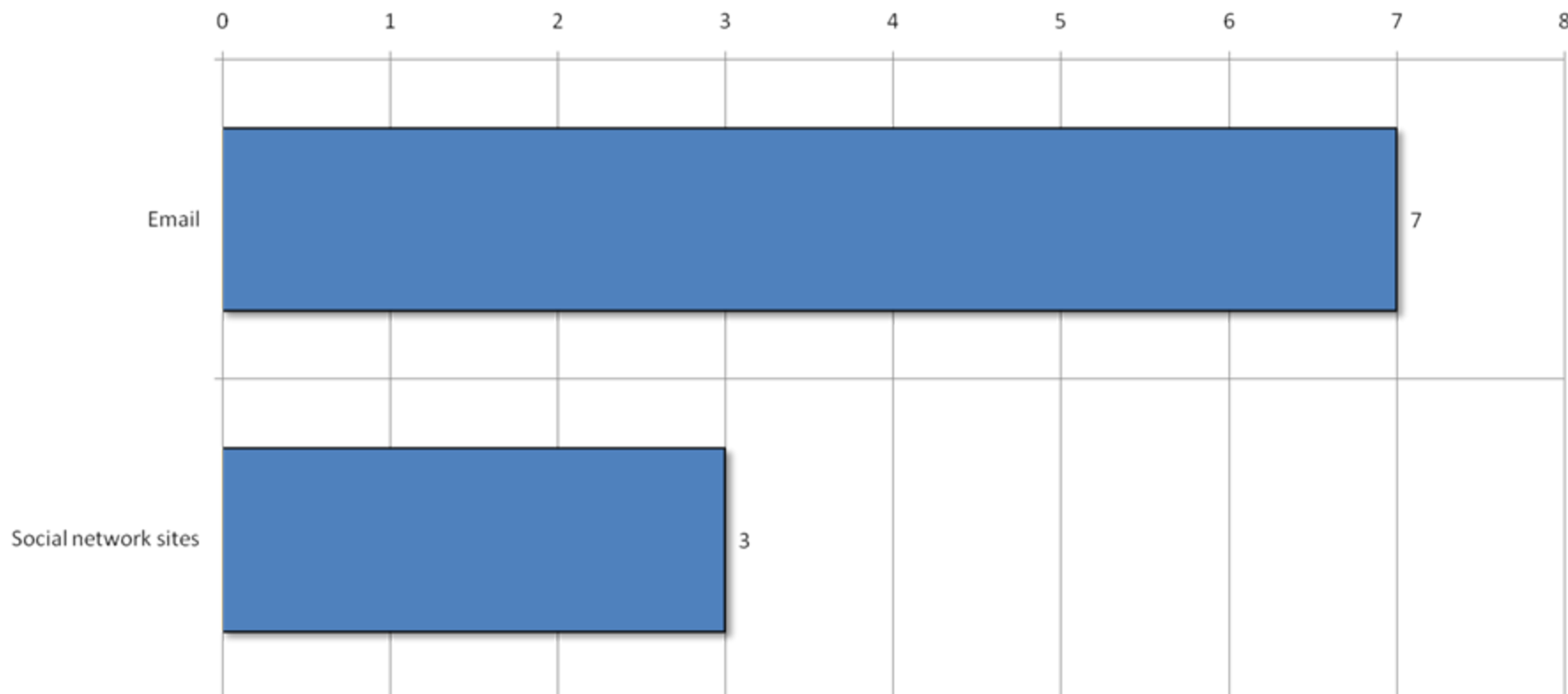
Q92: How would you rate the security threat for each messaging/collaboration tool?



Messaging/Collaboration security

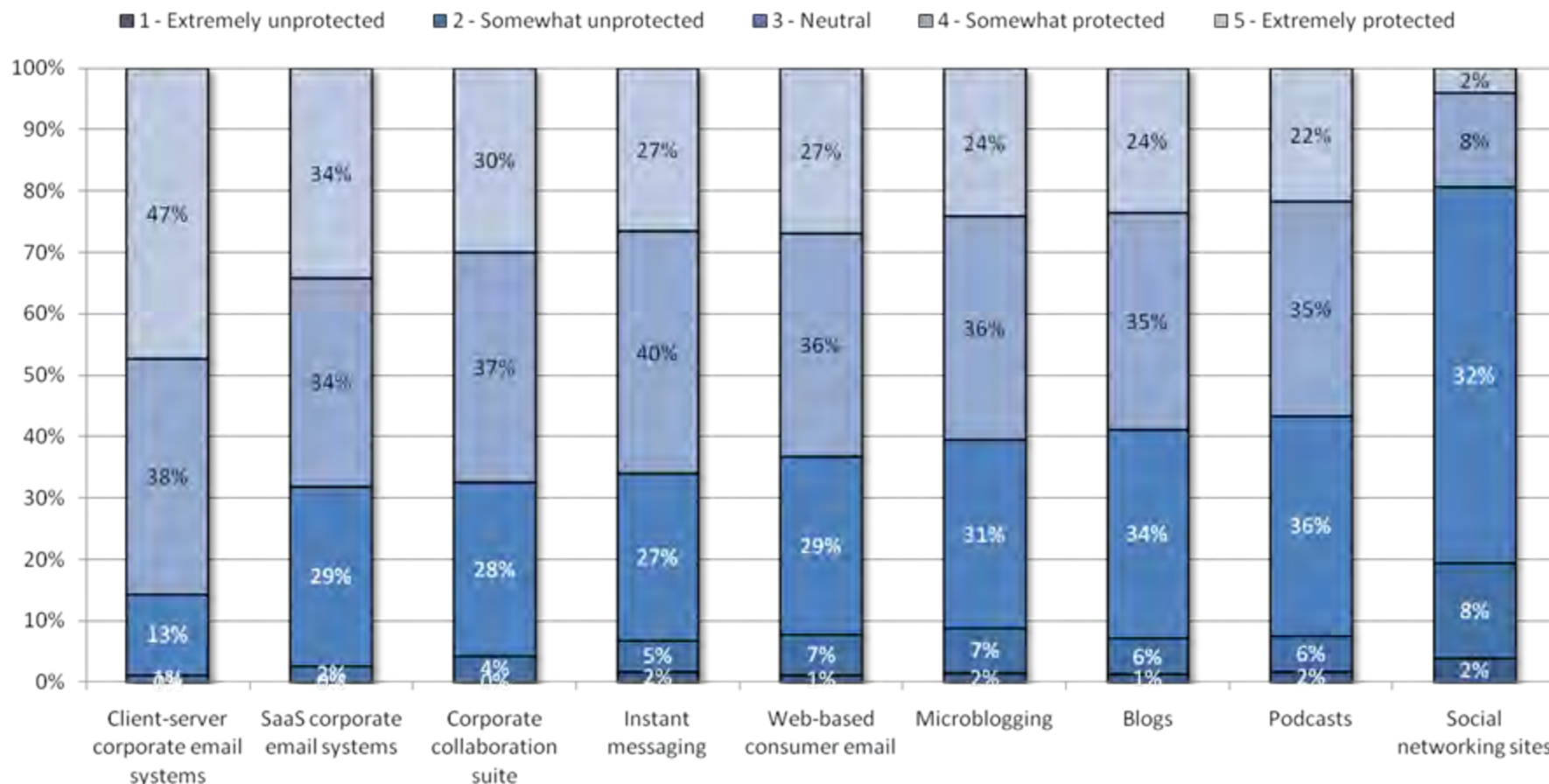
Q93: How many security individual incidents have you experienced worldwide within your organization for each of these messaging/collaboration tools in the past 12 months?

(Medians shown)



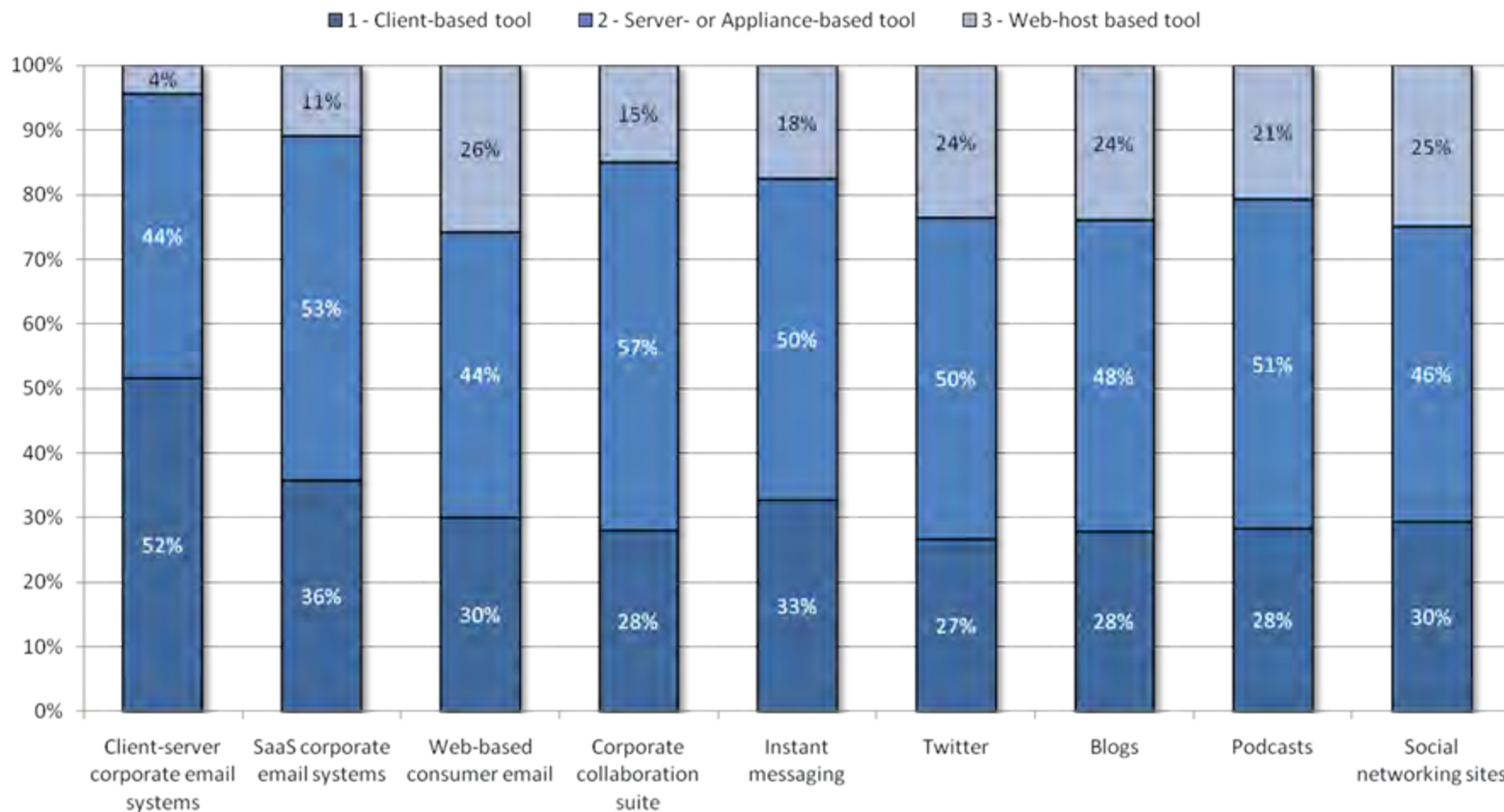
Messaging/Collaboration protection

Q94: How well-protected are you for each of these messaging/collaboration tools?



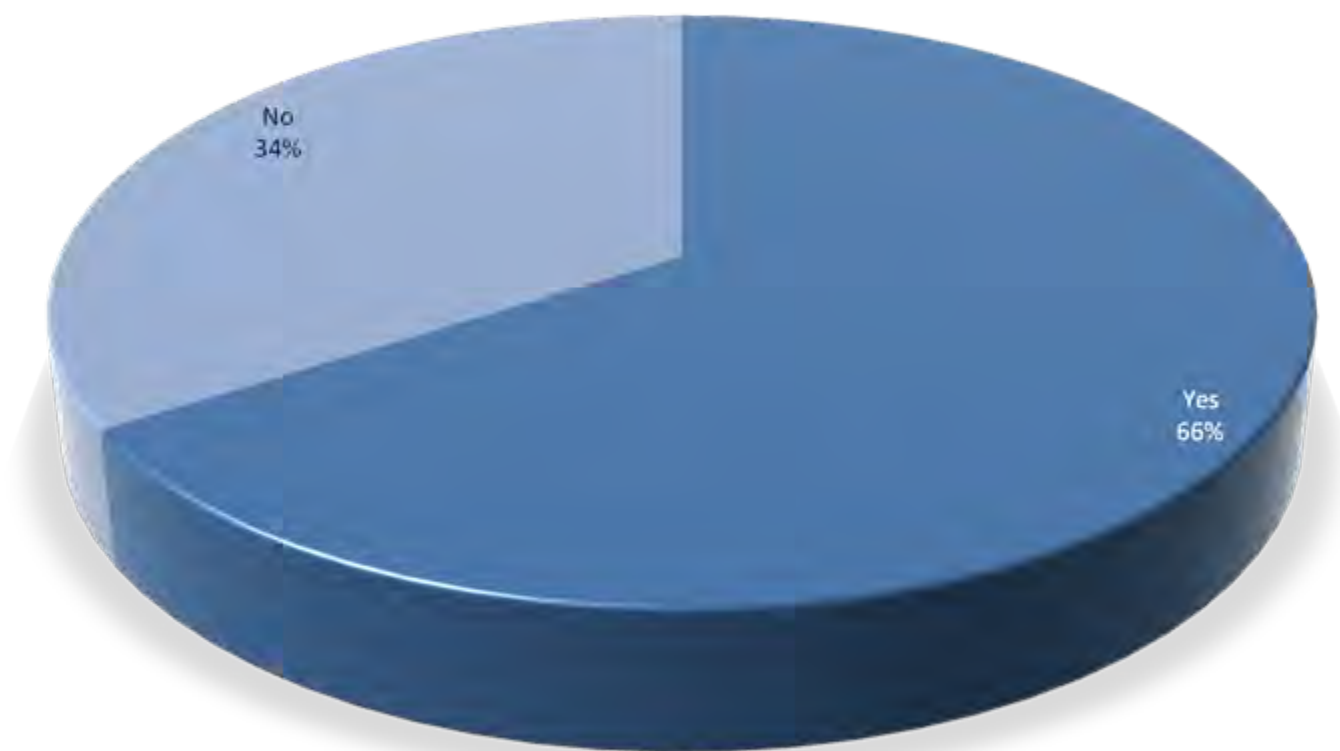
Messaging/Collaboration protection

Q95: What kind of tool do you use to protect each of the following?



