# 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**

Appendix

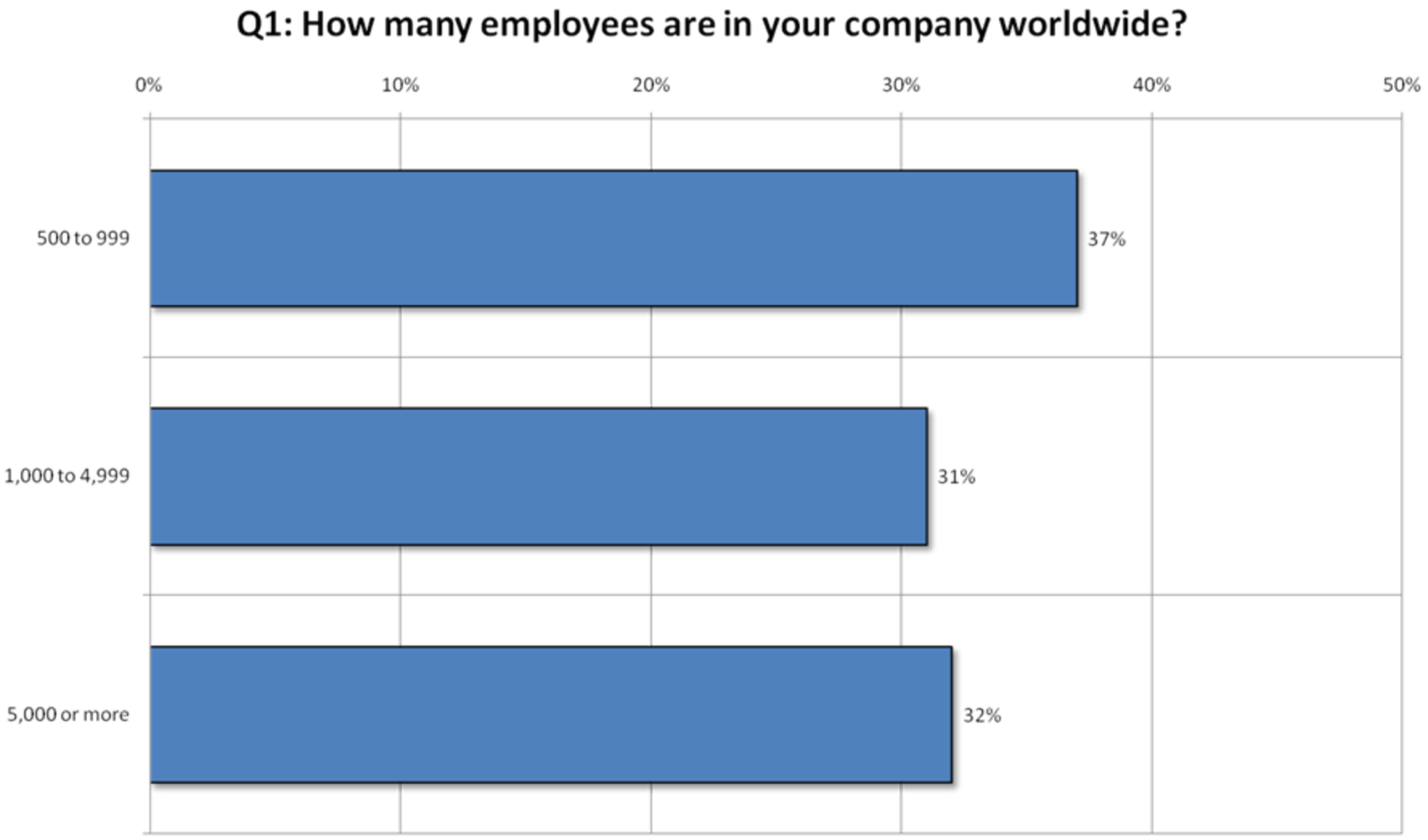
# Full slide deck (all questions)

# Methodology

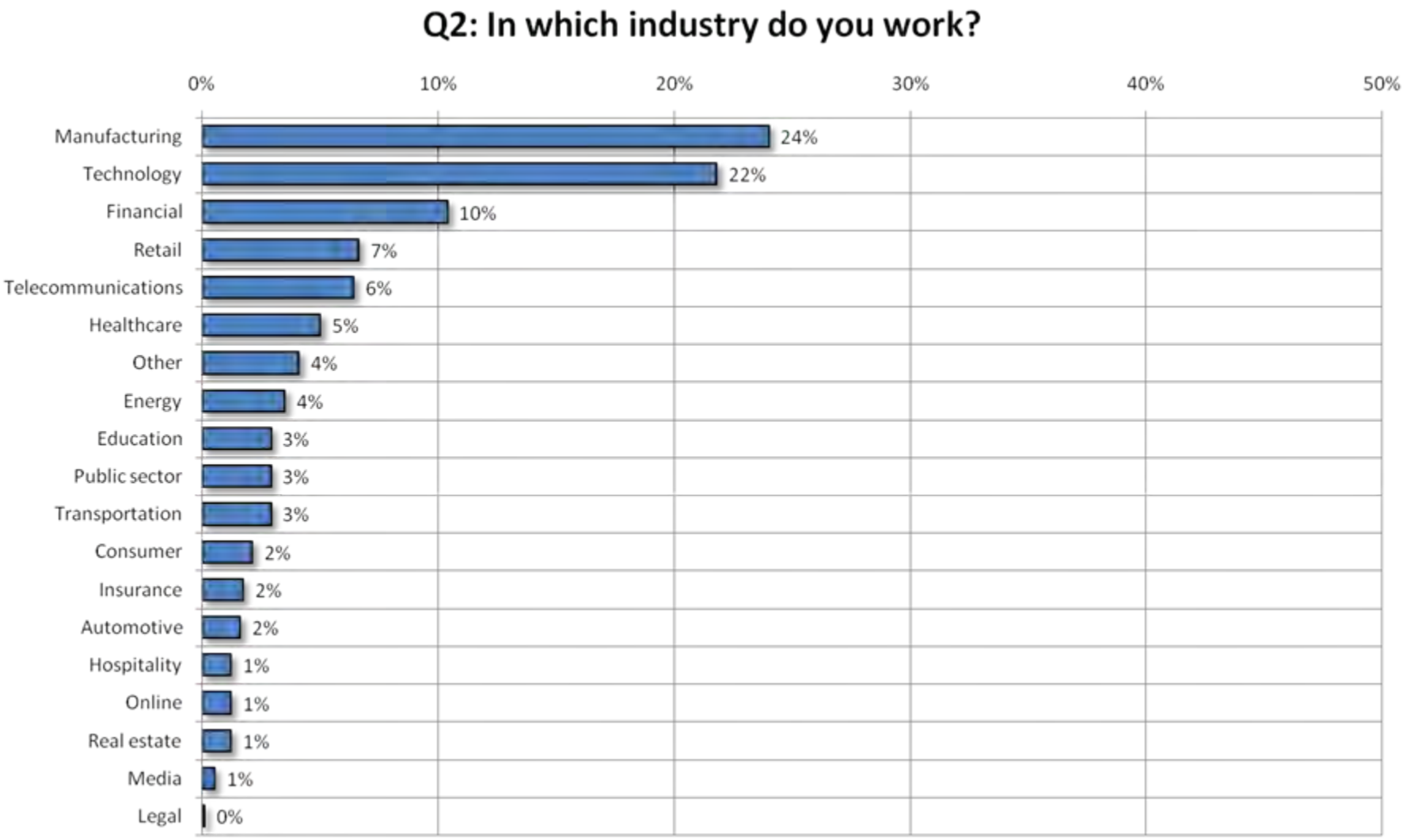
- Applied Research performed survey
- January 2010
- 2,100 worldwide responses
- Small enterprise (500 – 999 employees)
- Medium enterprise (1,000 – 4,999 employees)
- Large enterprise (5,000 or more employees)

# Demographics

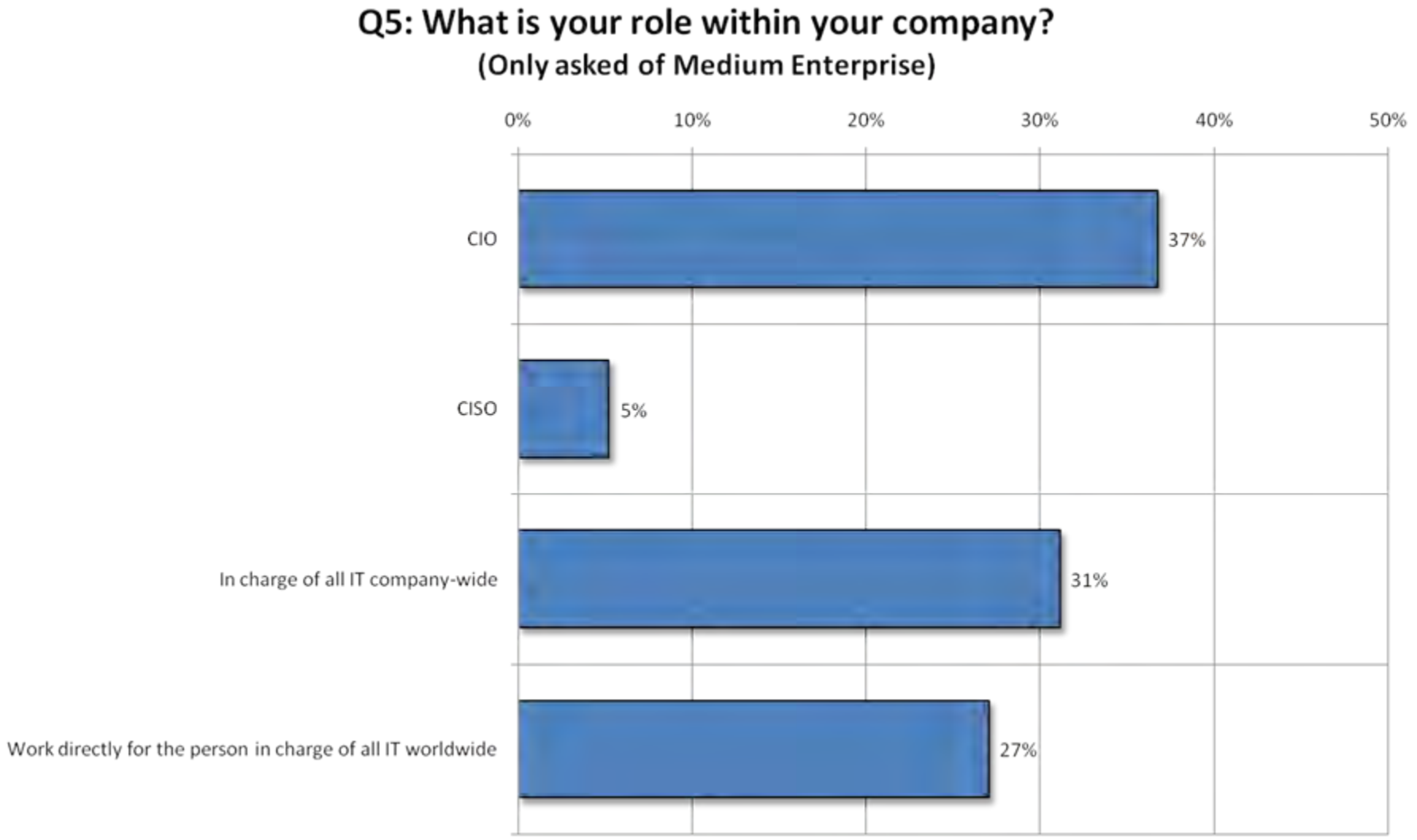
# Company size



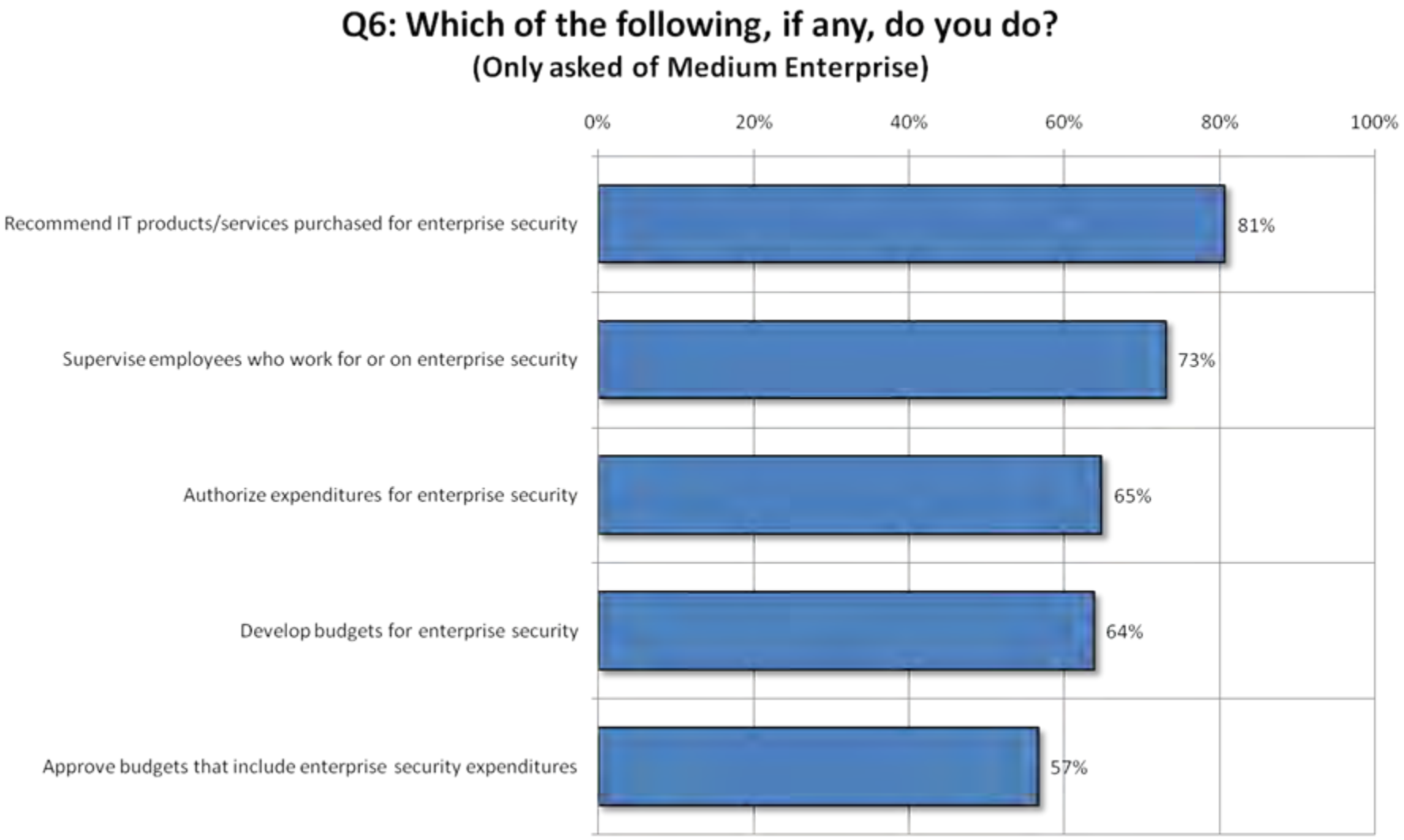
# Industries


Q2: In which industry do you work?
0%
10%
20%
30%
40%
50%
Manufacturing 24%
Technology 22%
Financial 10%
Retail 7%
Telecommunications 6%
Healthcare 5%
Other 4%
Energy 4%
Education 3%
Public sector 3%
Transportation 3%
Consumer 2%
Insurance 2%
Automotive 2%
Hospitality 1%
Online 1%
Real estate 1%
Media 1%
Legal 0%