Hosted security

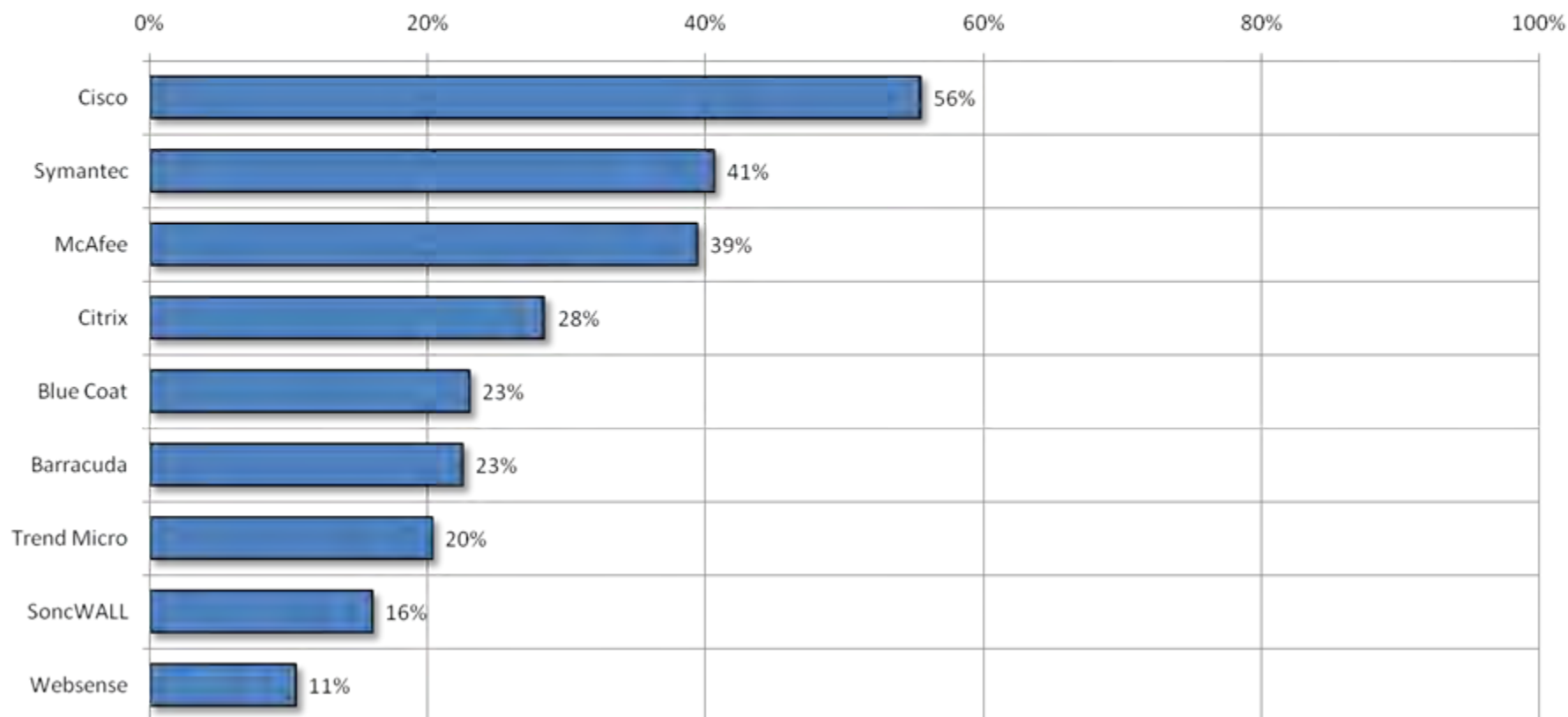
Q96: Do you have a gateway or hosted security product in front of your messaging/collaboration tools?



Hosted security

Q97: Which gateway or hosted security product(s) do you use in front of your messaging collaboration tools? Mark all that apply.

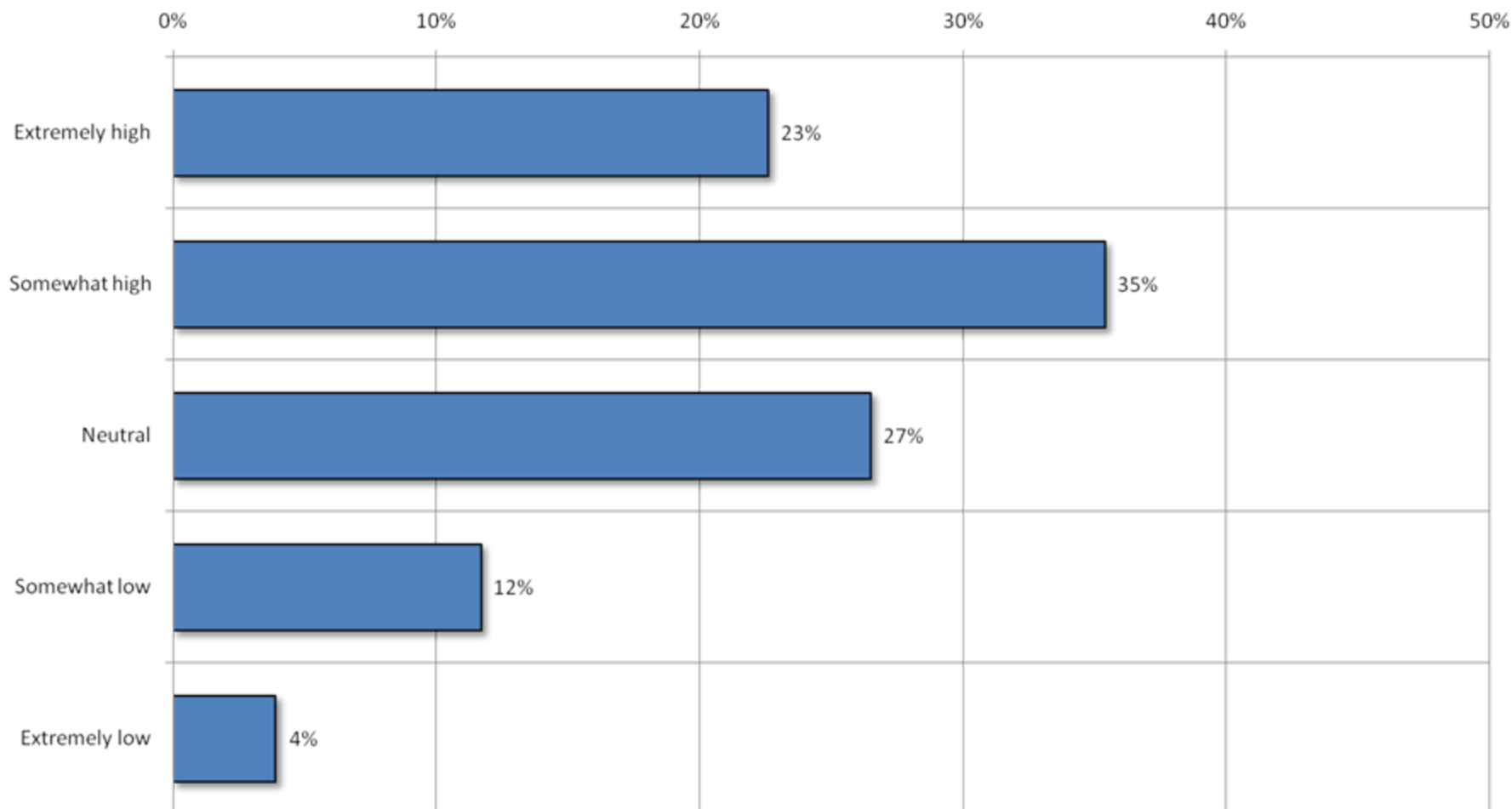
(Asked only of those who have a gateway or hosted security product in front of their messaging/collaboration tools)



Web Security

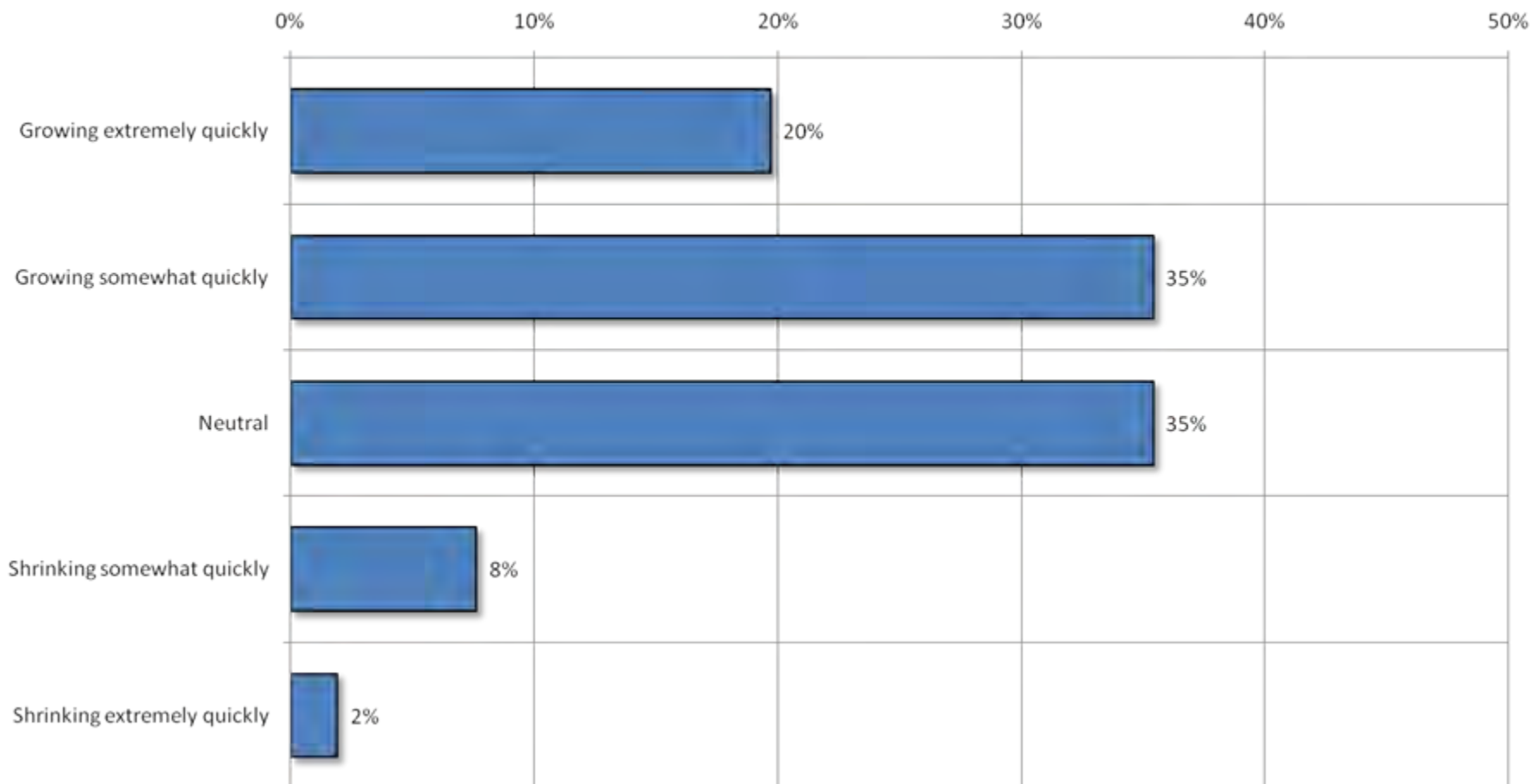
Web property security

Q98: How would you rate the security threat for your web properties?



Web property security

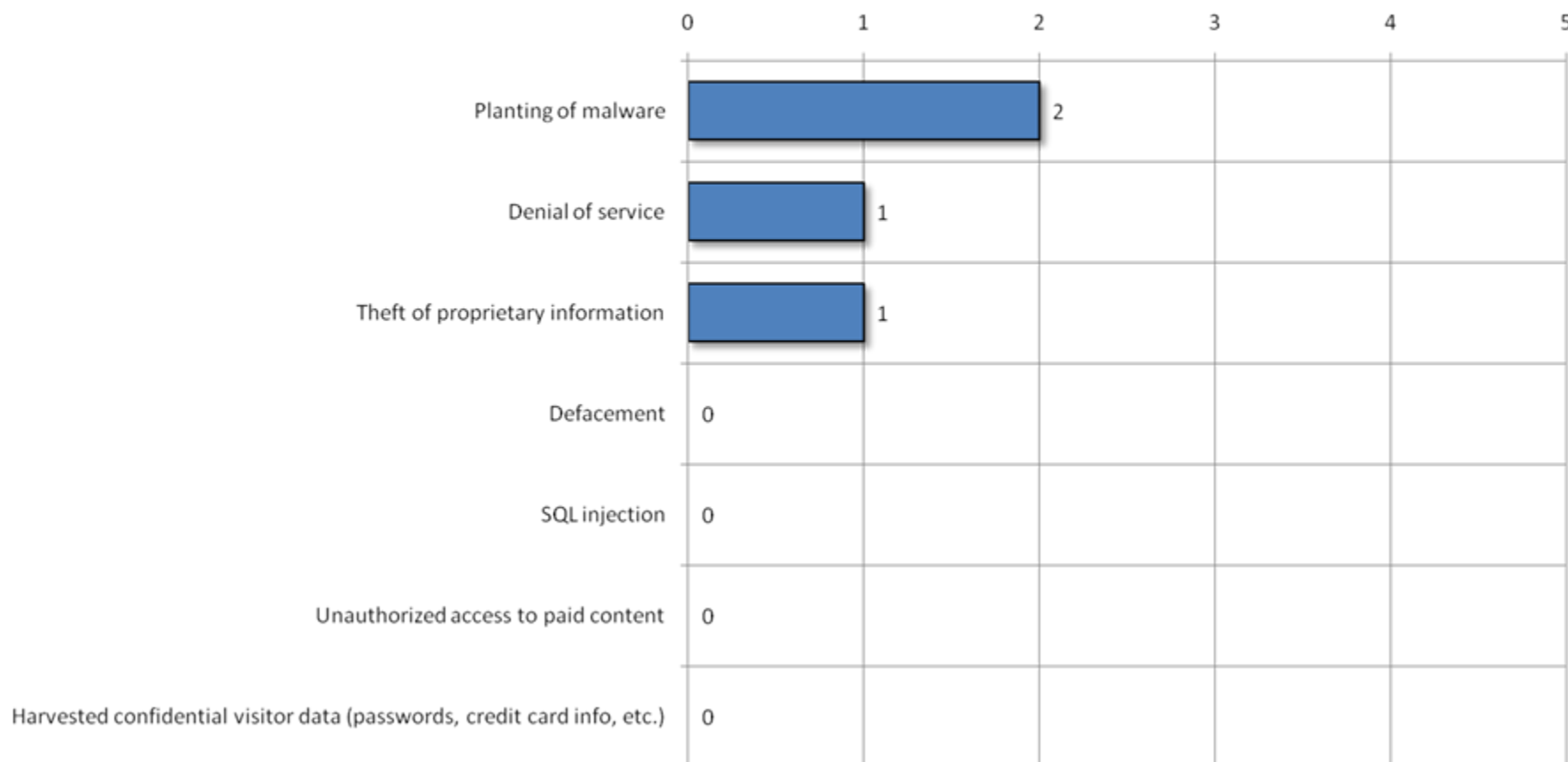
Q99: How is the security threat for your web properties changing over the next 12 months?



Web property attacks

Q100: How many of each of these types of attacks has your organization sustained against your web properties over the past 12 months?

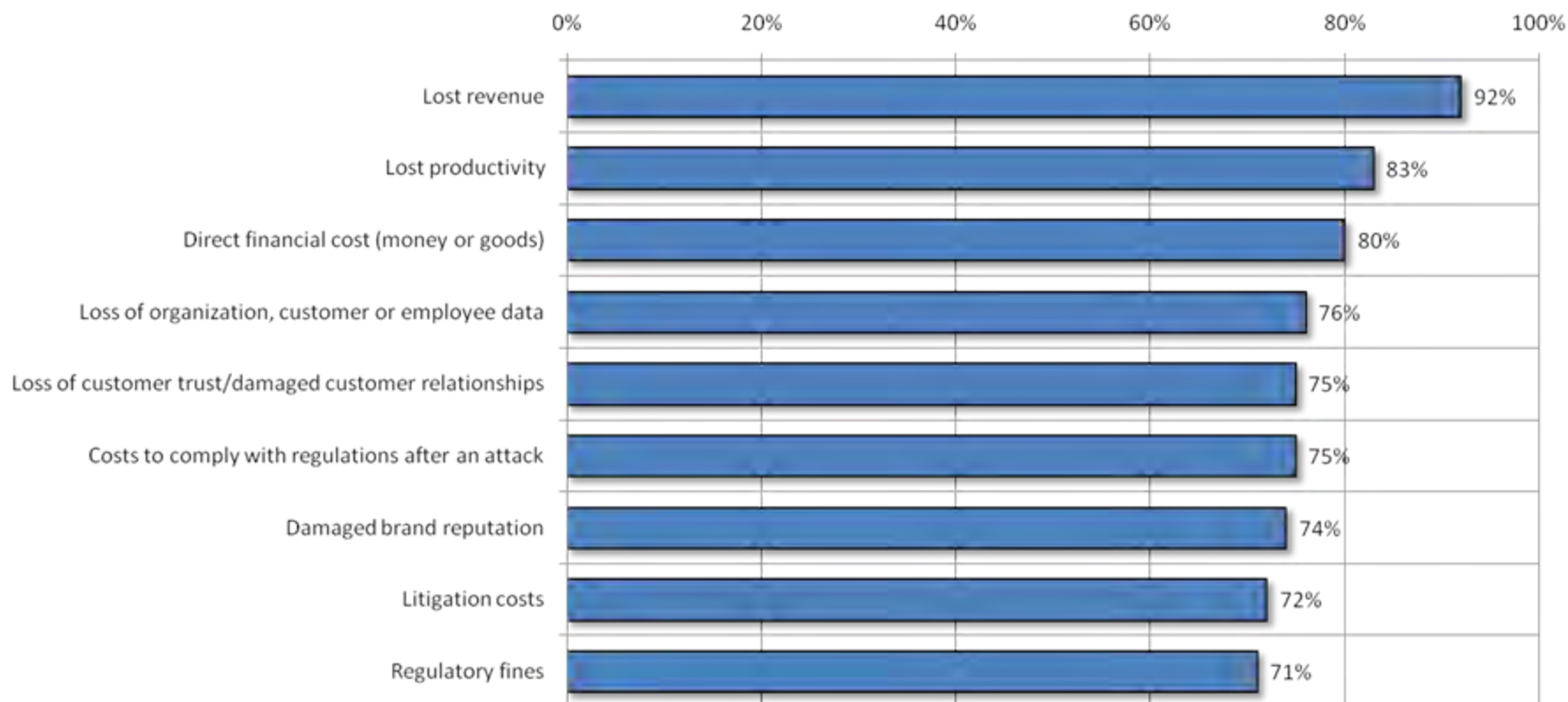
(Medians shown)



Web property attack costs

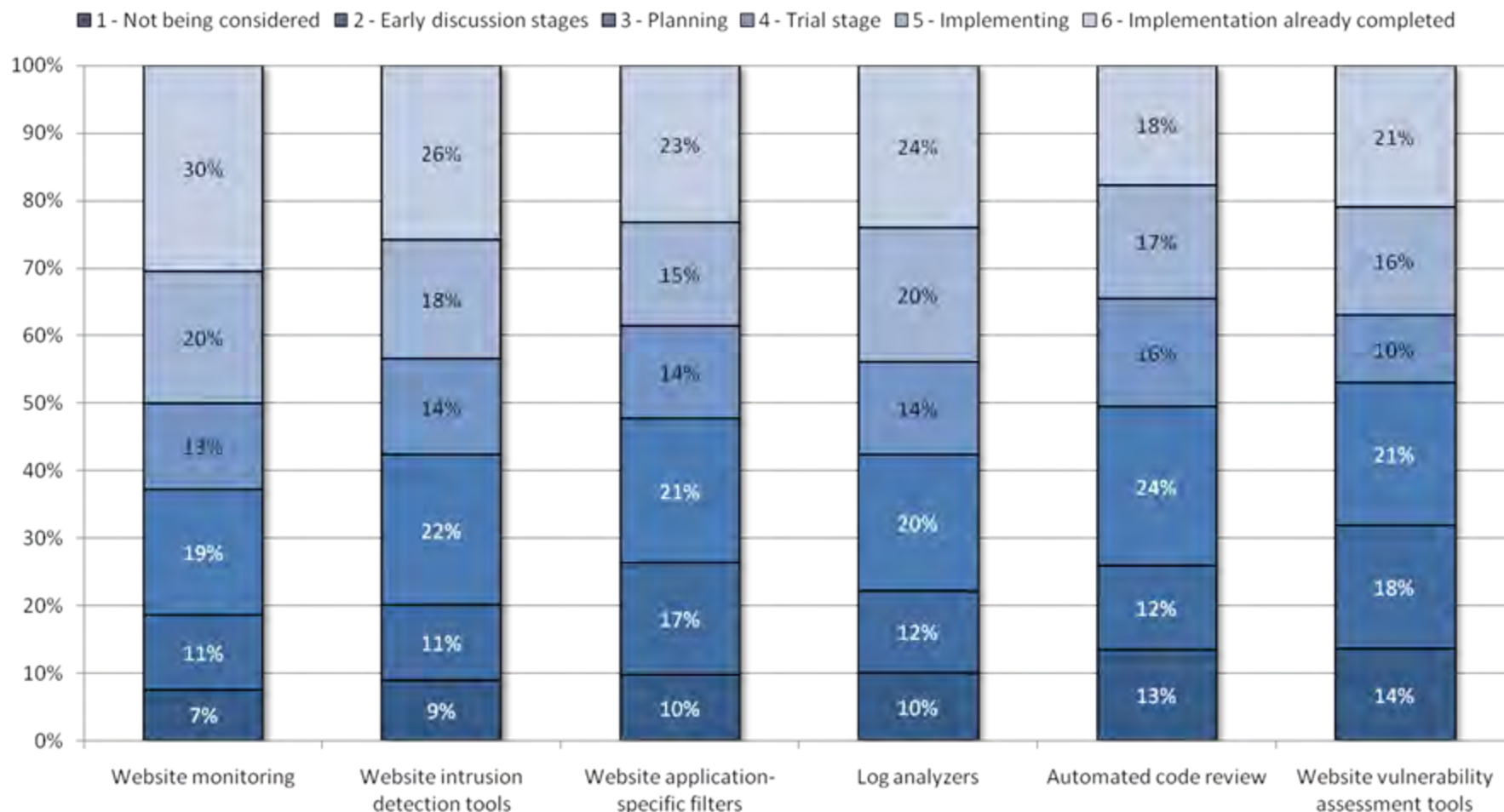
Q101: Which of the following costs has your organization experienced in the past 12 months?

(Asked only of those who sustained at least one attack on web properties in the past 12 months)



Safeguards

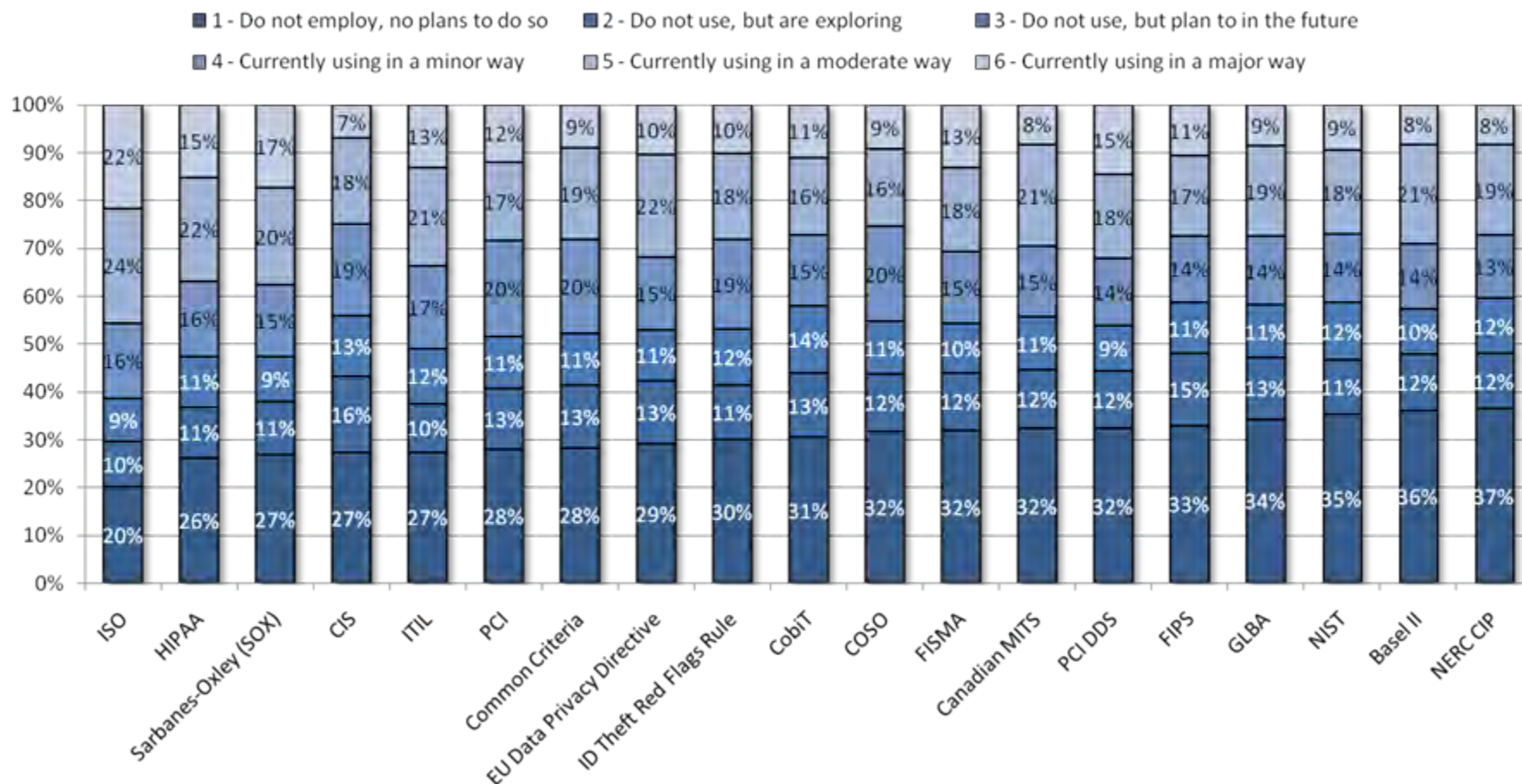
Q102: What is your involvement with each of these types of safeguards?



Compliance

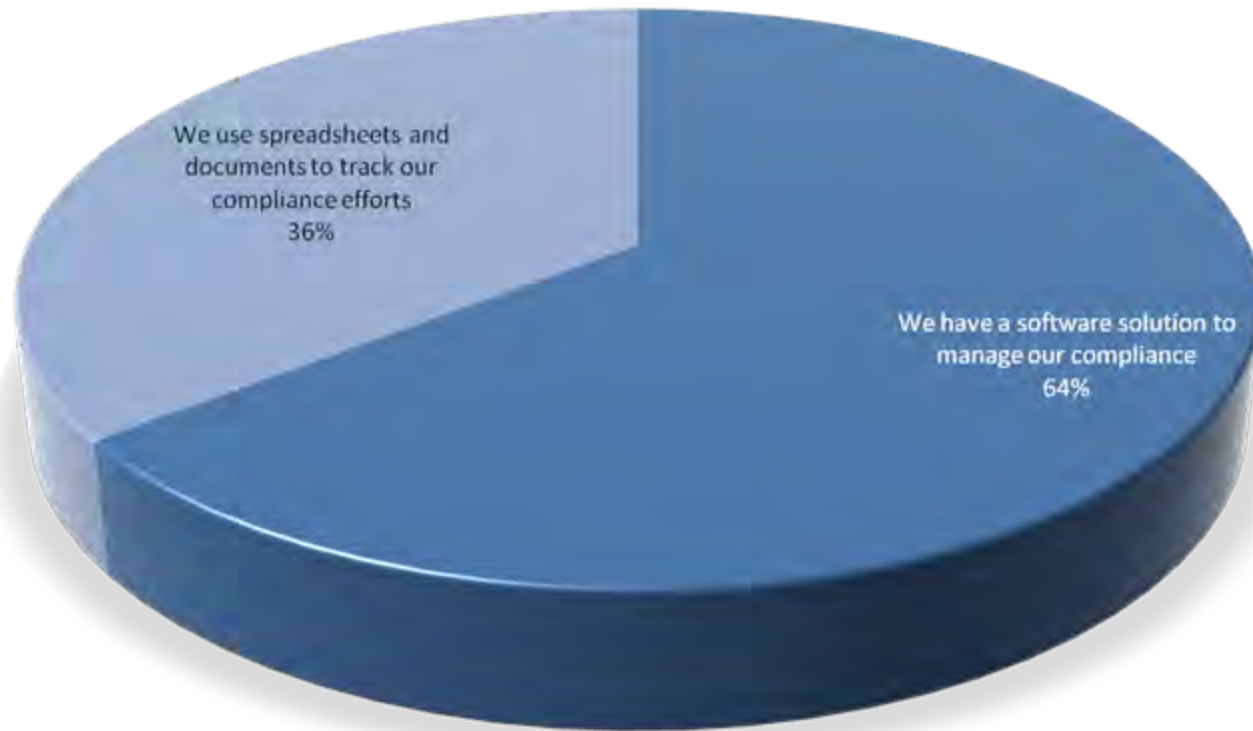
Standards and frameworks

Q103: What is your involvement with the following standards/frameworks?