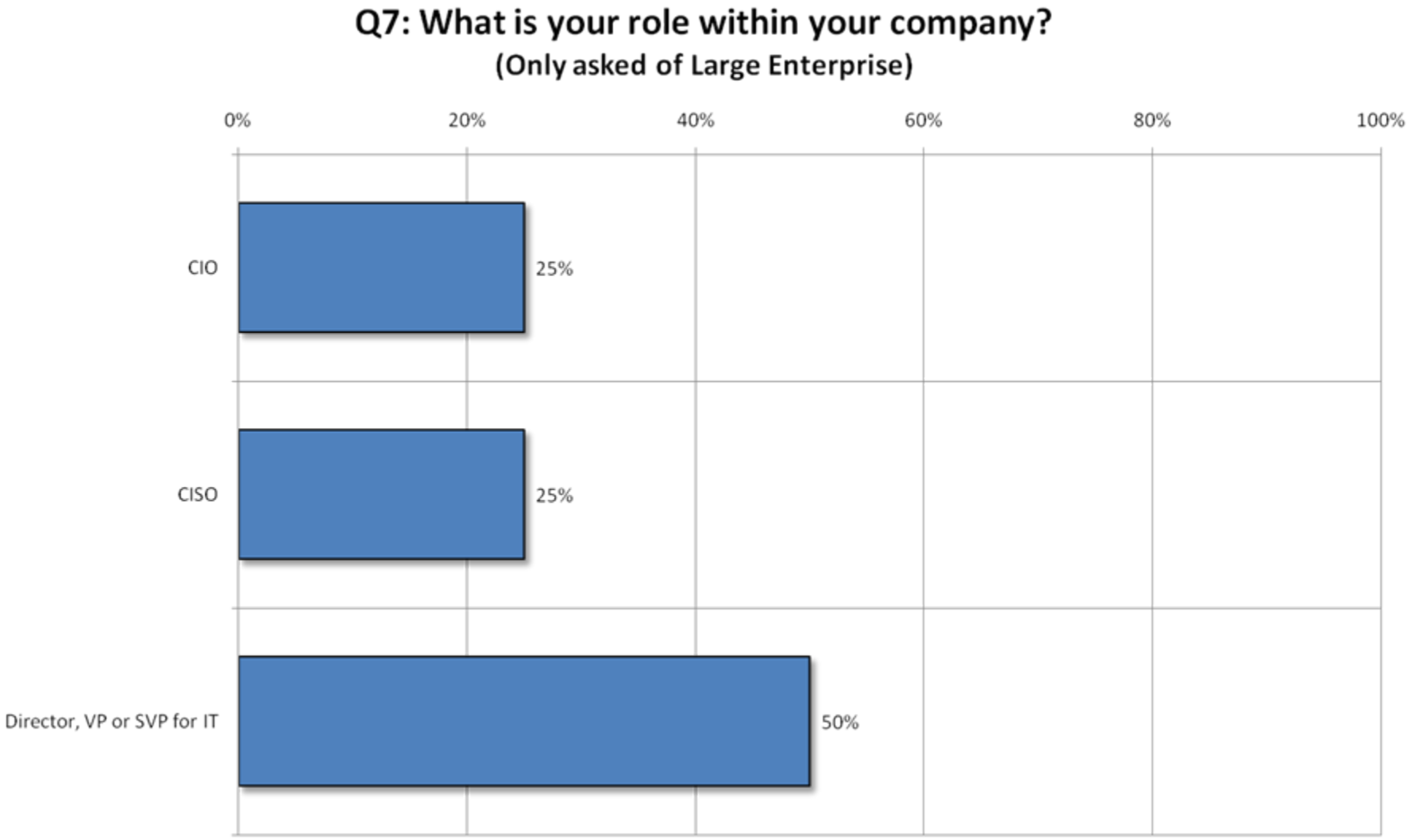
# Medium enterprise



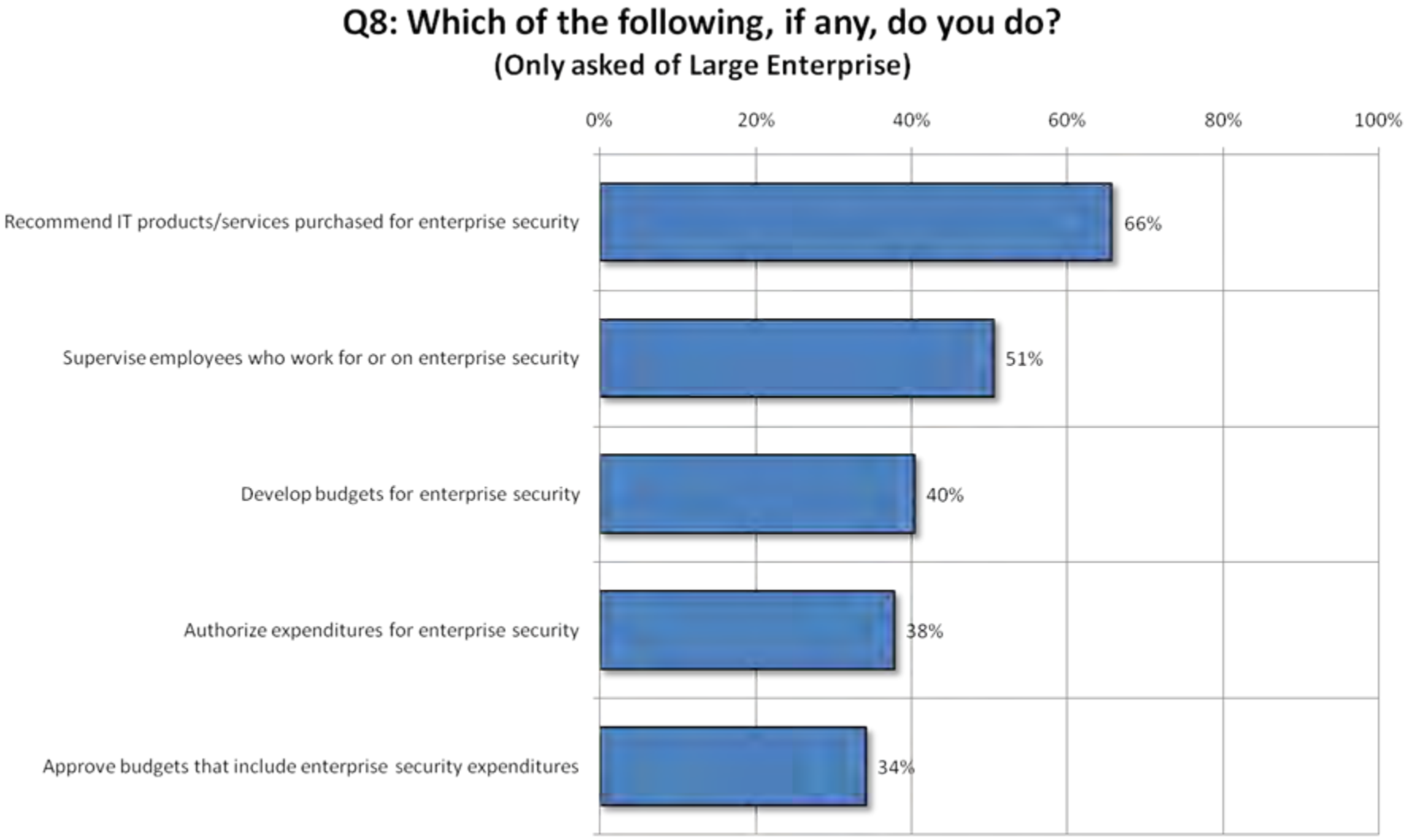
# Medium enterprise



# Large enterprise

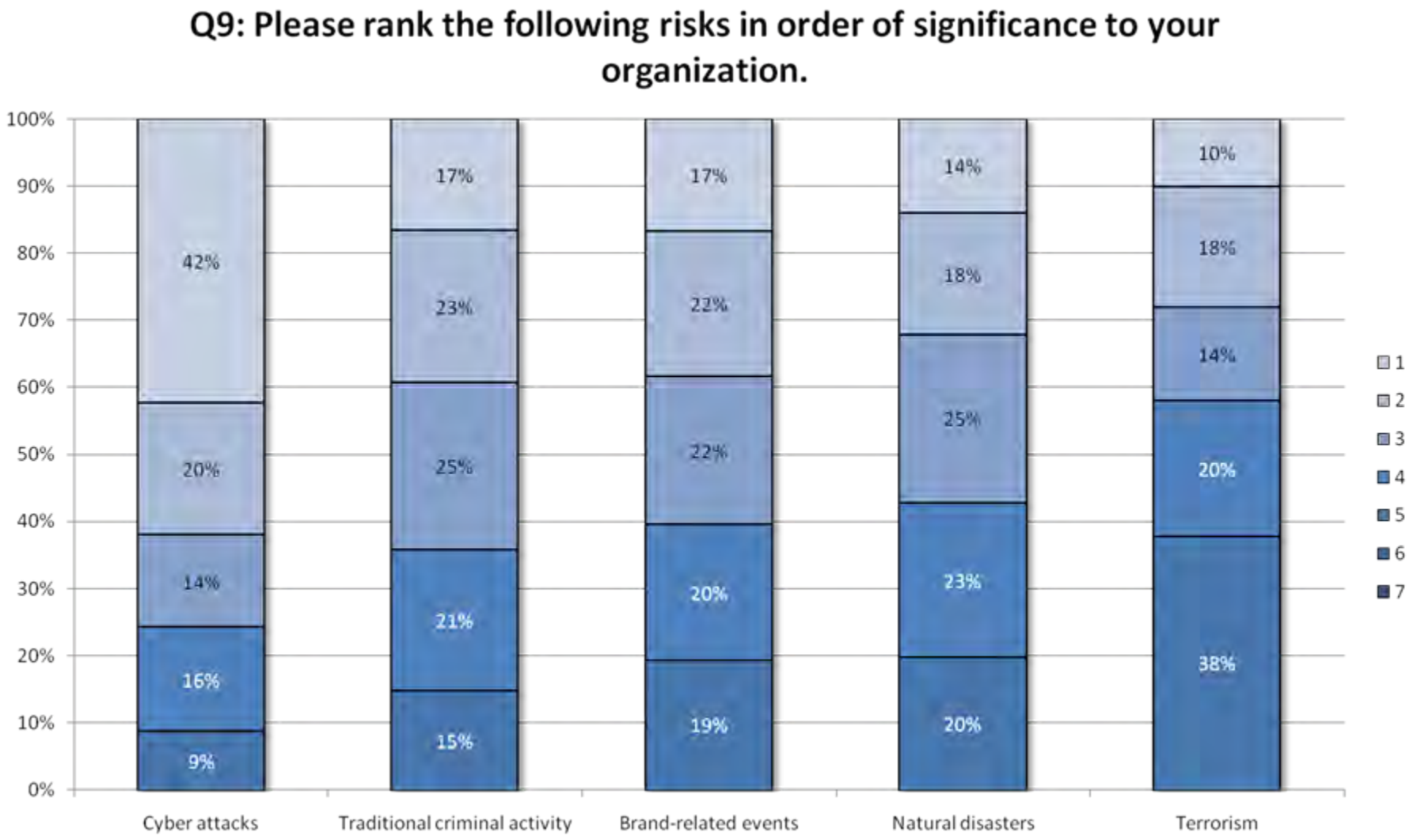


# Large enterprise

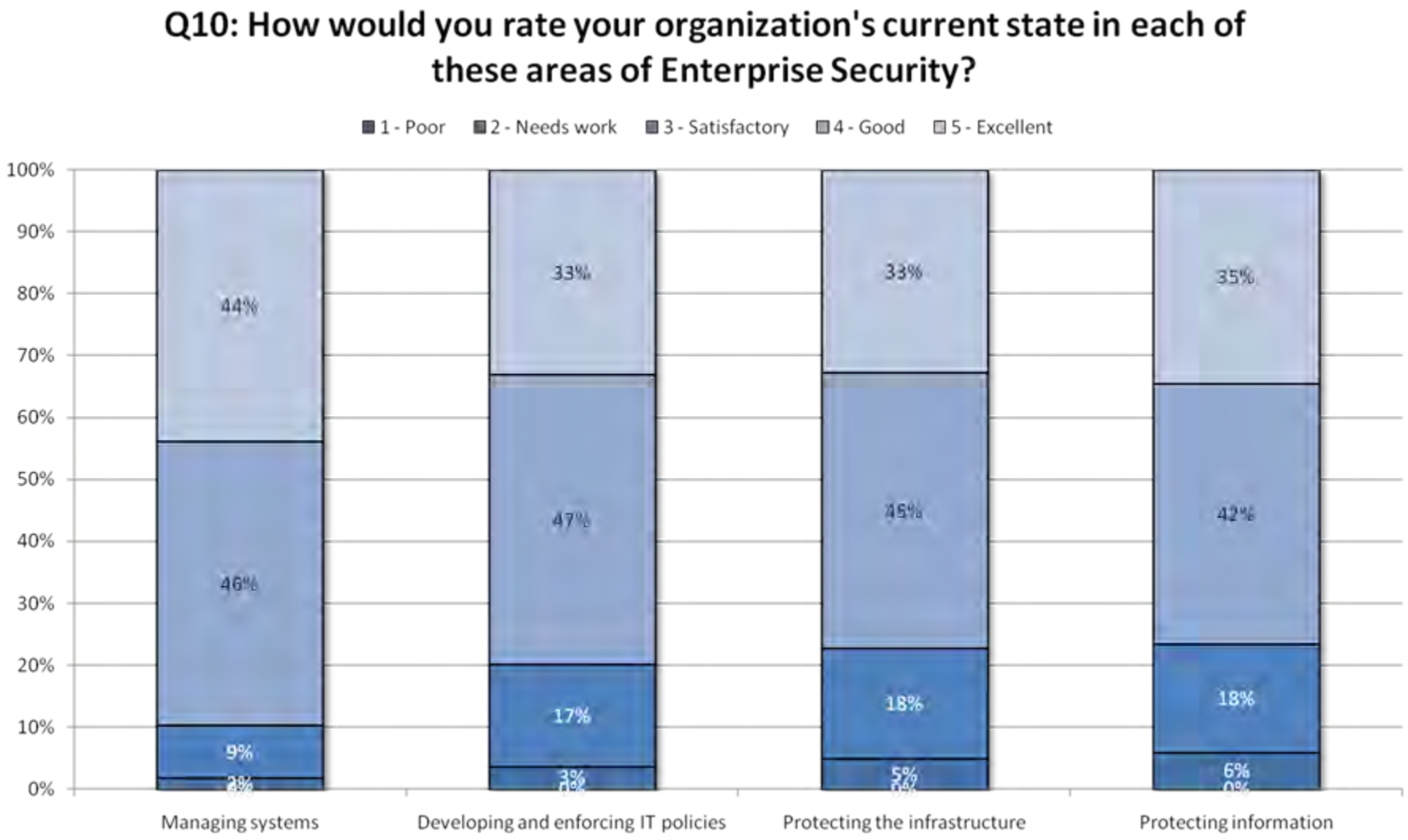


# Objectives

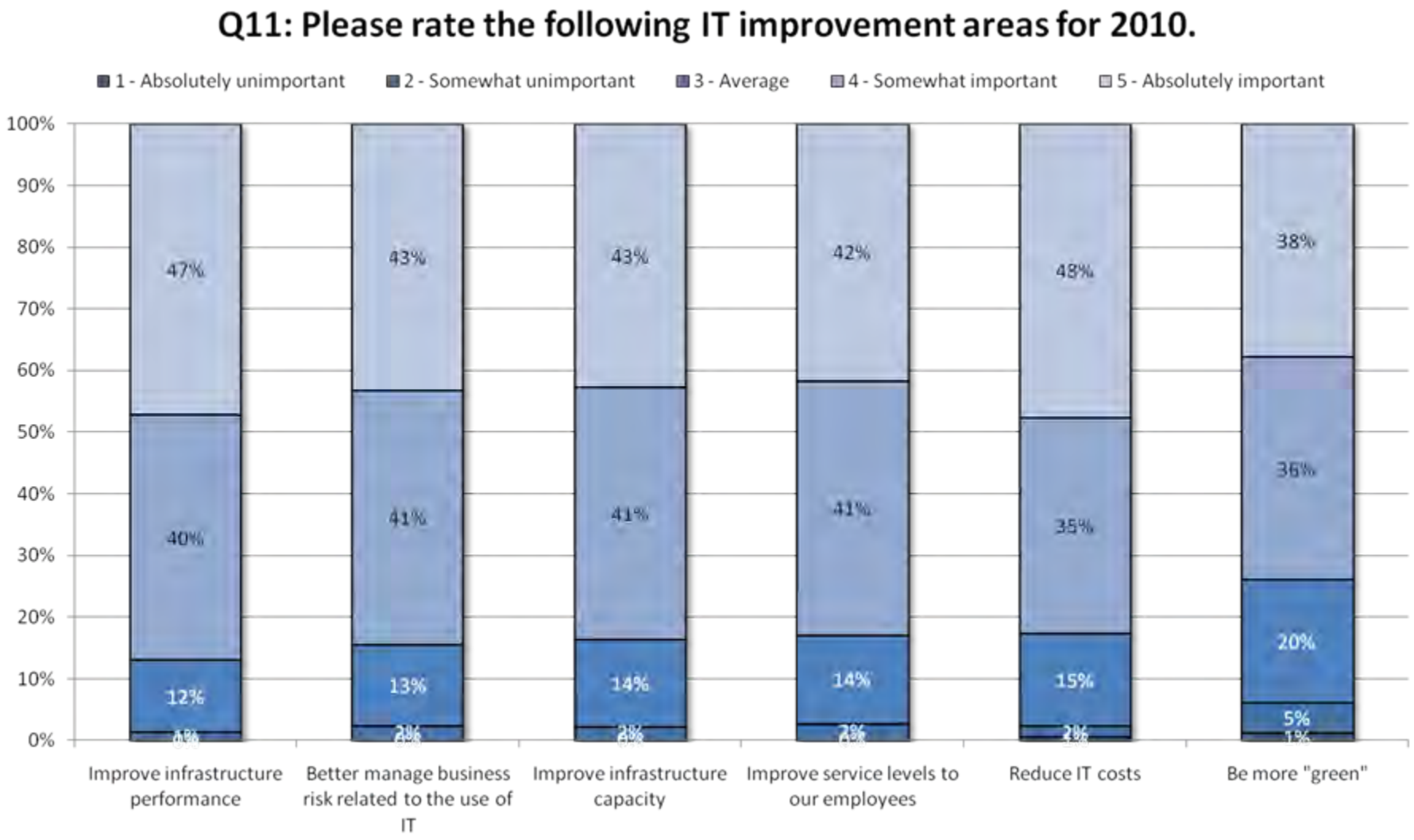
# Security risks



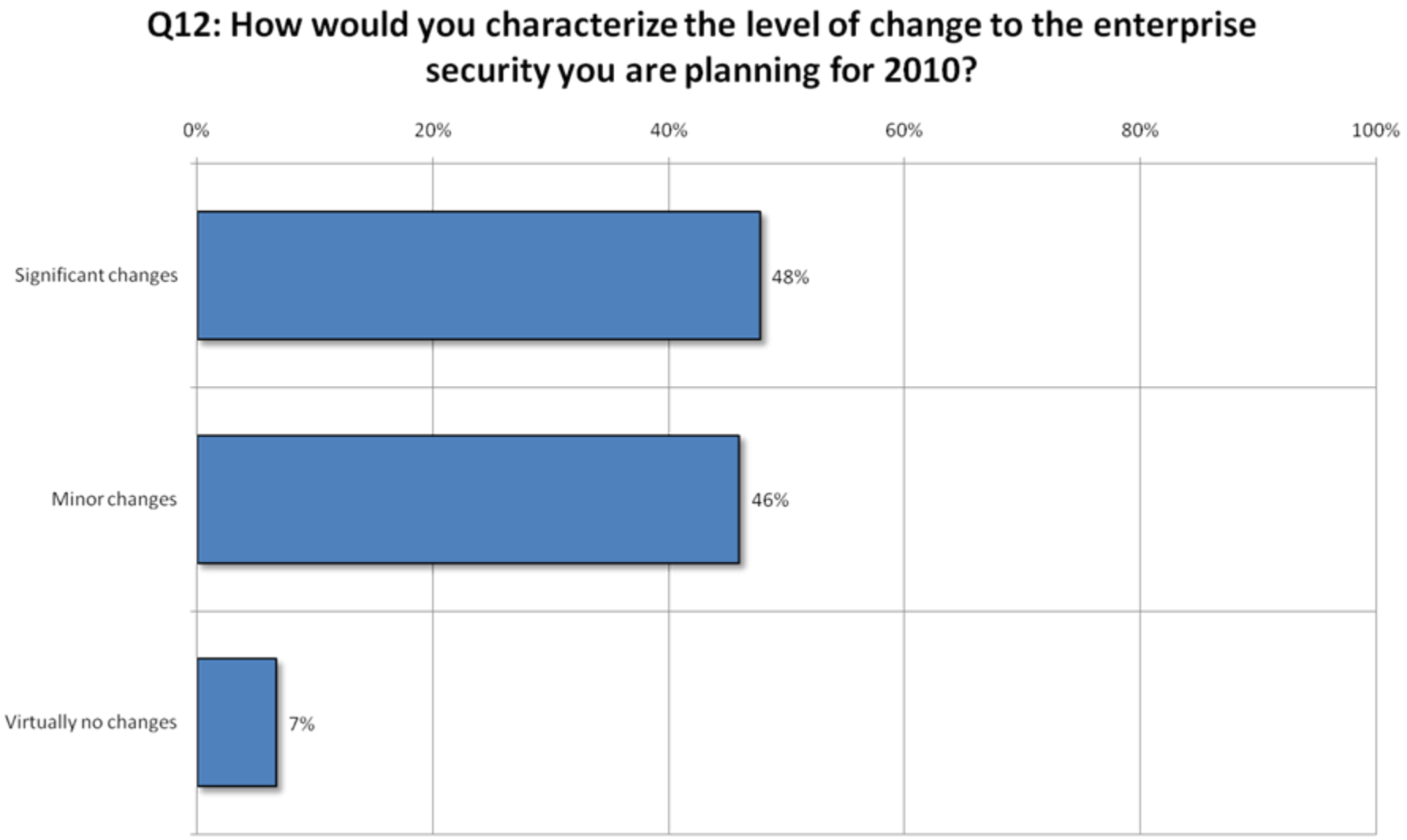
# Enterprise security status



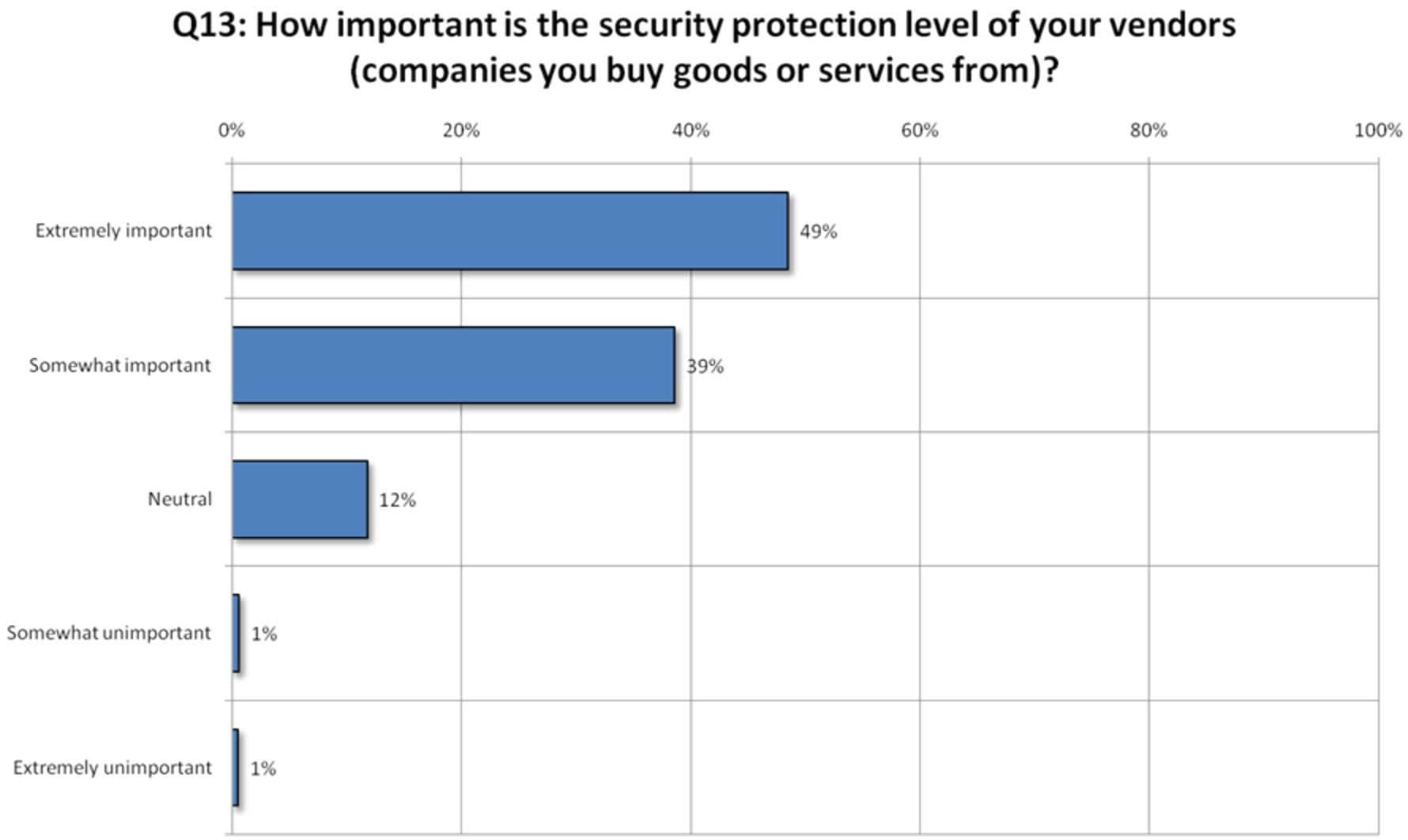
# IT improvements



# Planned change for enterprise security

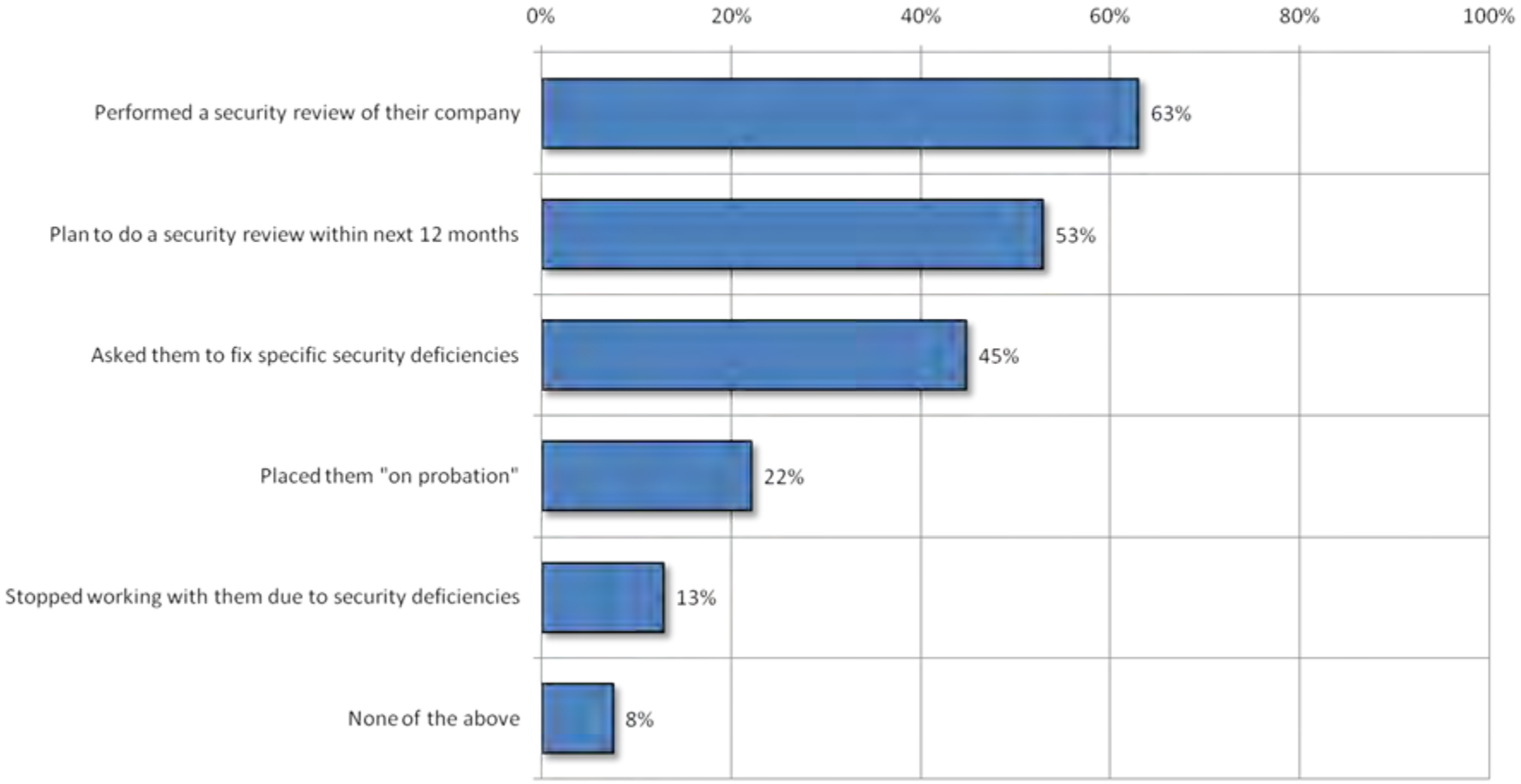


# Vendor security protection



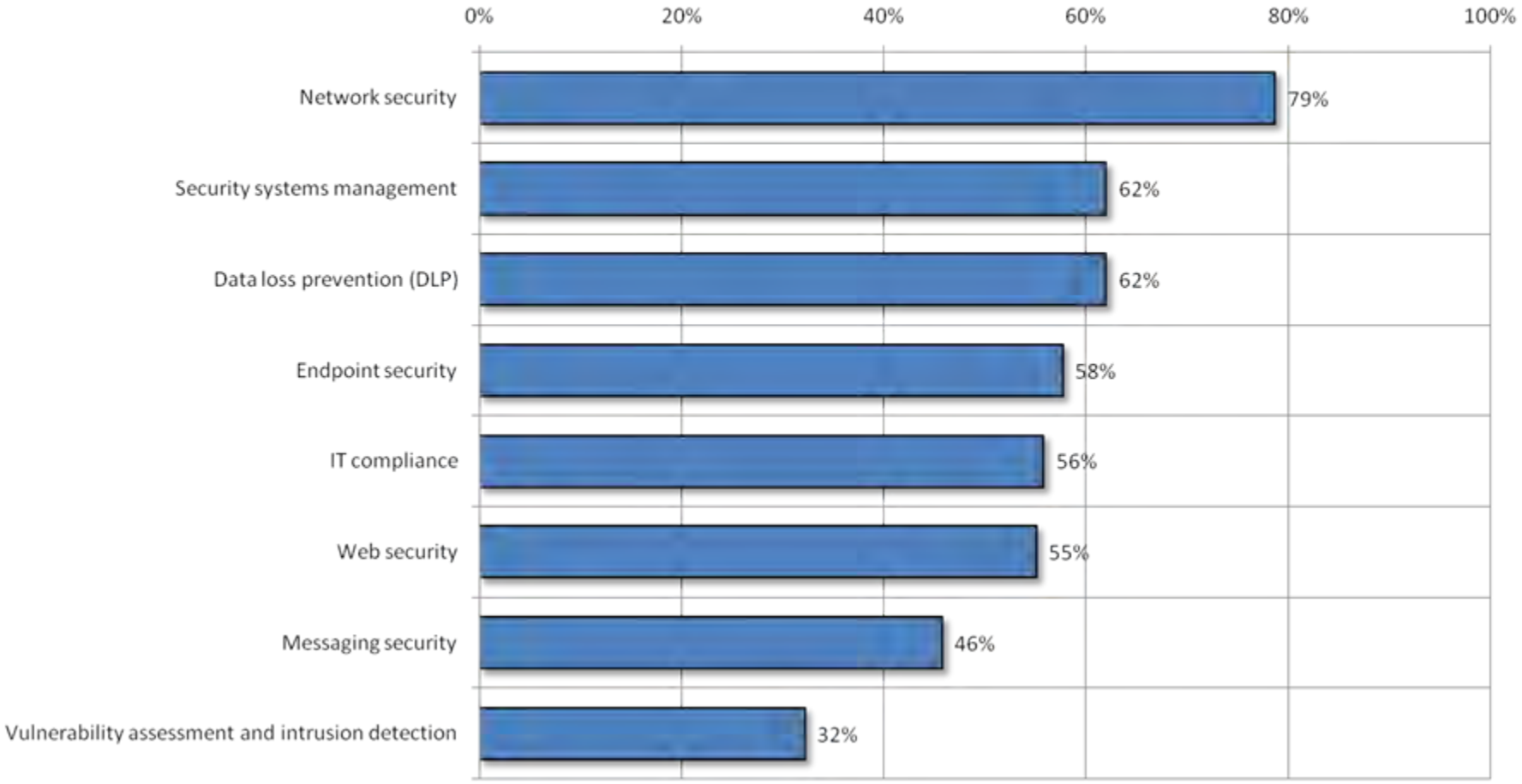
# Vendor security

## 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.**

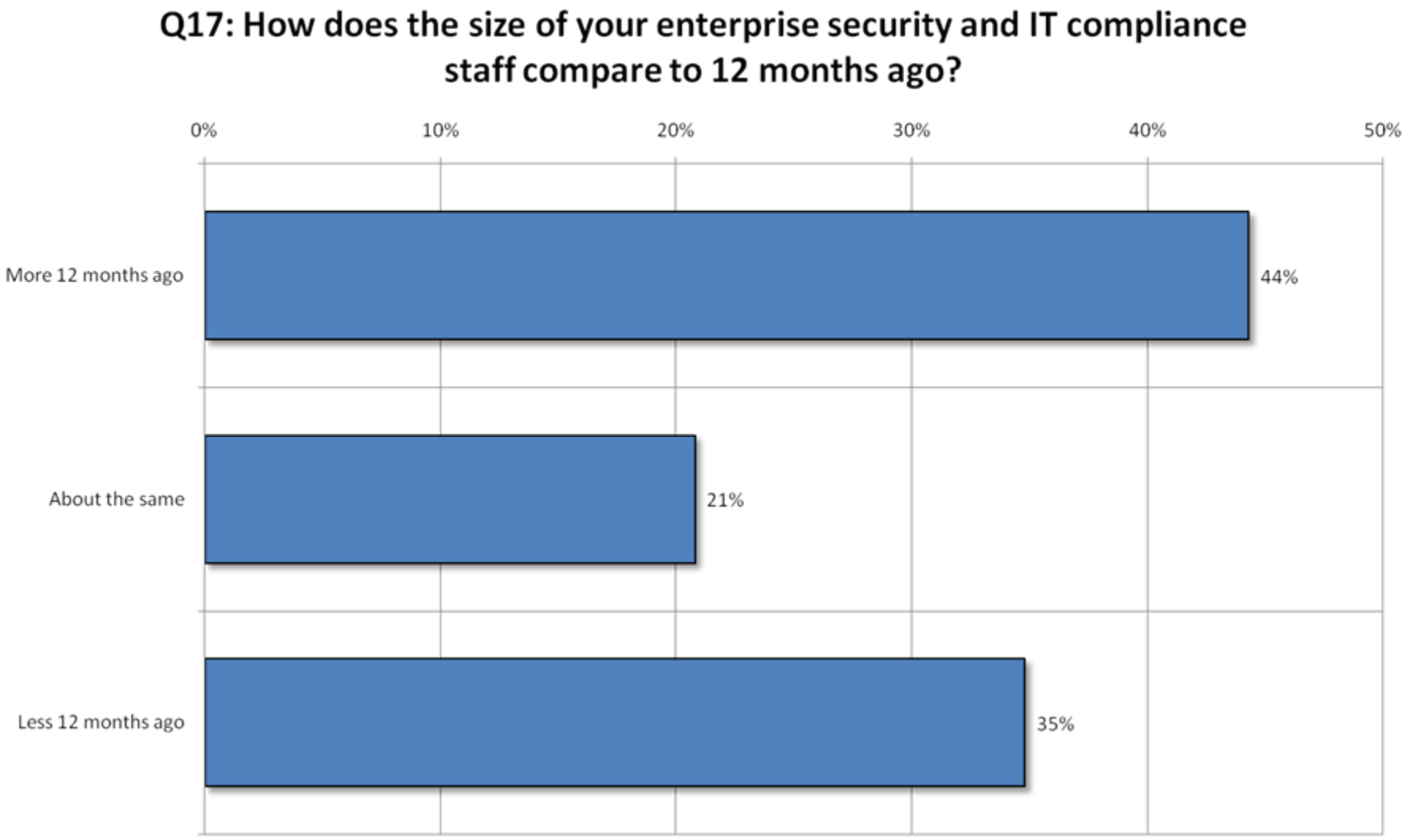


# Staffing & Budget

# Enterprise security staff

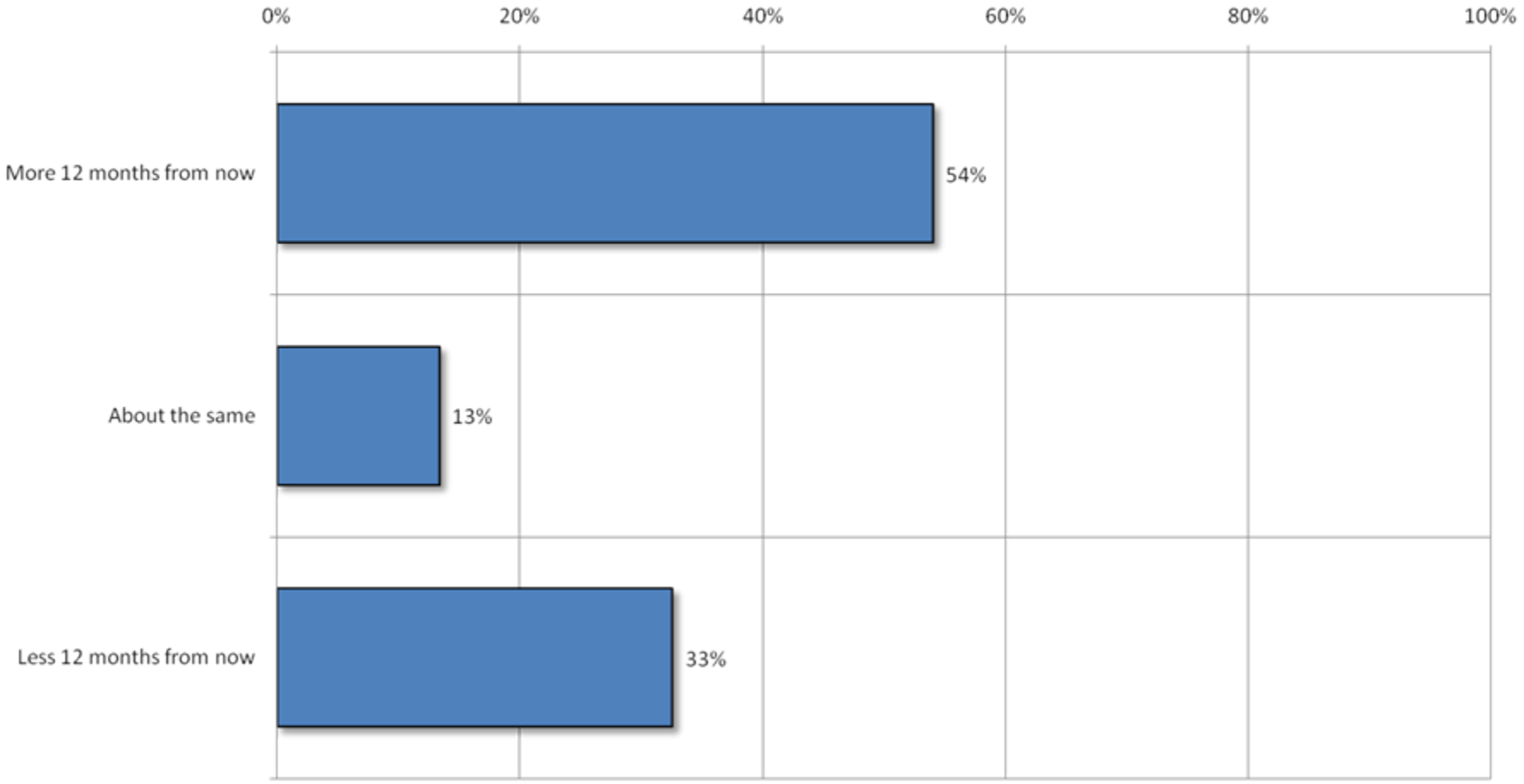
| Q16: Roughly how many people work on enterprise security or IT compliance in your organization worldwide? | |
|---|---|
| Median | 120 people |

# Enterprise security staff



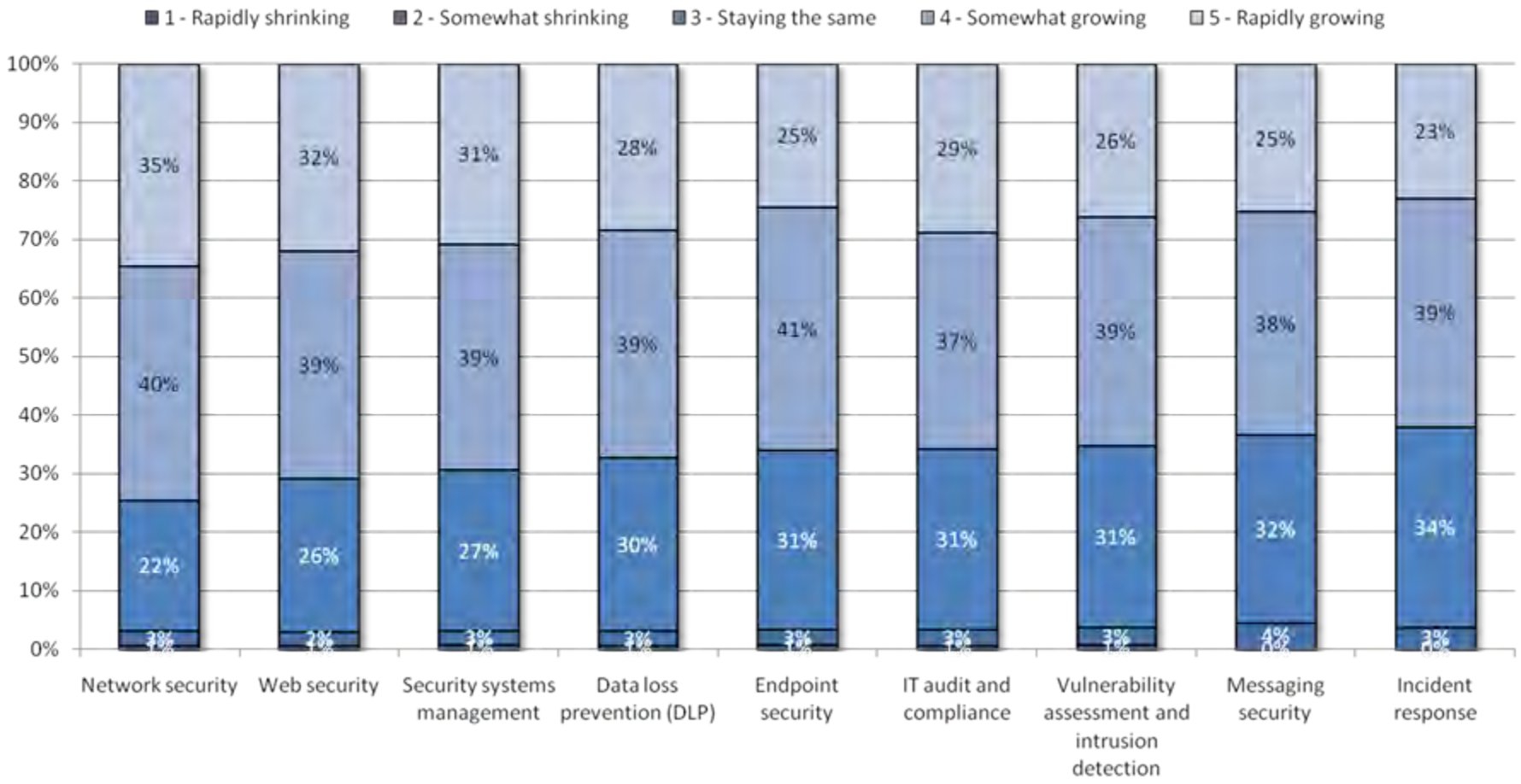
# Enterprise security staff

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



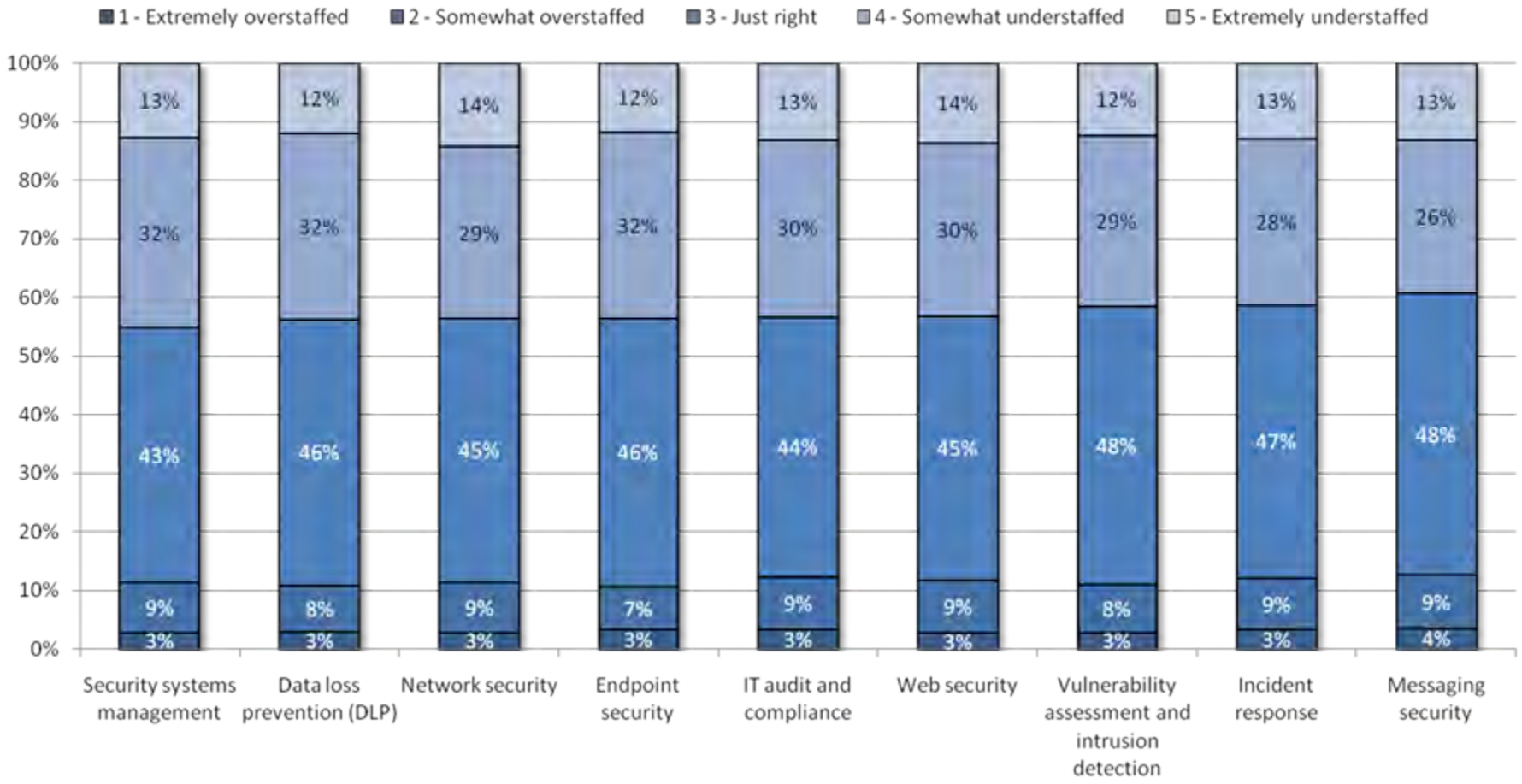
# Manpower capacity change

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



# Manpower capacity staffing

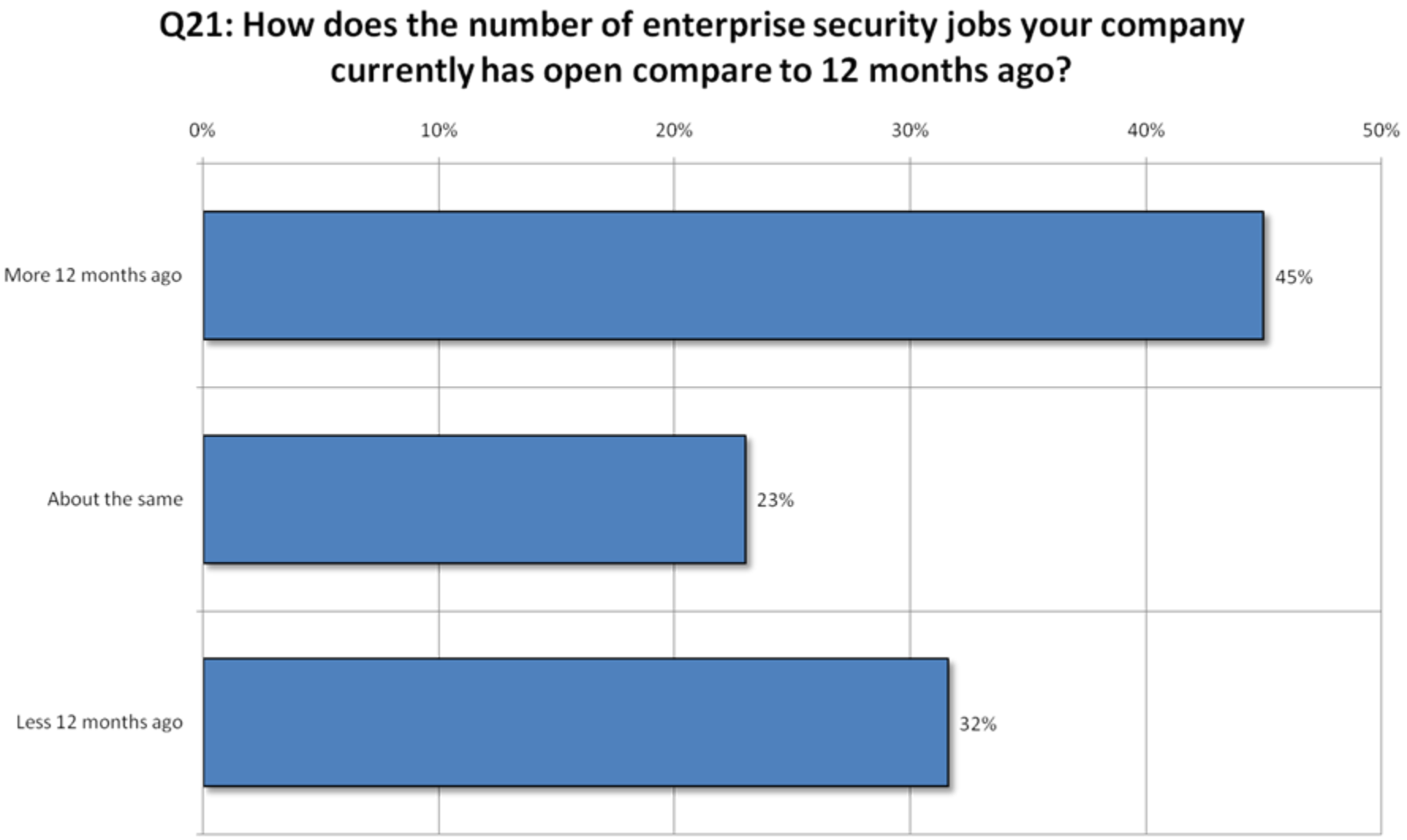
## Q19b: How would you characterize your manpower capacity for each of the following enterprise security skill sets?



# Enterprise security job requisitions

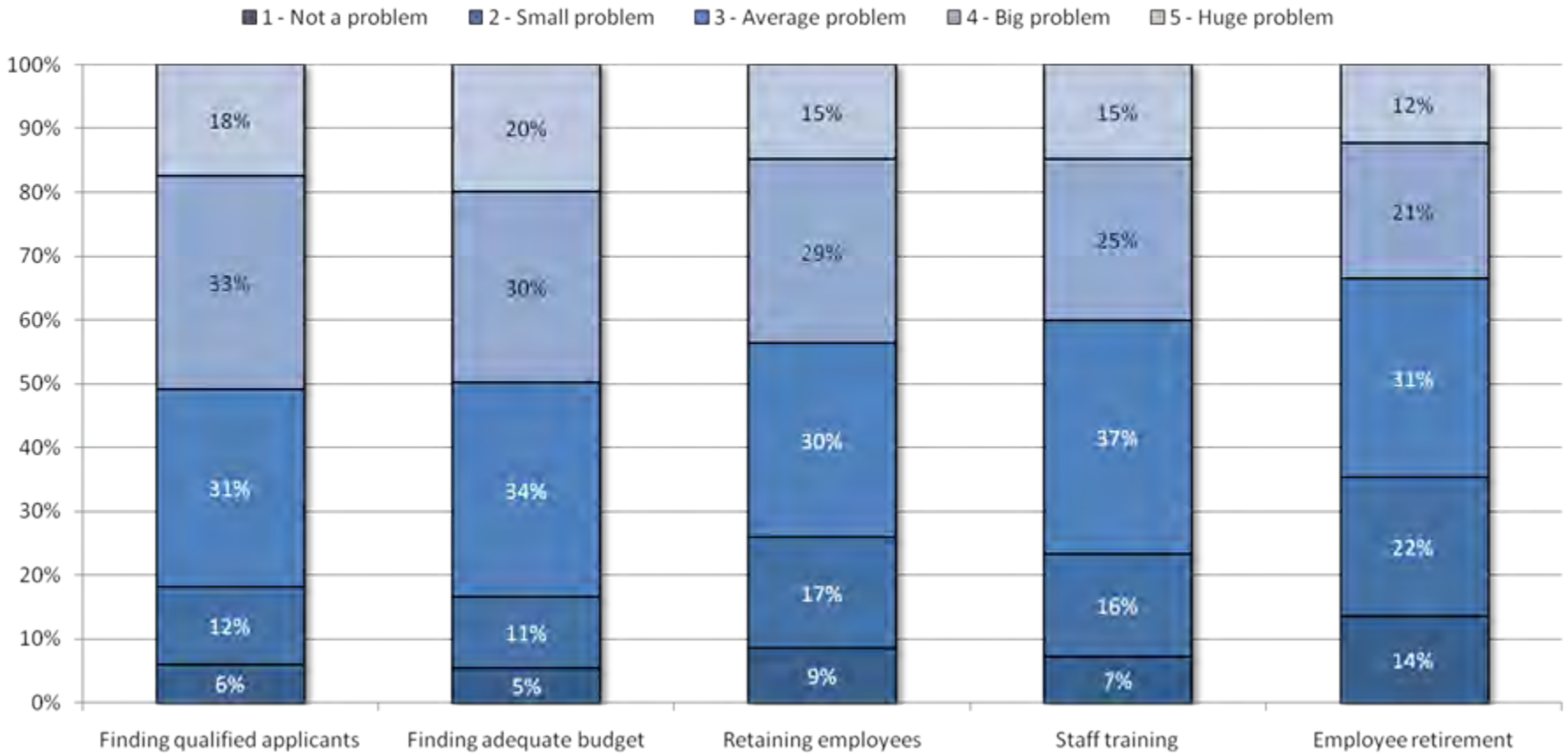
| Q20: How many requisitions for enterprise security jobs does your company have open worldwide at the moment? | |
|---|---|
| Median | 20 requisitions |

# Enterprise security job requisitions



# 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

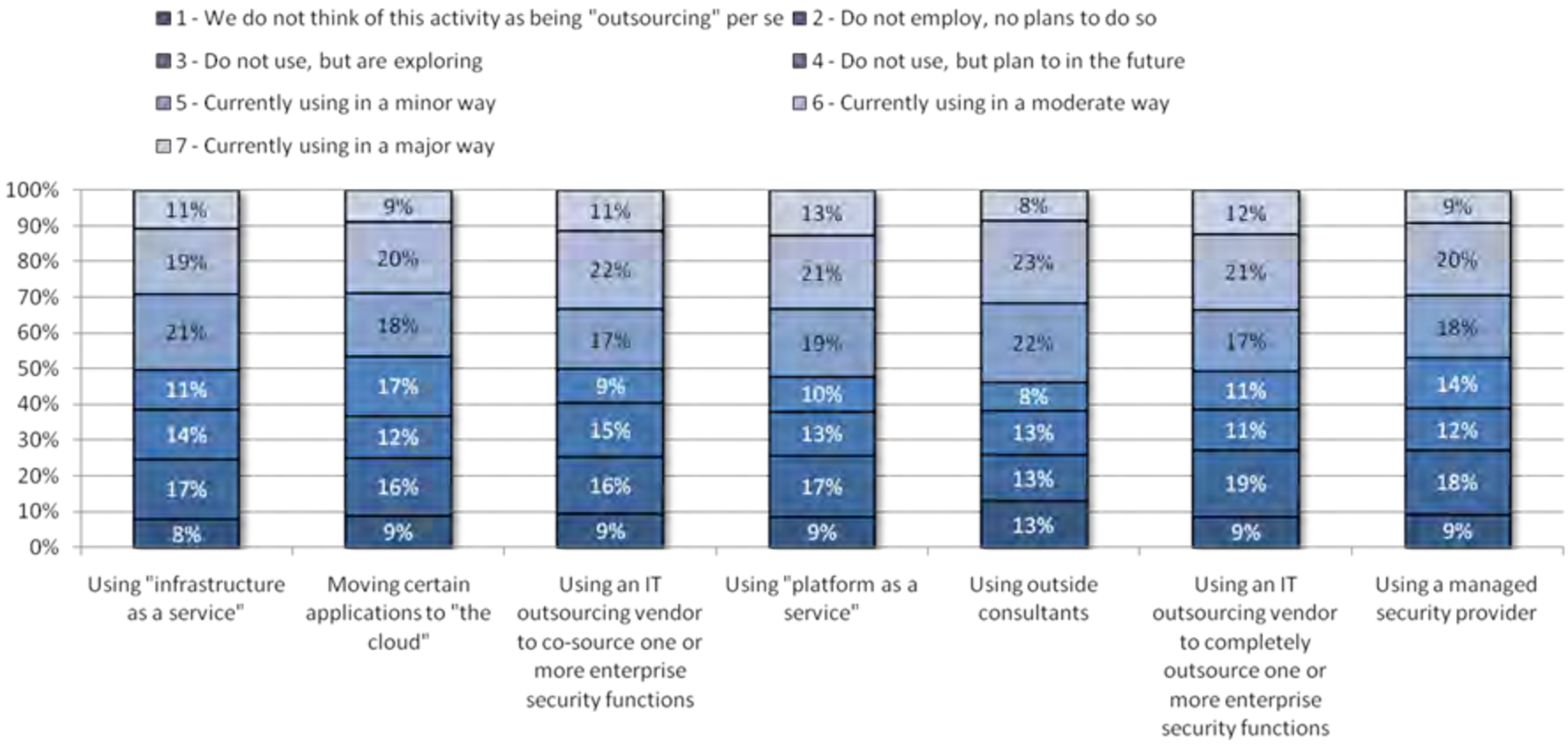
| Q24: What is the percentage change for your enterprise security budgets over 2009? | |
|---|---|
| Median | 11% |