Standard compliance

Q104: How automated are your efforts to comply with the various standards, frameworks, and regulations?



Compliance budget

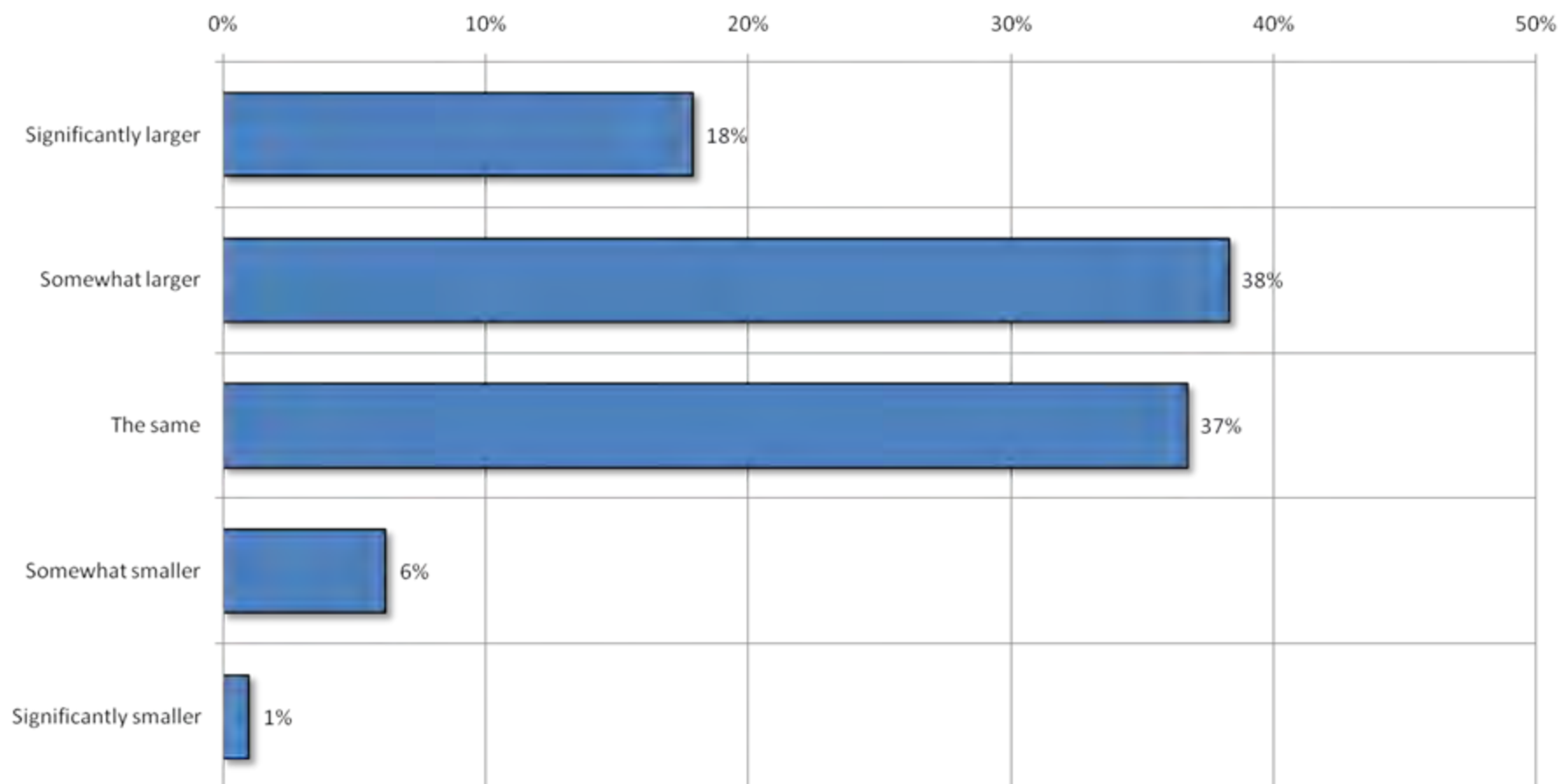
Q105: What is your total budget for compliance efforts worldwide?

Median

\$200,000

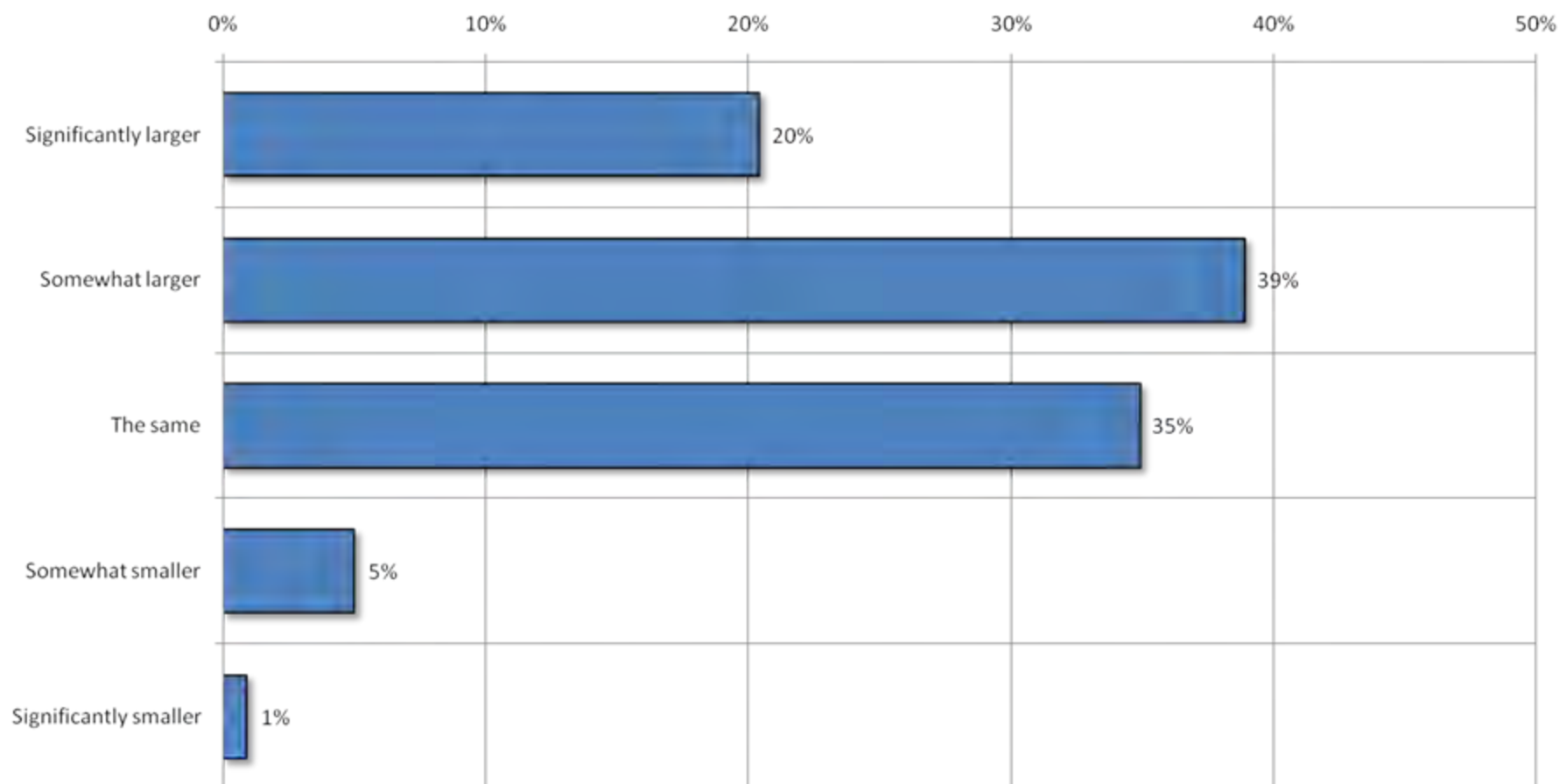
Compliance budget

Q106: How is your current compliance budget compared to the past 12 months?



Compliance budget

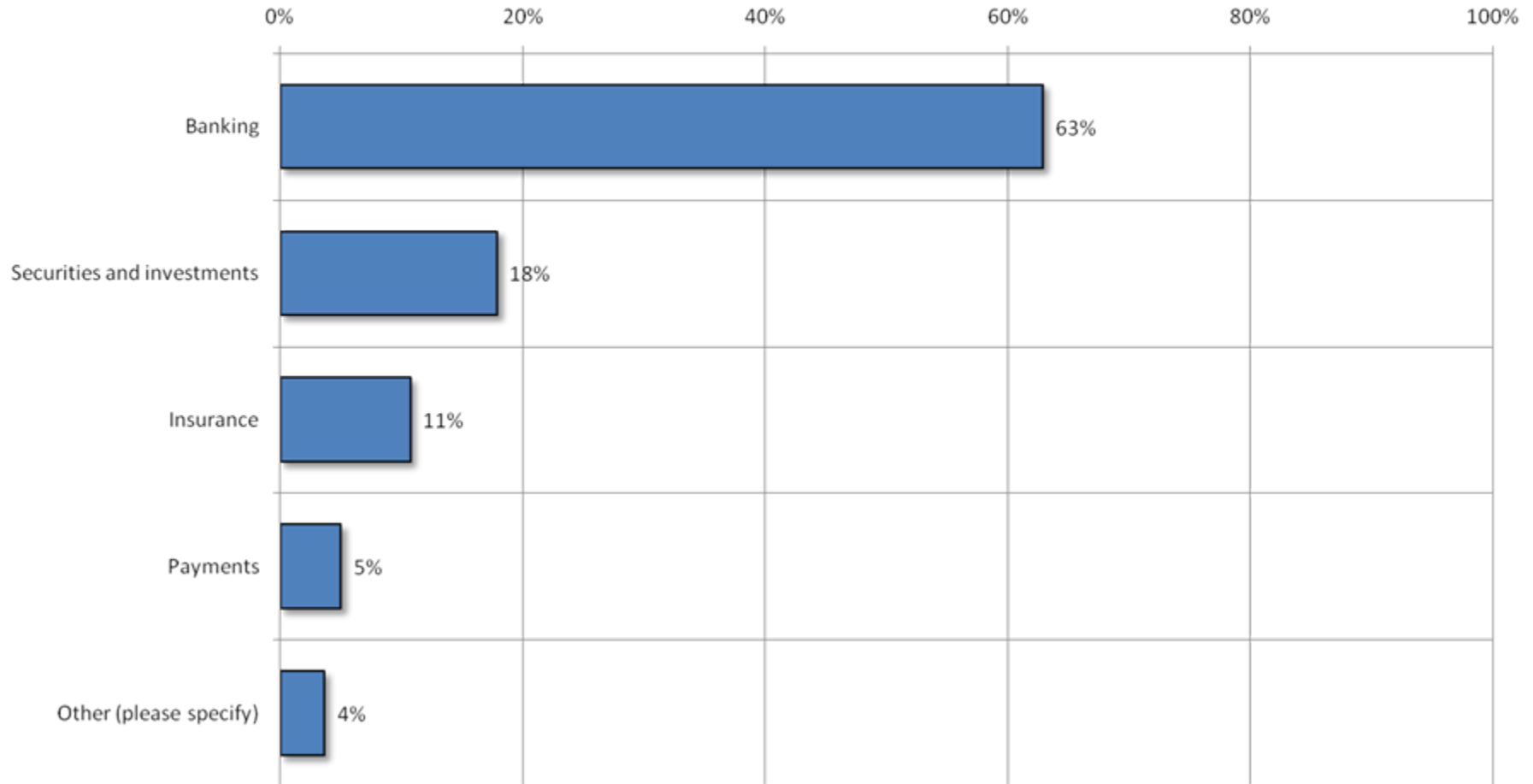
Q107: How do you expect the next 12 months' budget to compare to this years?



Industry Verticals: Financial

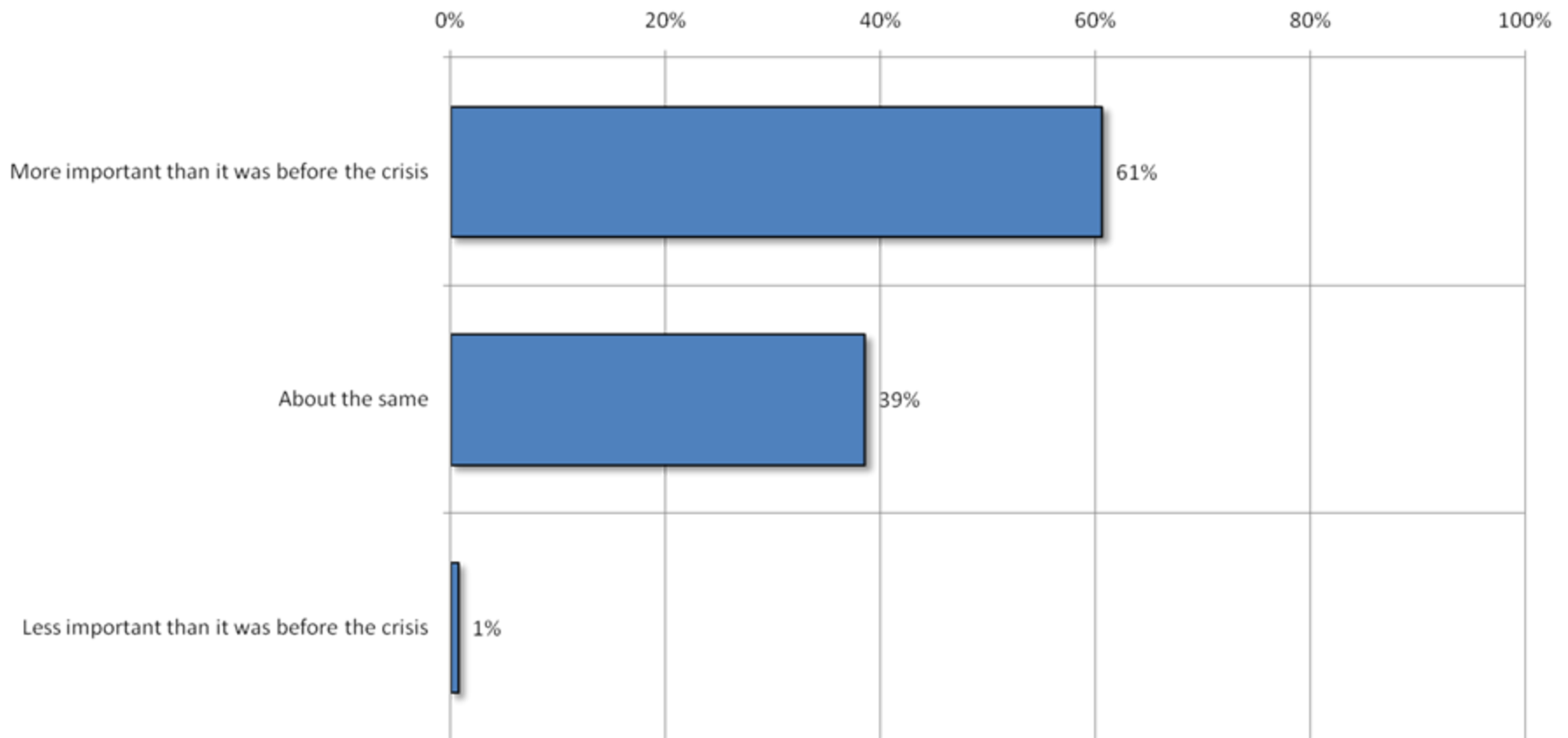
Industry Verticals: Financial

Q108: Which best describes your organization?
(Only asked of Financial Companies)