# 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% |

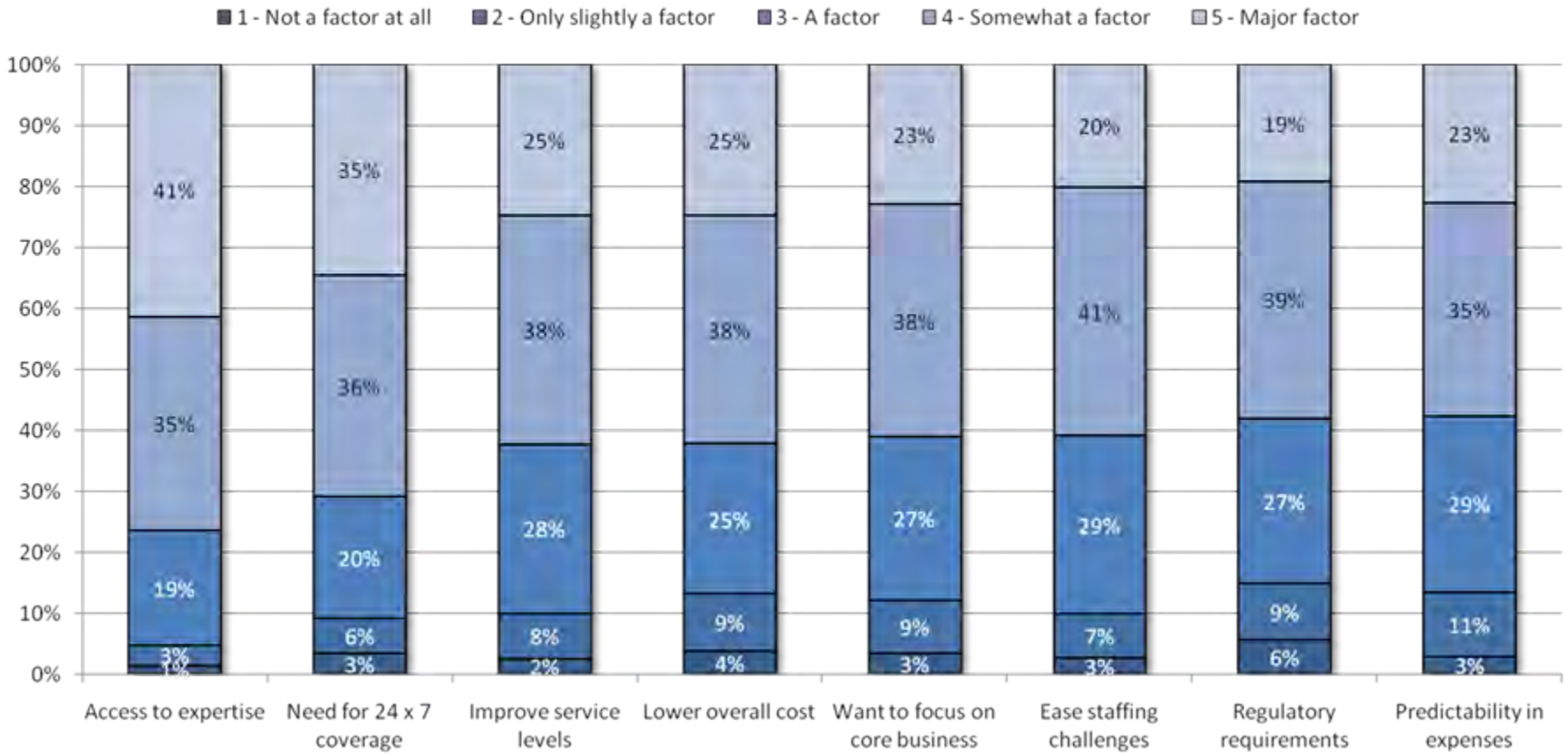
# Outsourcing

## 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?



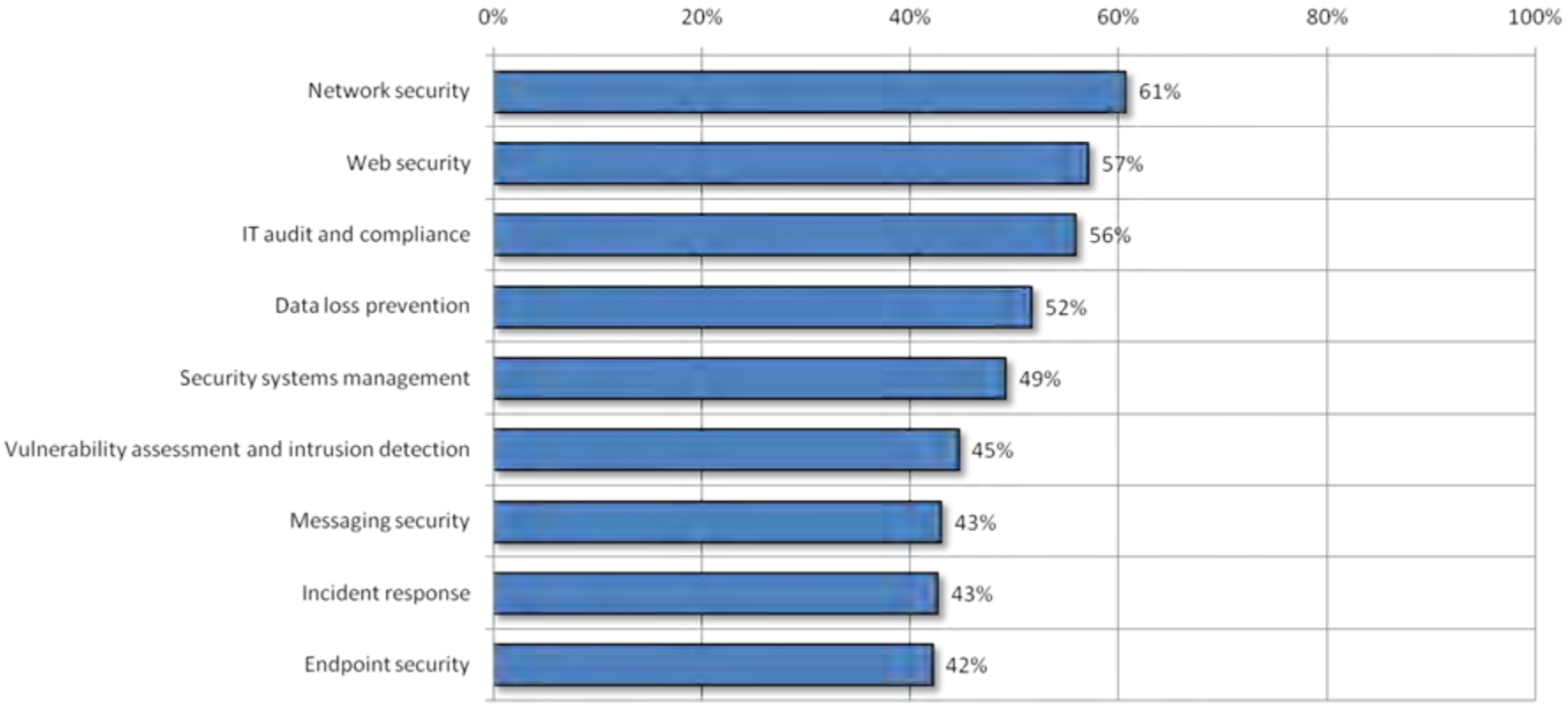
# Outsourcing

## 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)



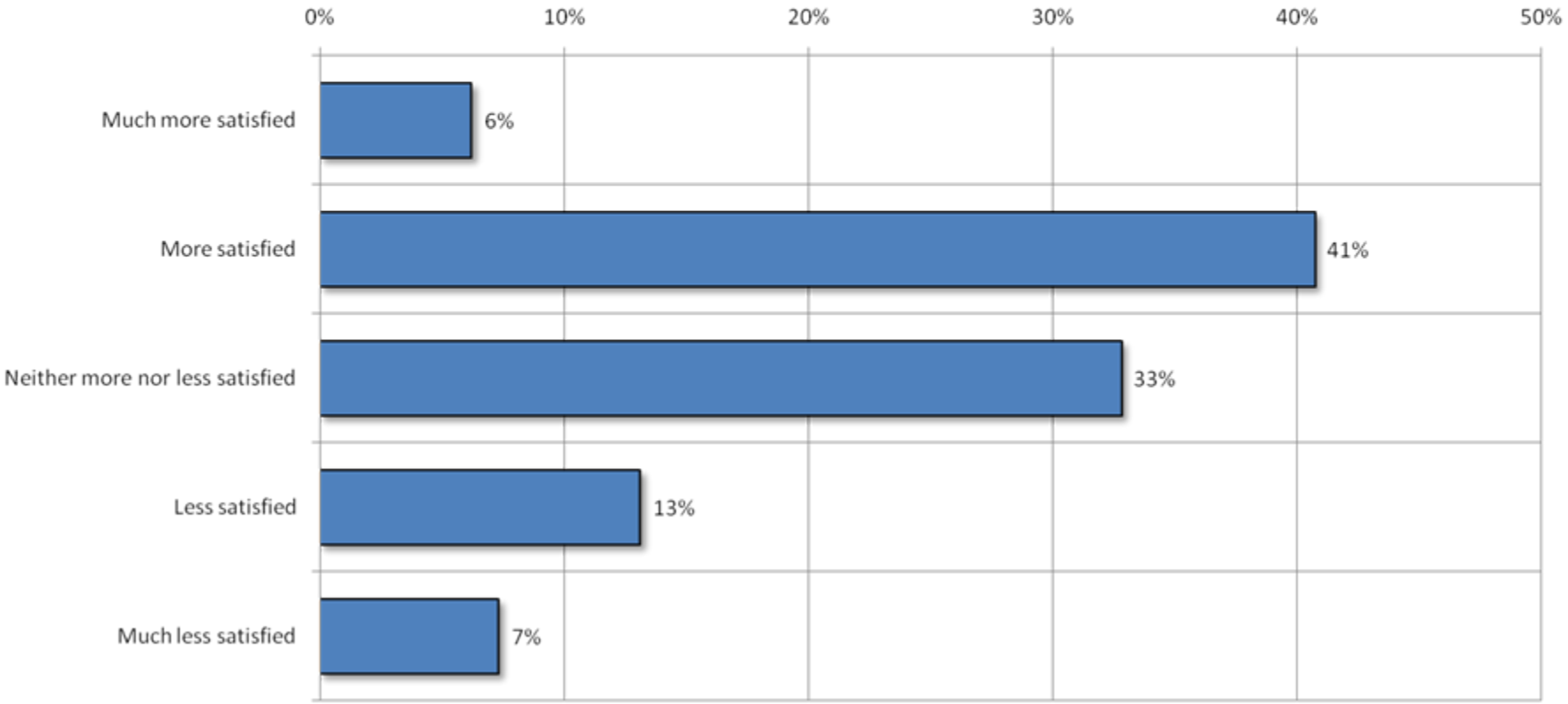
# Outsourcing

**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)**



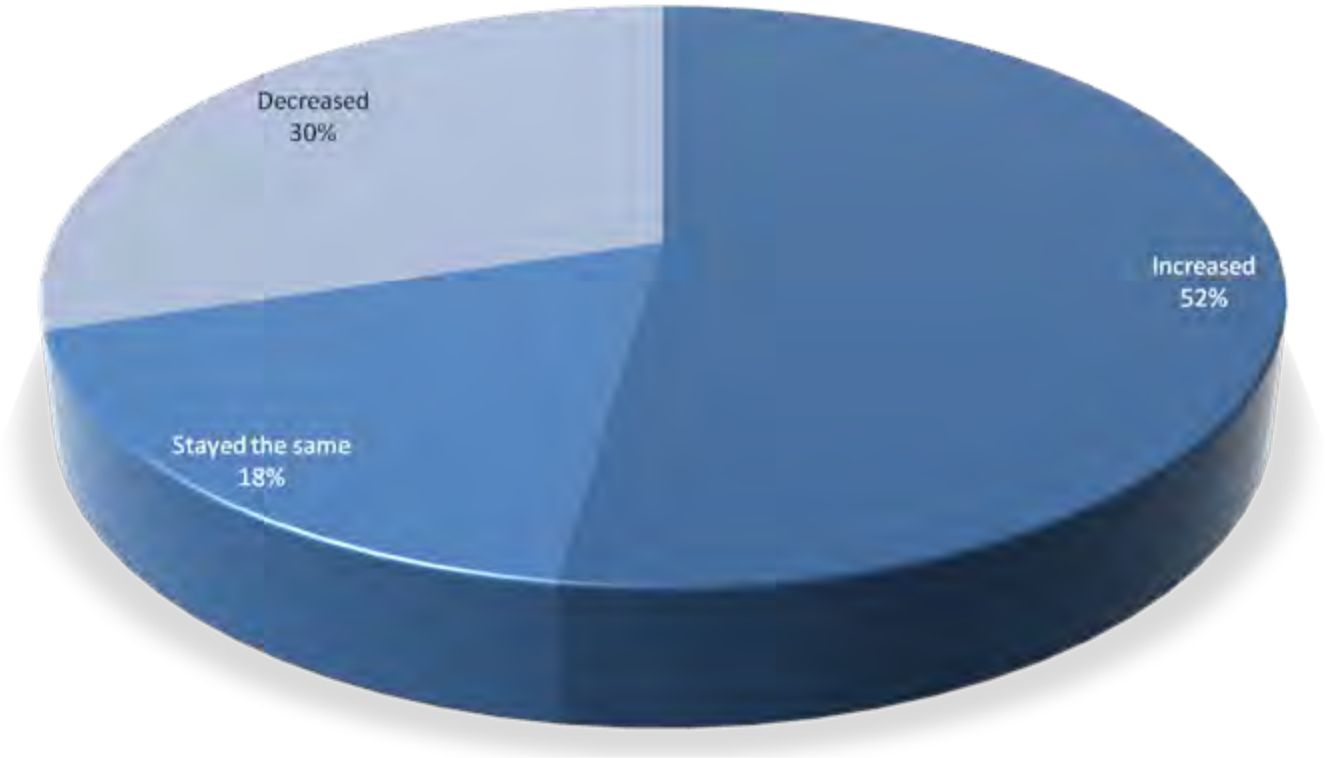
# Outsourcing impact

**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**



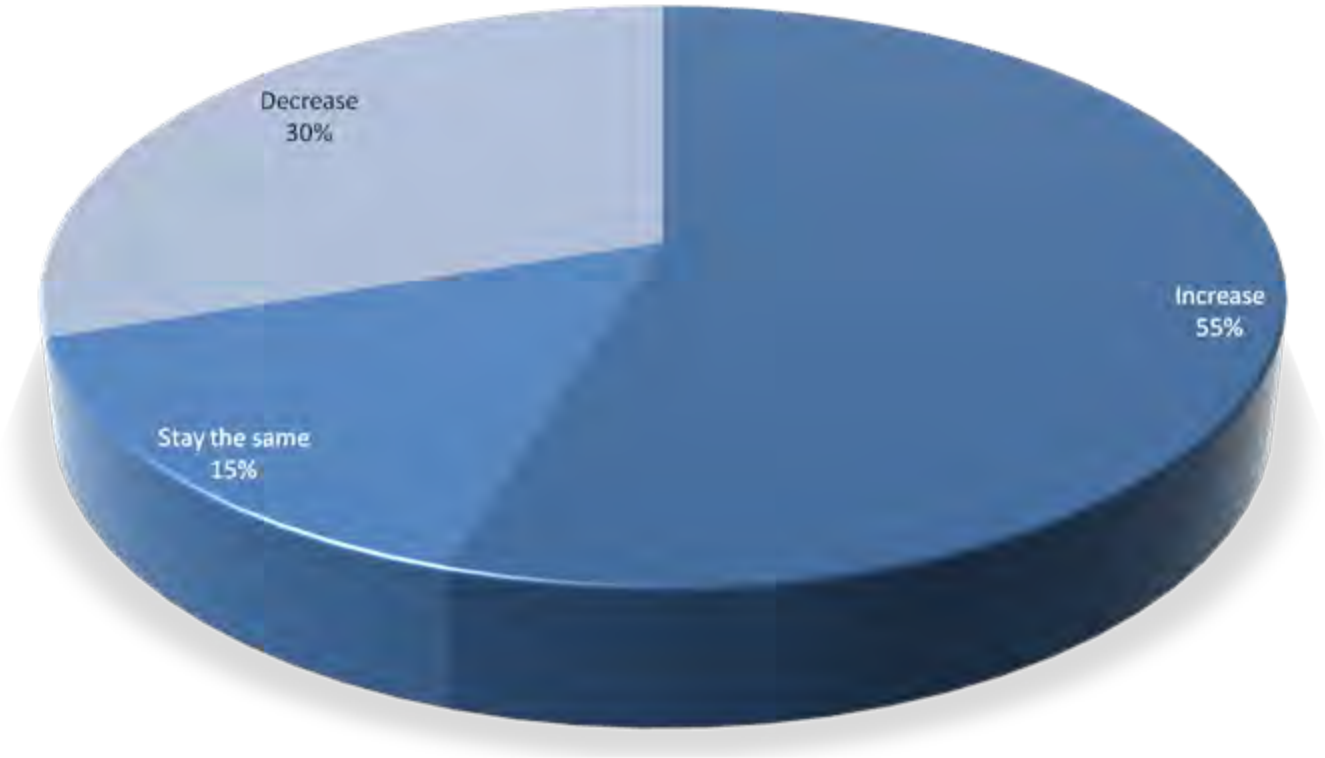
# Training budget

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



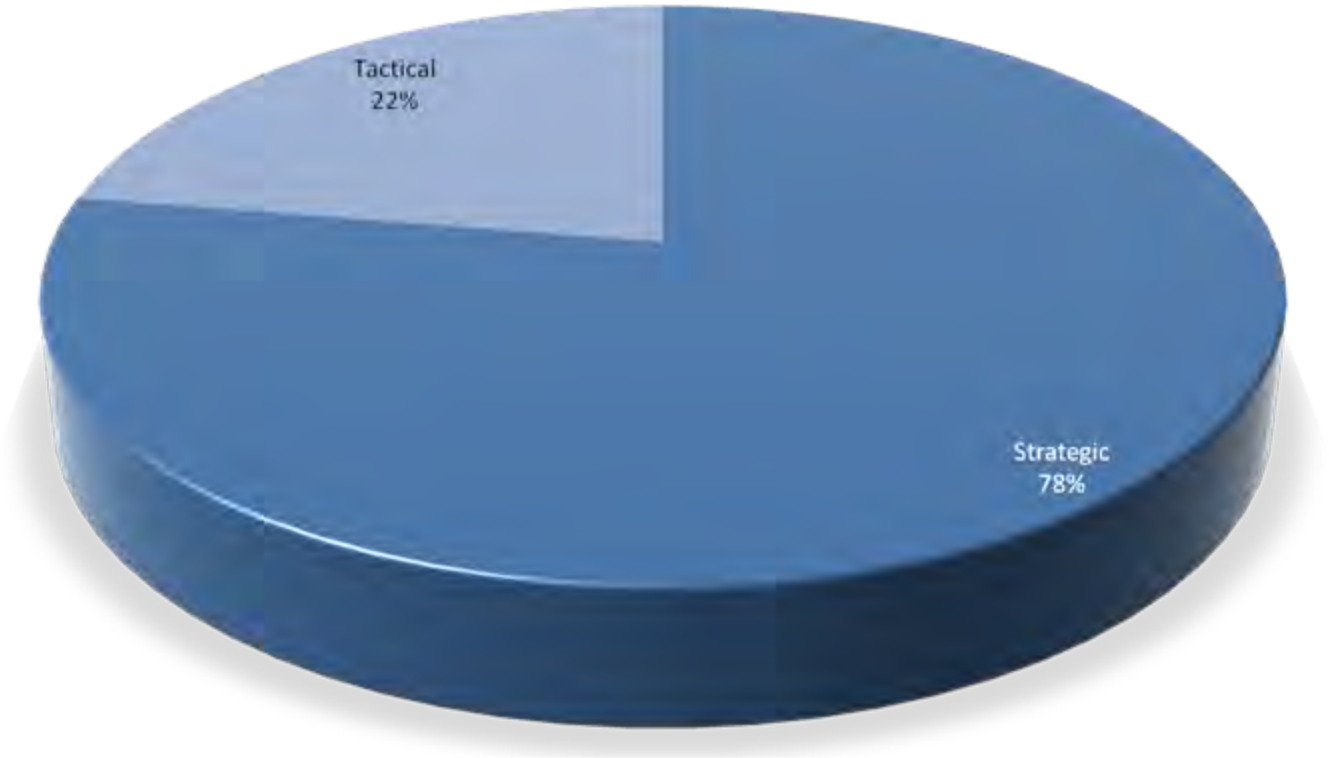
# Training budget

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



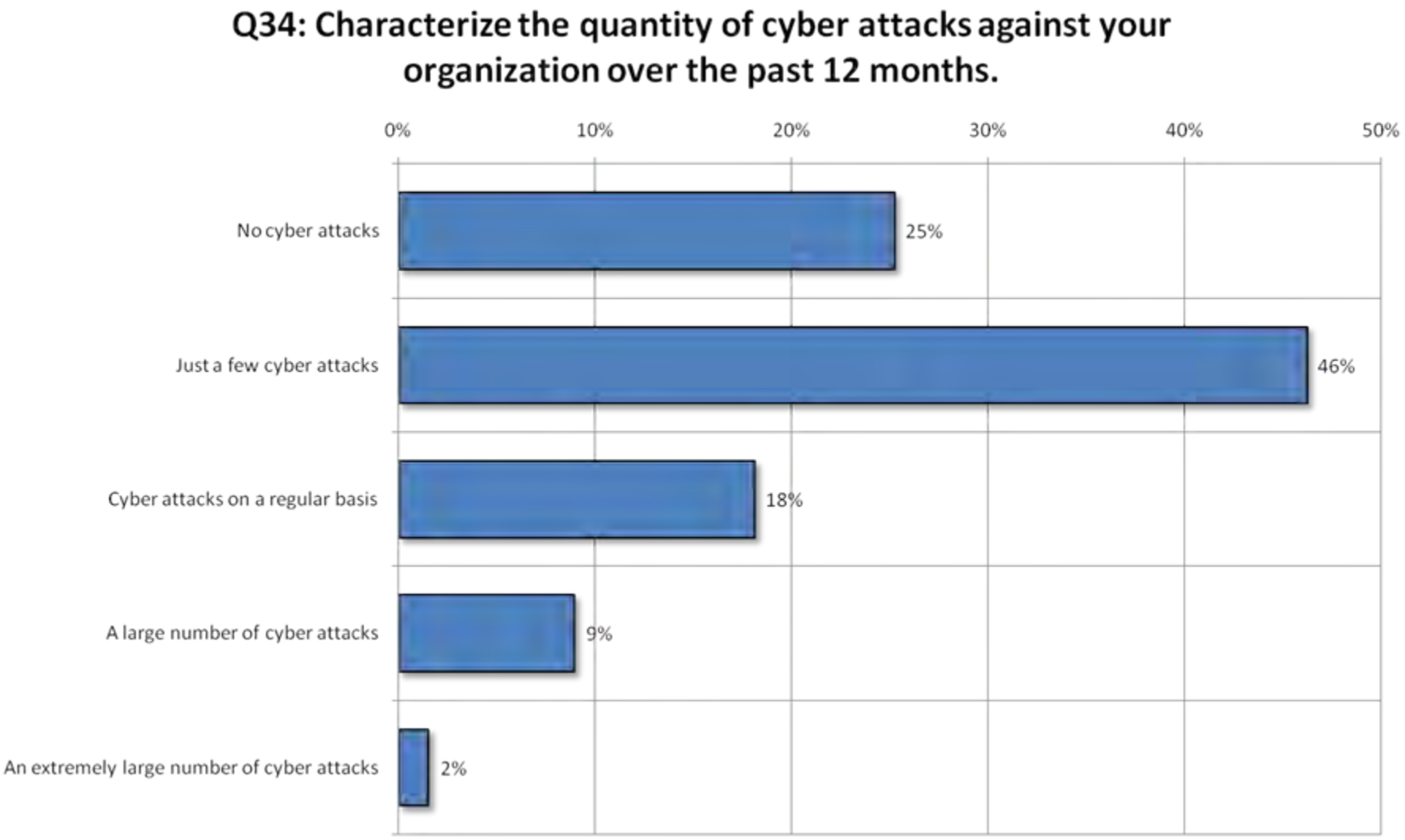
# Training

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

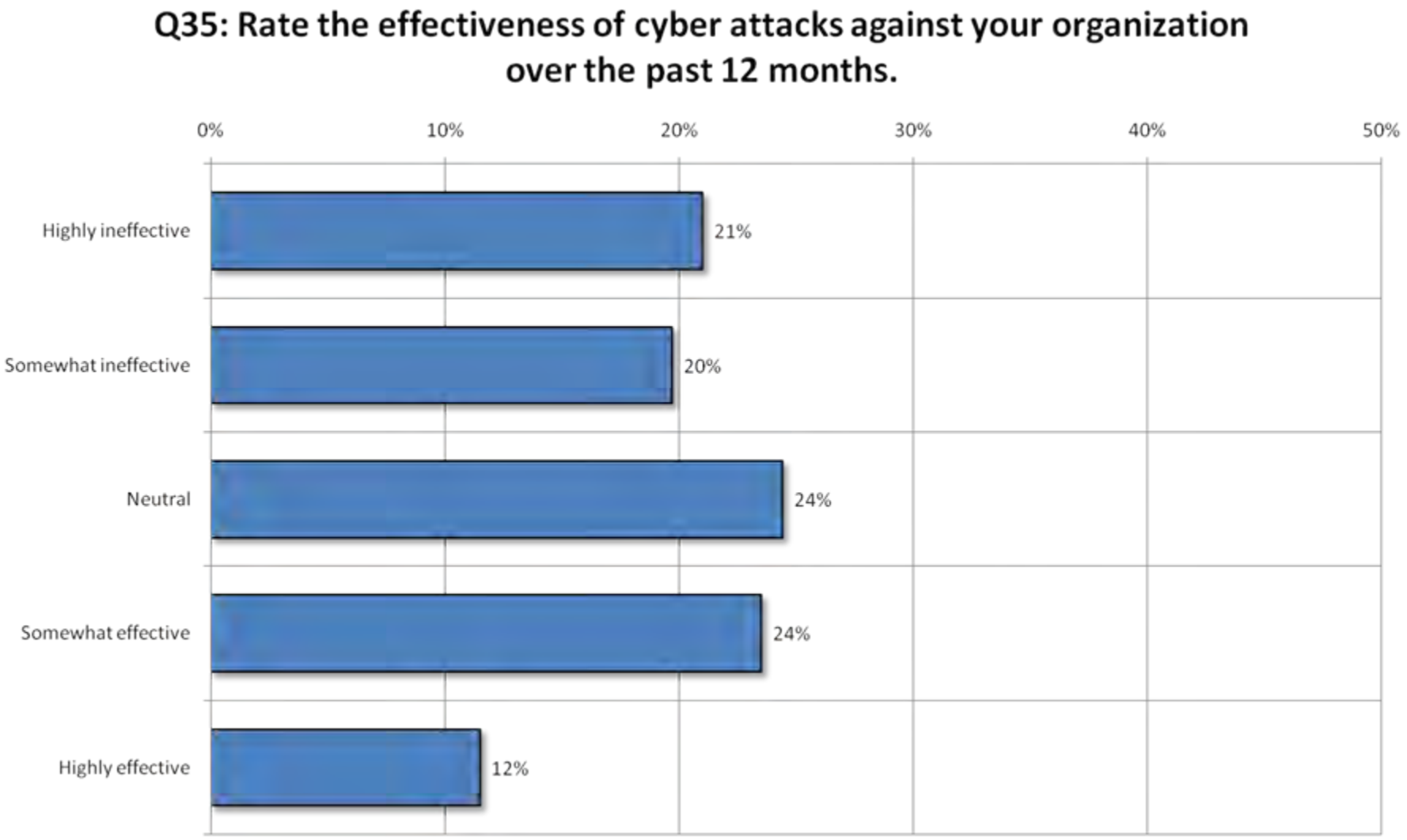


# Attacks & Remediation

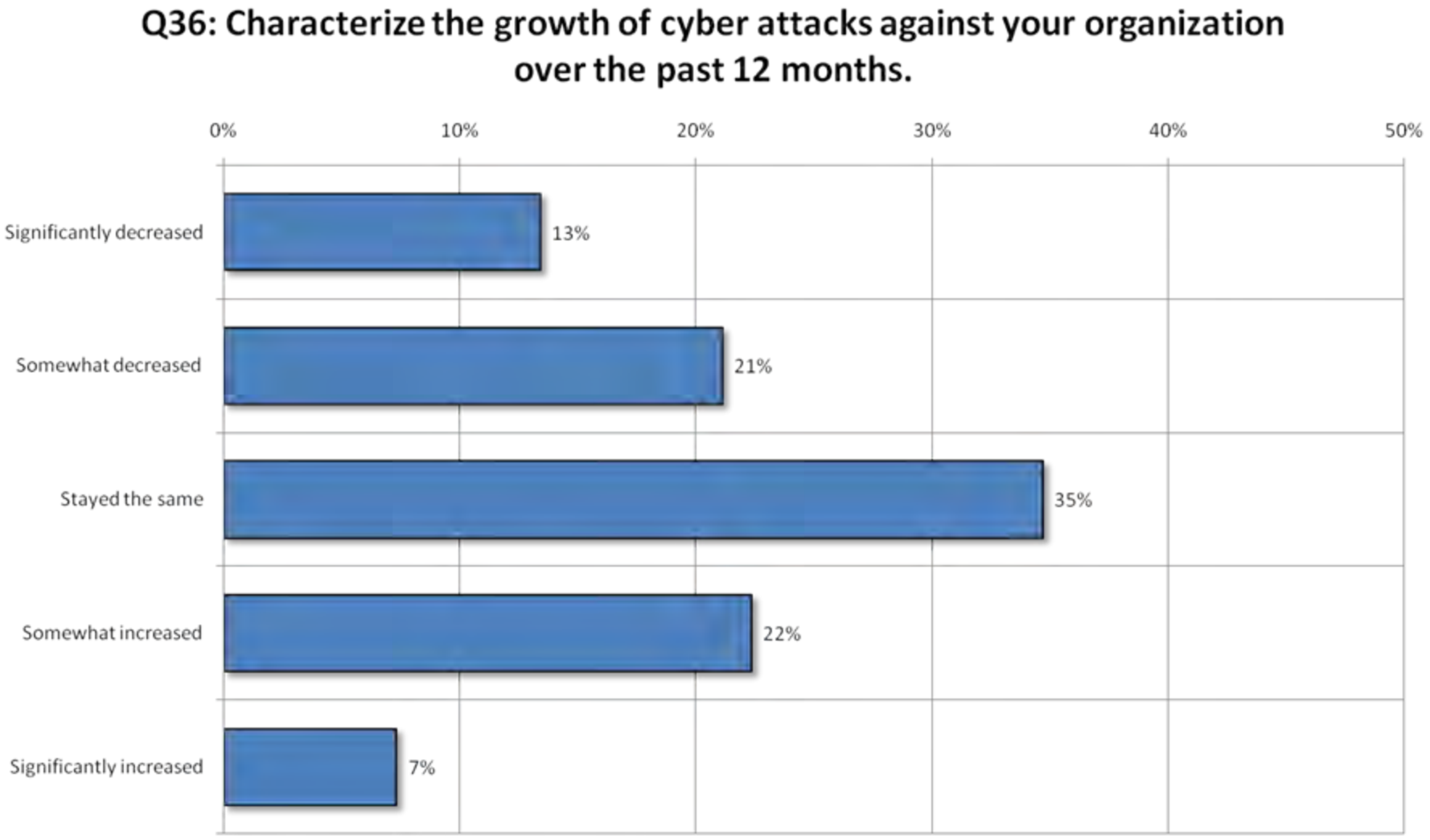
# Cyber attacks



# Cyber attacks

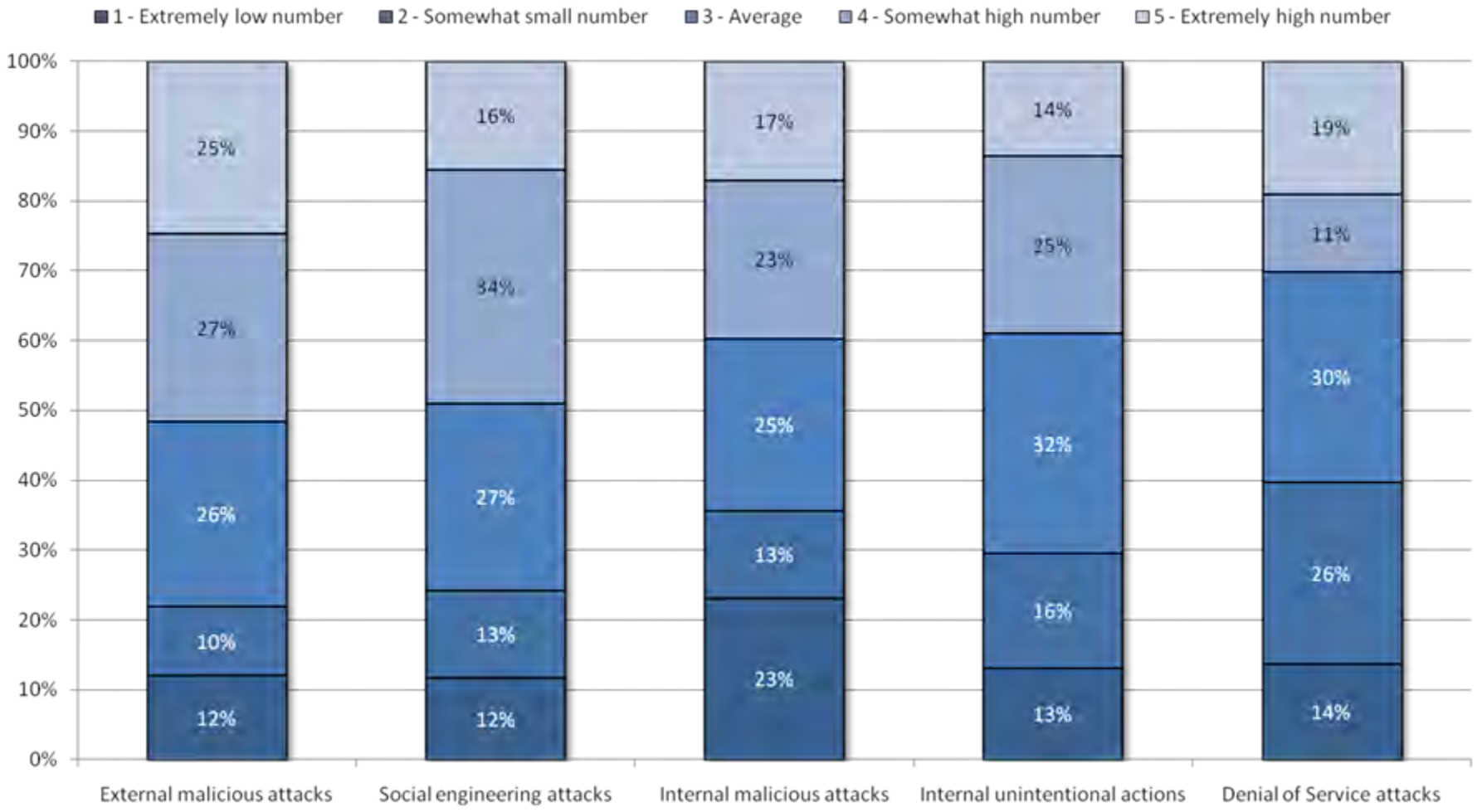


# Cyber attacks

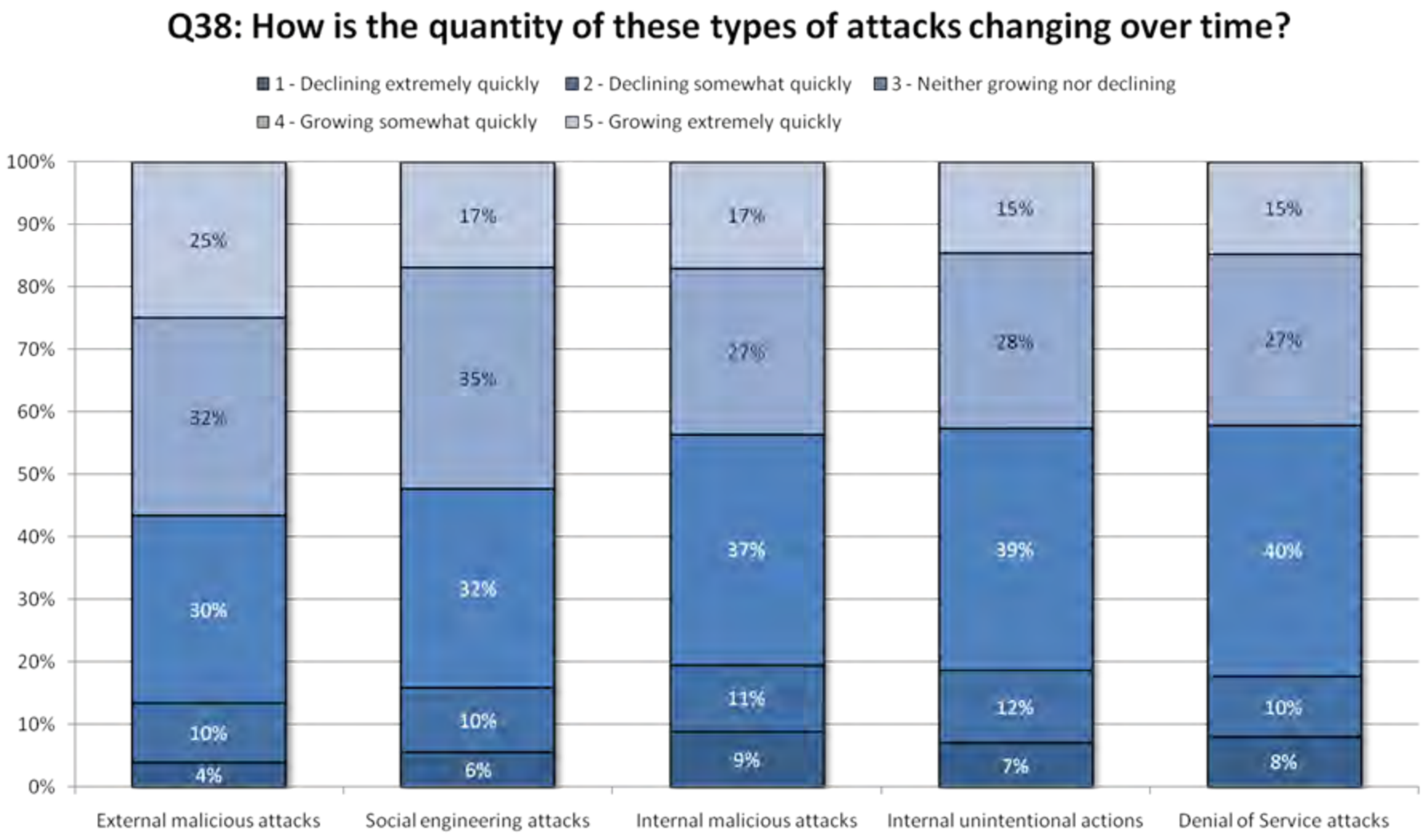


# Cyber attacks

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

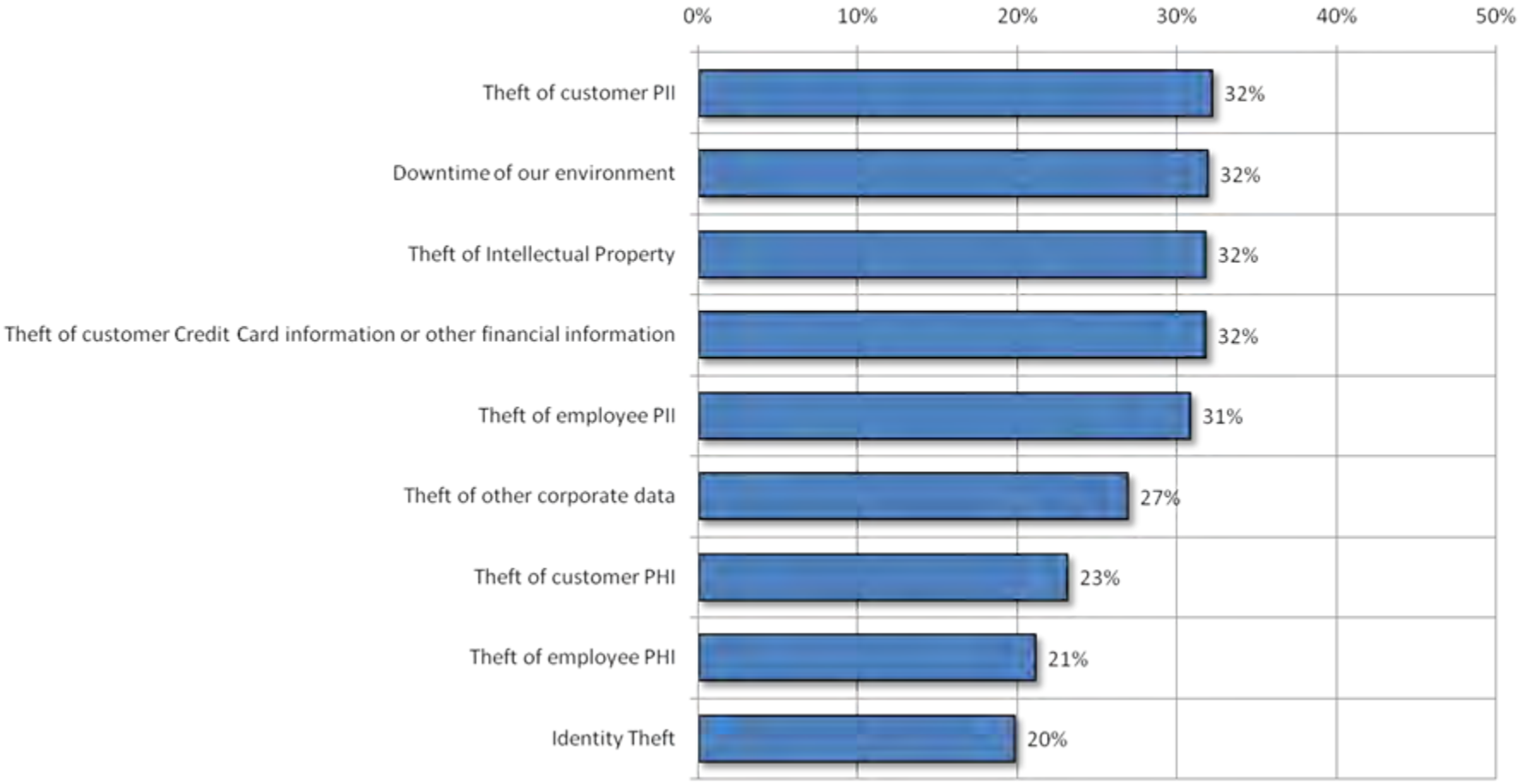


# Cyber attacks



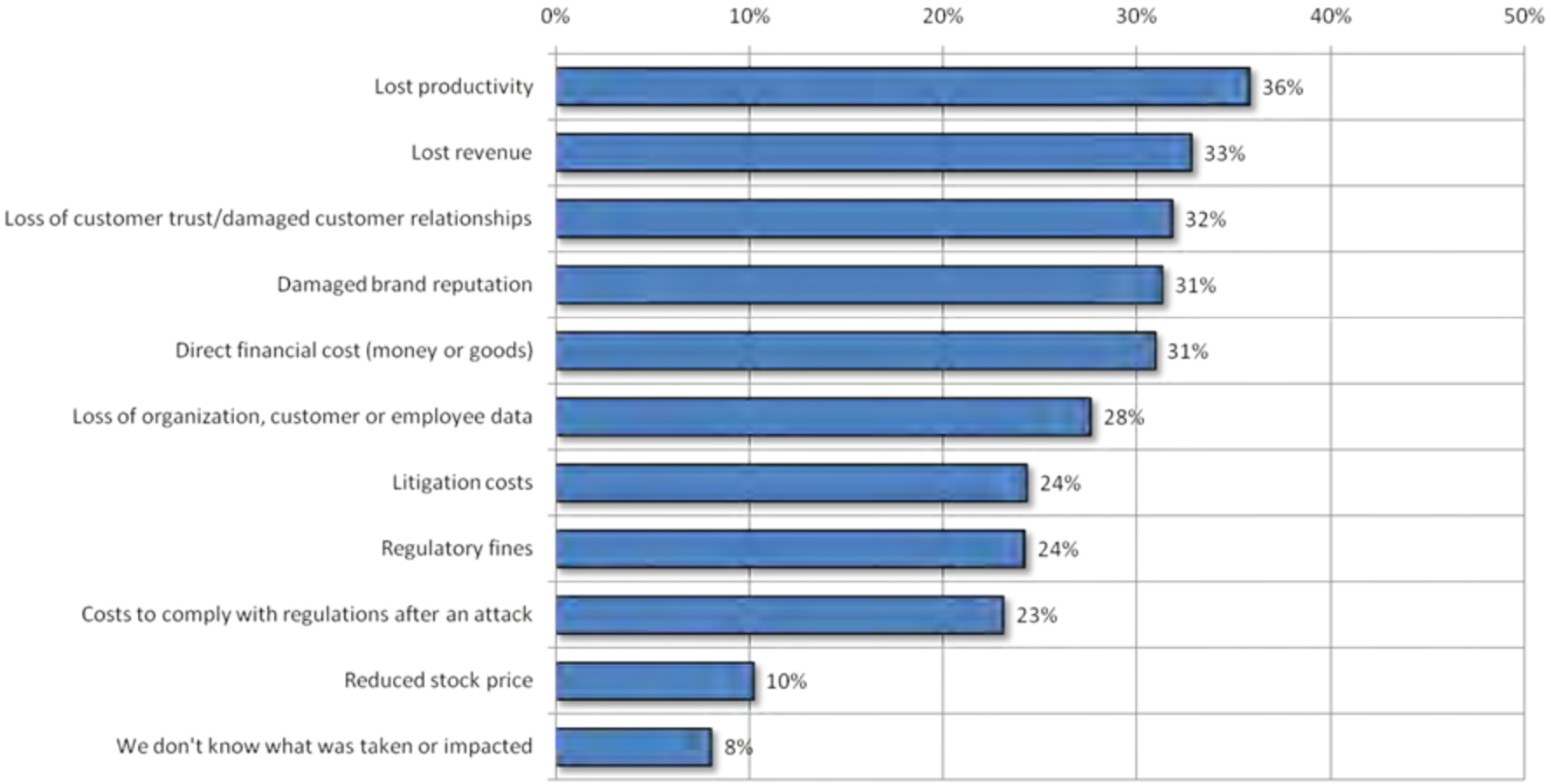
# Cyber losses

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

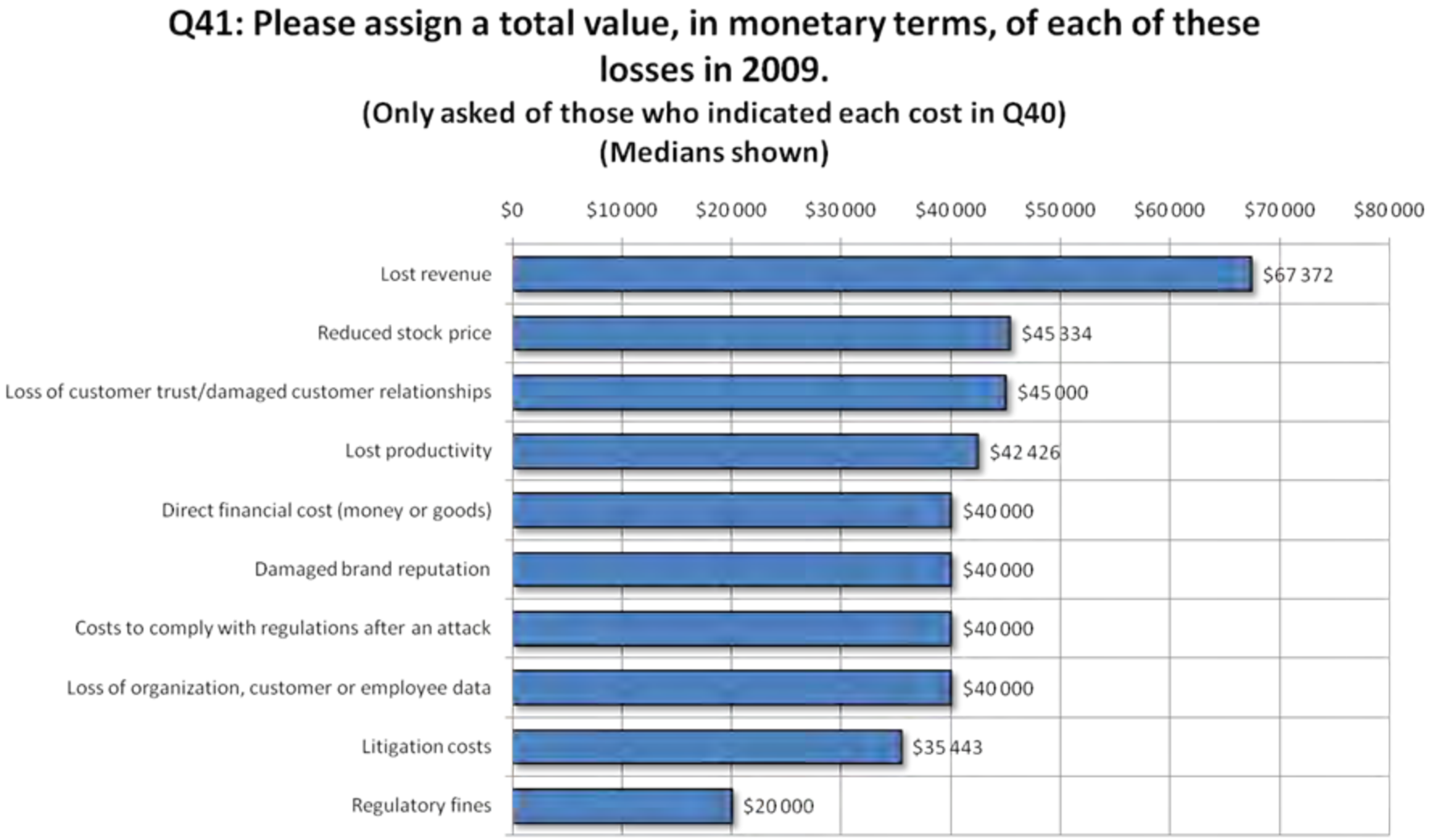


# Cyber attack costs

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

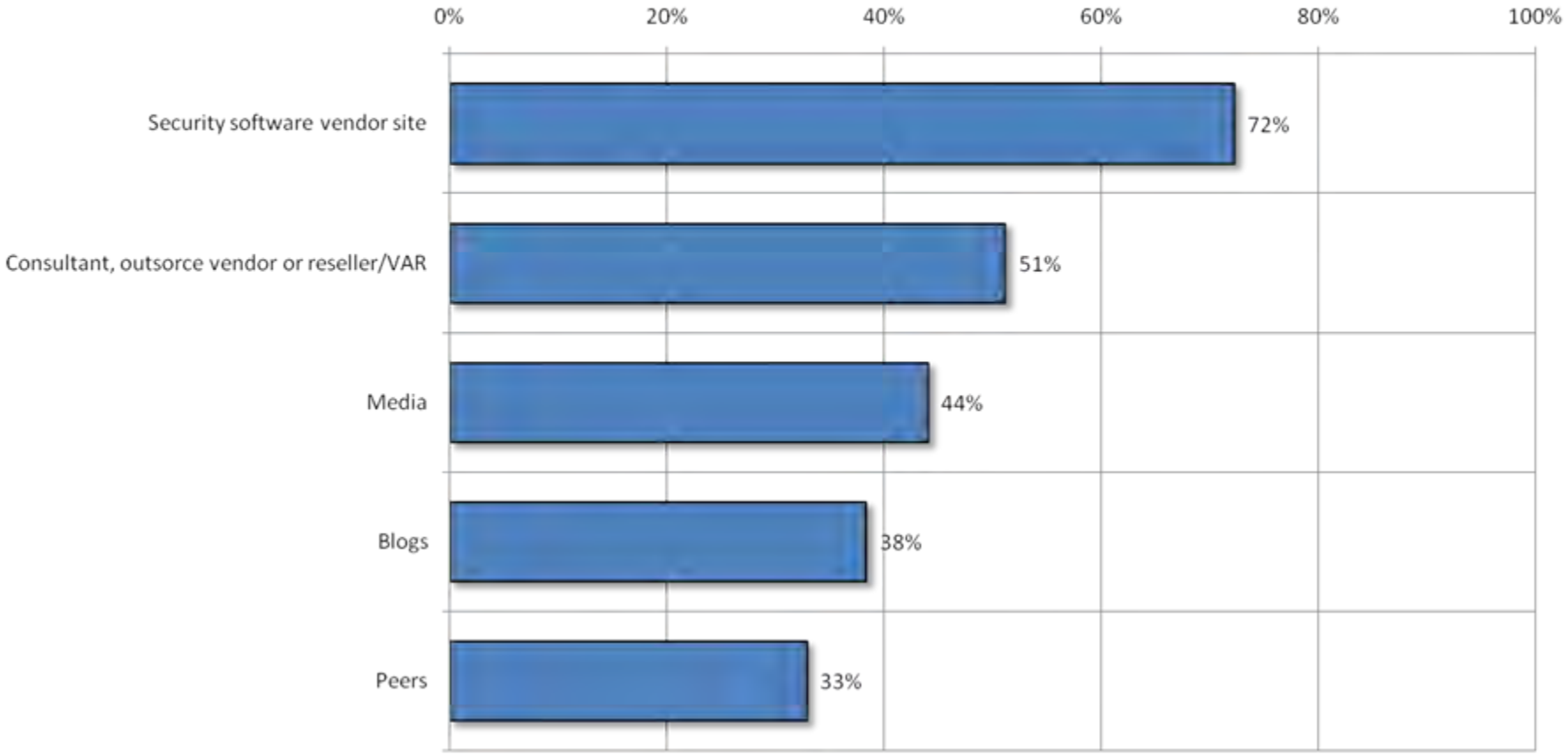


# Cyber attack costs



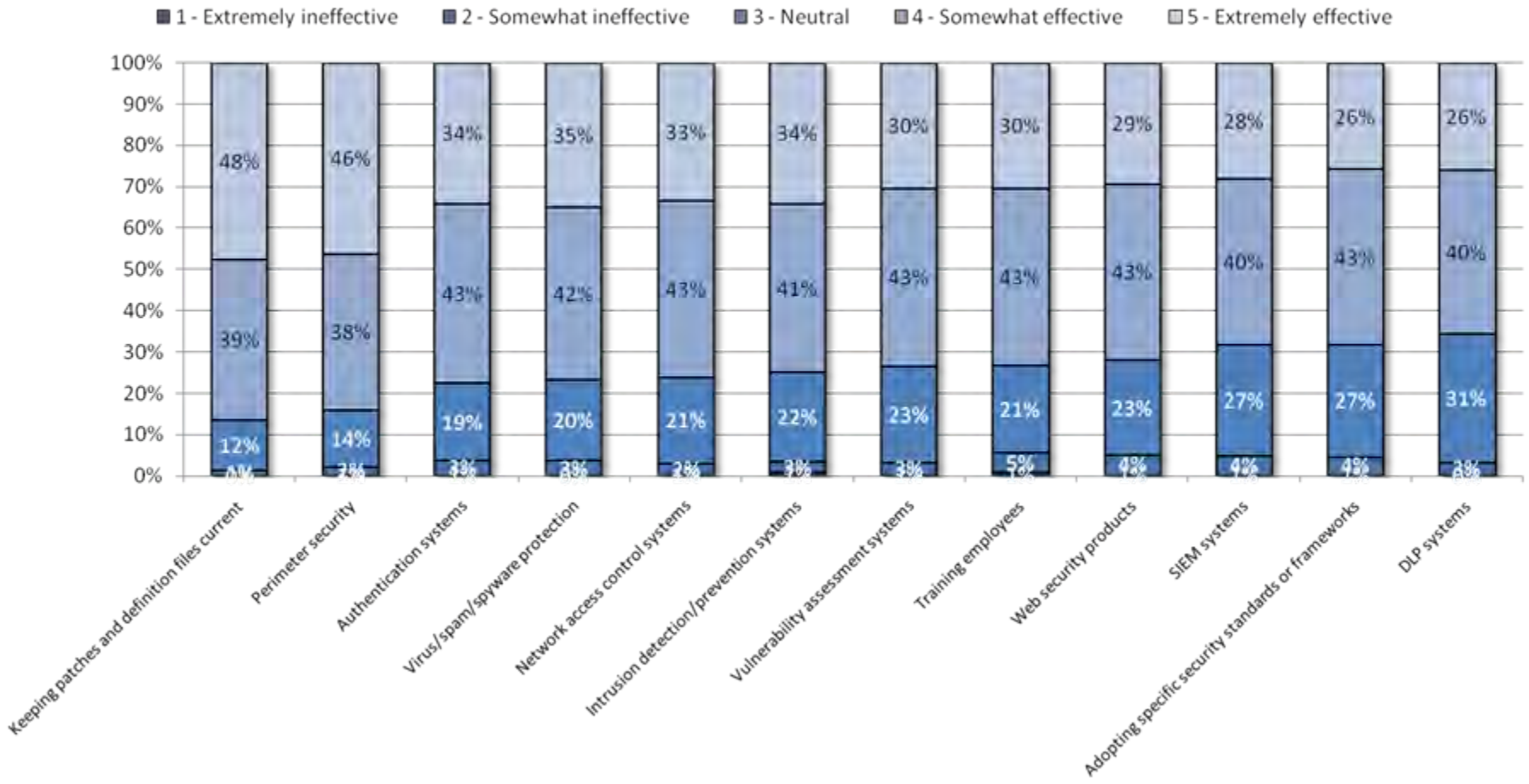
# Cyber attack info

**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.**



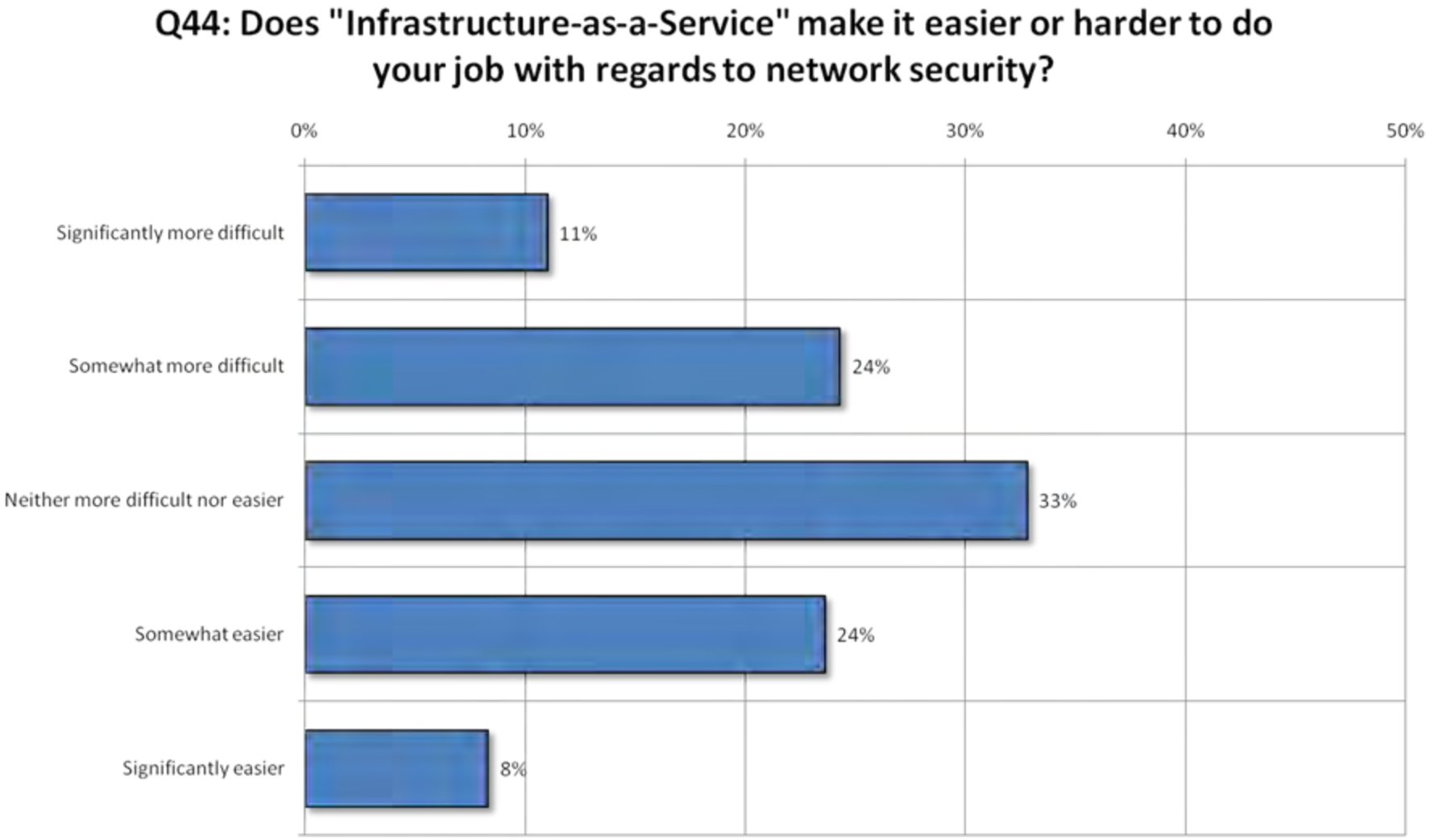
# Safeguards

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

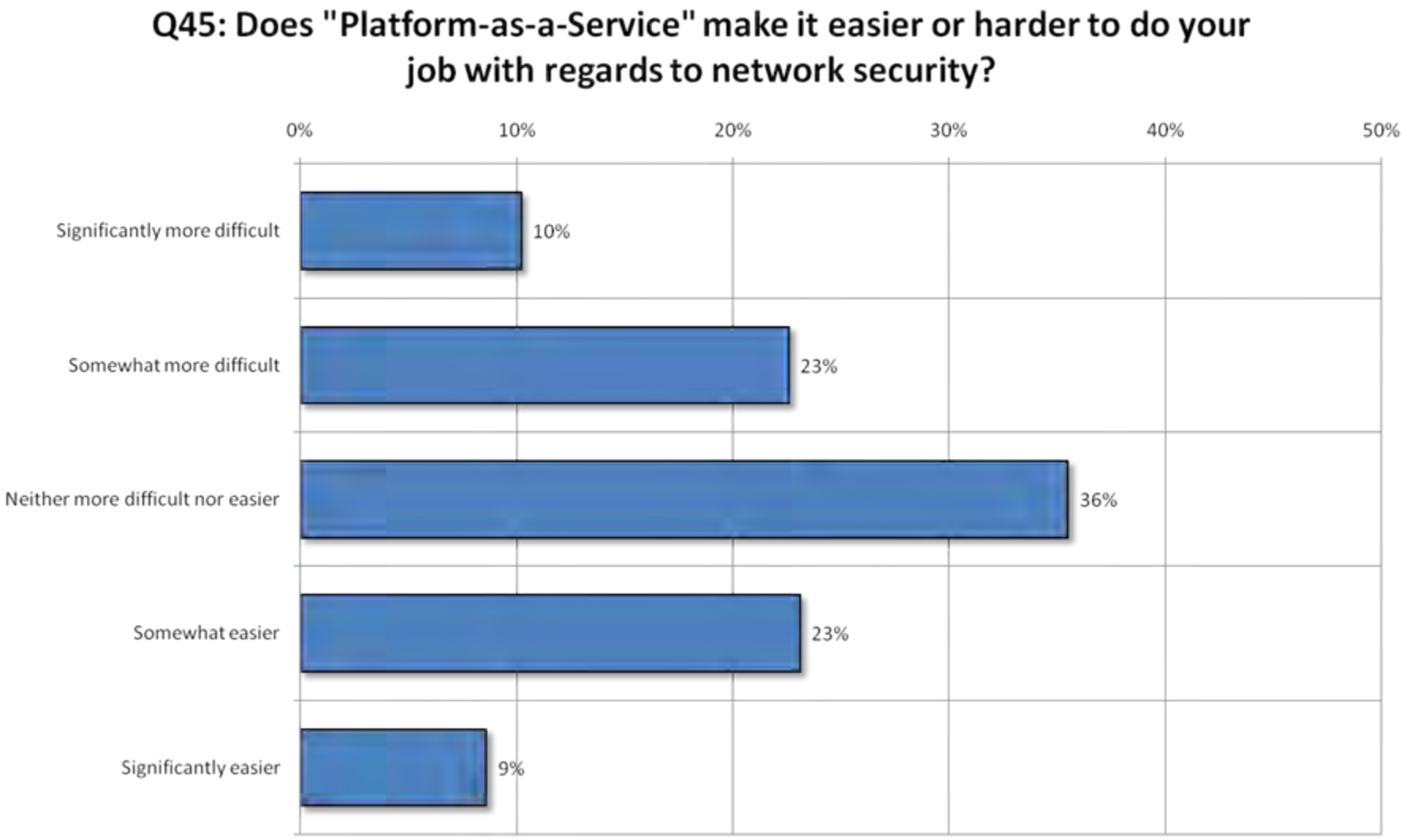


# Network Security

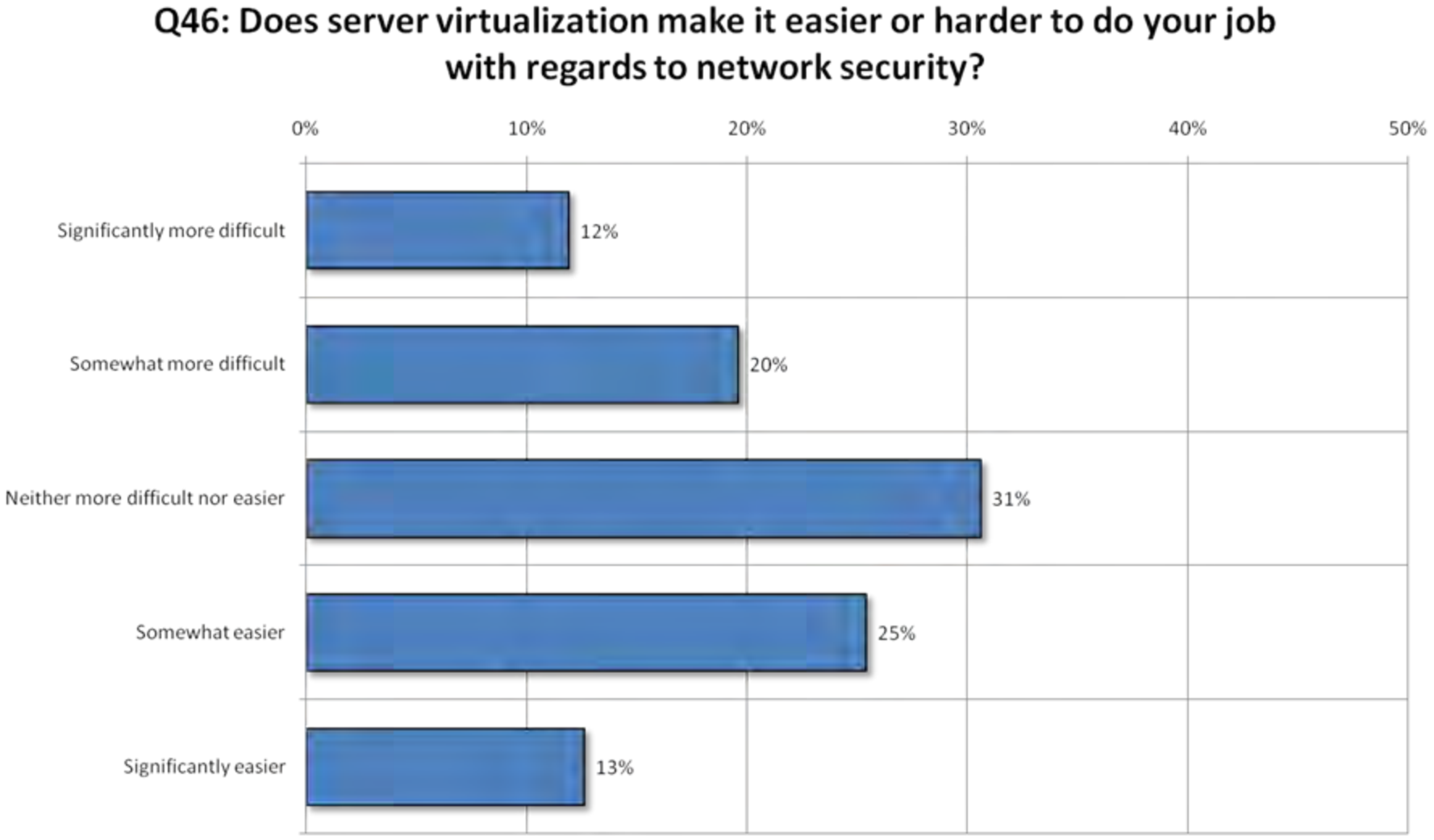
# IaaS and network security



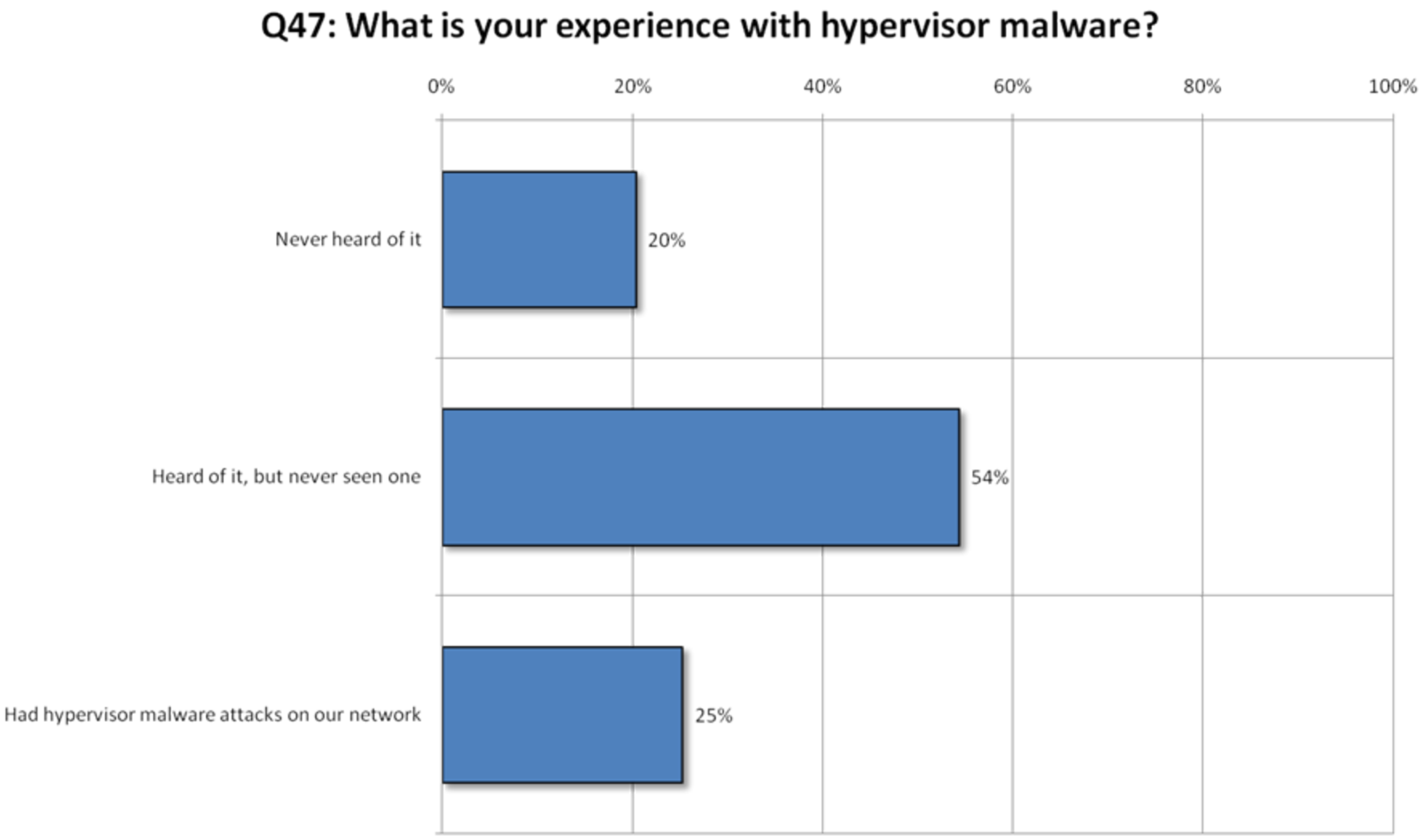
# PaaS and network security



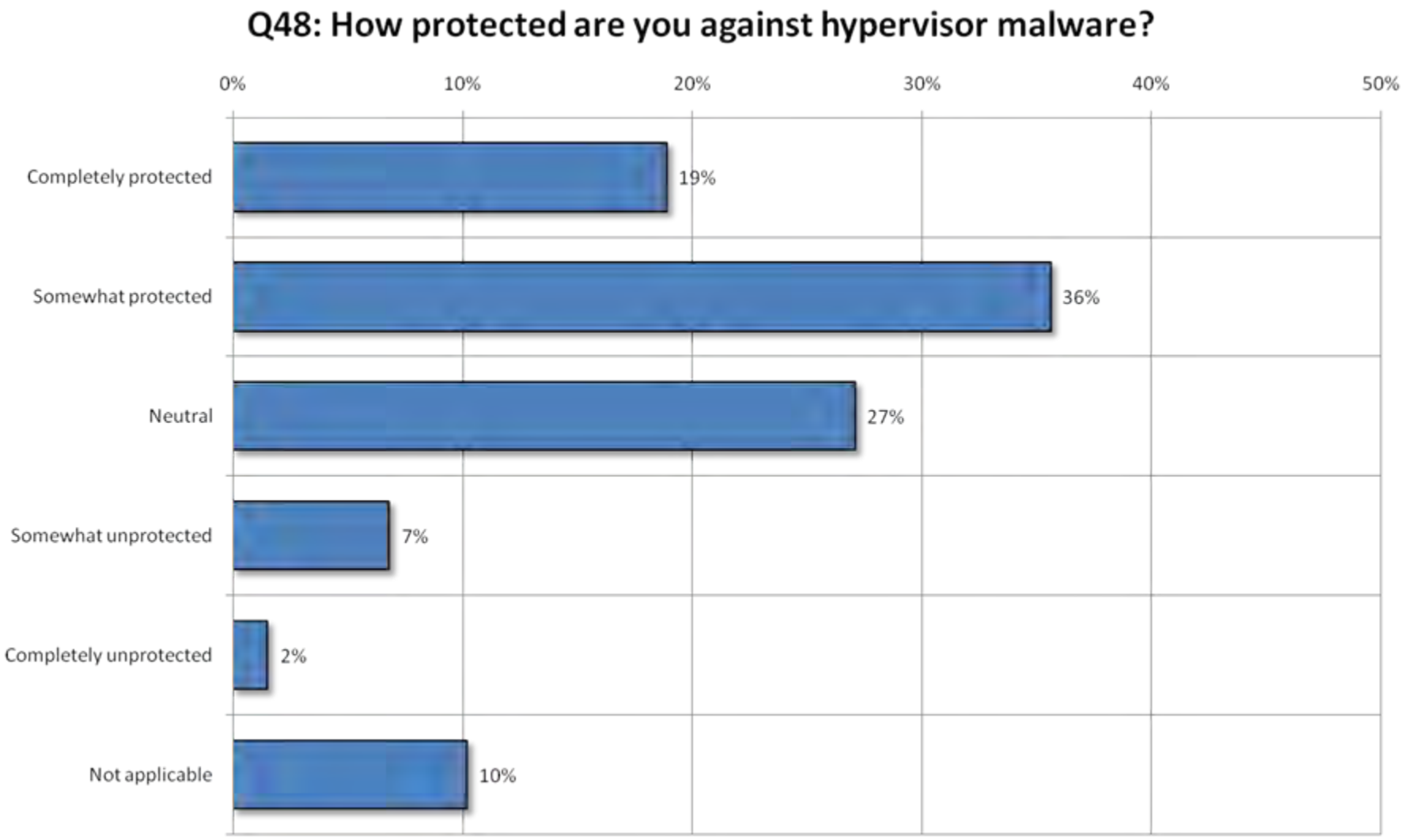
# Server virtualization and network security