Industry Verticals: Financial

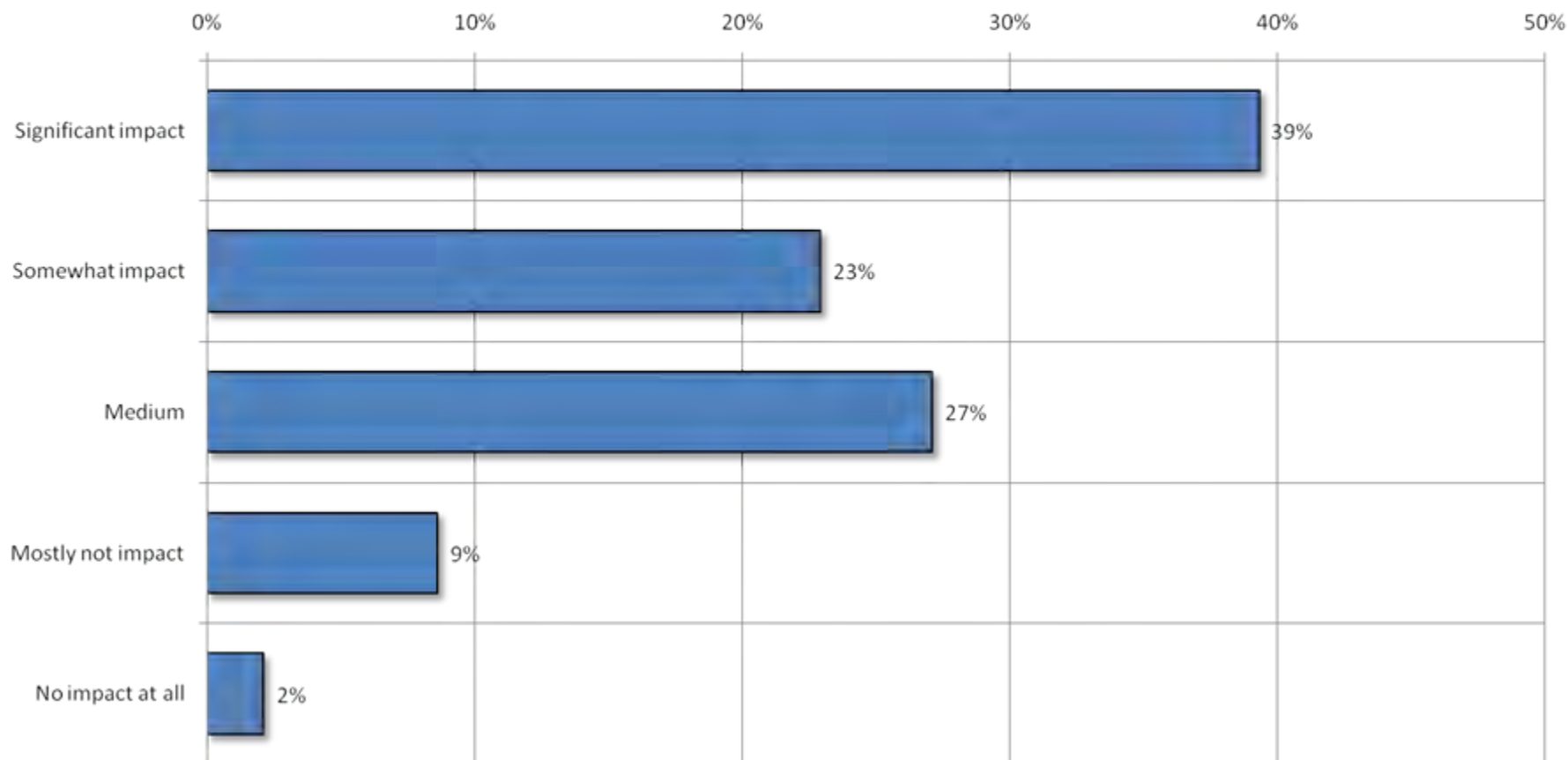
**Q109: Considering the financial crisis of the past year, do you find your
IT security to be...?**
(Only asked of Financial Companies)



Industry Verticals: Financial

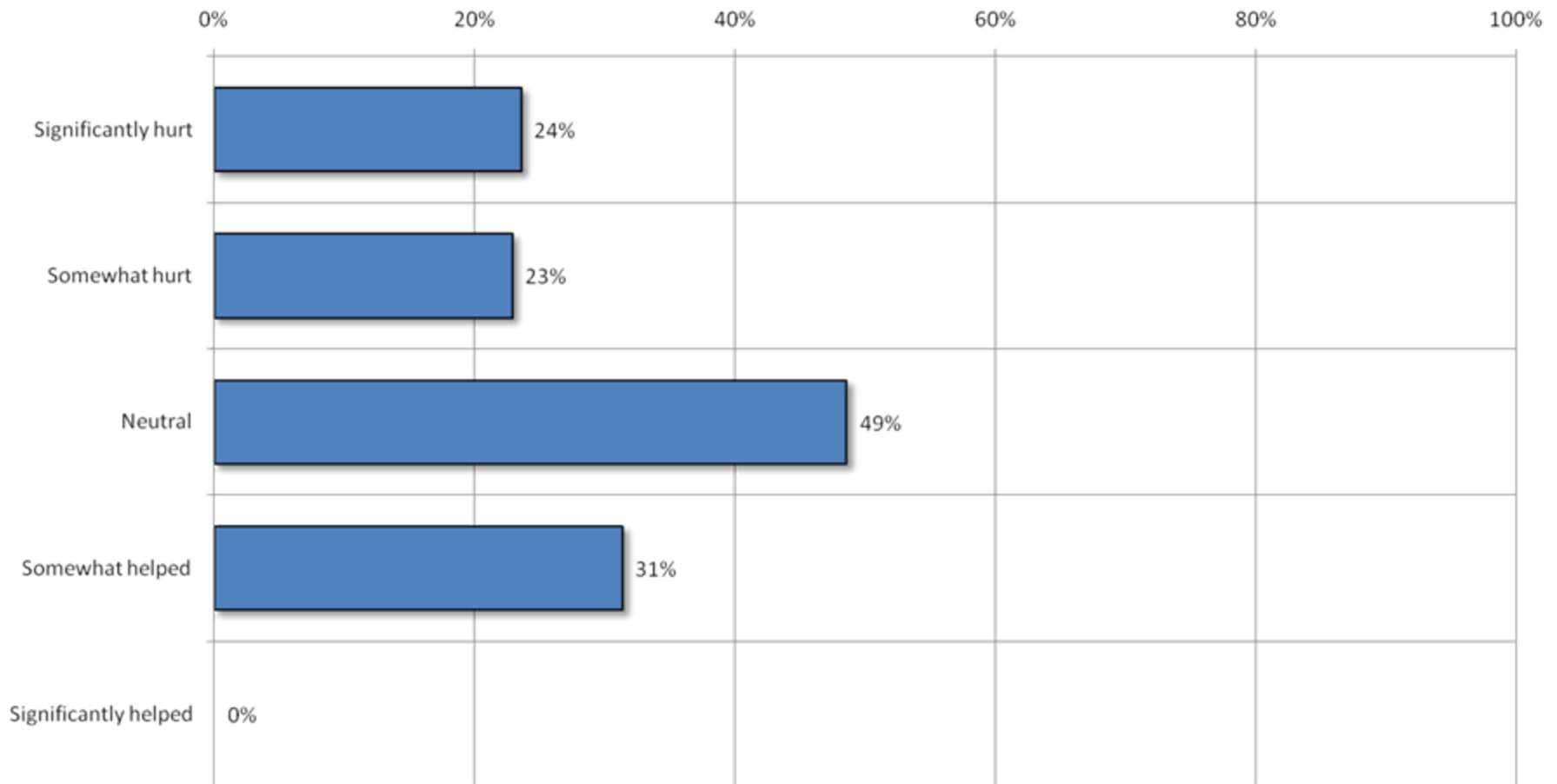
Q110: How much will your security strategy impact your ability to grow your customer base?

(Only asked of Financial Companies)



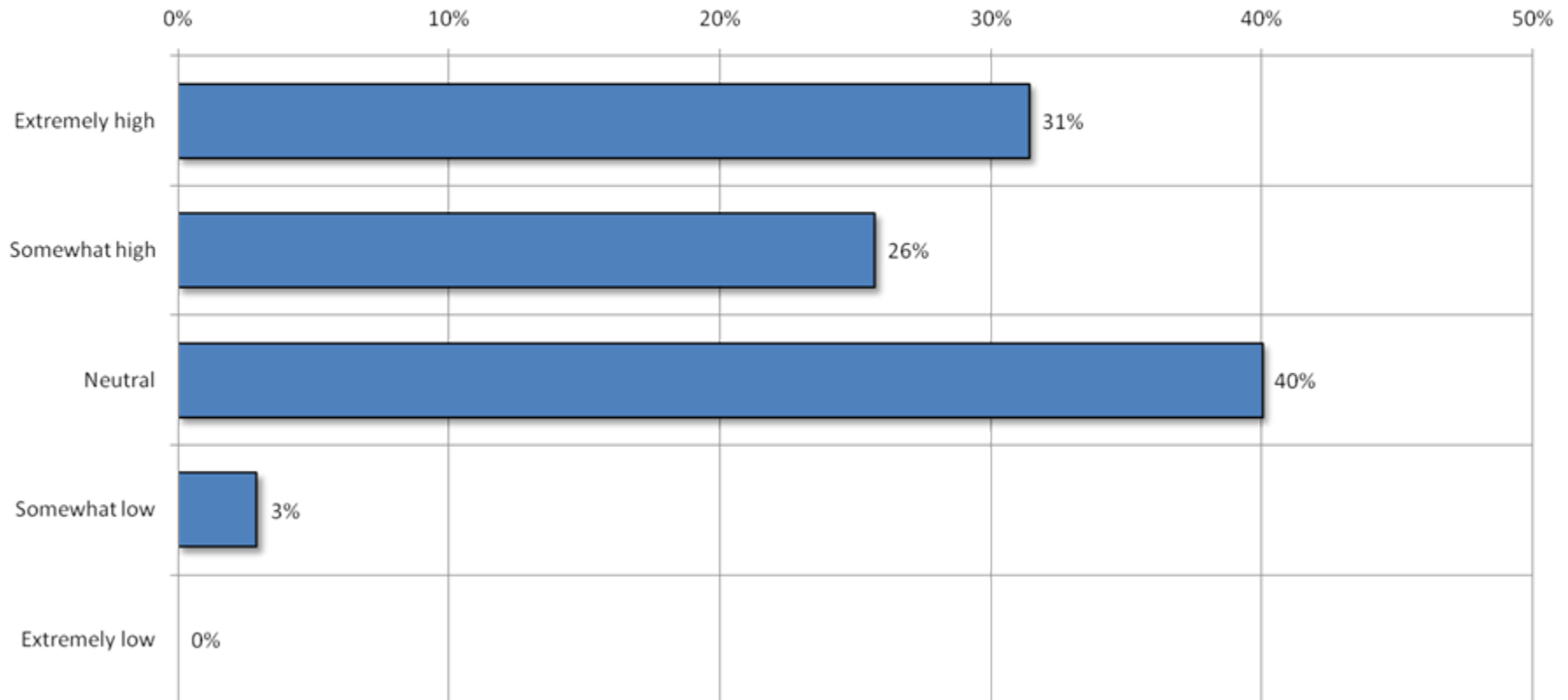
Industry Verticals: Financial

Q111: How has the financial crisis affected your IT security?
(Only asked of Financial Companies)



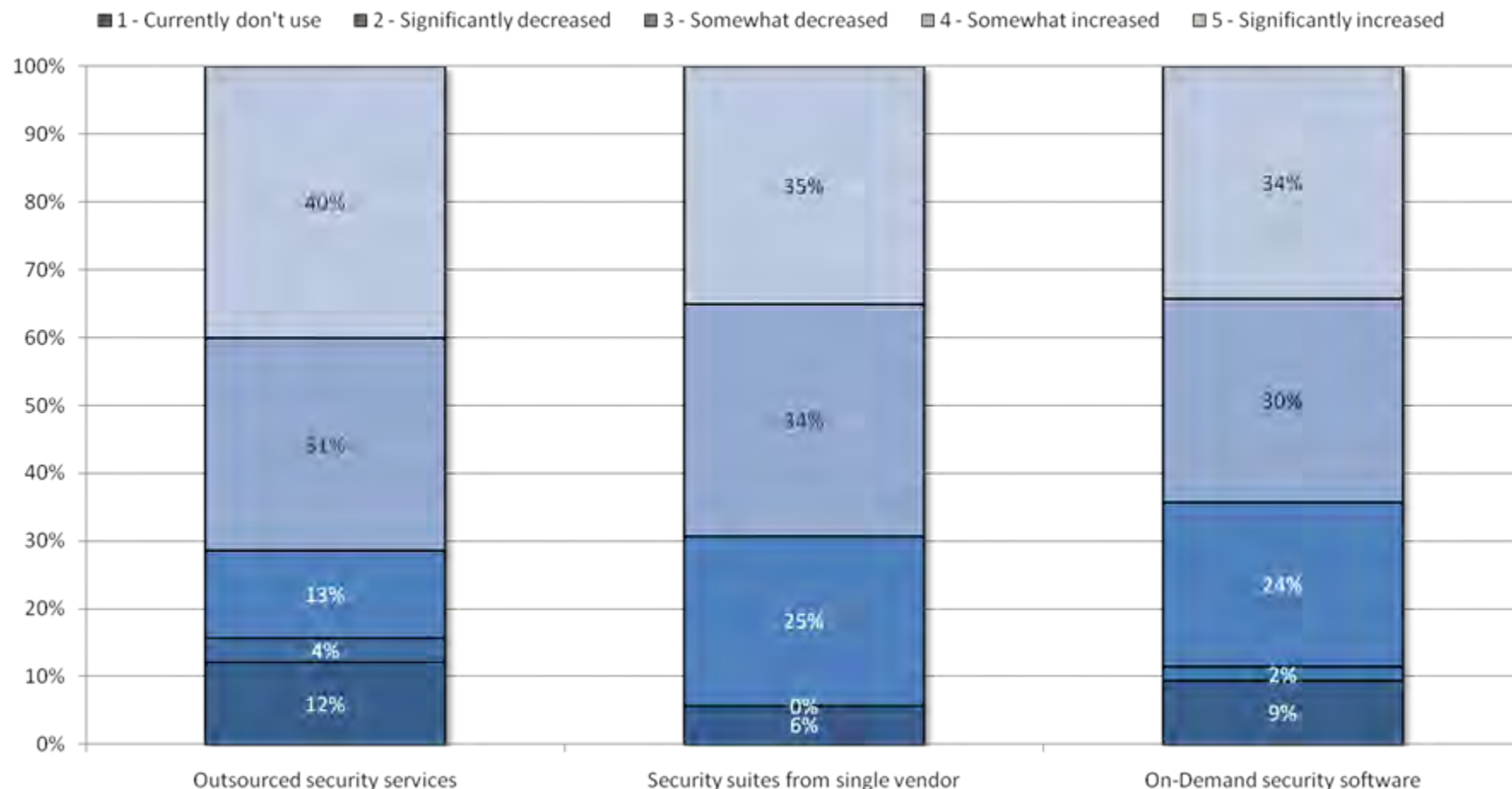
Industry Verticals: Financial

Q112: How would you rank the importance of having an integrated approach to security across delivery channels (branch, online, call center, mobile, ATM, etc.)?
(Only asked of Financial Companies)



Industry Verticals: Financial

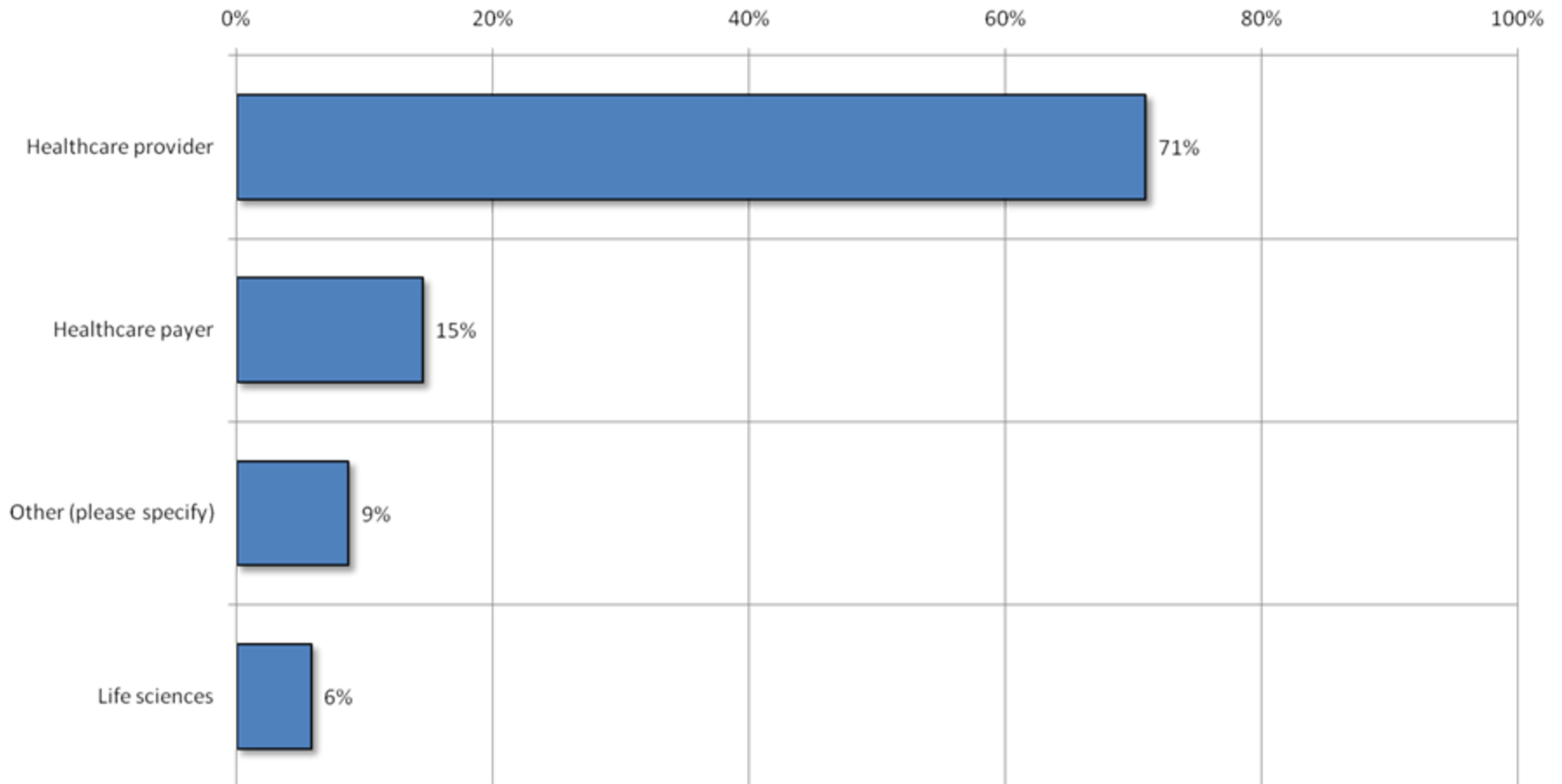
Q113: What best describes your use of the following?
(Only asked of Financial Companies)



Industry Verticals: Healthcare

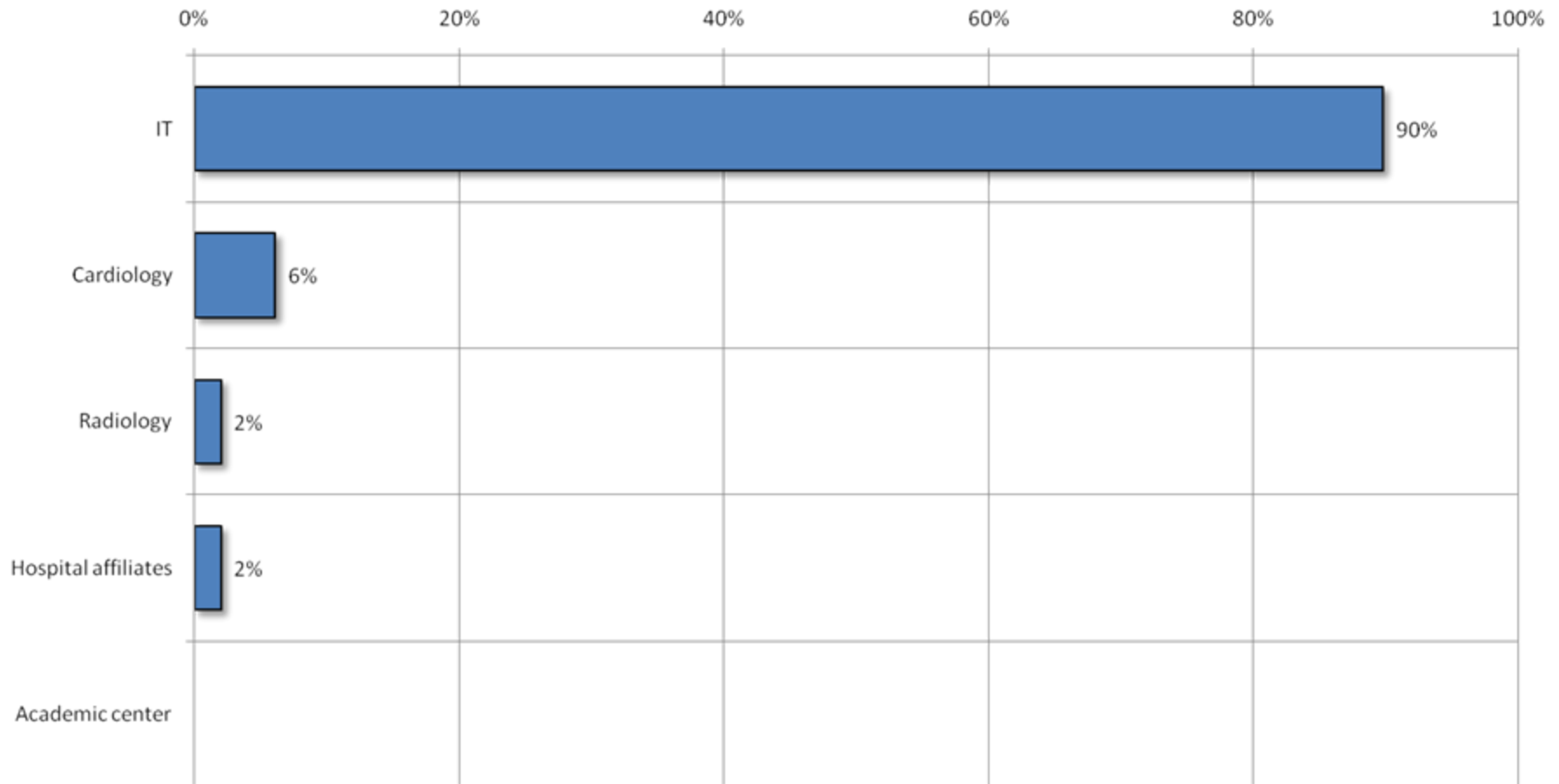
Industry Verticals: Healthcare

Q114: Which of the following best describes your organization?
(Only asked of Healthcare Companies)



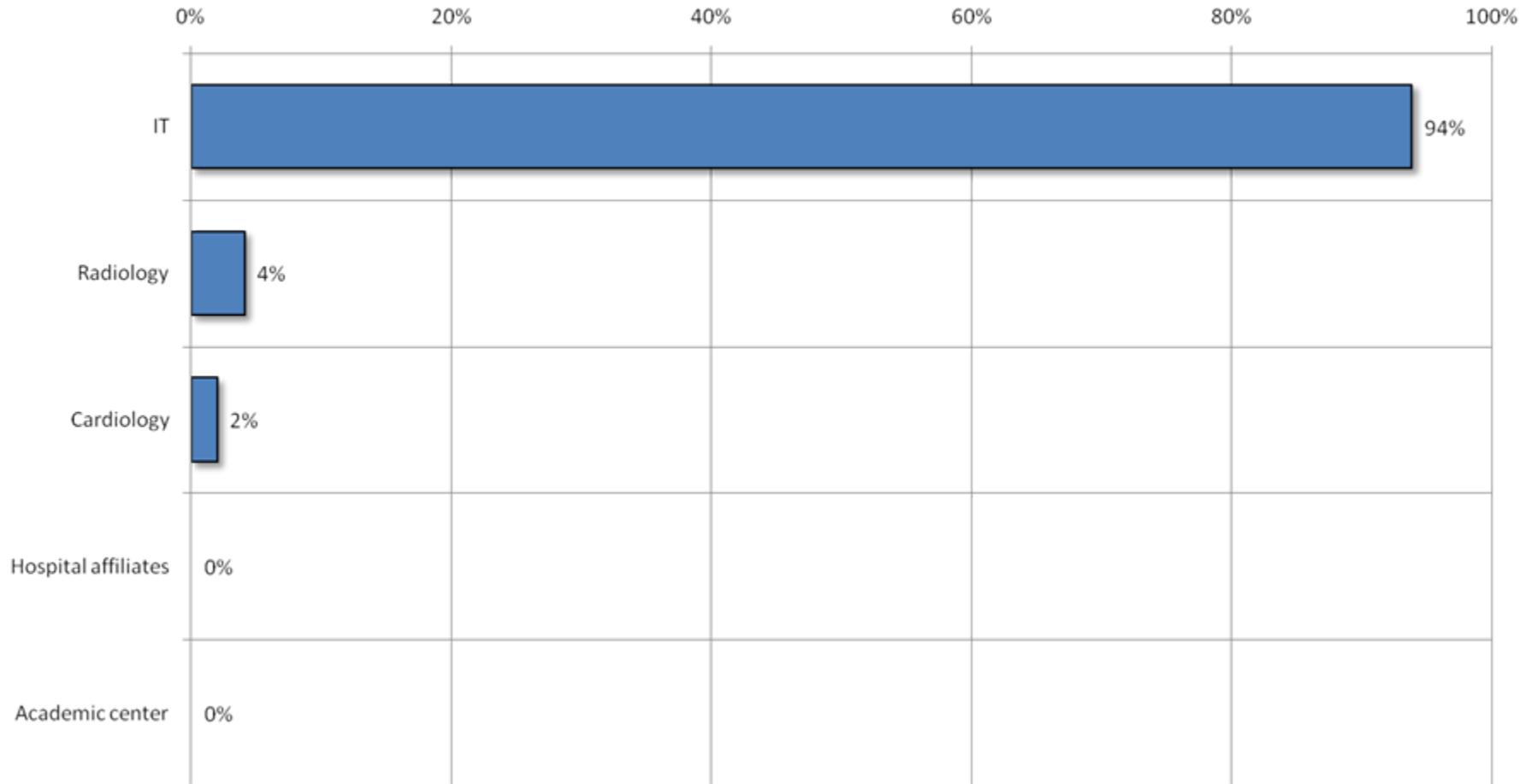
Industry Verticals: Healthcare

Q115: Who owns the budget for security in your organization?
(Only asked of Healthcare Companies)