# Hypervisor malware

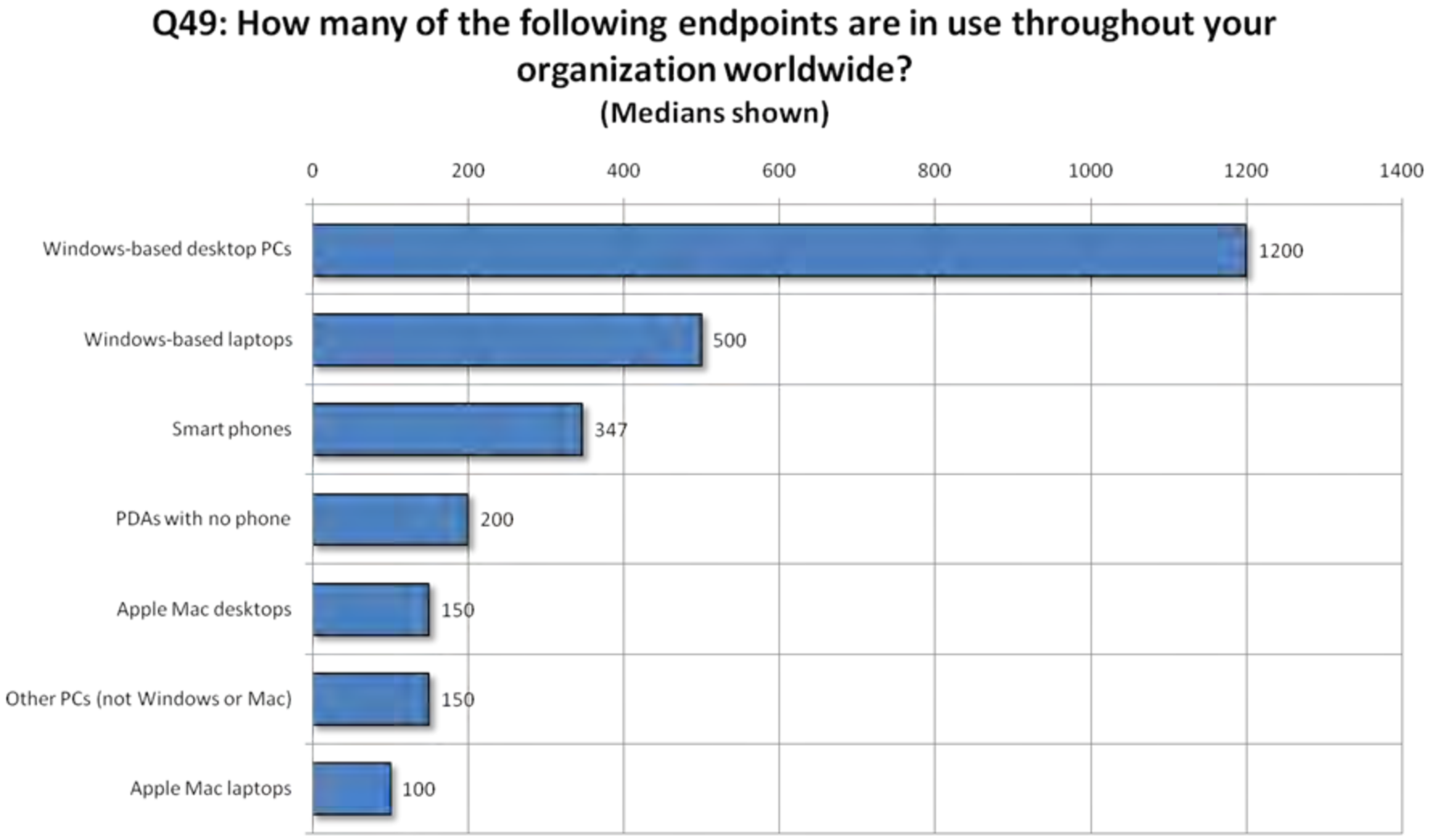


# Hypervisor malware



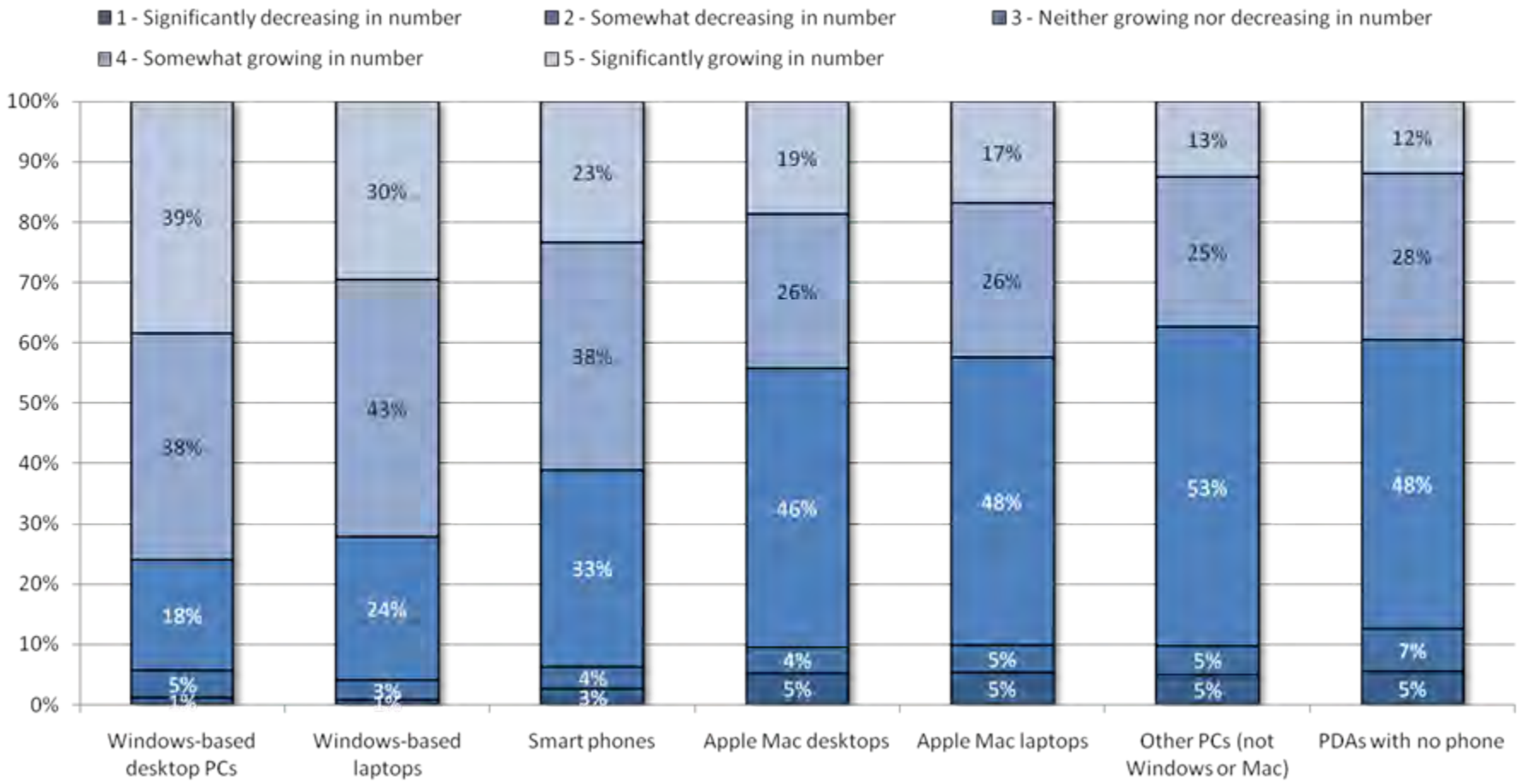
# Endpoint Security

# Endpoint types



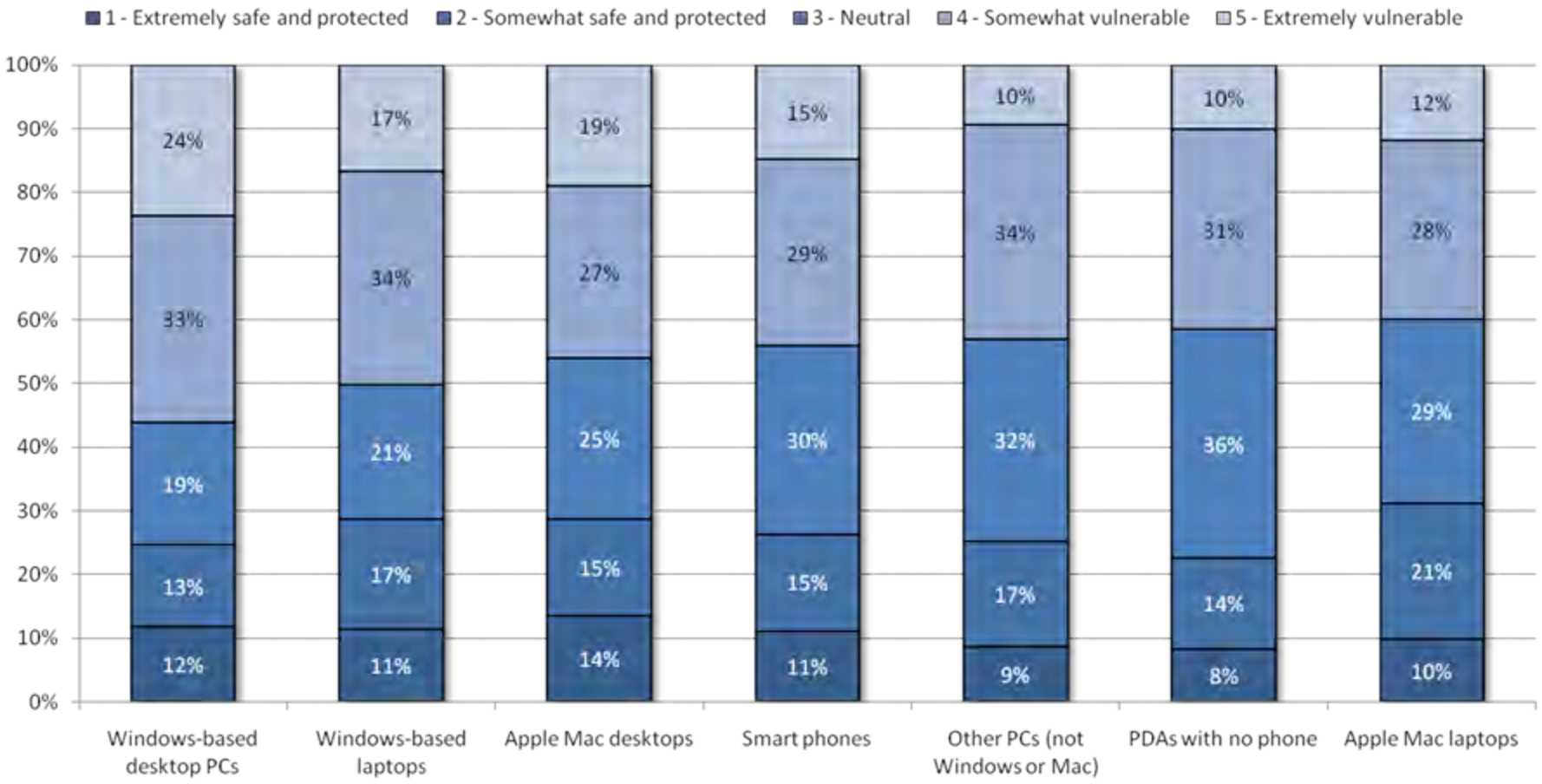
# Endpoint types

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

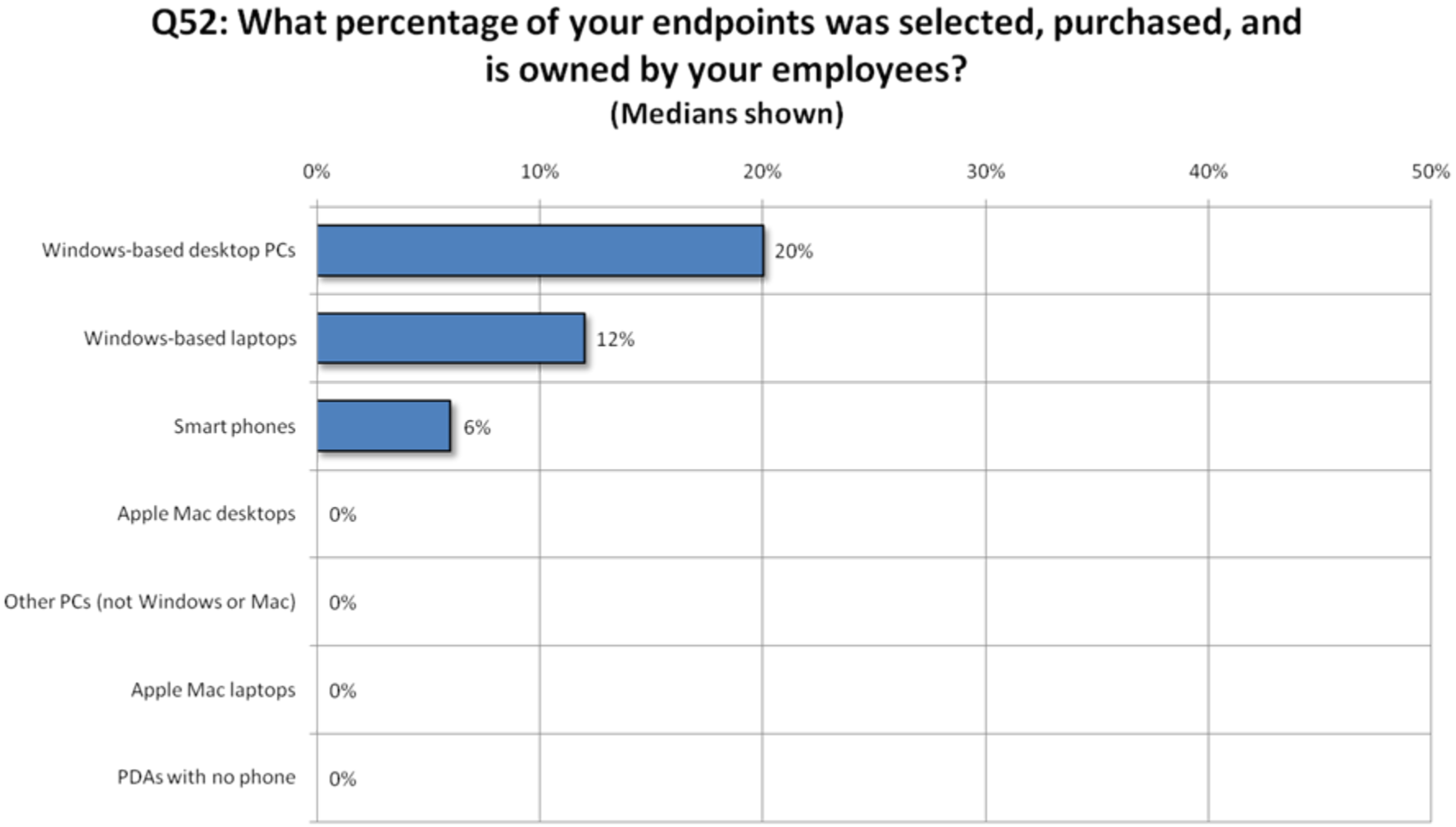


# Endpoint vulnerability

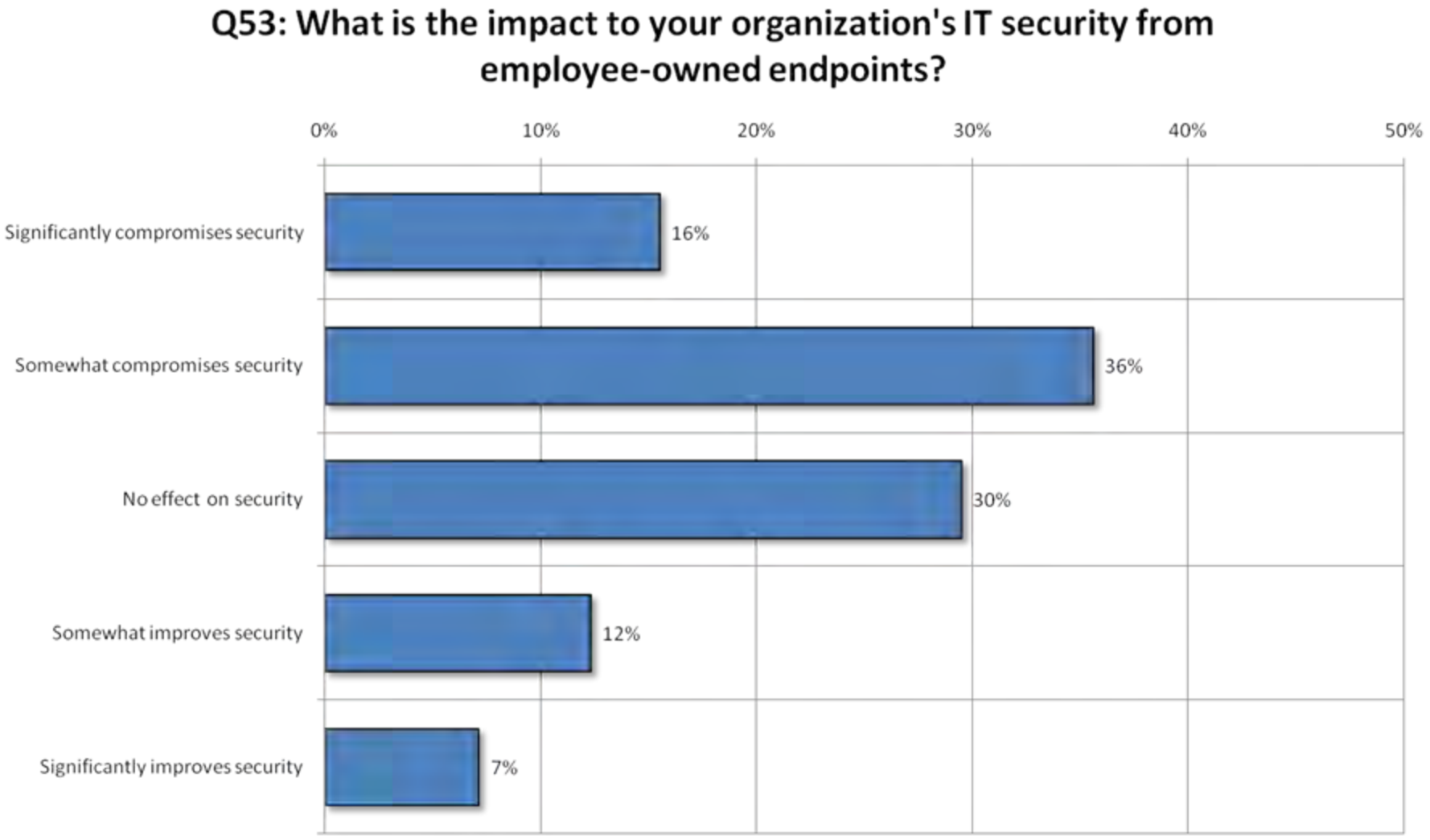
## Q51: How vulnerable are each of these endpoints? (Asked only for those endpoints used)