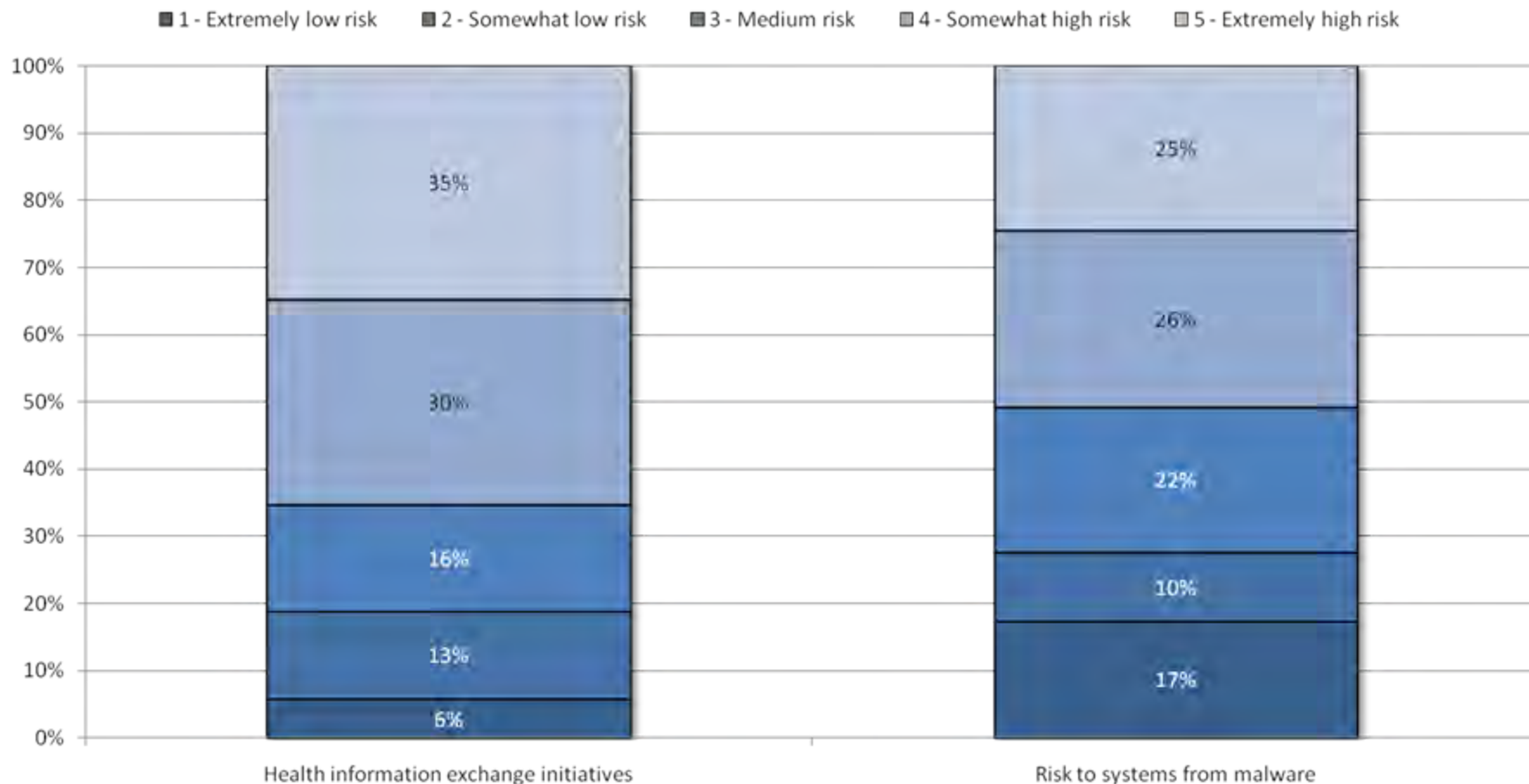
Industry Verticals: Healthcare

Q116: Who manages security in your organization?
(Only asked of Healthcare Companies)



Industry Verticals: Healthcare

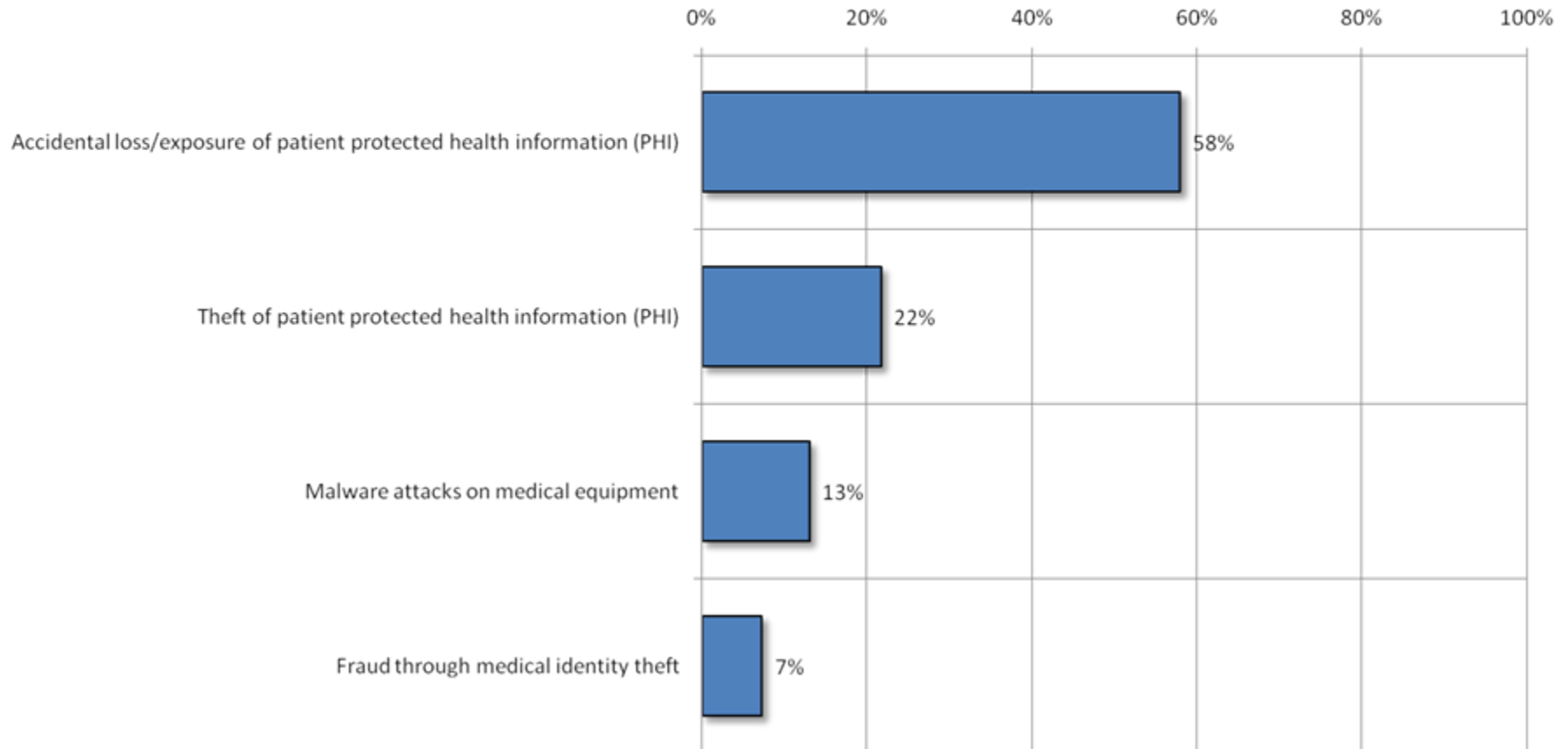
**Q117: Please rate the following initiatives in terms of security risk:
(Only asked of Healthcare Companies)**



Industry Verticals: Healthcare

Q118: Which of the following have you experienced in the past 12 months?

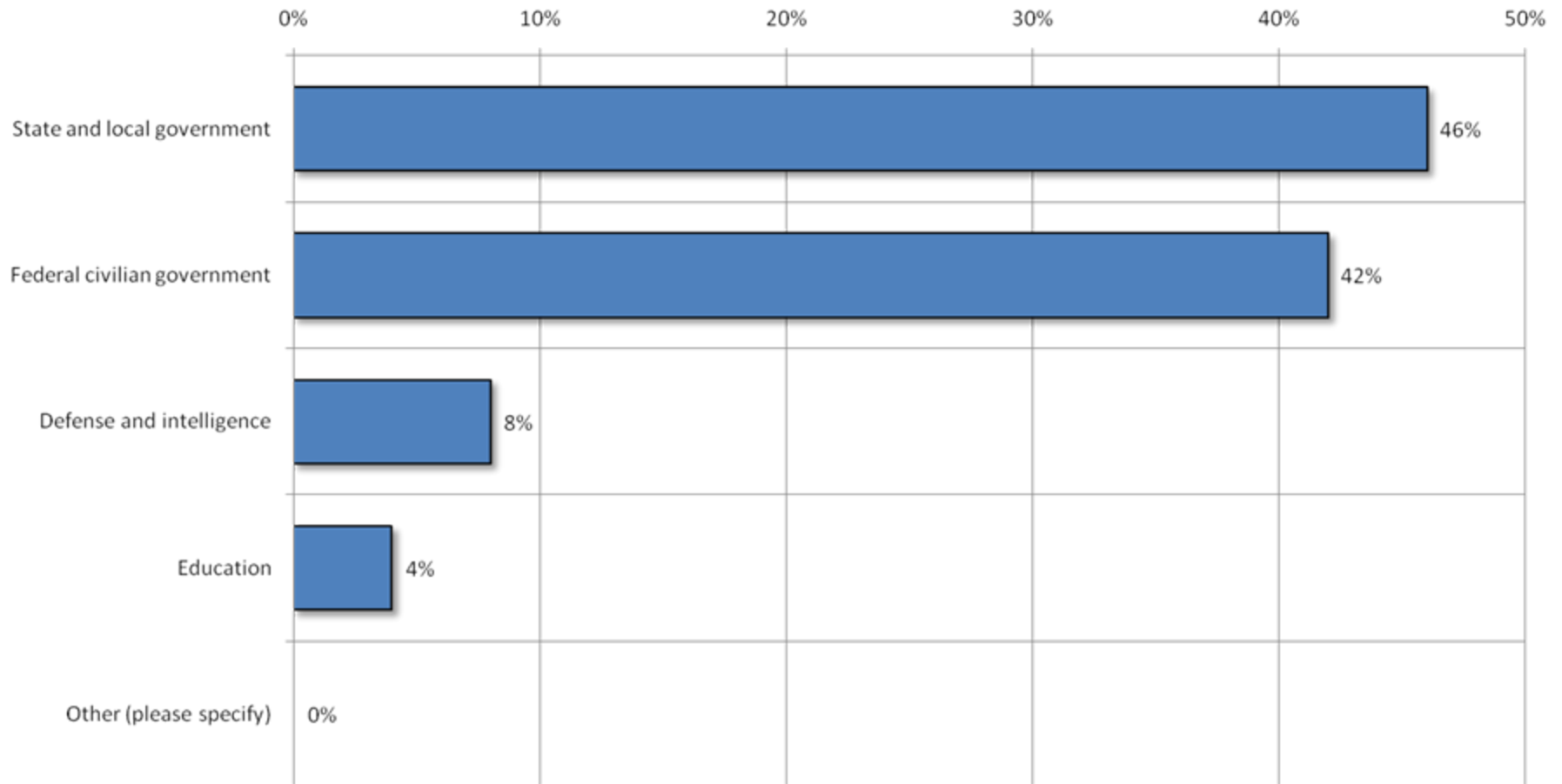
(Only asked of Healthcare Companies)



Industry Verticals: Public Sector (US)

Industry Verticals: Public Sector (US)

Q119: What best describes your organization?
(Only asked of Public Sector Companies in the US)



Industry Verticals: Public Sector (US)

Q120: What percentage of your *security* funding is coming from national stimulus funding currently?

Median

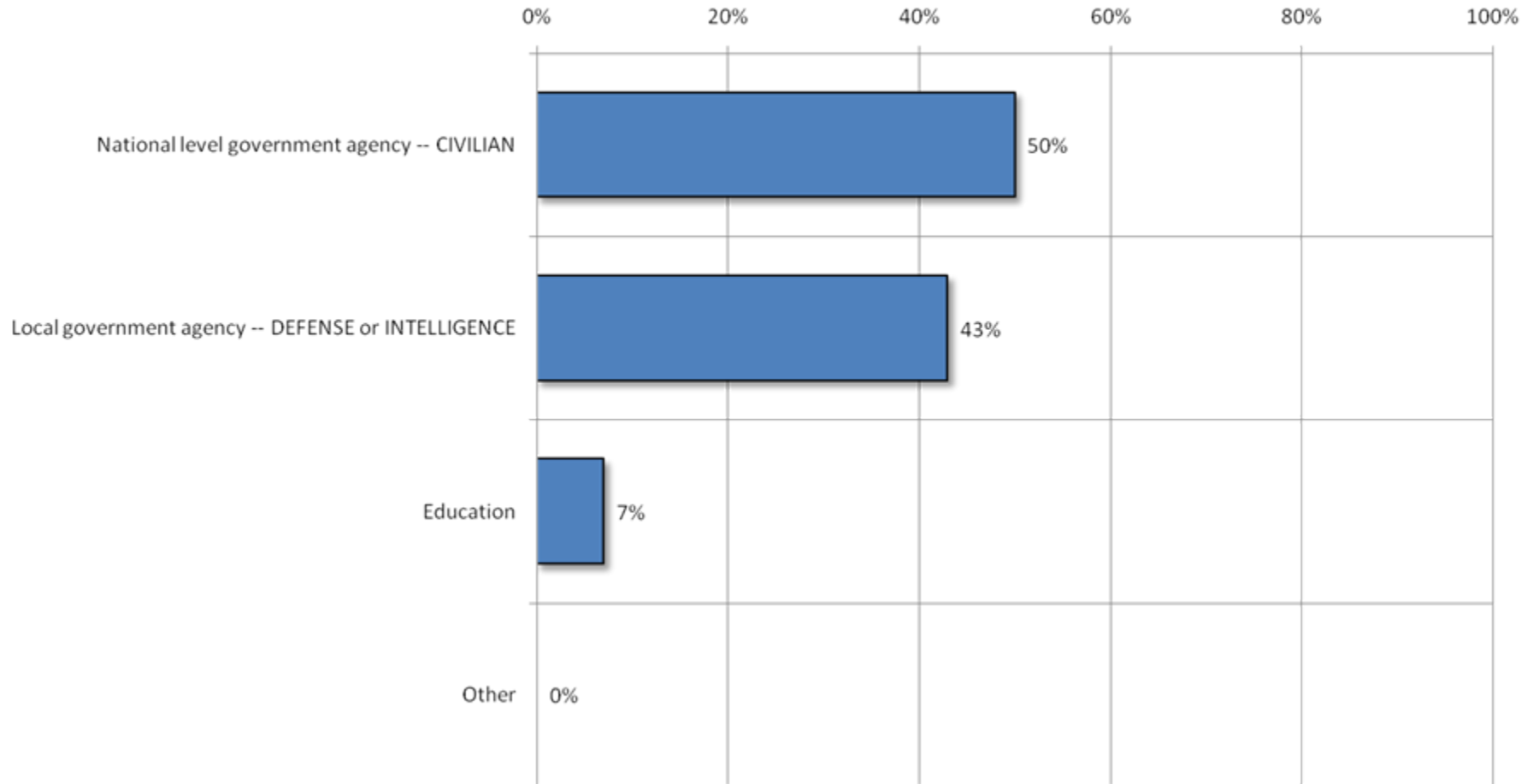
0%

Industry Verticals: Public Sector (Non-US)



Industry Verticals: Public Sector (Non-US)

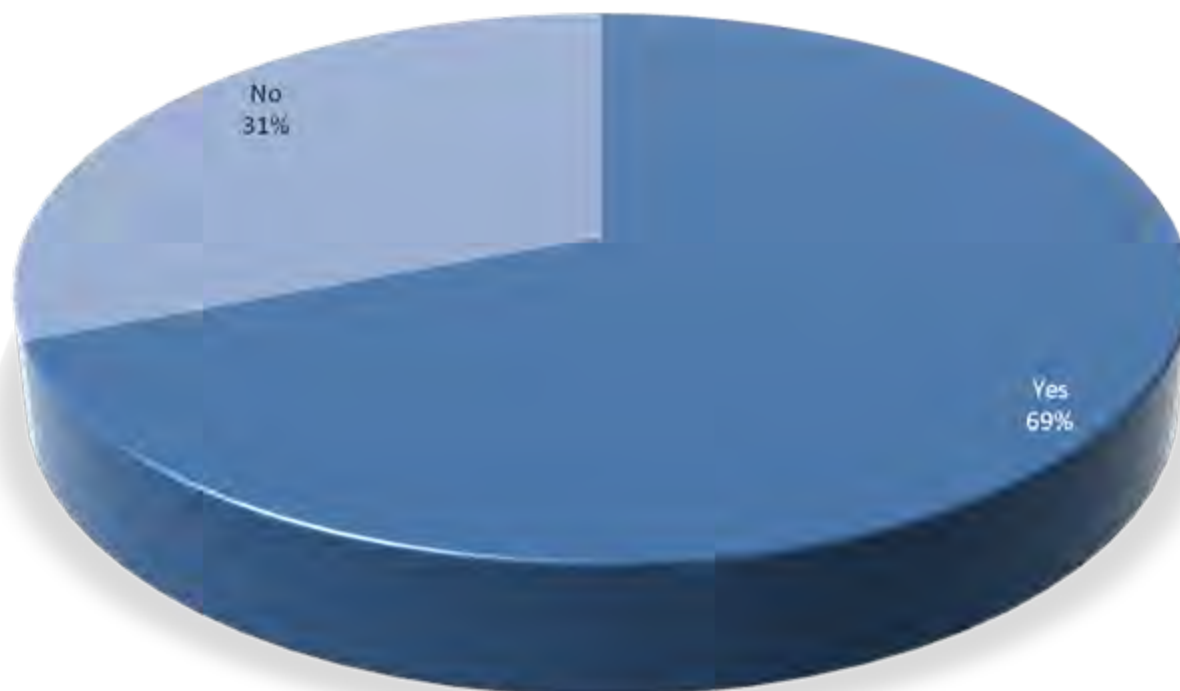
Q121: Which best describes your organization?
(Only asked of Public Sector Companies not located in the US)



Industry Verticals: Public Sector (Non-US)

Q122: Do you leverage integrators/consultants to support your *security* efforts?

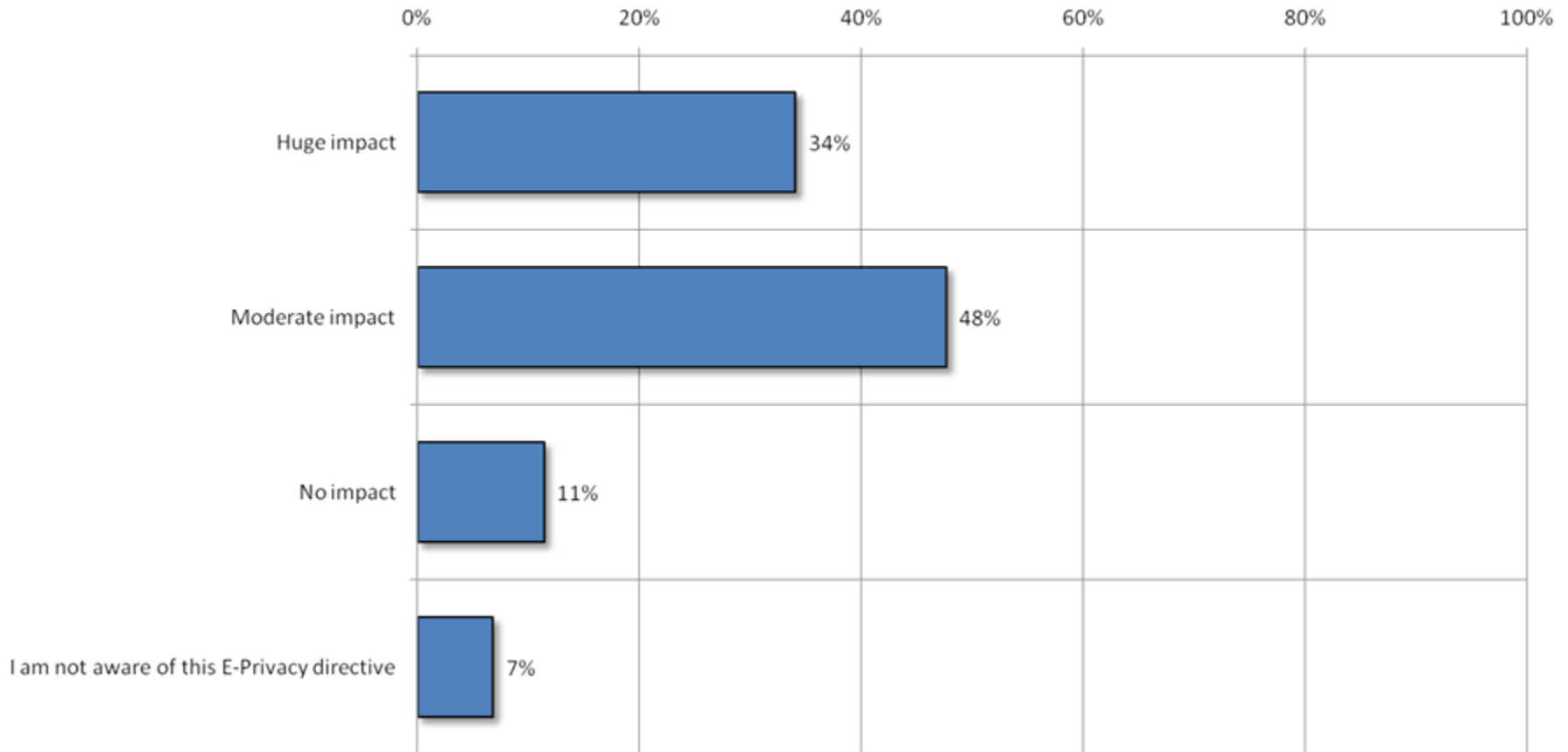
(Only asked of Public Sector Companies not located in the US)



Industry Verticals: Telecommunications

Industry Verticals: Telecommunications

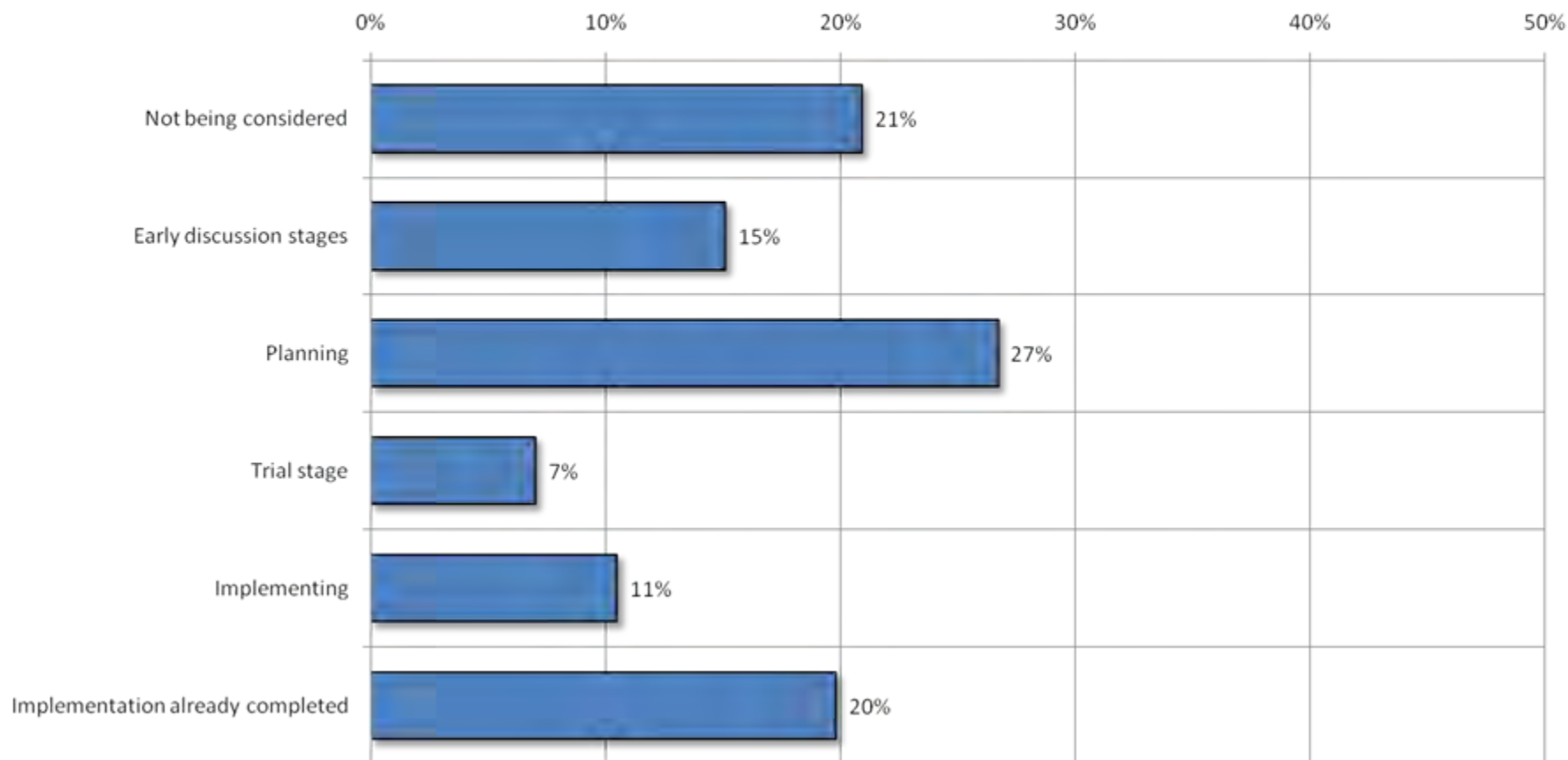
Q123: How do you rate the impact of Data Breach Notification for your security spending in the next coming months?
(Only asked of Telecommunications Companies in select countries)



Industry Verticals: Telecommunications

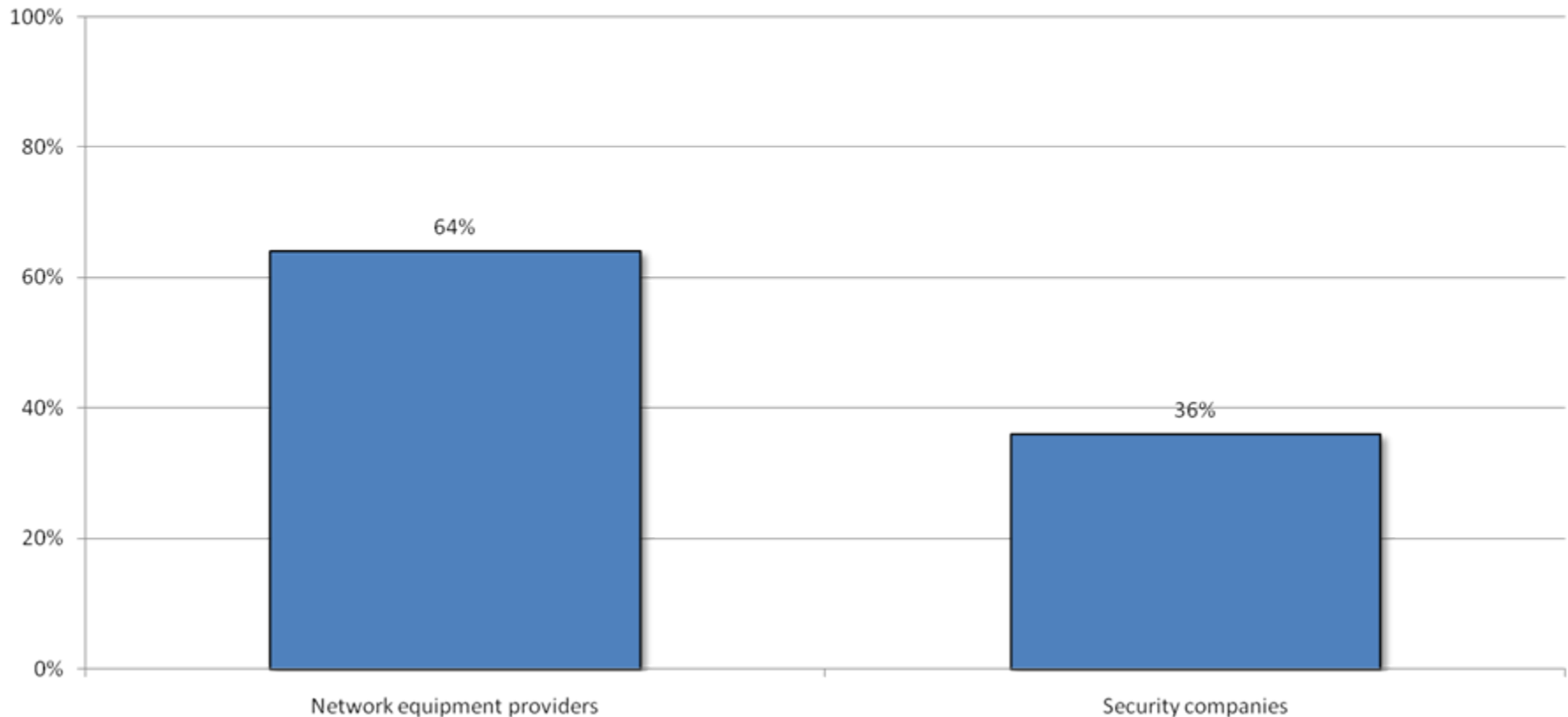
Q124: Do you plan to offer Managed Security Services to your customers?

(Only asked of Telecommunications Companies)



Industry Verticals: Telecommunications

Q125: As you are transforming your Telecommunications network into a modern Next Generation Network (NGN) based on ALL-IP, who do you consider as the major security vendors?
(Only asked of Telecommunications Companies)



Industry Verticals: Telecommunications

Q126: How importantly do you rank security in the NGN?
(Only asked of Telecommunications Companies)