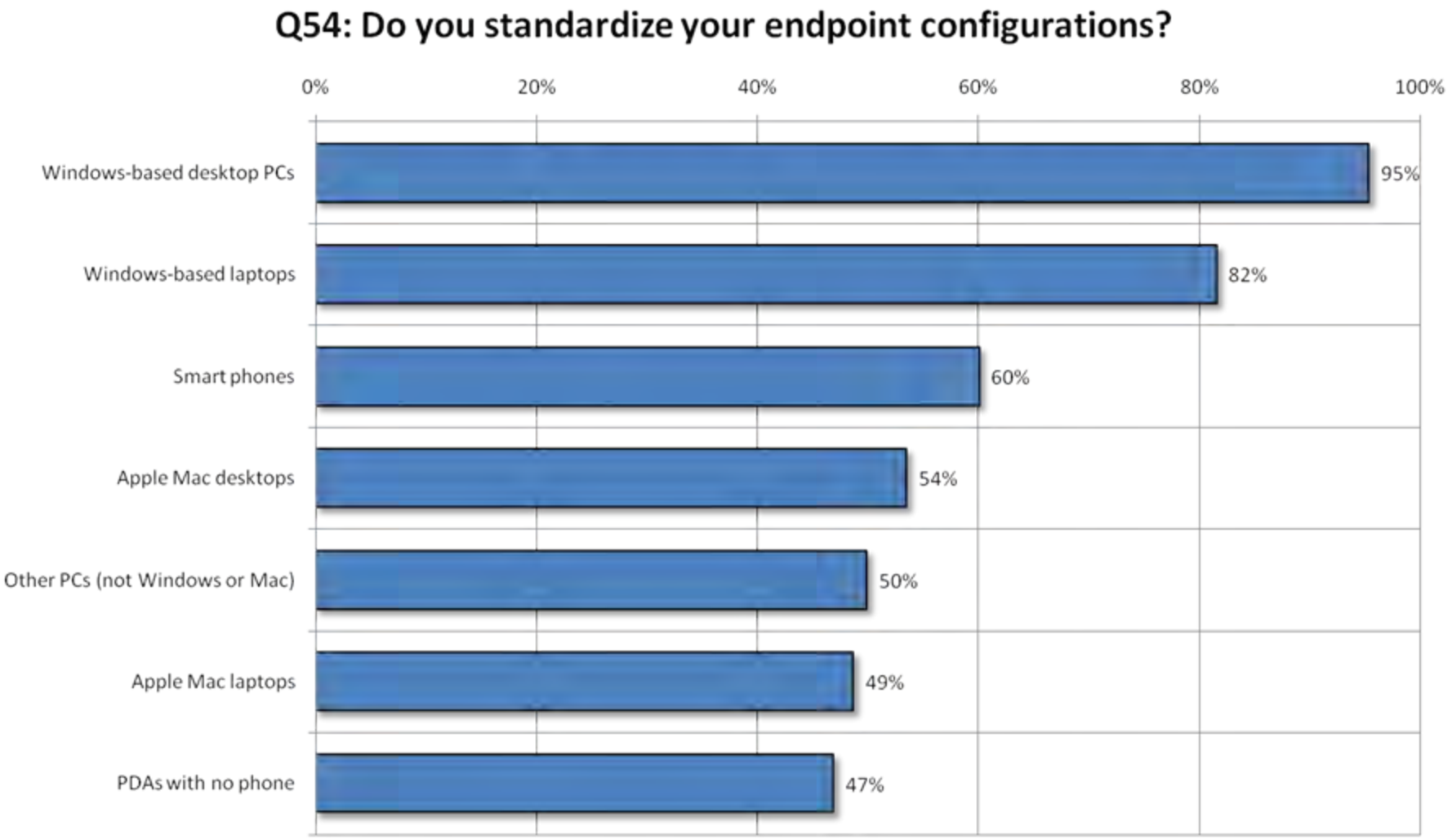
# Employee-owned endpoints



# Employee-owned endpoints

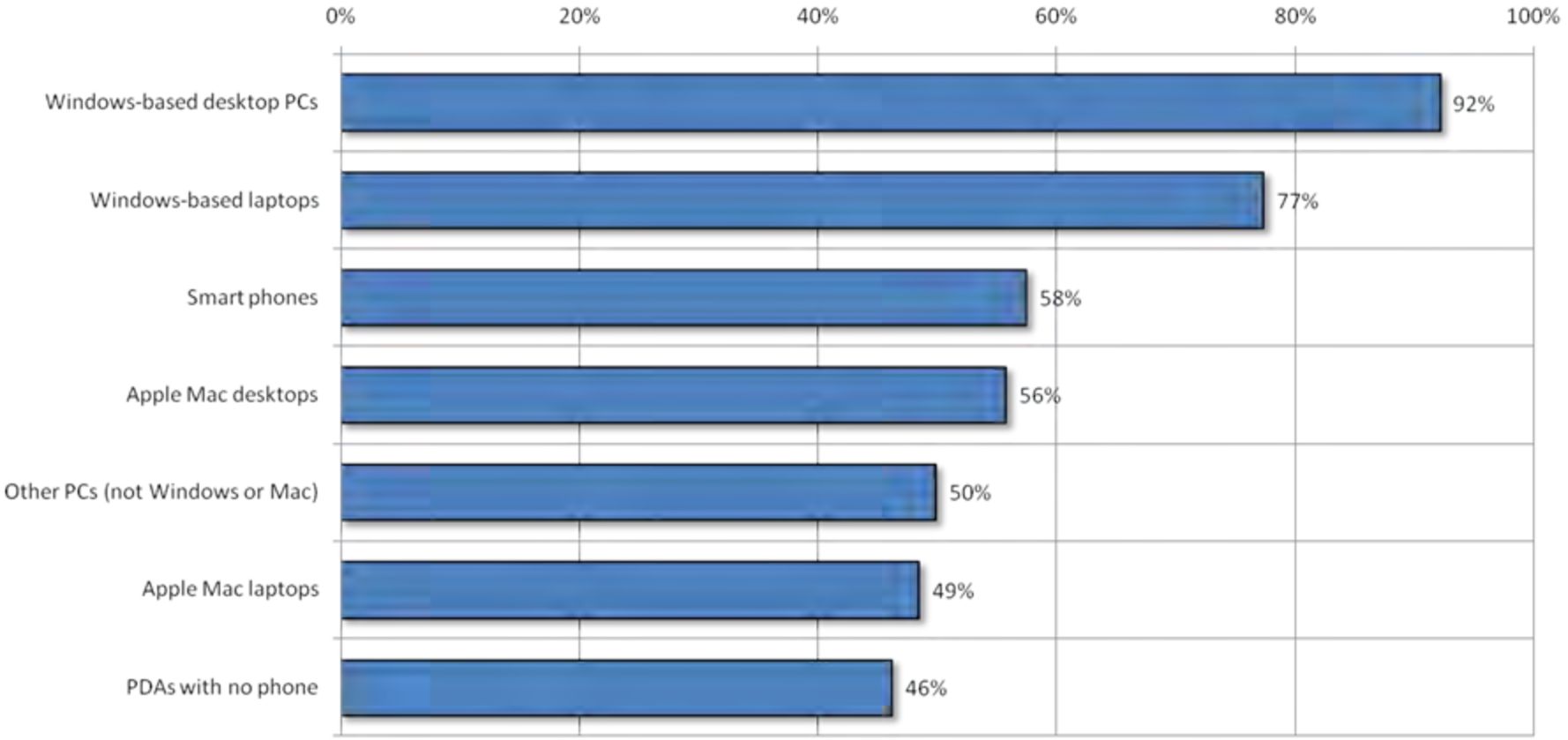


# Endpoint standardization

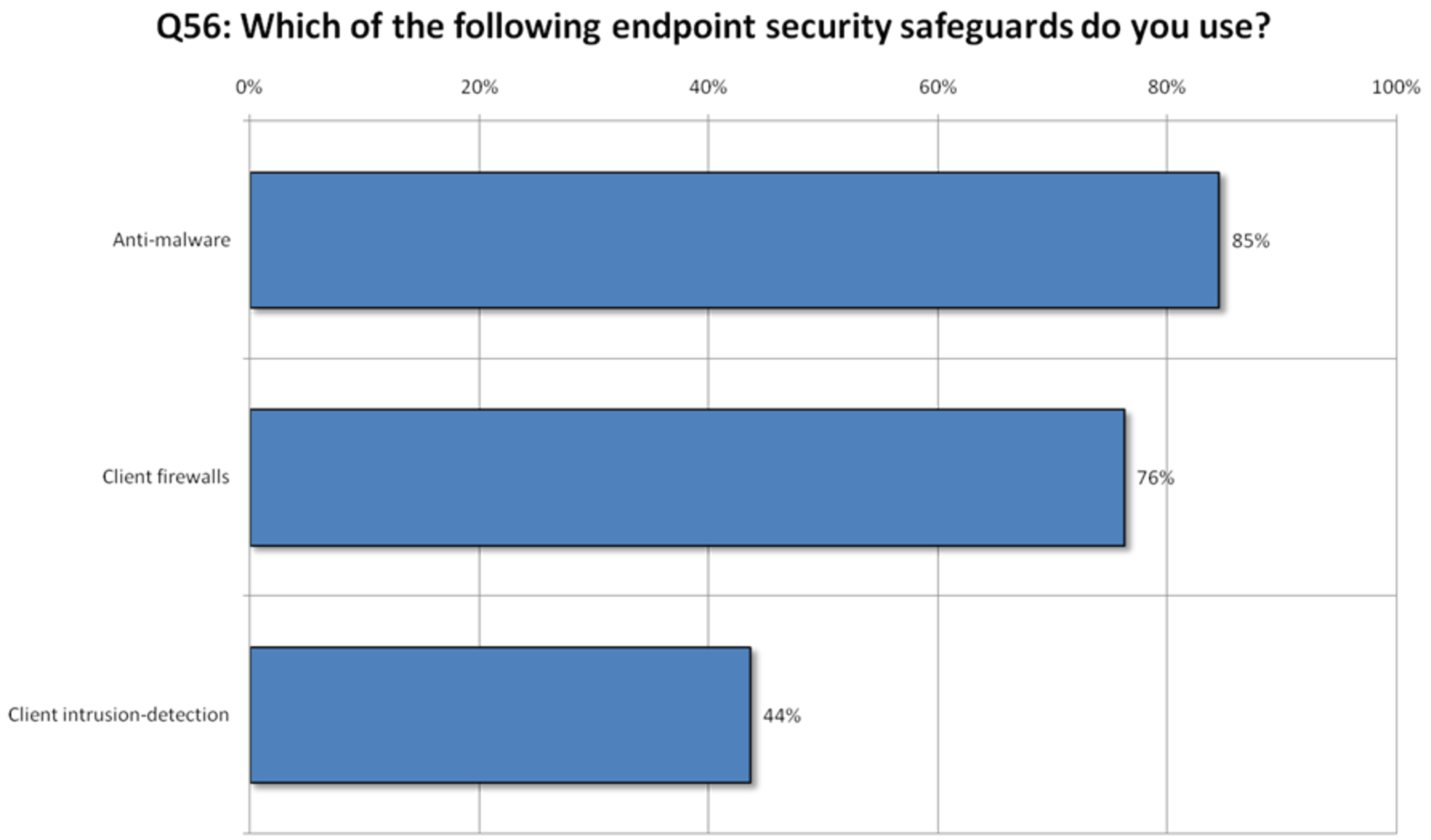


# Endpoint control

**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?**

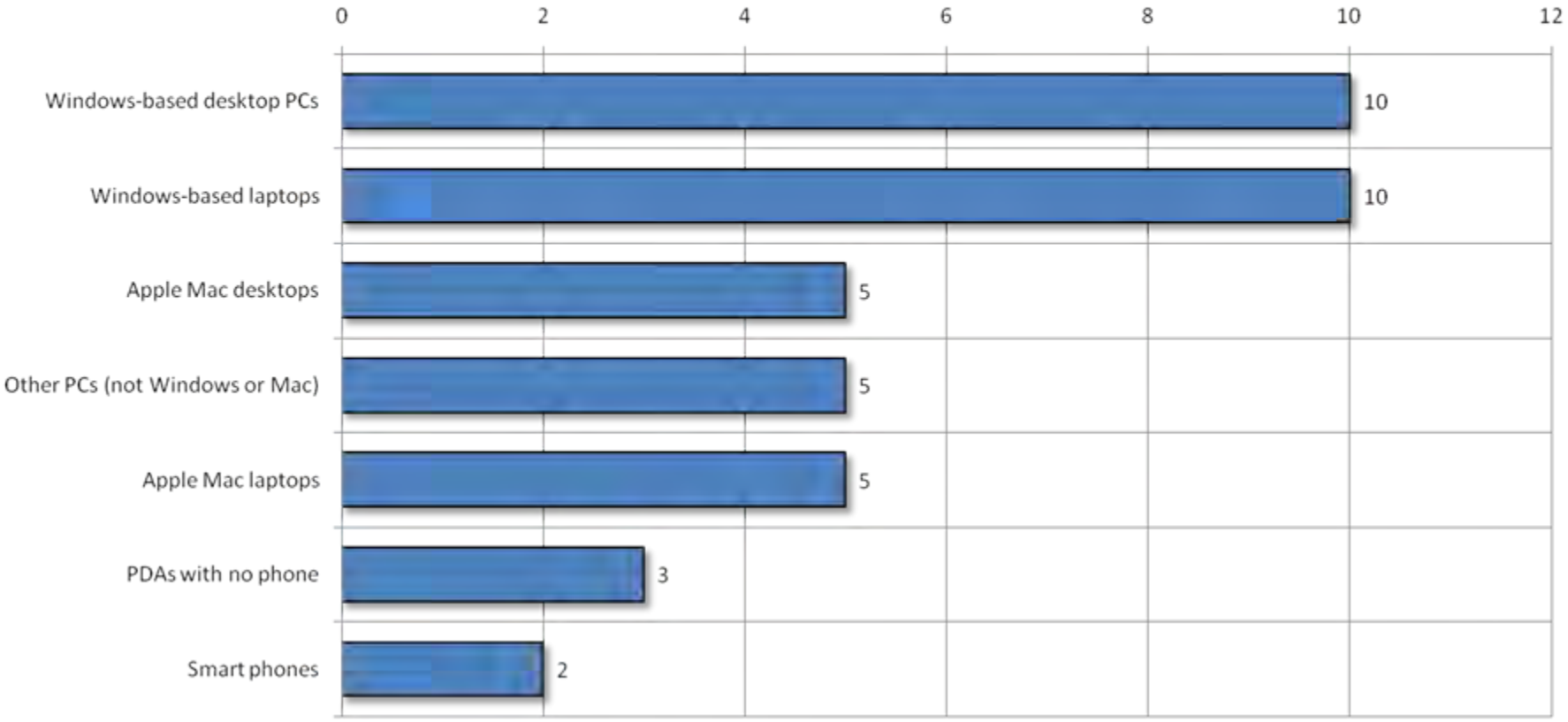


# Endpoint safeguards

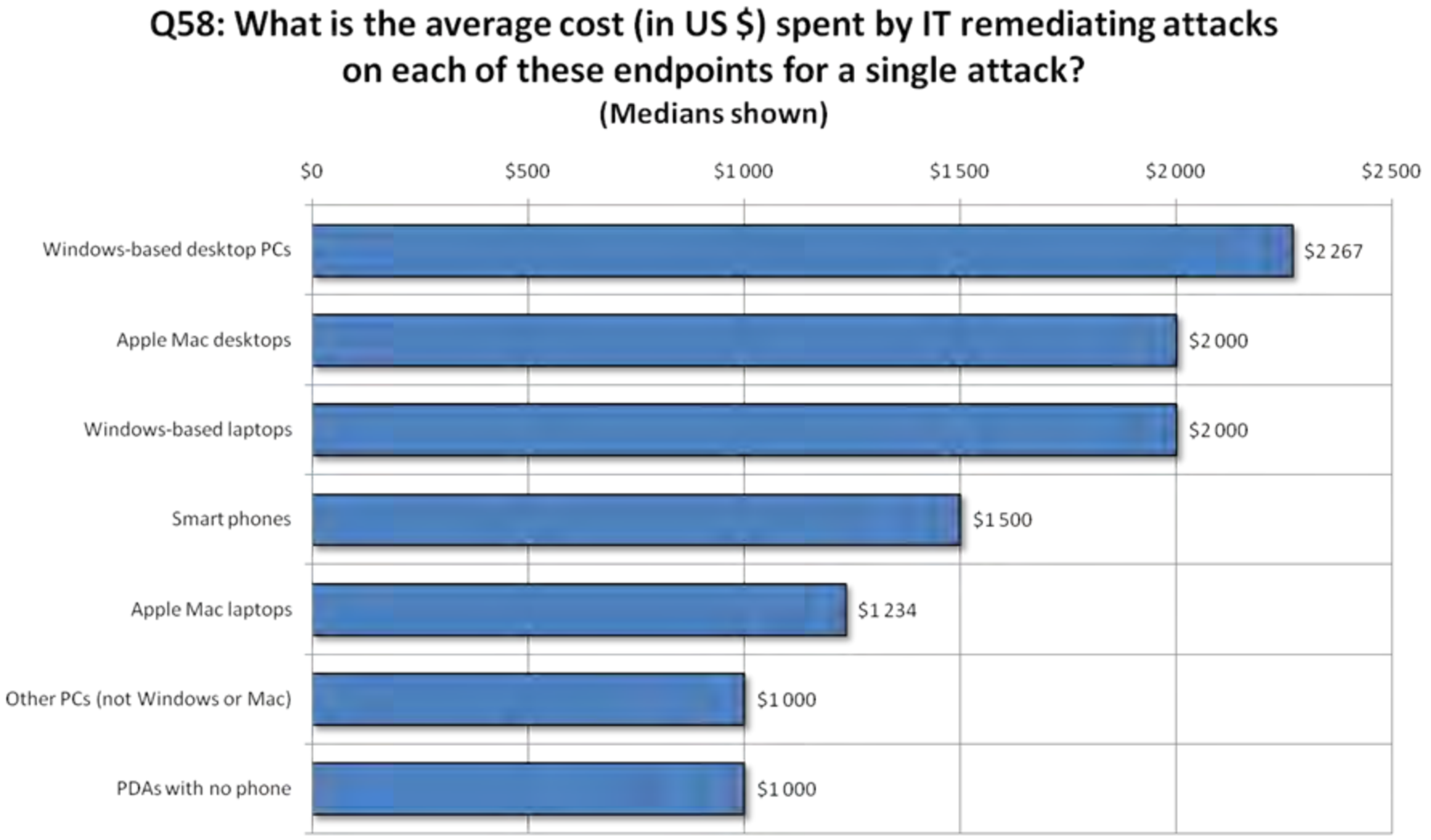


# Endpoint attacks

**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)**



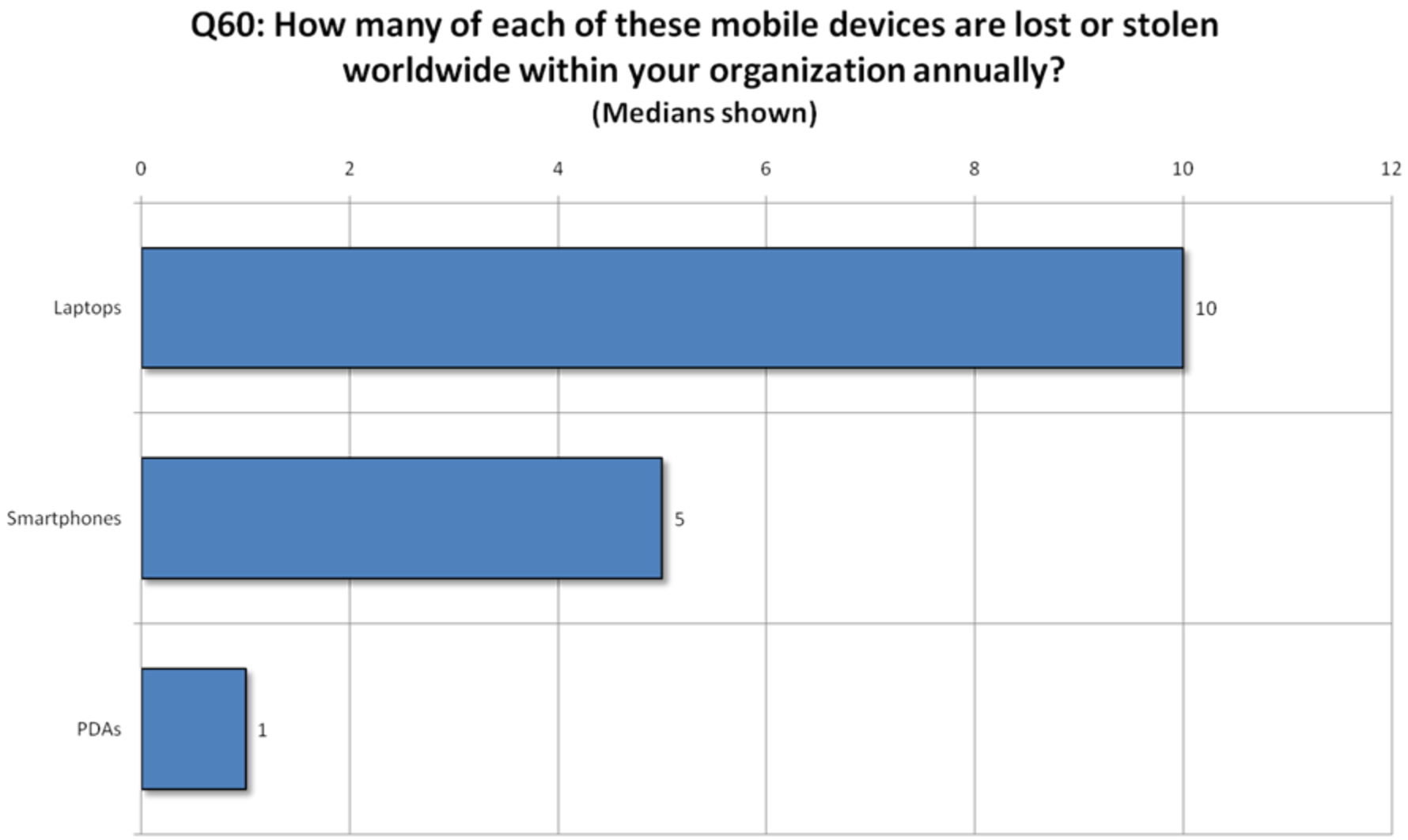
# Attack remediation costs



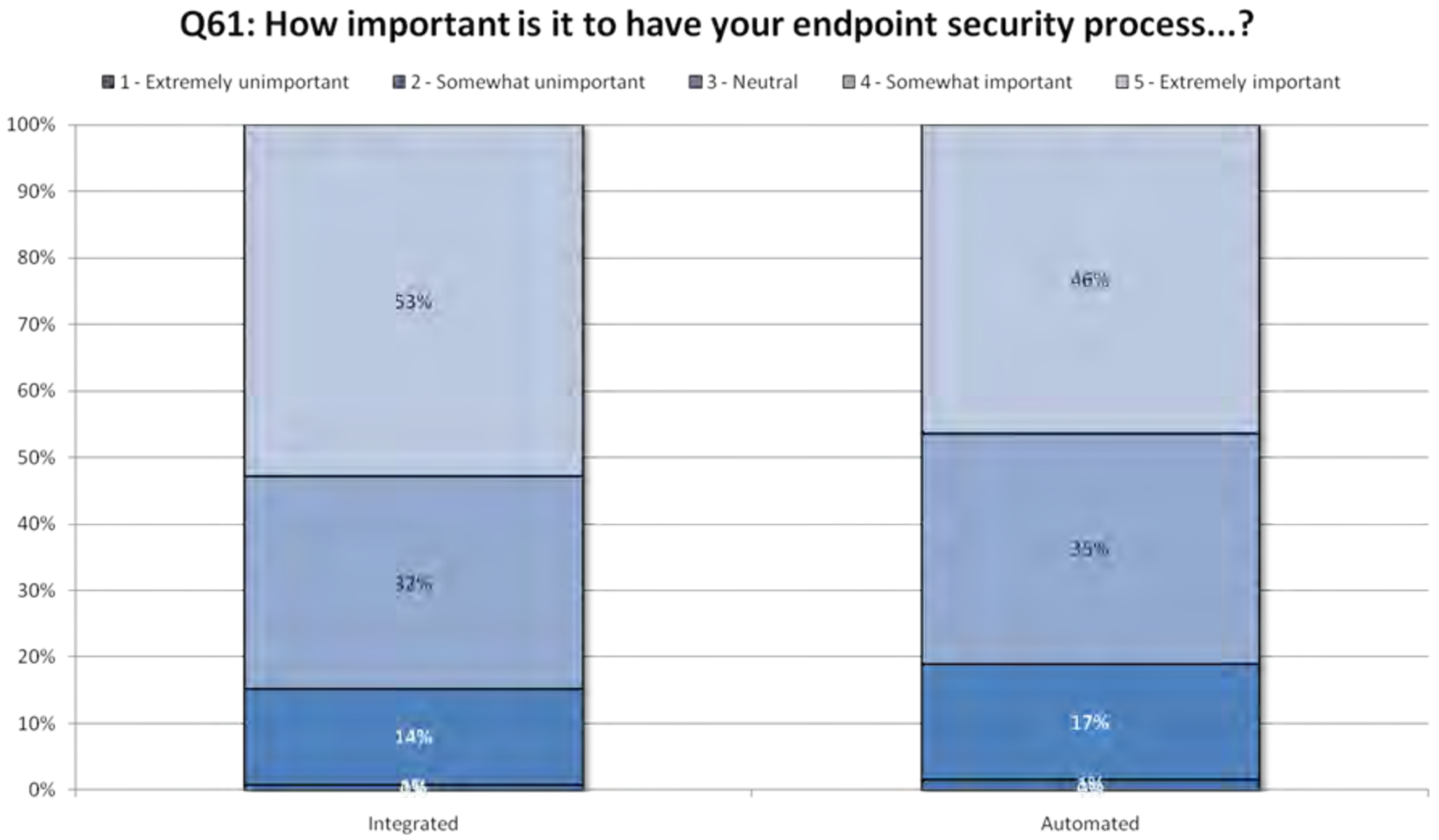
# Endpoint attack causes

| 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% |

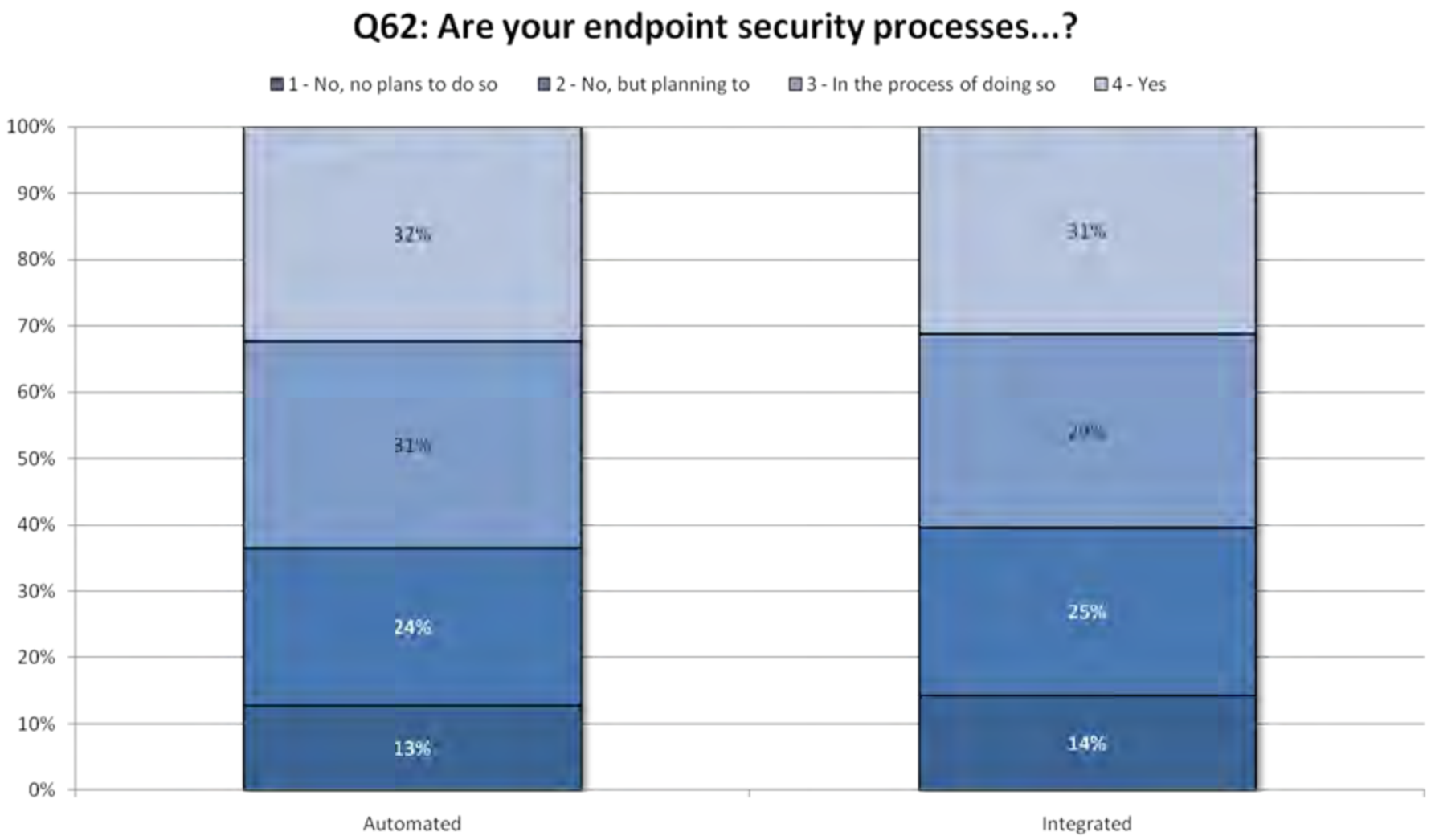
# Lost devices



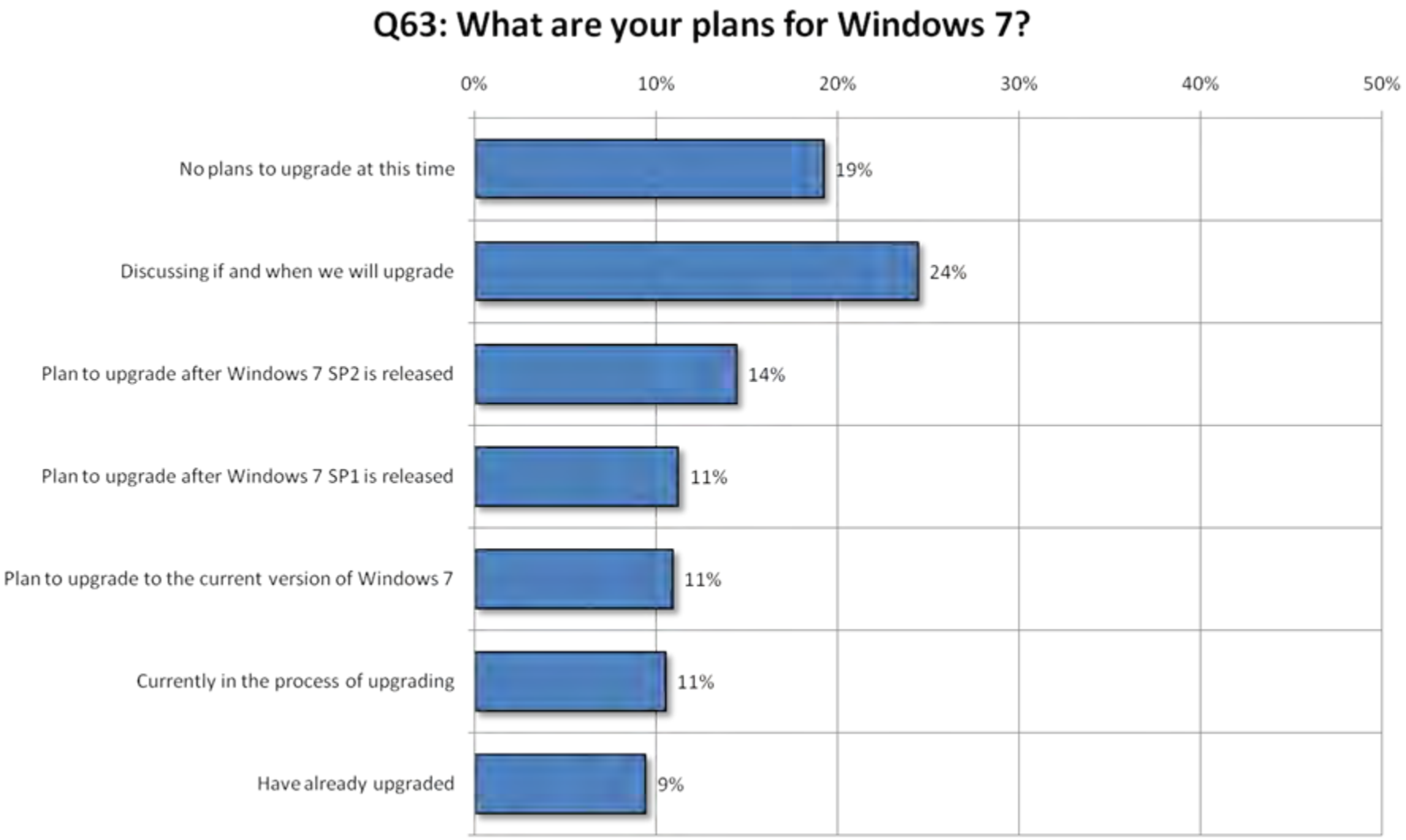
# Endpoint security processes



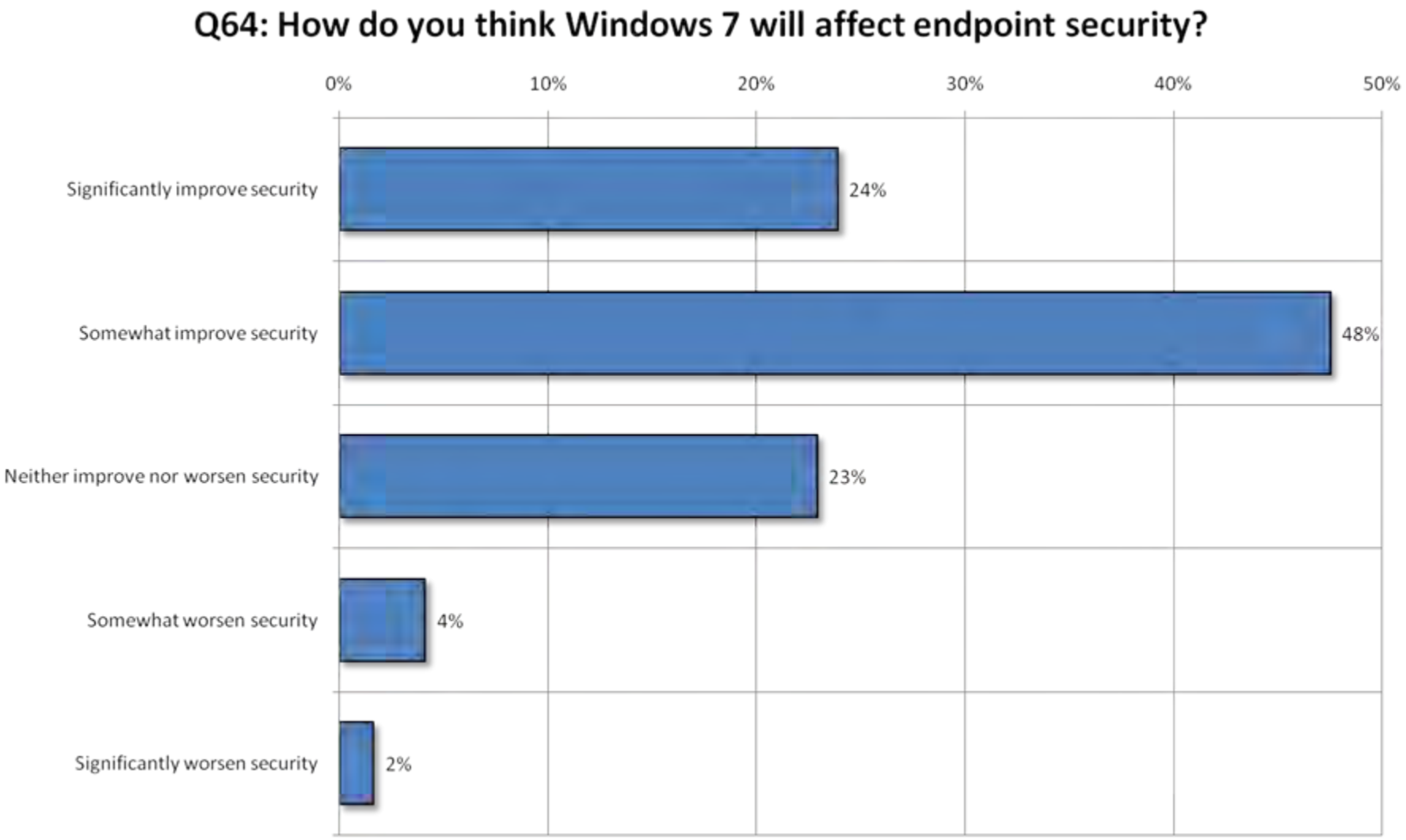
# Endpoint security processes



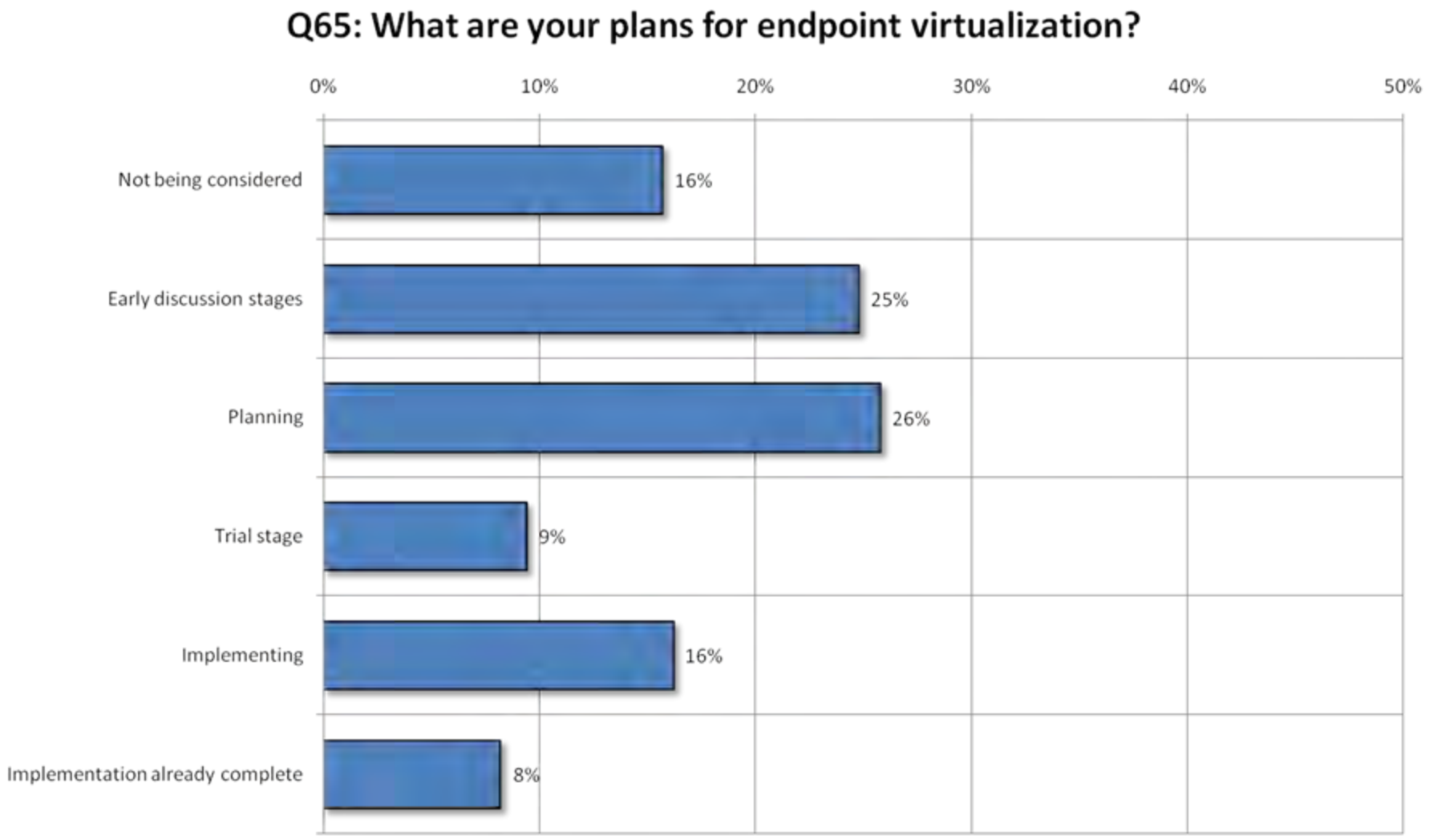
# Windows 7


Q63: What are your plans for Windows 7?
0%
10%
20%
30%
40%
50%
No plans to upgrade at this time
19%
Discussing if and when we will upgrade
24%
Plan to upgrade after Windows 7 SP2 is released
14%
Plan to upgrade after Windows 7 SP1 is released
11%
Plan to upgrade to the current version of Windows 7
11%
Currently in the process of upgrading
11%
Have already upgraded
9%

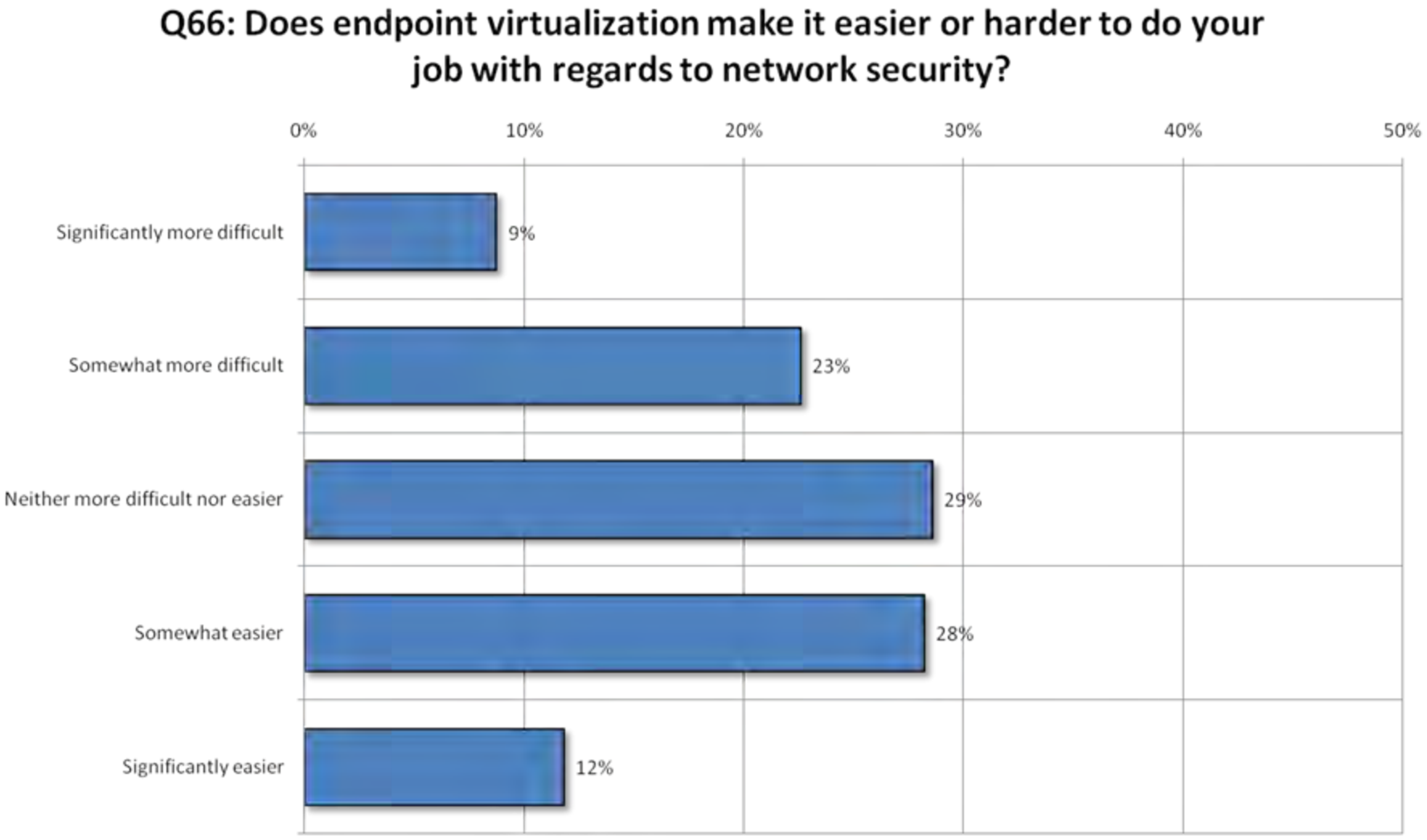
# Windows 7


Q64: How do you think Windows 7 will affect endpoint security?
0%
10%
20%
30%
40%
50%
Significantly improve security
24%
Somewhat improve security
48%
Neither improve nor worsen security
23%
Somewhat worsen security
4%
Significantly worsen security
2%

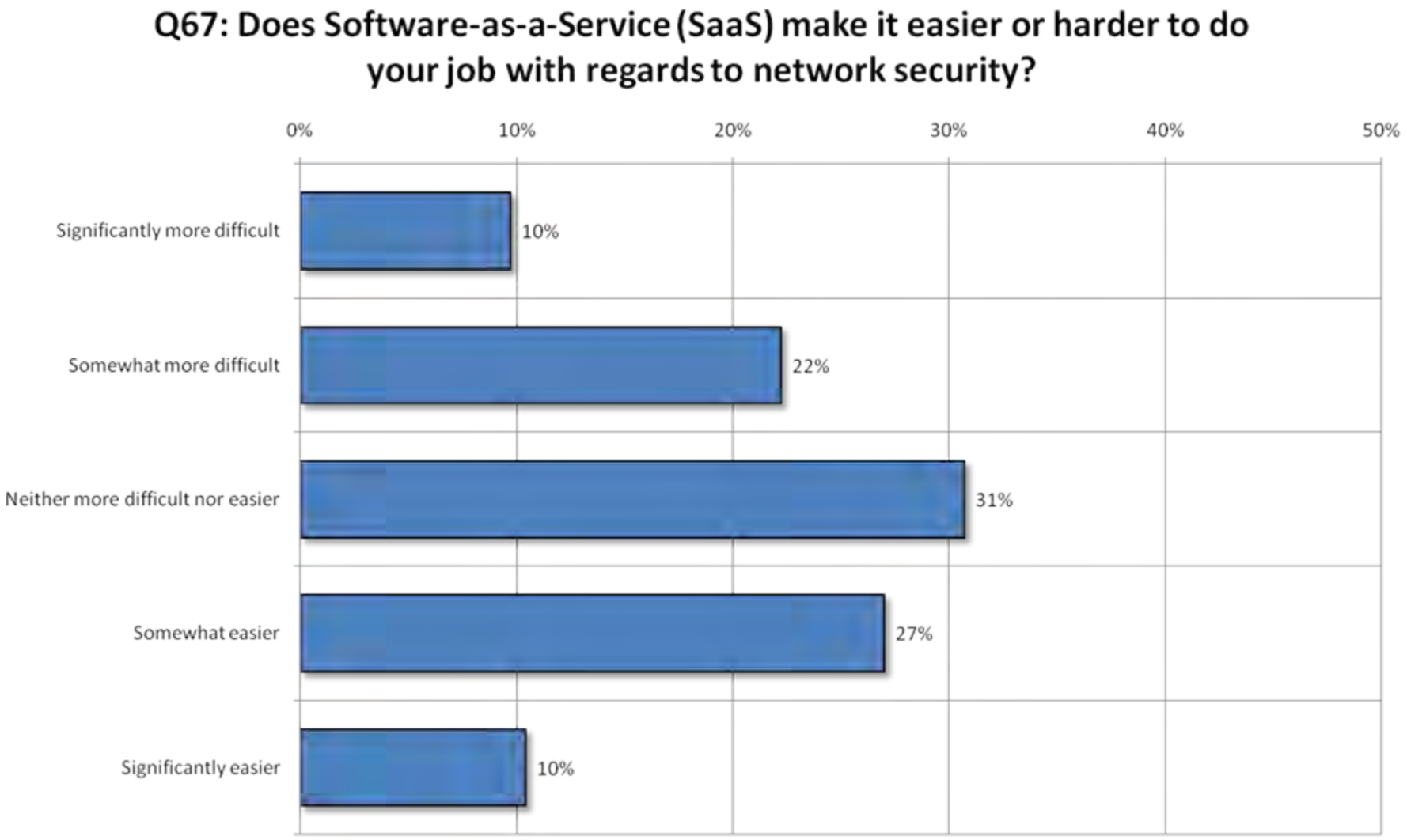
# Endpoint virtualization



# Endpoint virtualization

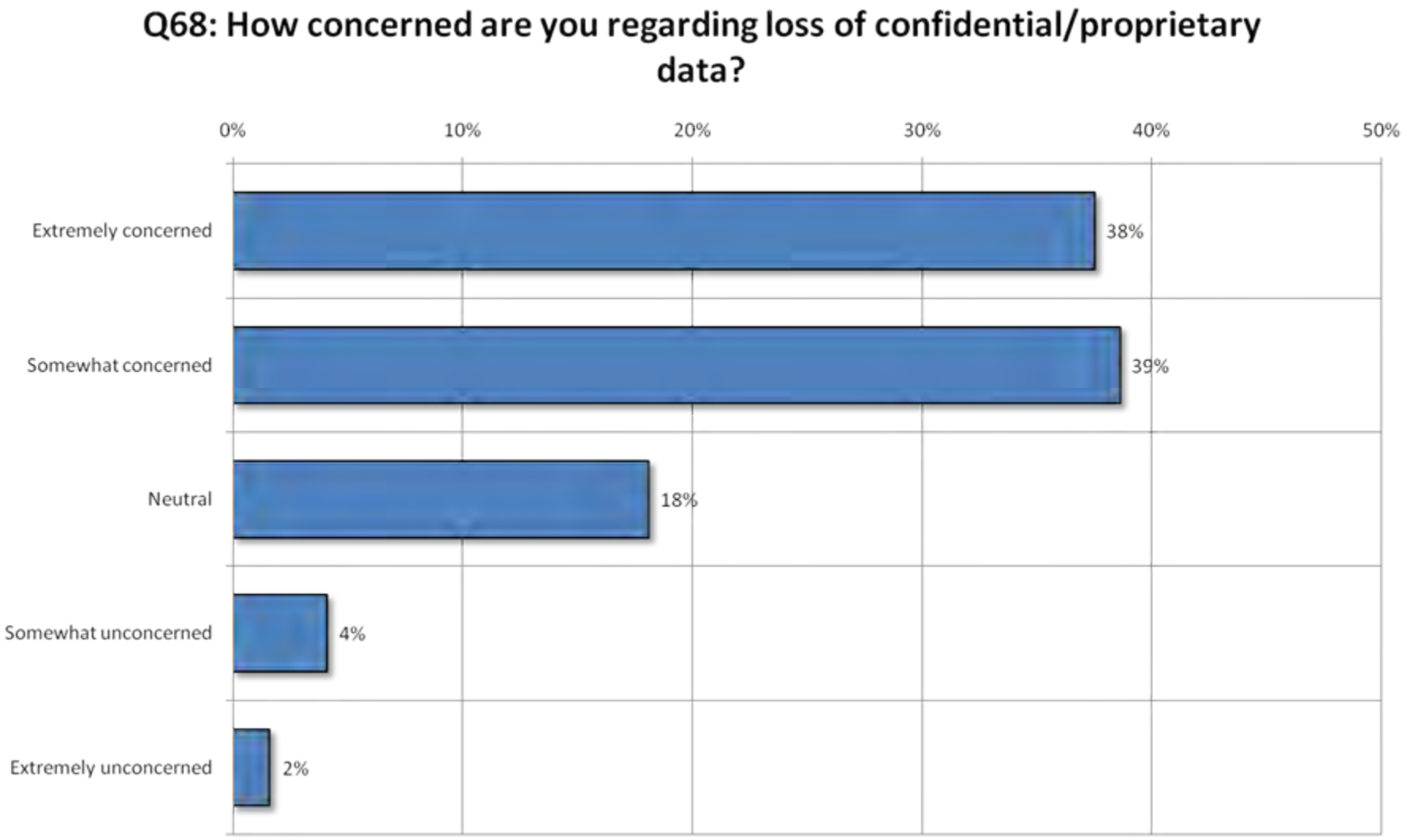


# Software-as-a-Service

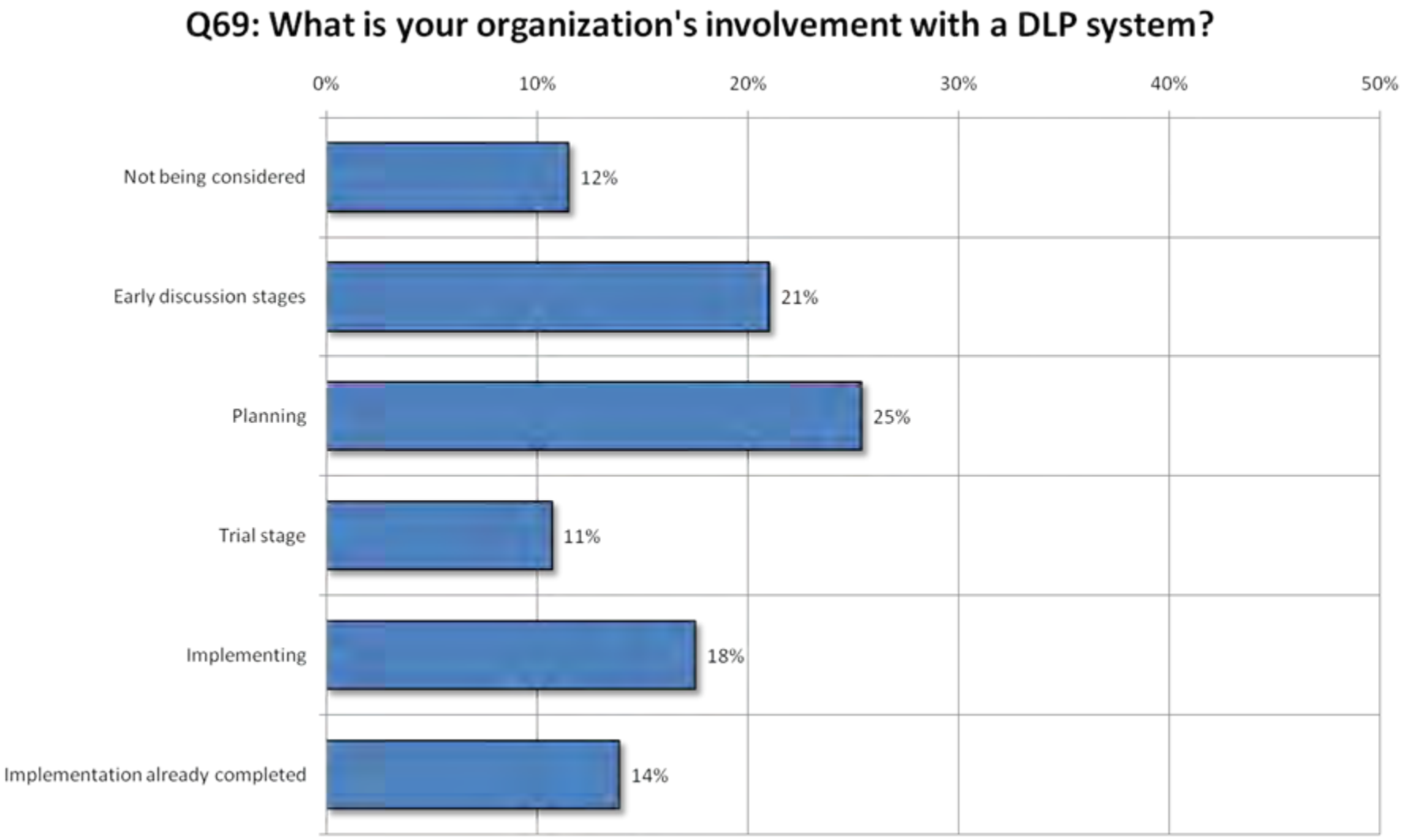


# Data Loss Prevention

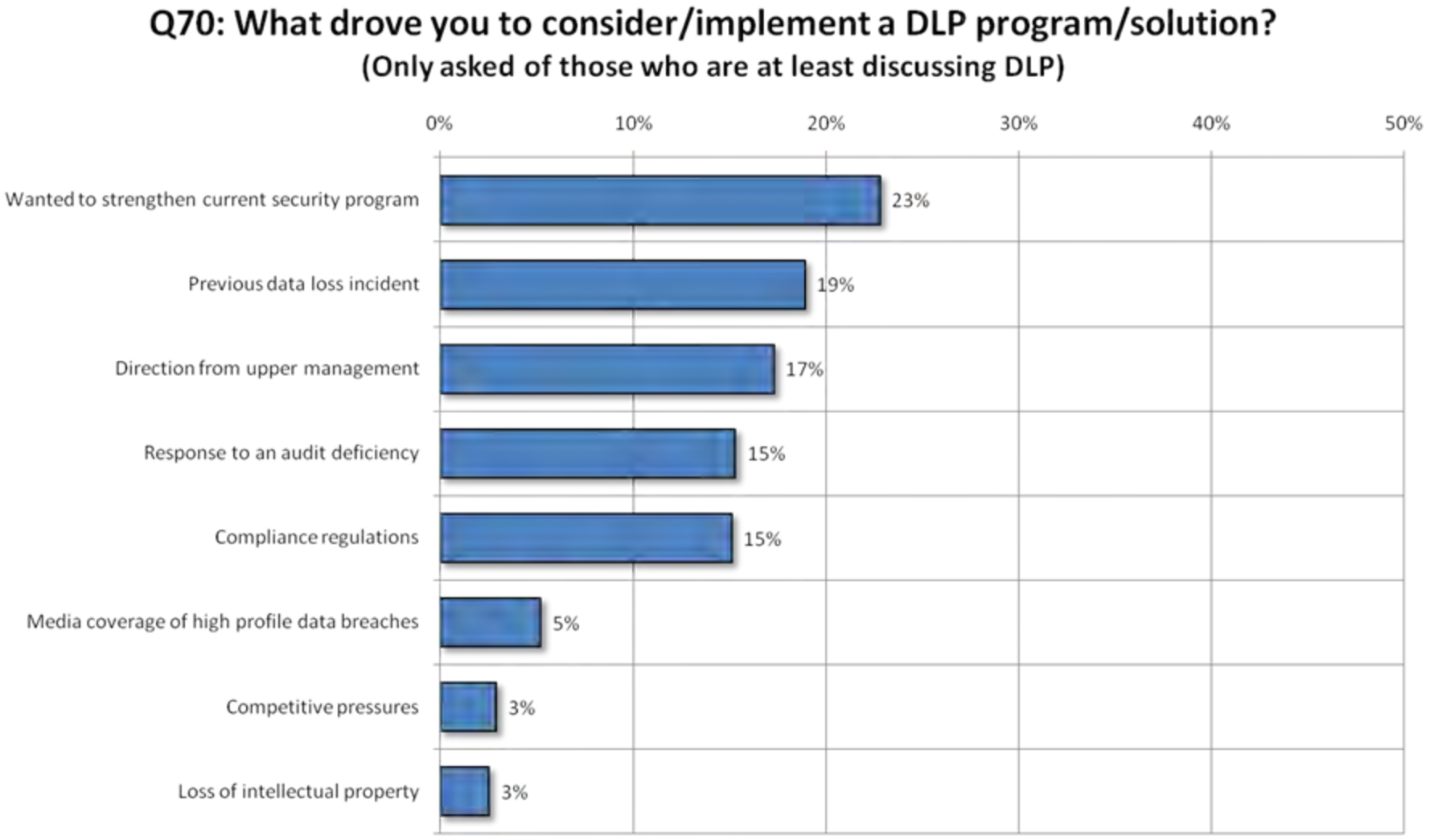
# Data loss concern



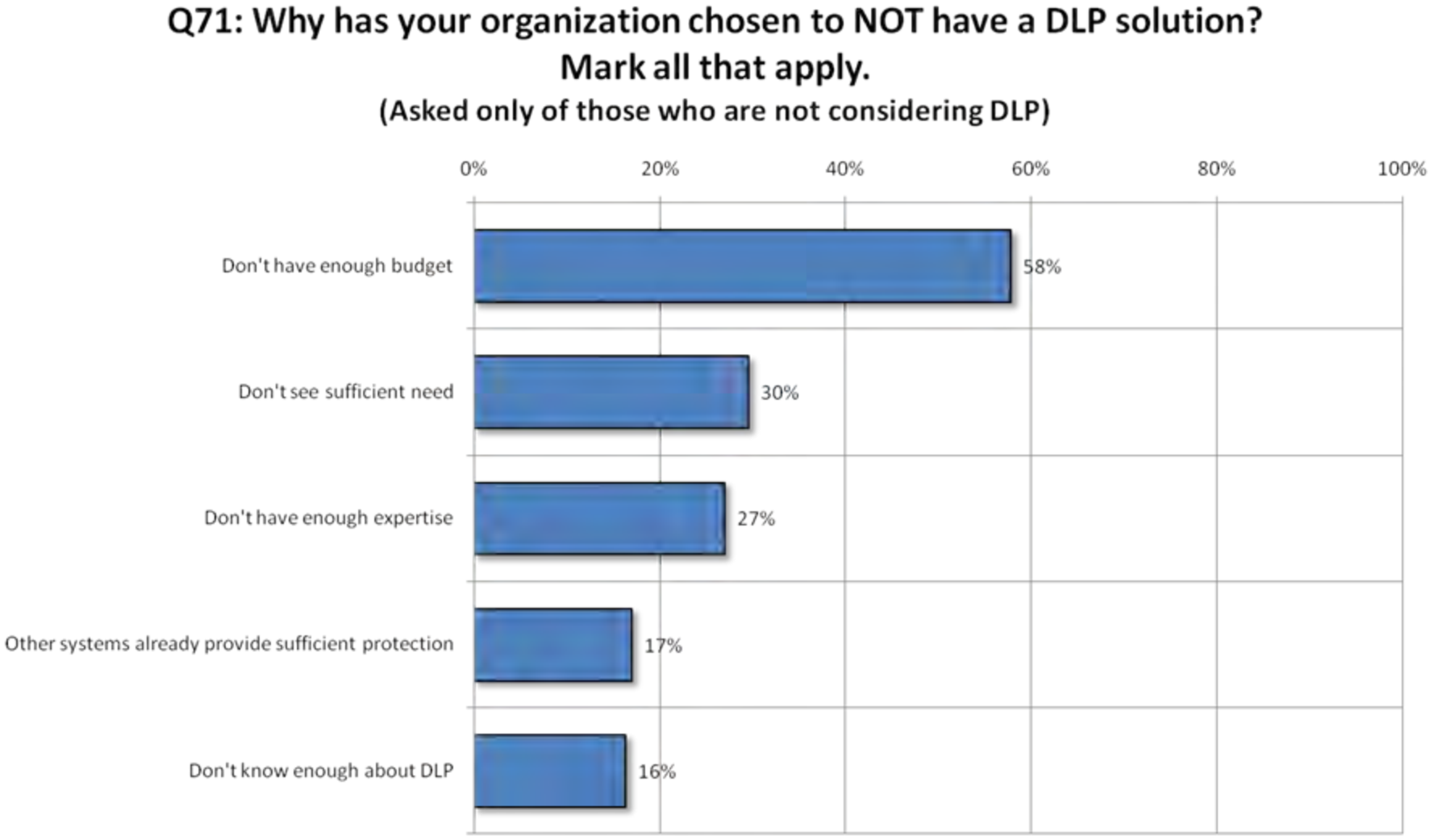
# Data loss prevention



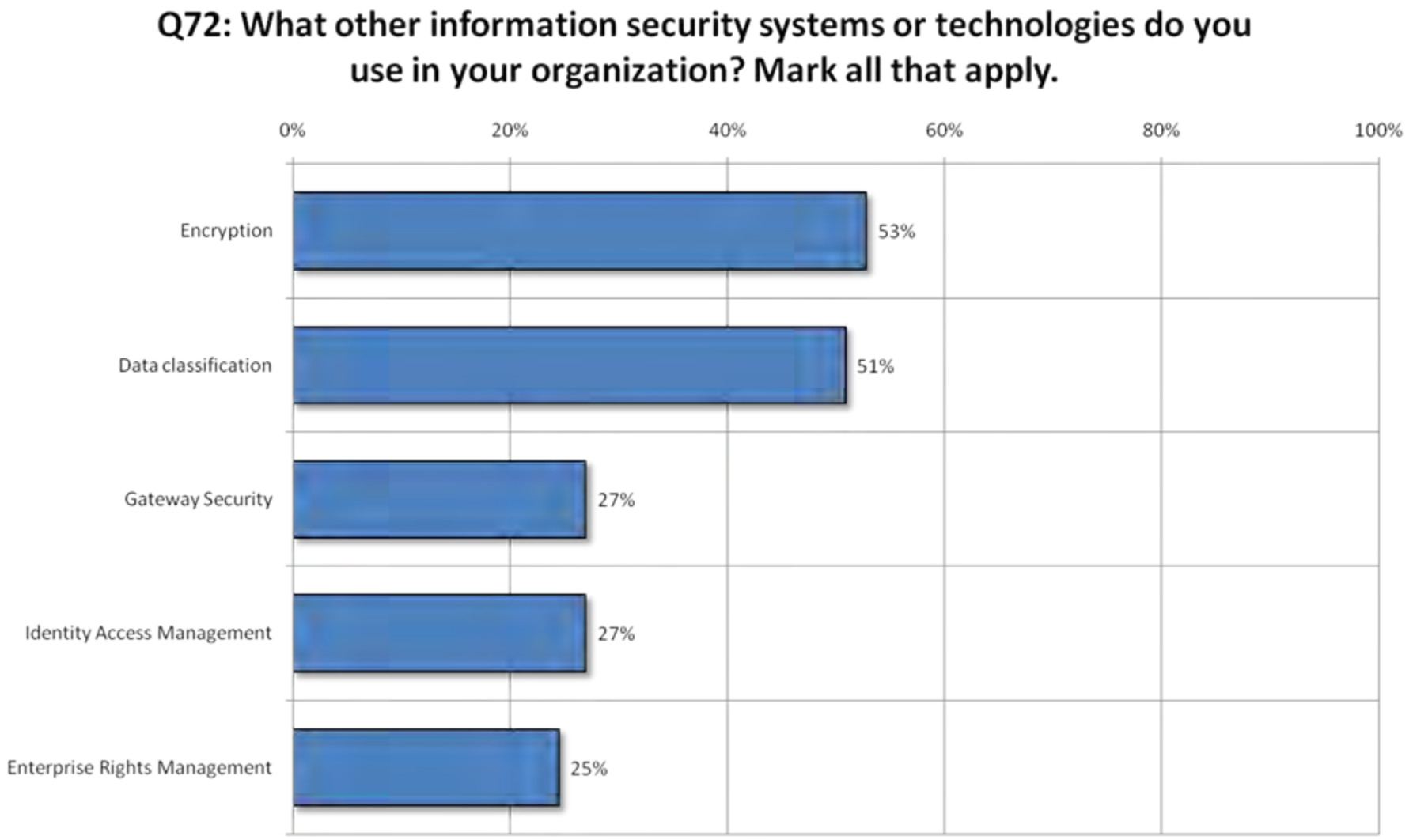
# Data loss prevention



# Data loss prevention

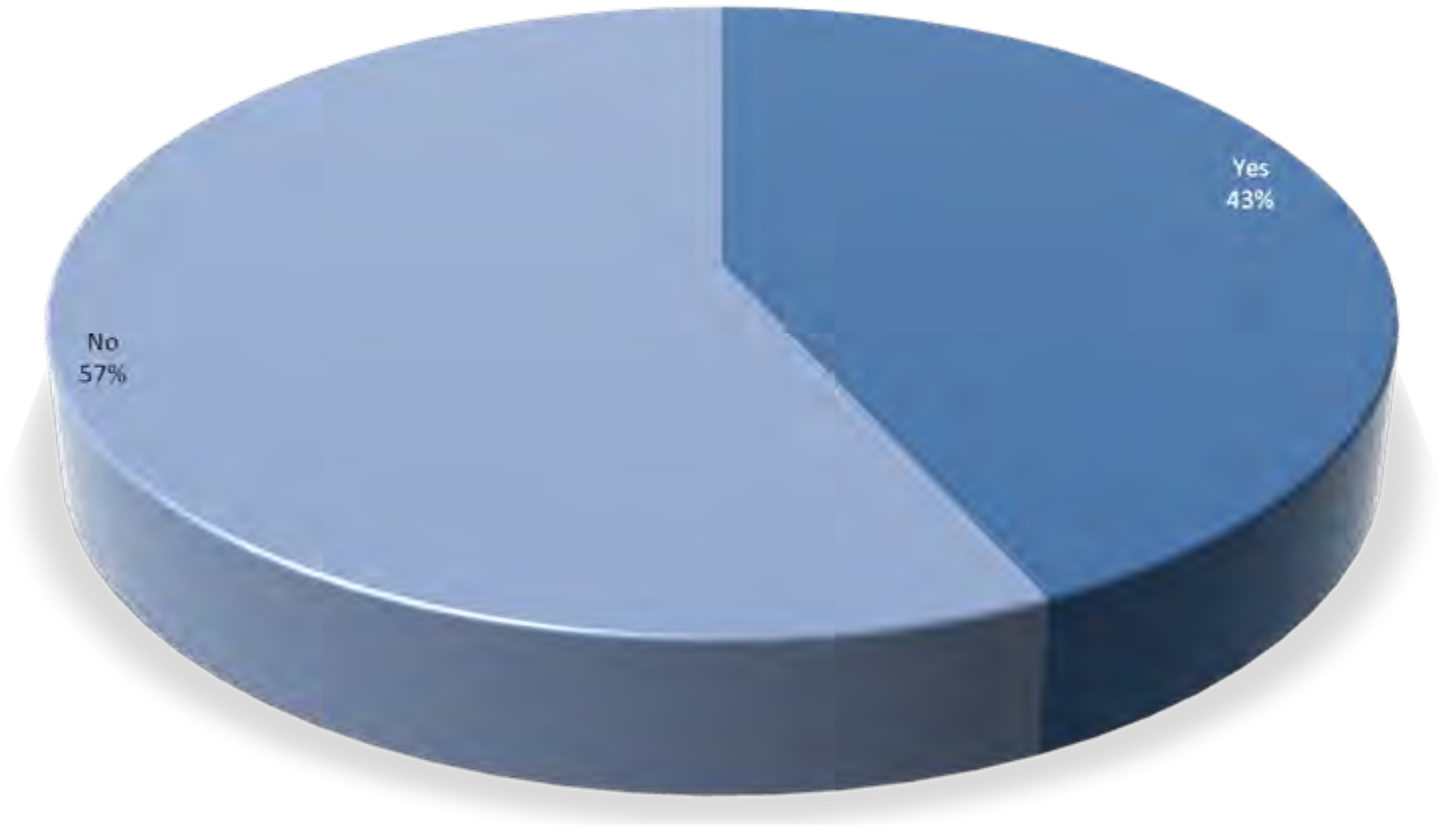


# Other information security systems



# Previous data loss

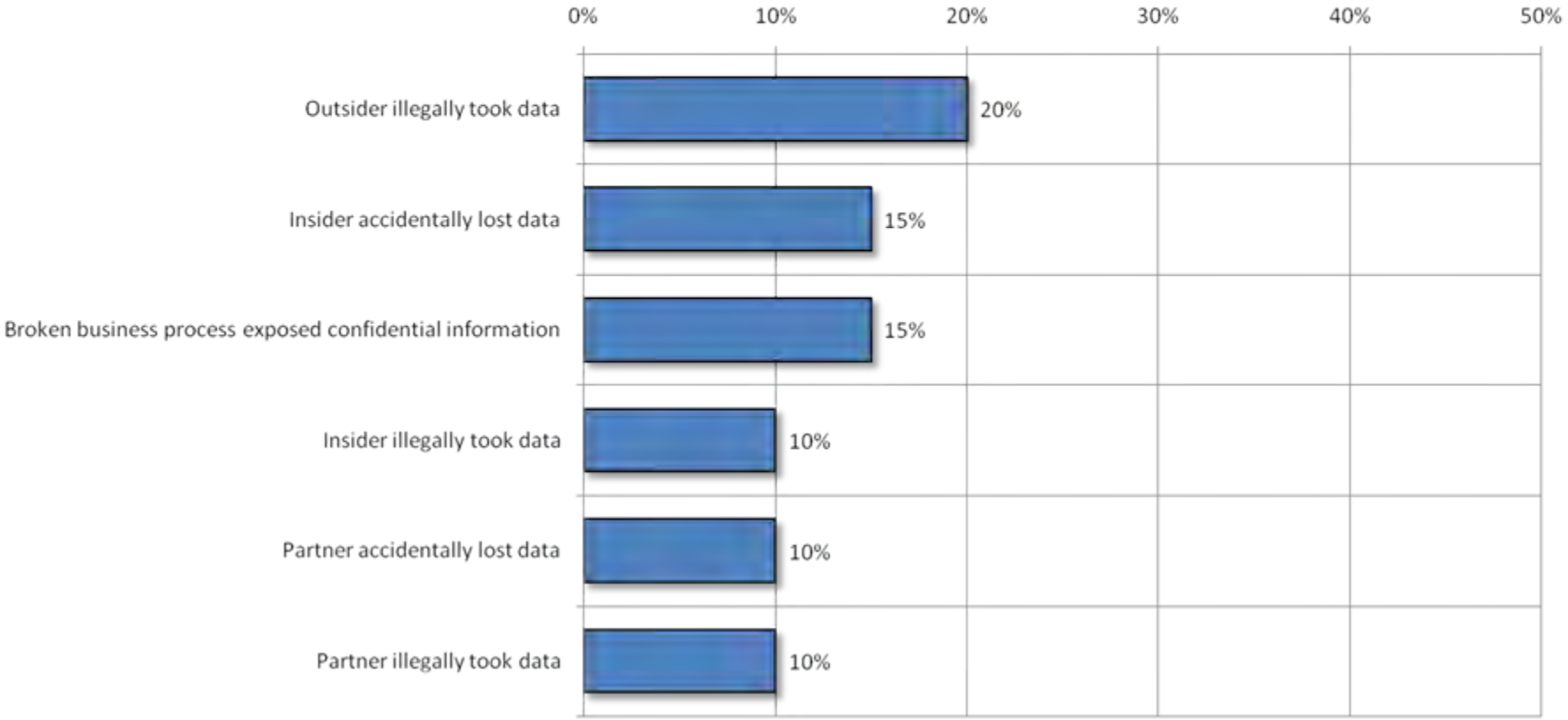
Q73: Have you lost confidential/proprietary data in the past?



# Previous data loss

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

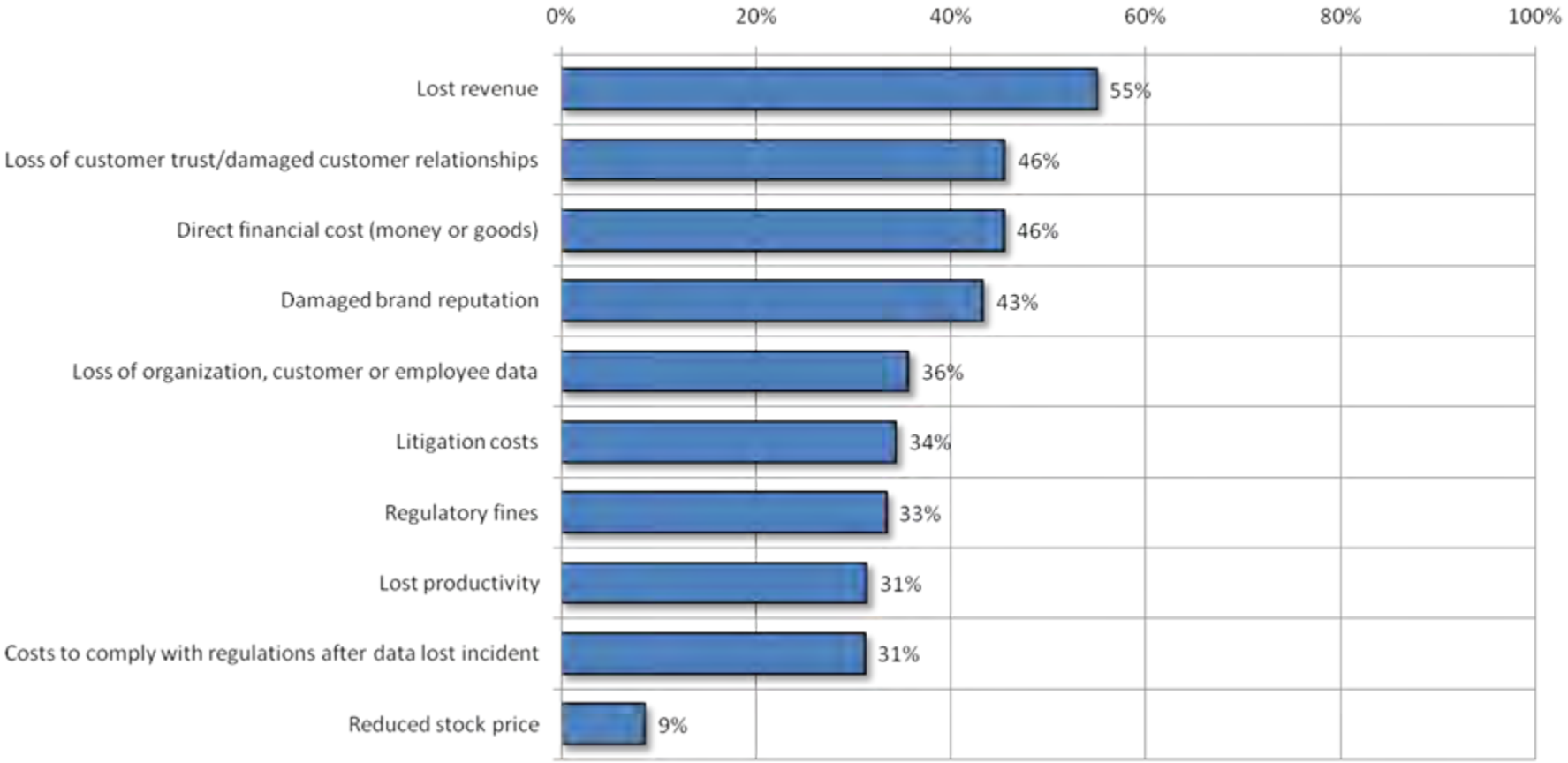
(Asked only of those who have lost confidential/proprietary data in the past)
(Means shown)



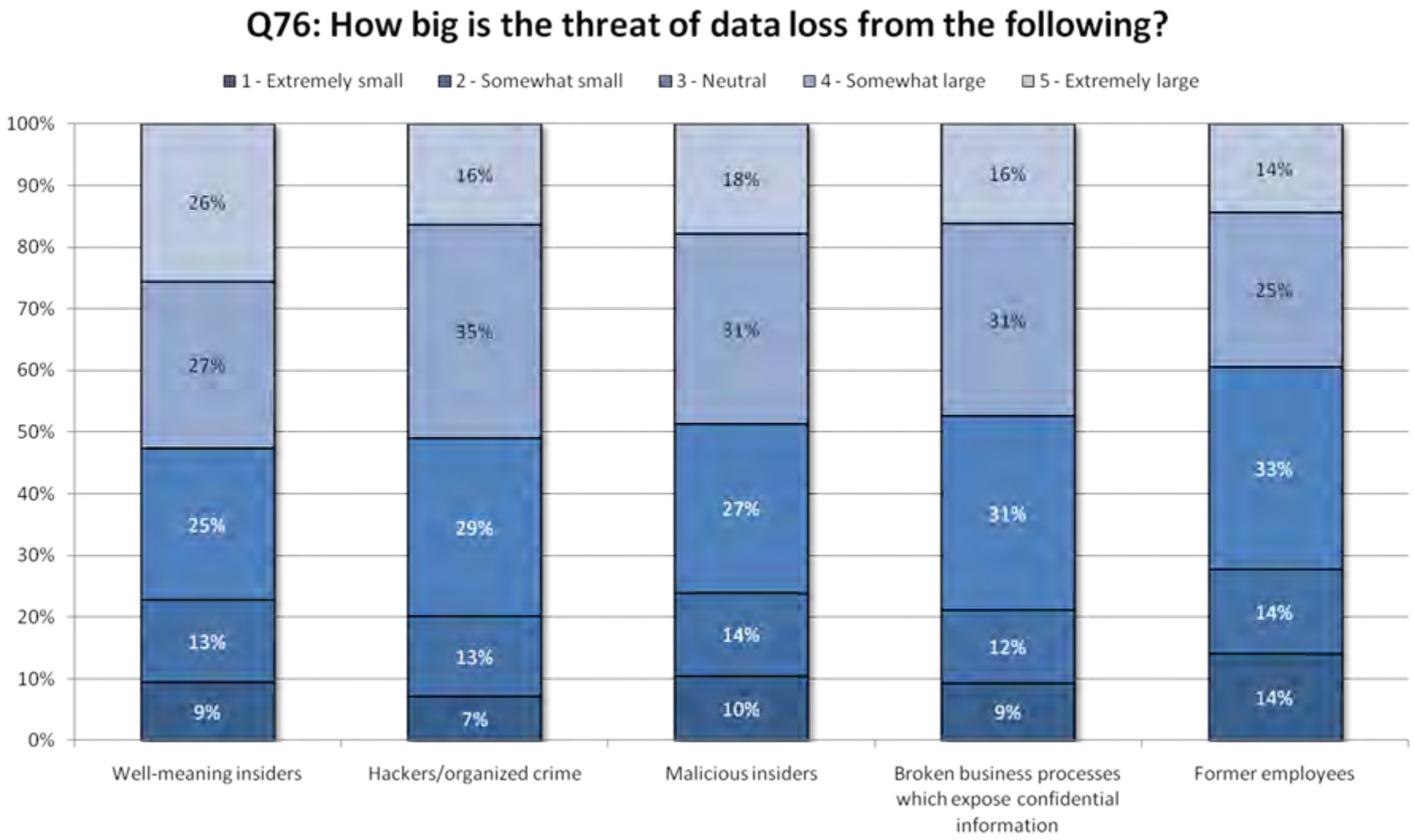
# Data loss consequences

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

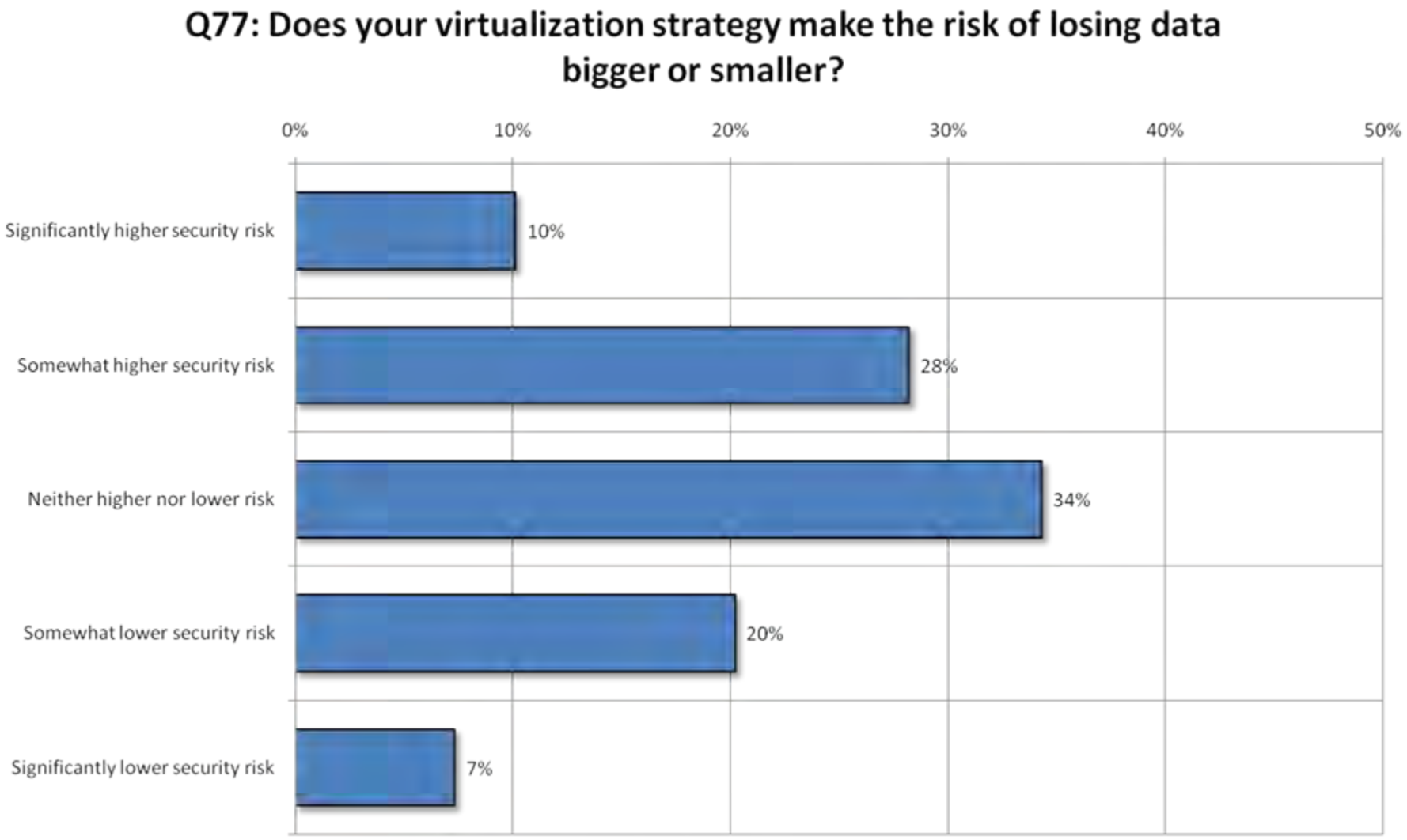
### (Asked only of those who have lost confidential/proprietary data in the past)



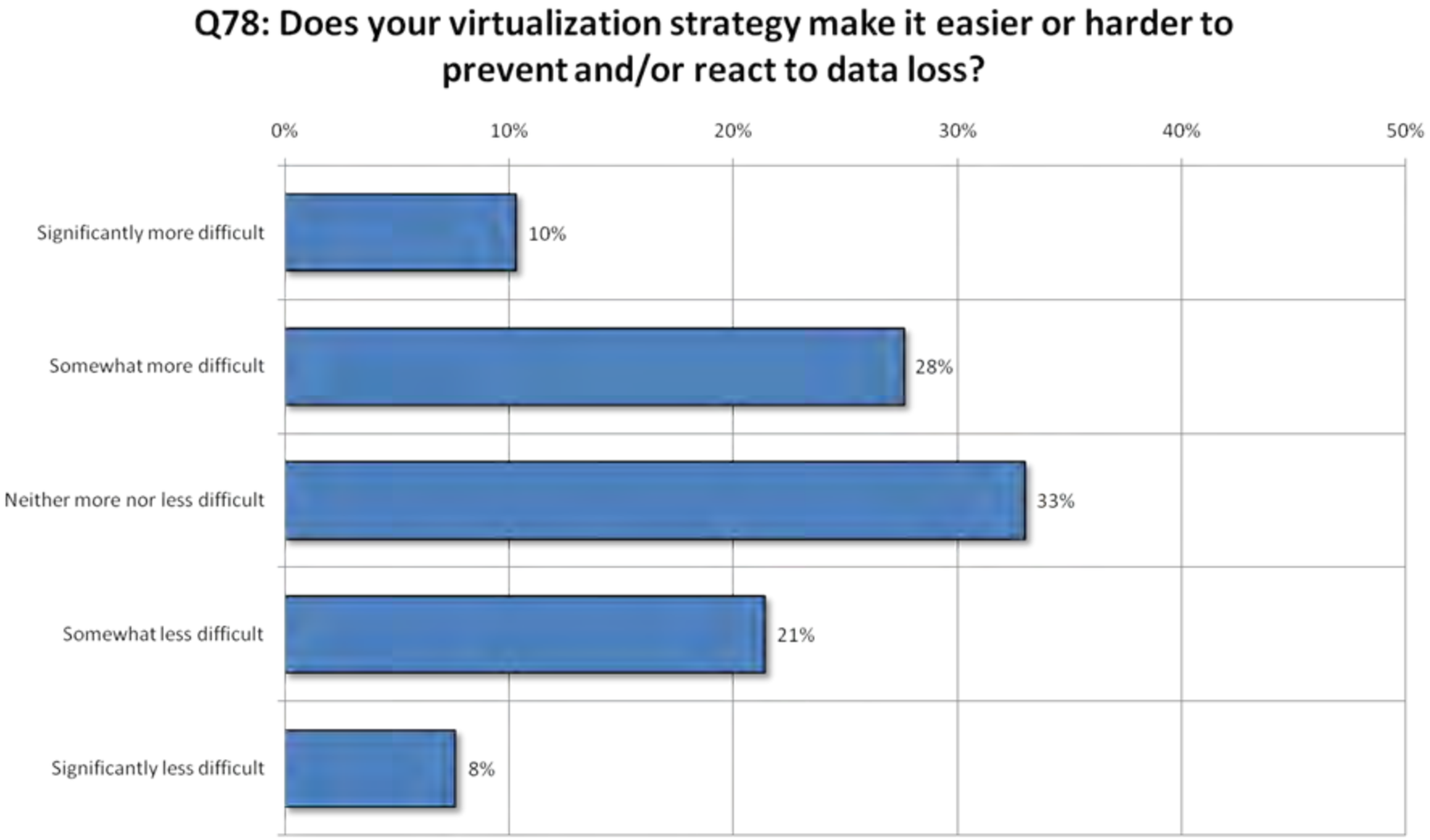
# Data loss threats



# Virtualization strategy

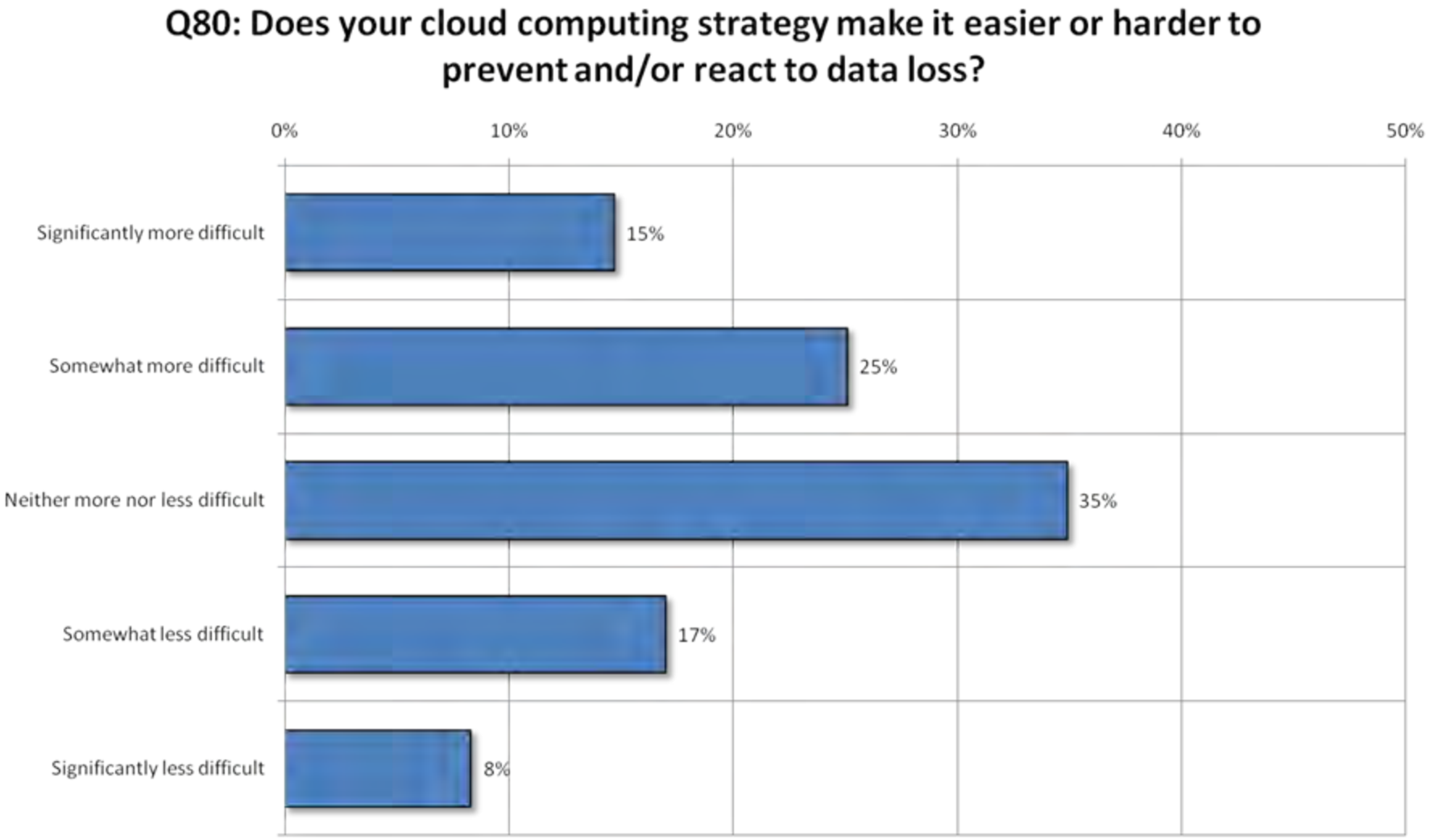


# Virtualization strategy



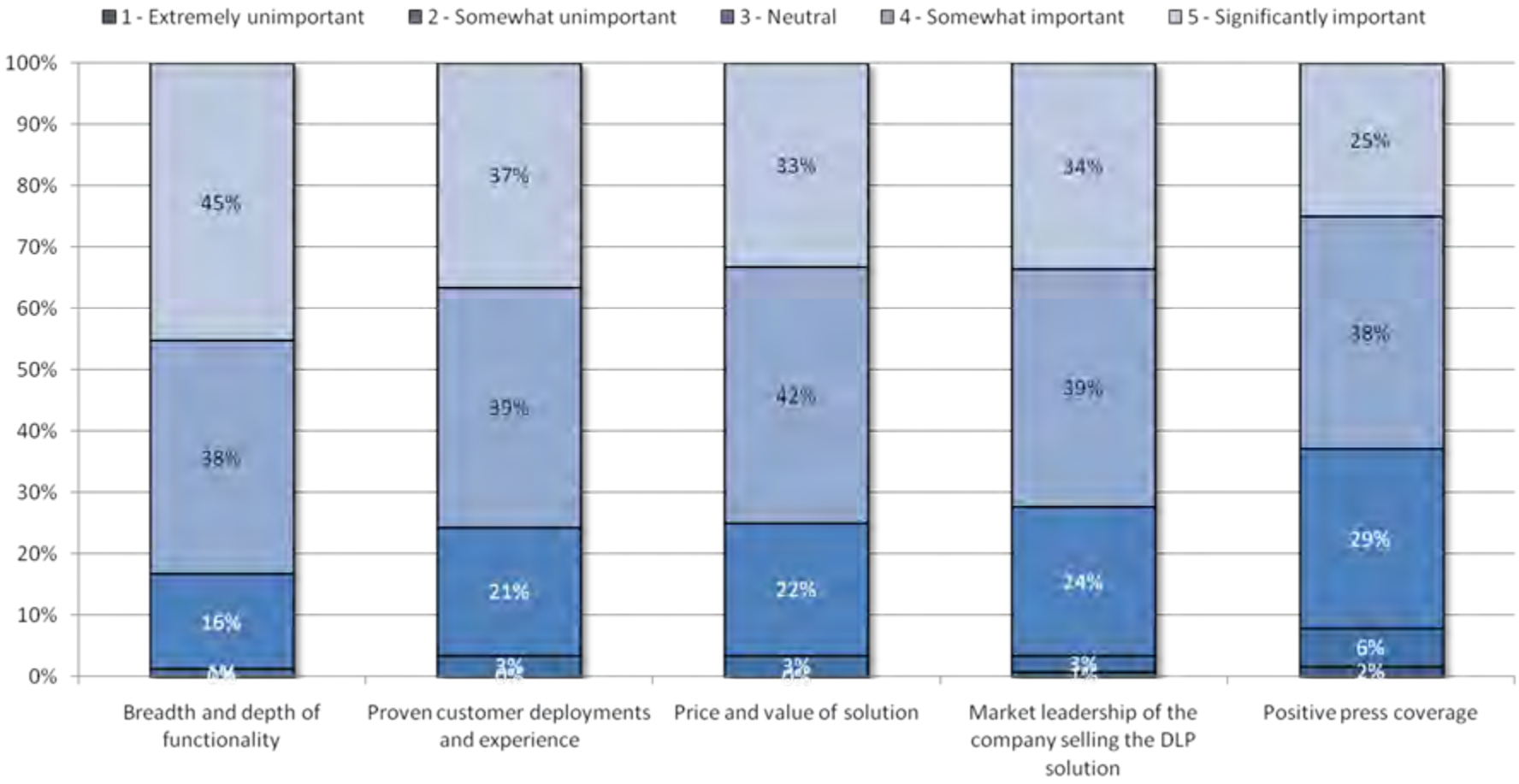
# Cloud computing strategy

# Cloud computing strategy



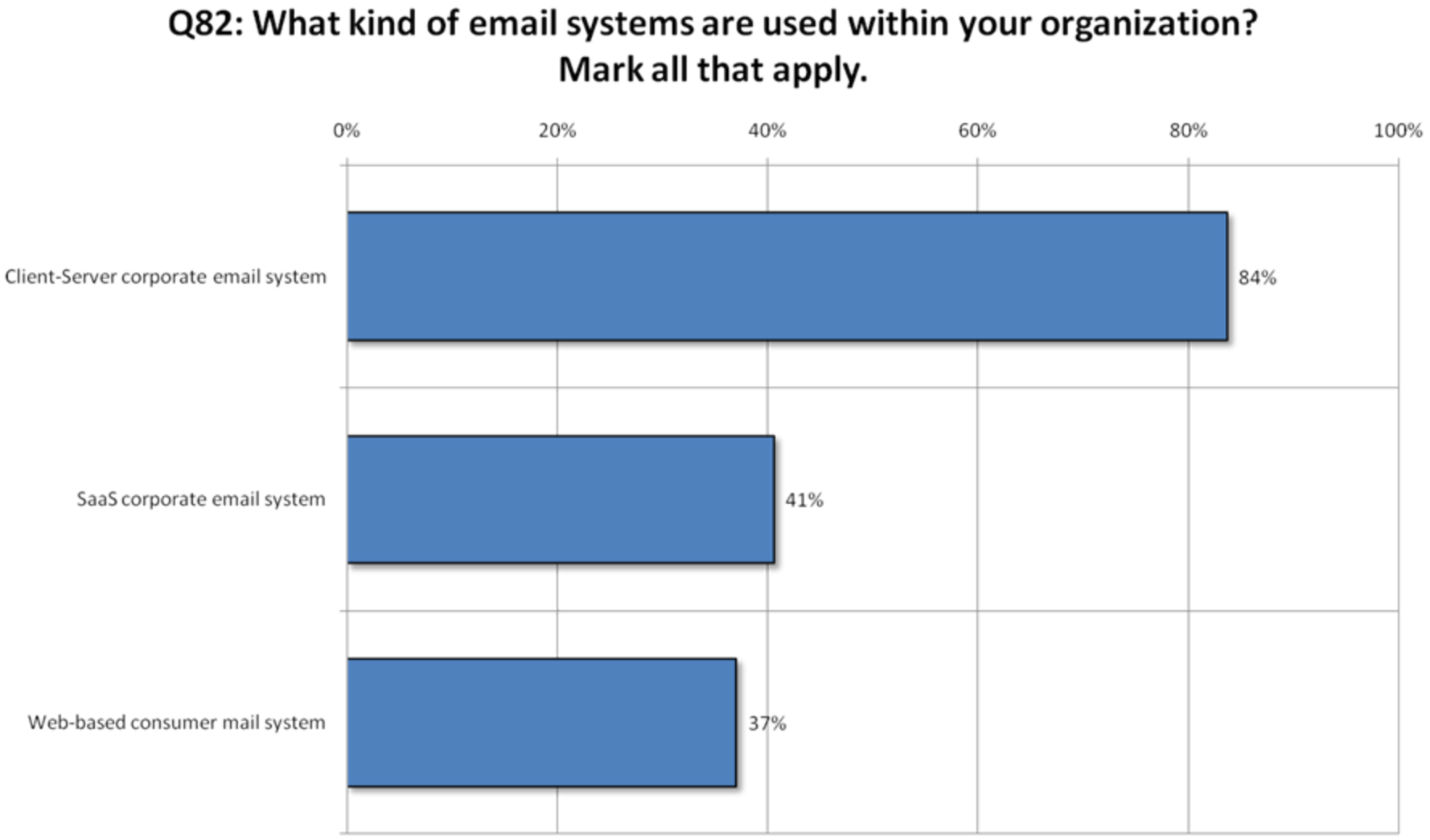
# DLP selection

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

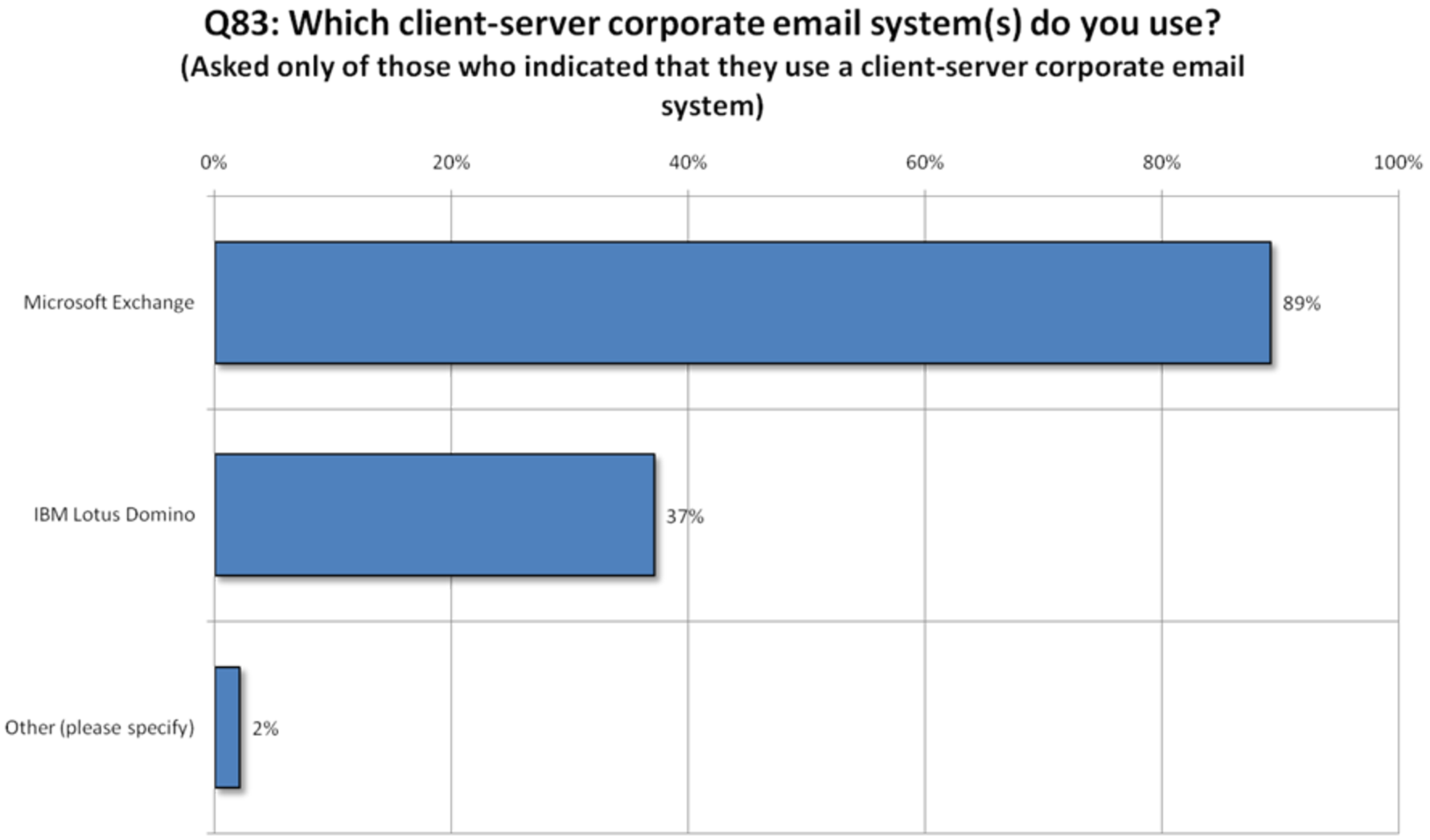


# Messaging/Collaboration Security

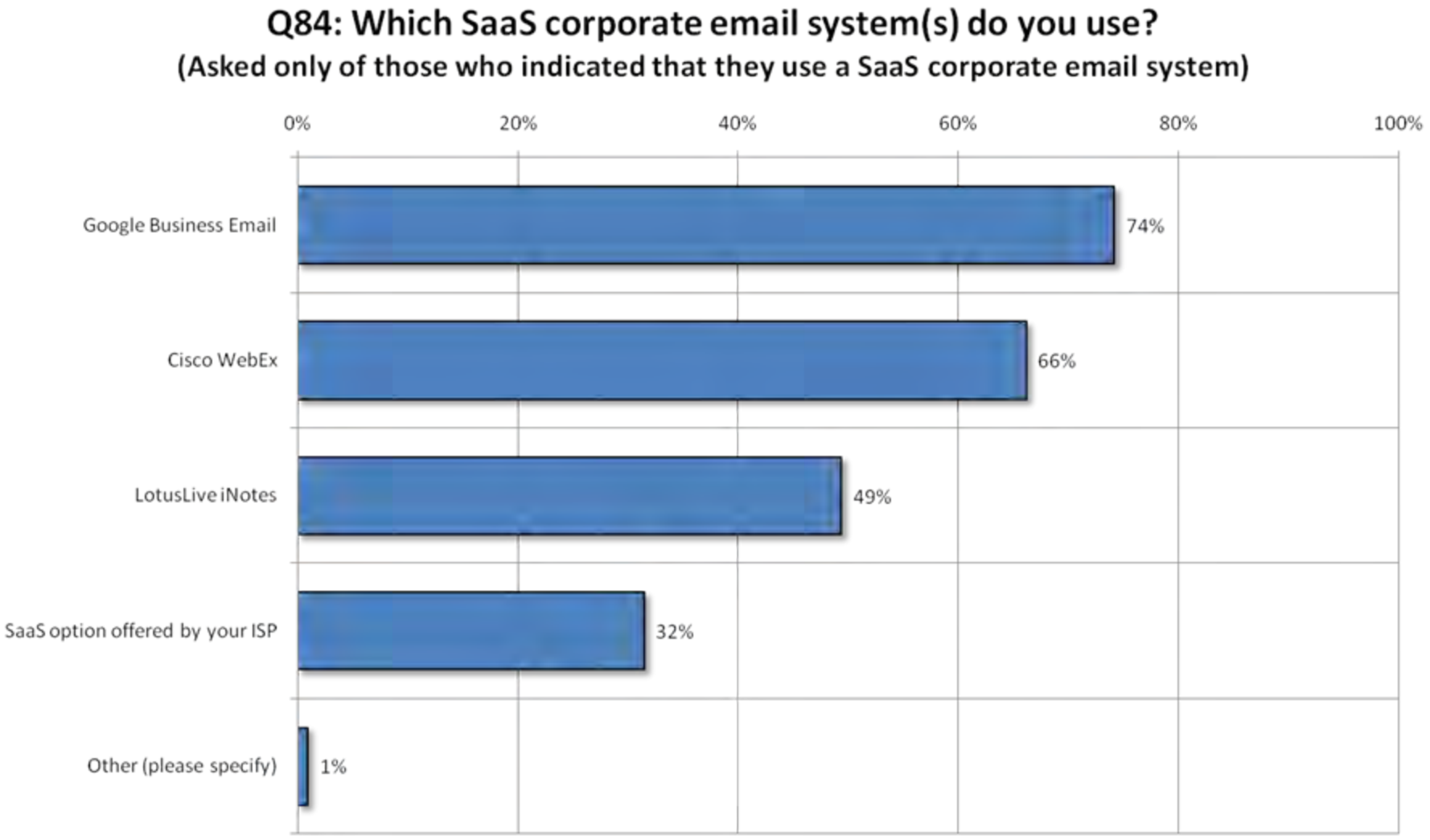
# Email systems



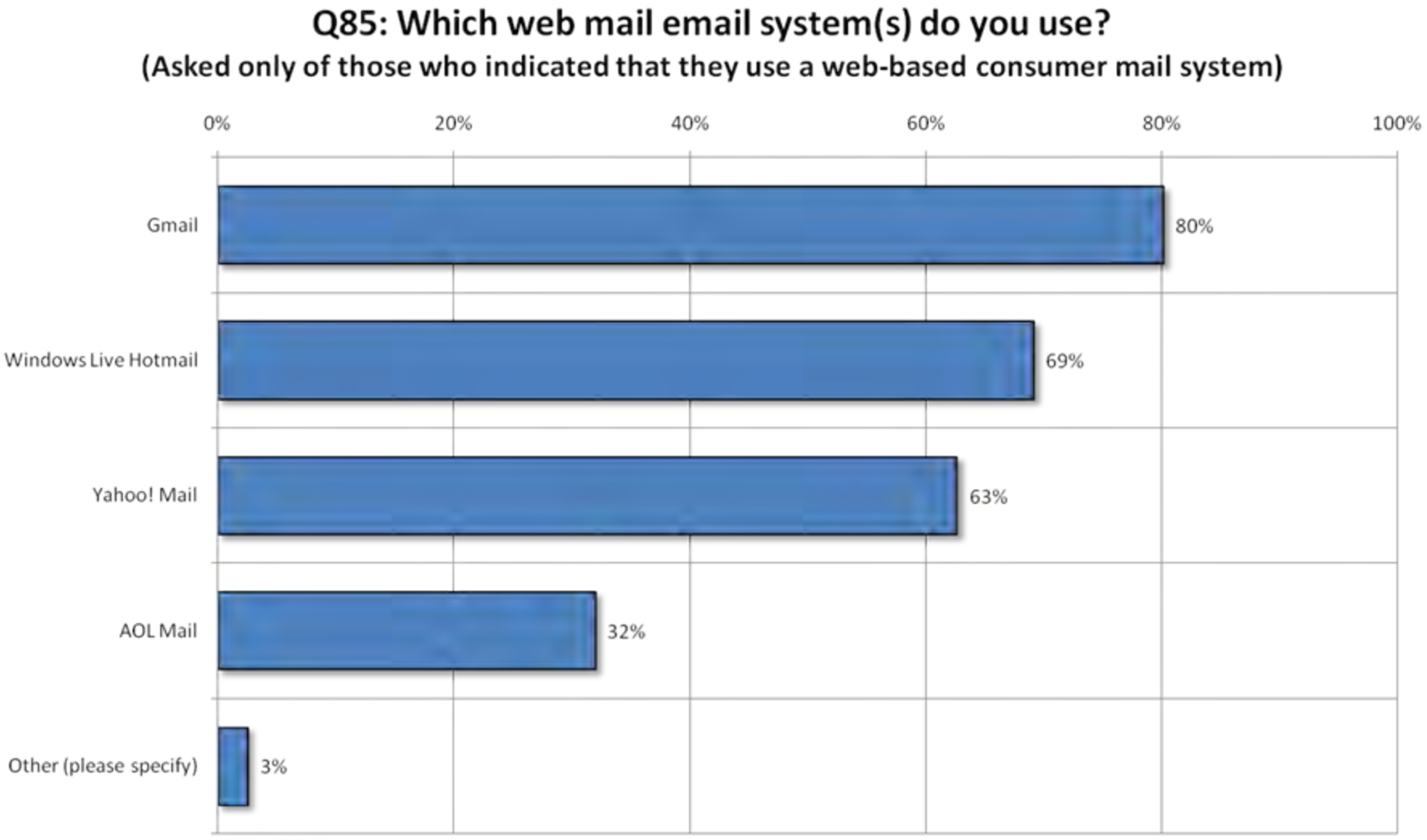
# Email systems



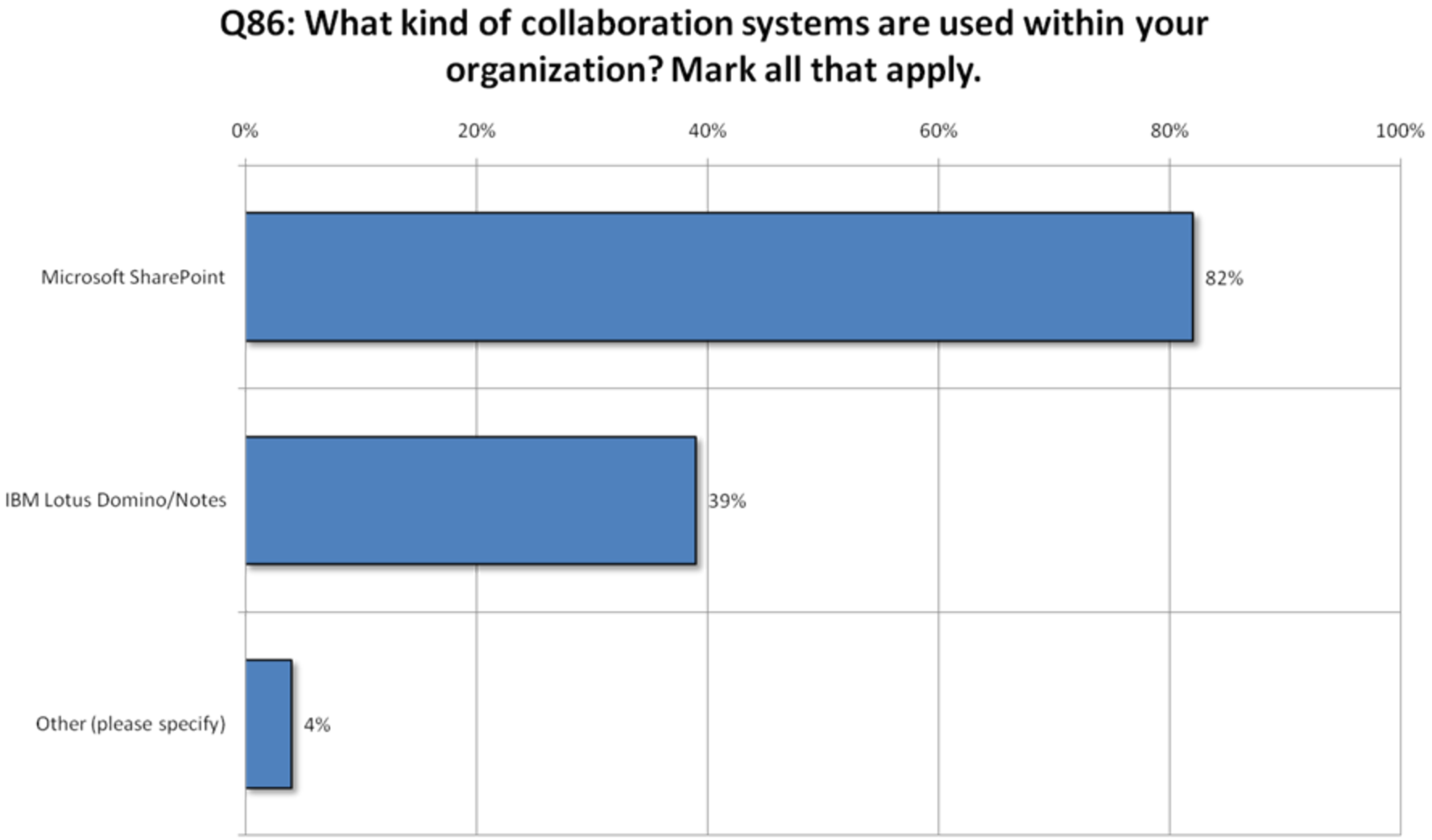
# Email systems



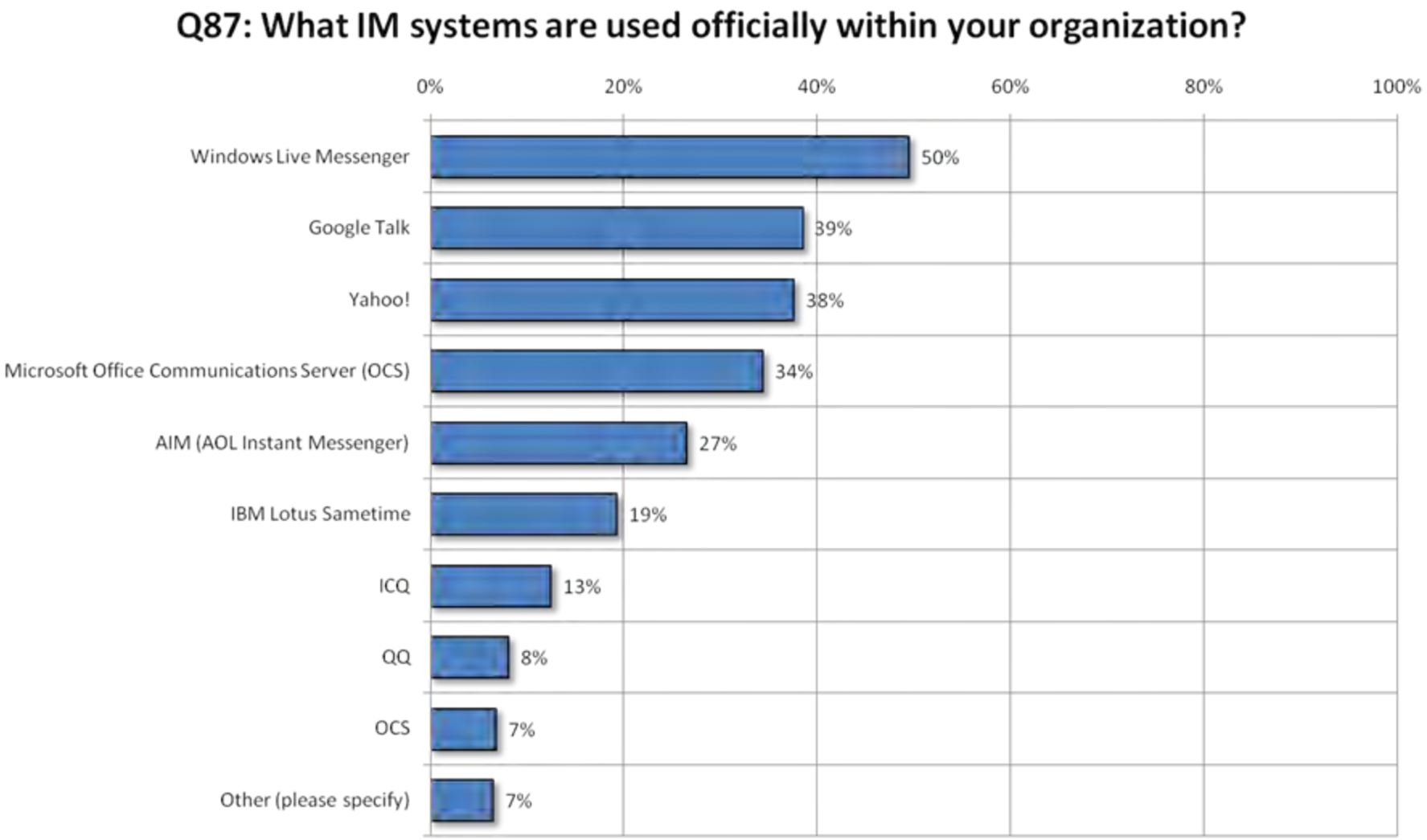
# Email systems



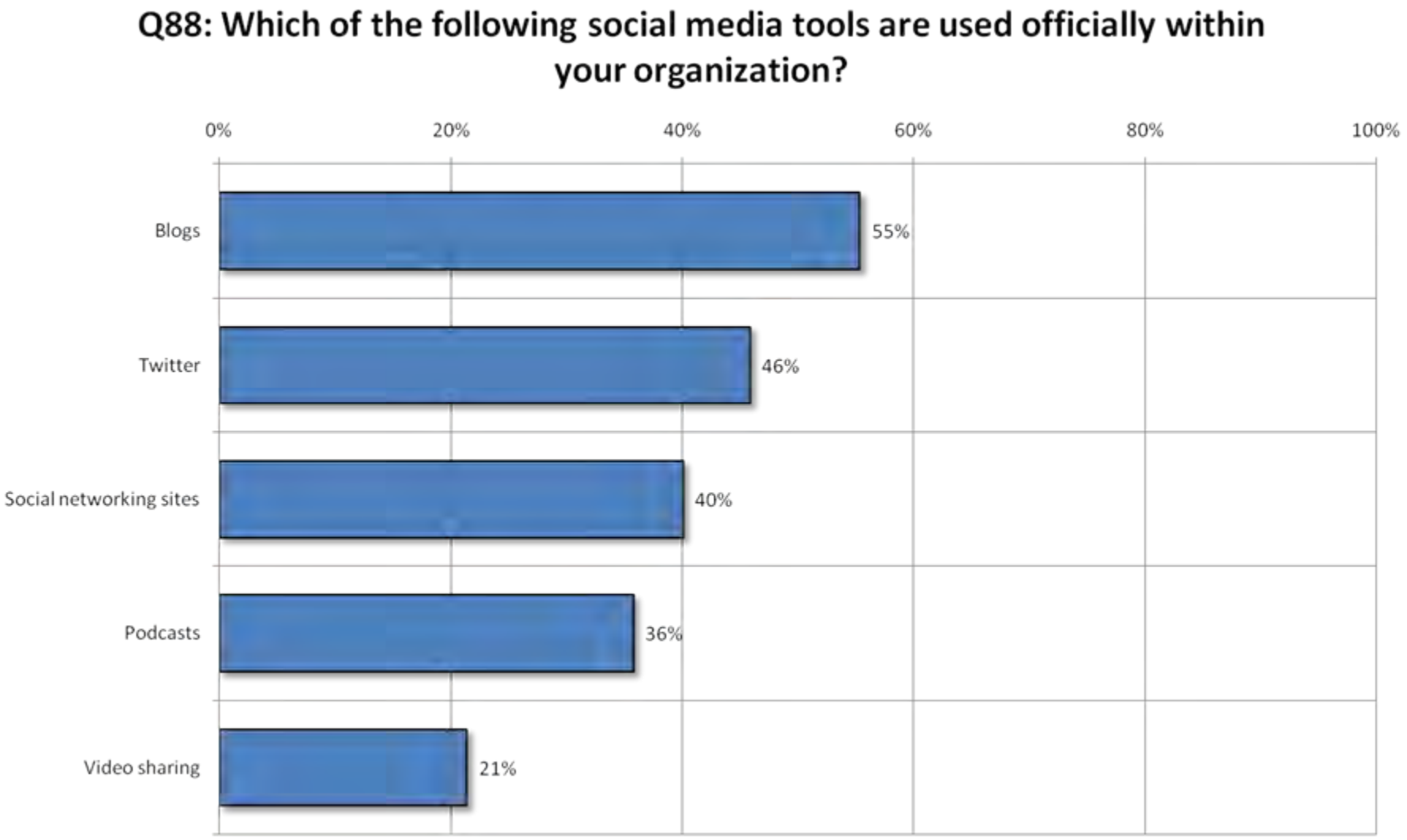
# Collaboration systems



# Instant messaging



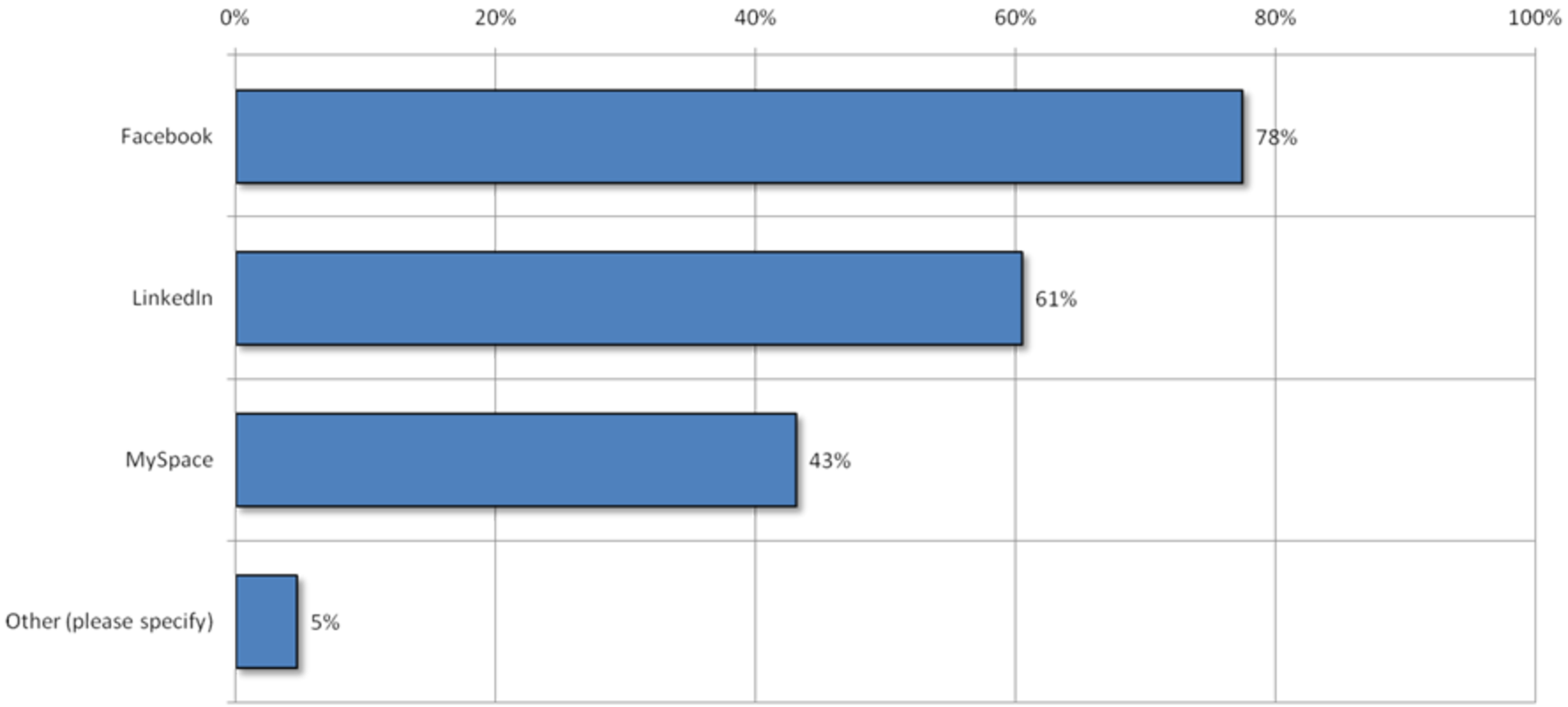
# Social media tools



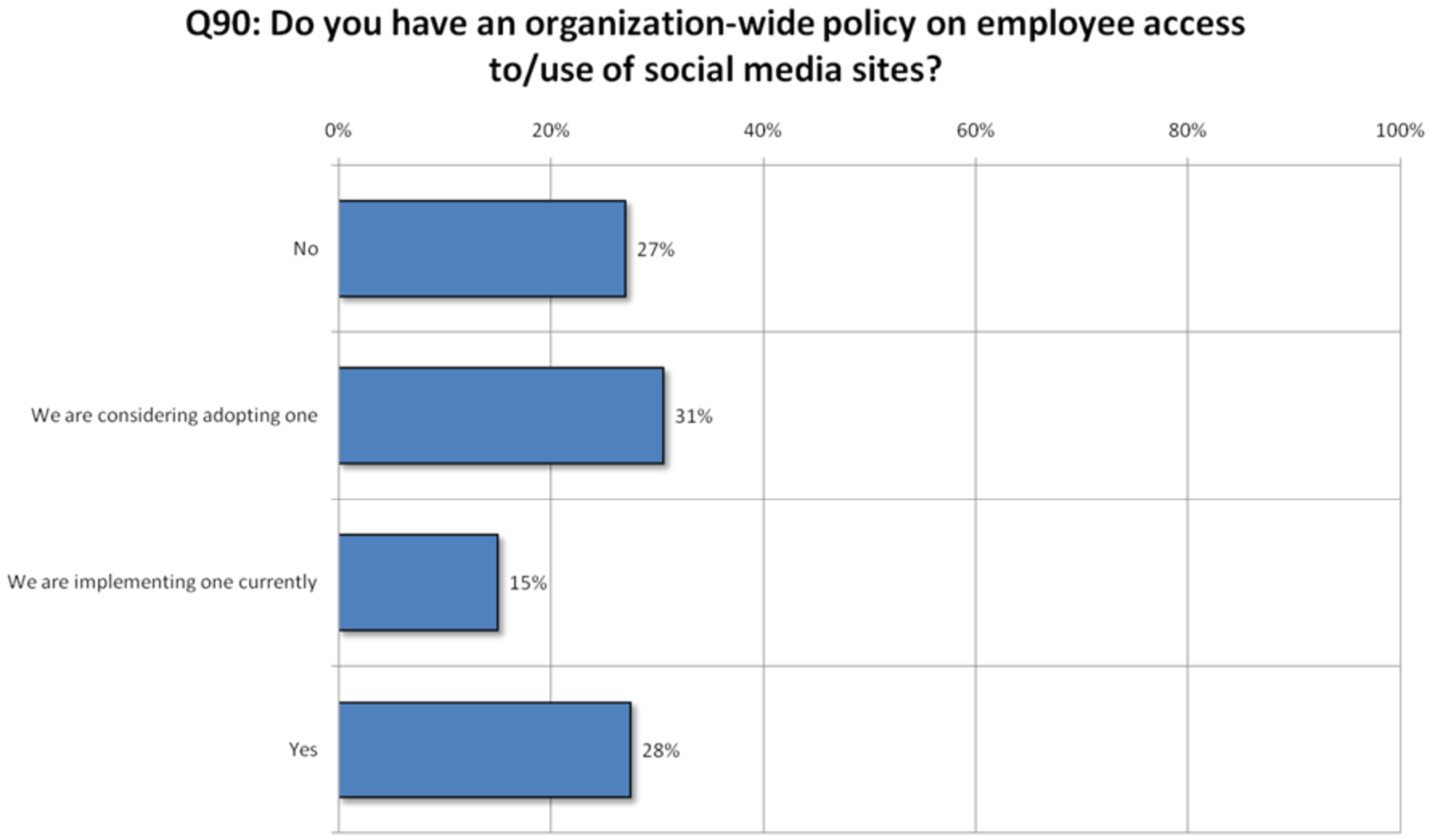
# Social networking sites

**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)**

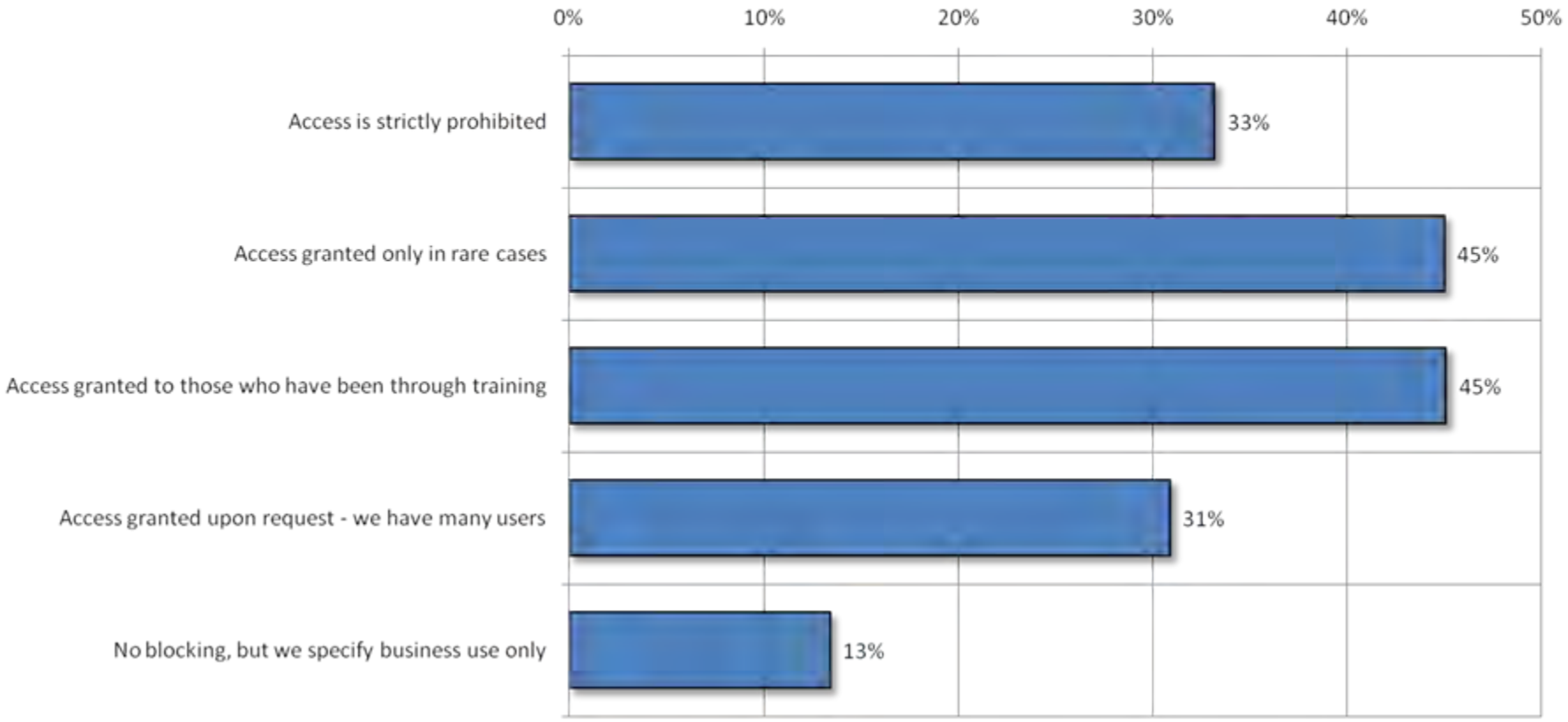


# Employee access to social media



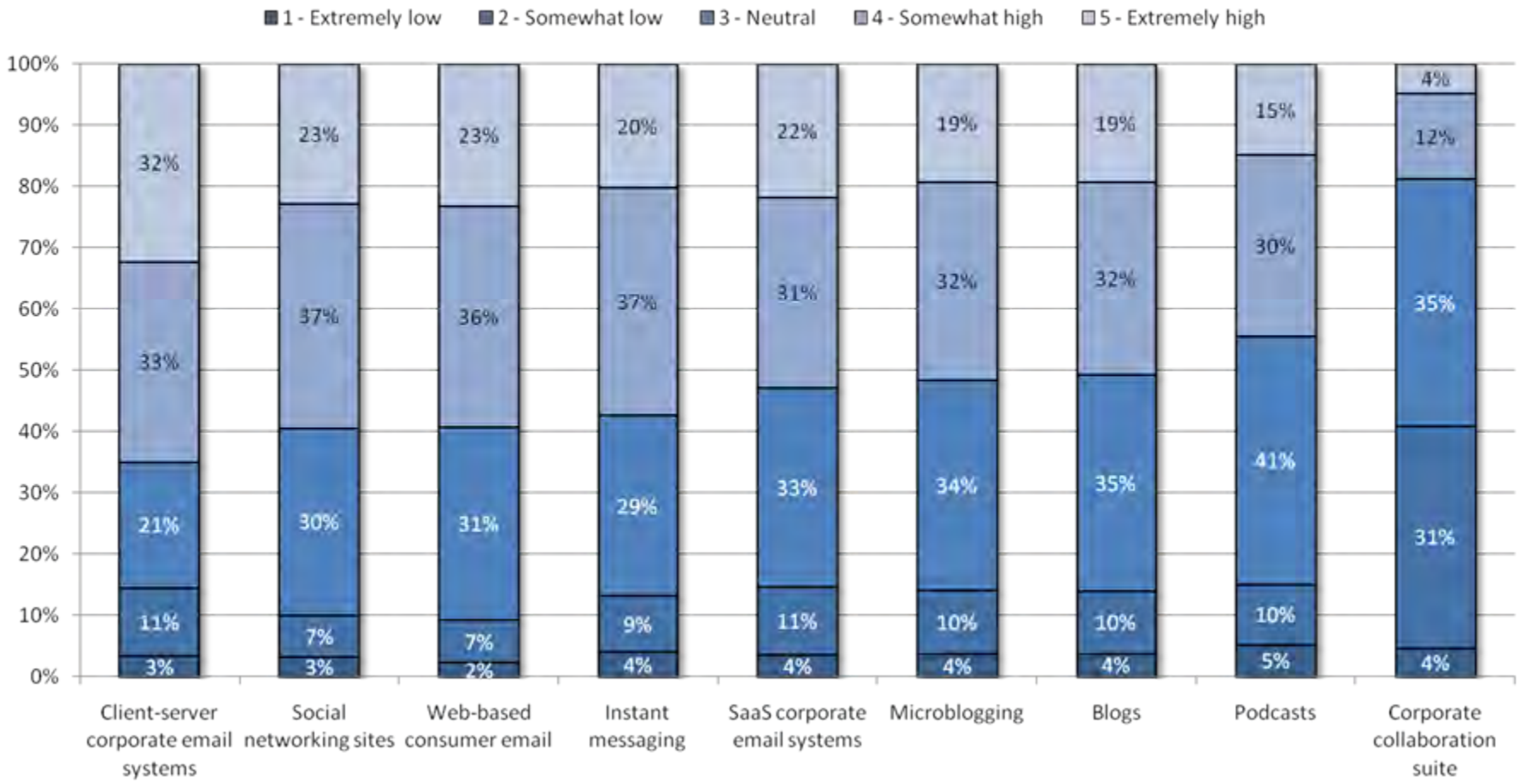
# Employee access to social media

**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)**



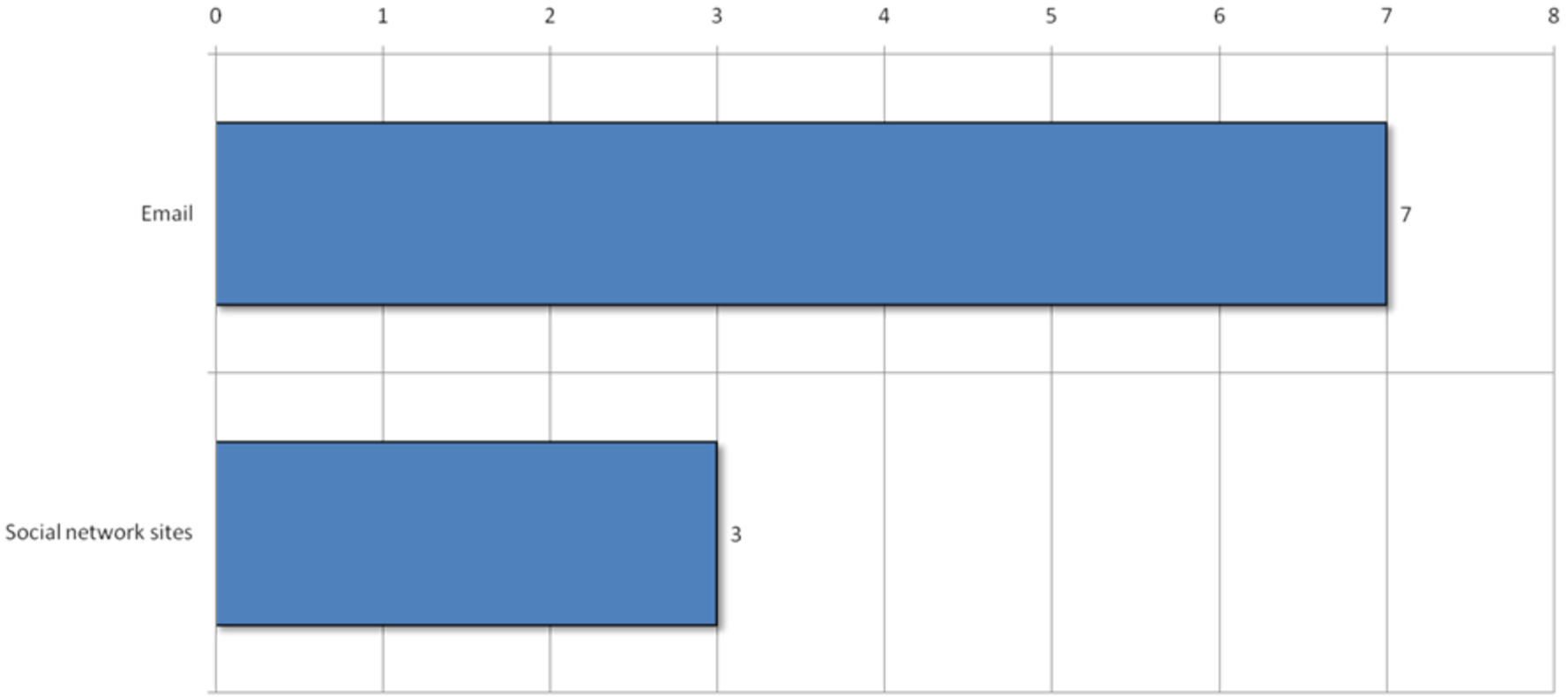
# Messaging/Collaboration threats

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

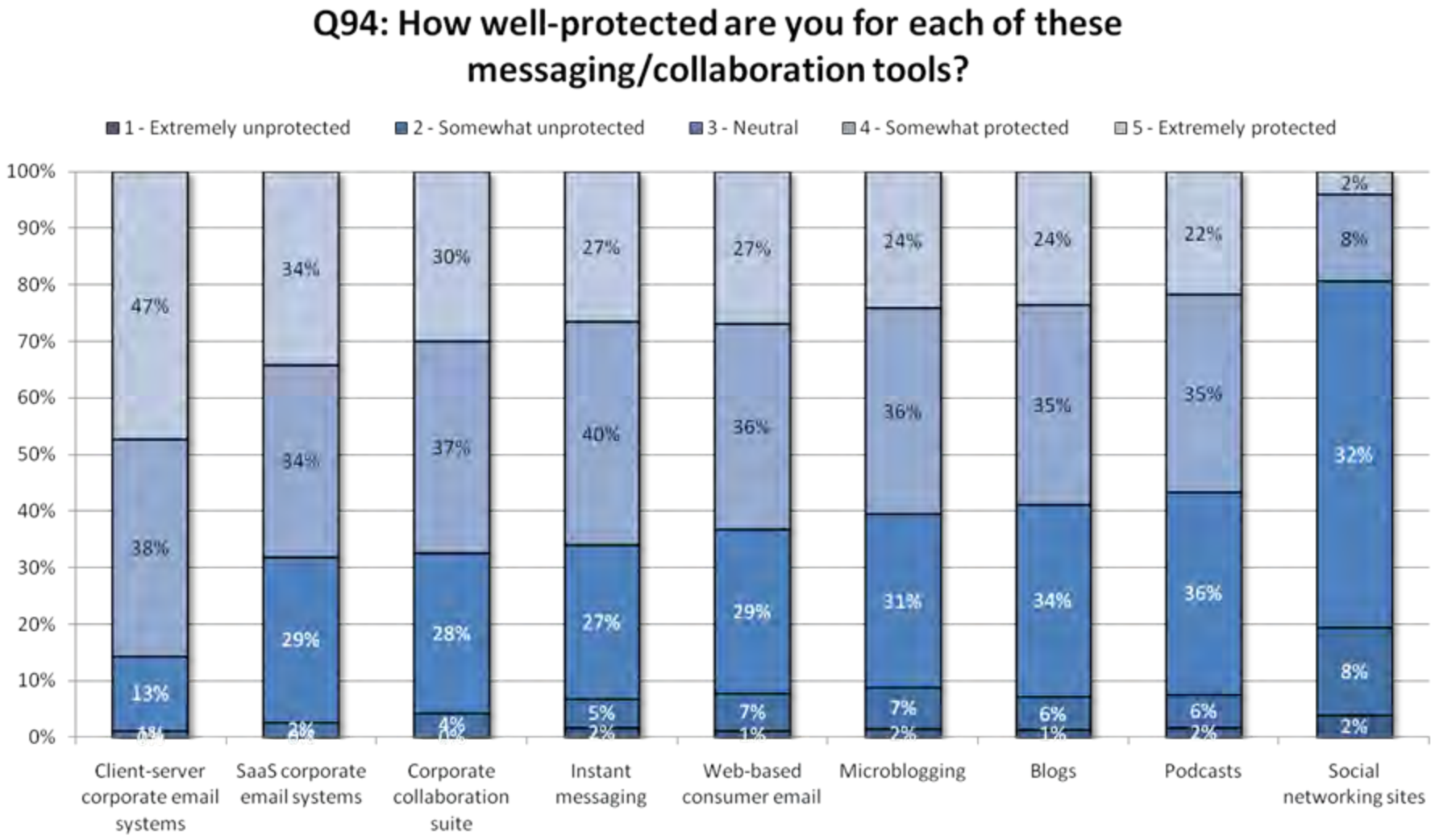


# Messaging/Collaboration security

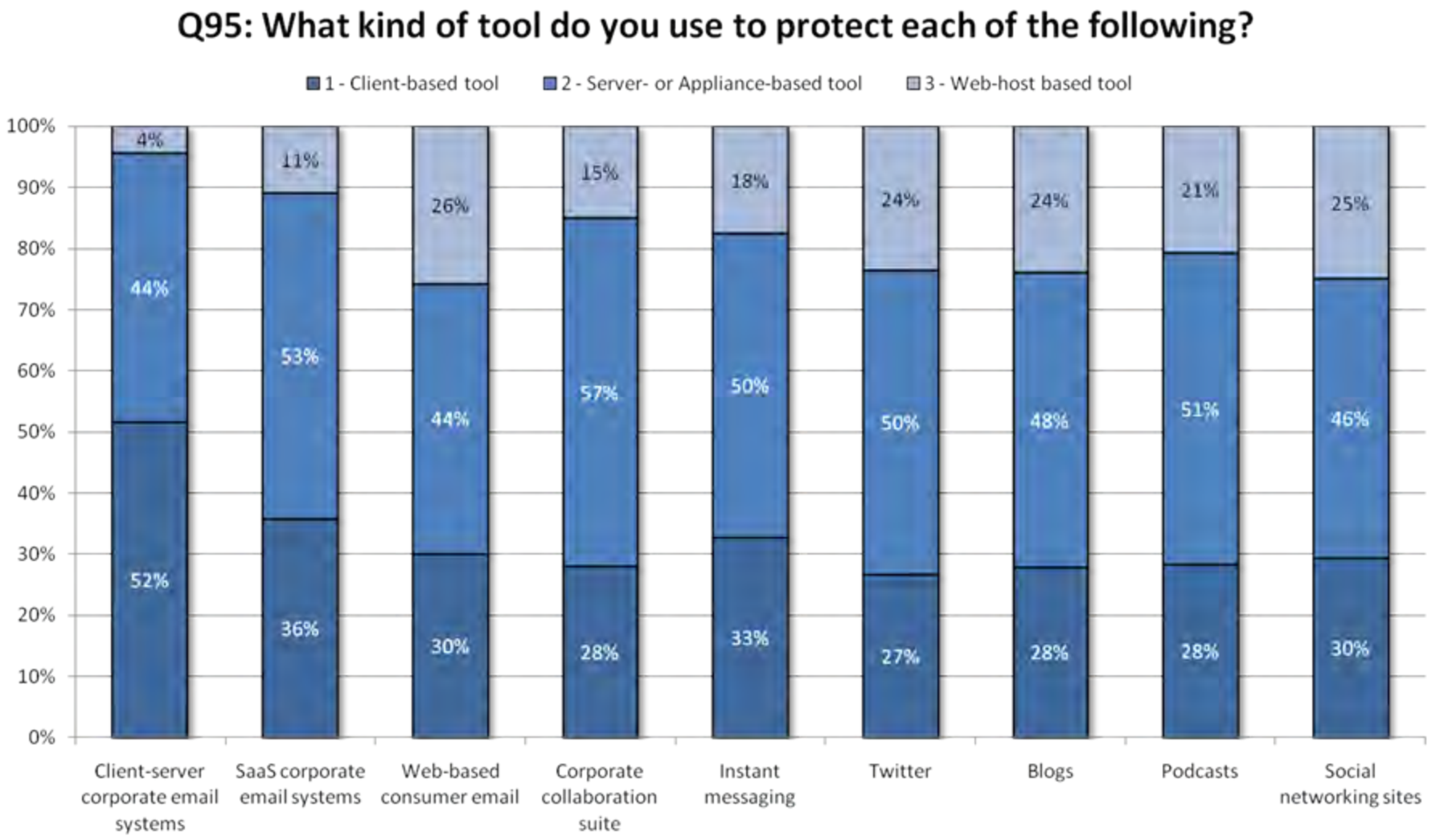
**Q93: How many security individual incidents have you experienced worldwide within your organization for each of these messaging/collaboration tools in the past 12 months?**
**(Medians shown)**



# Messaging/Collaboration protection

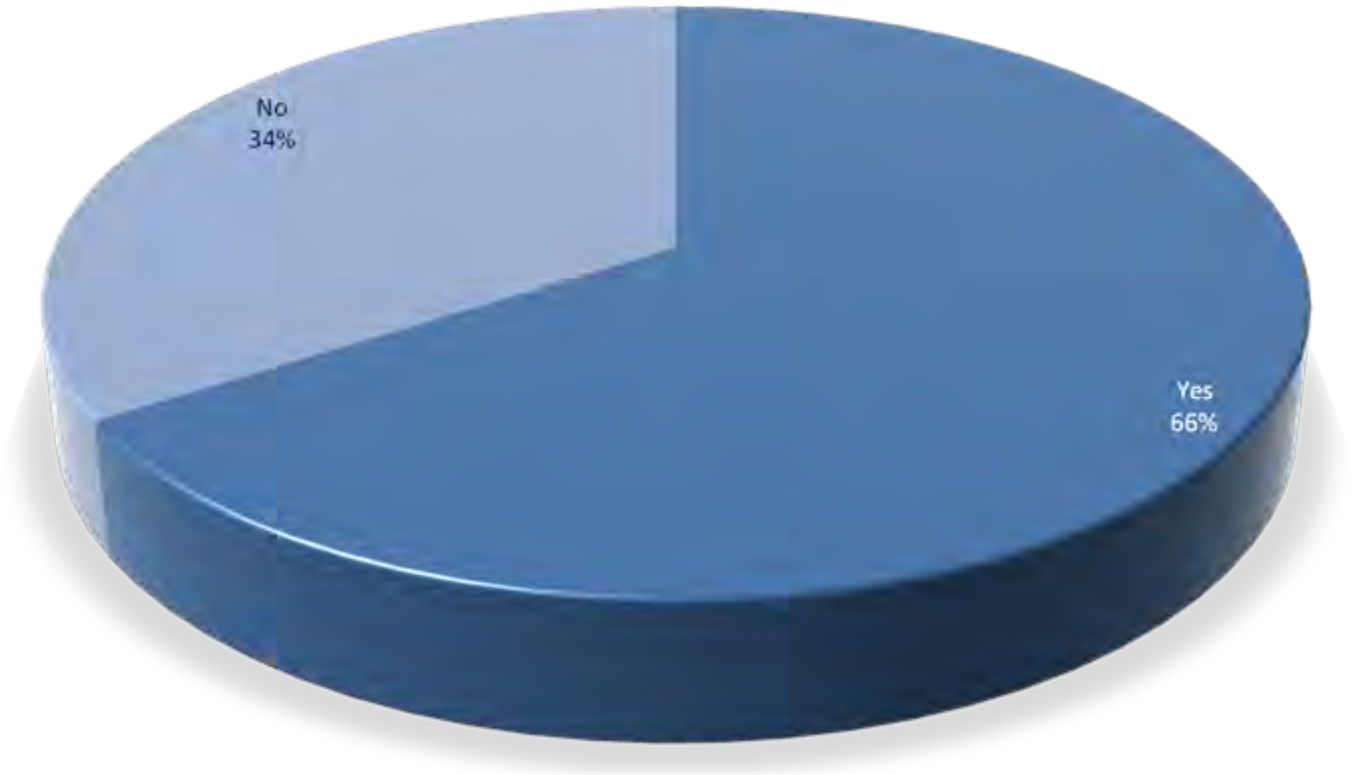


# Messaging/Collaboration protection



# Hosted security

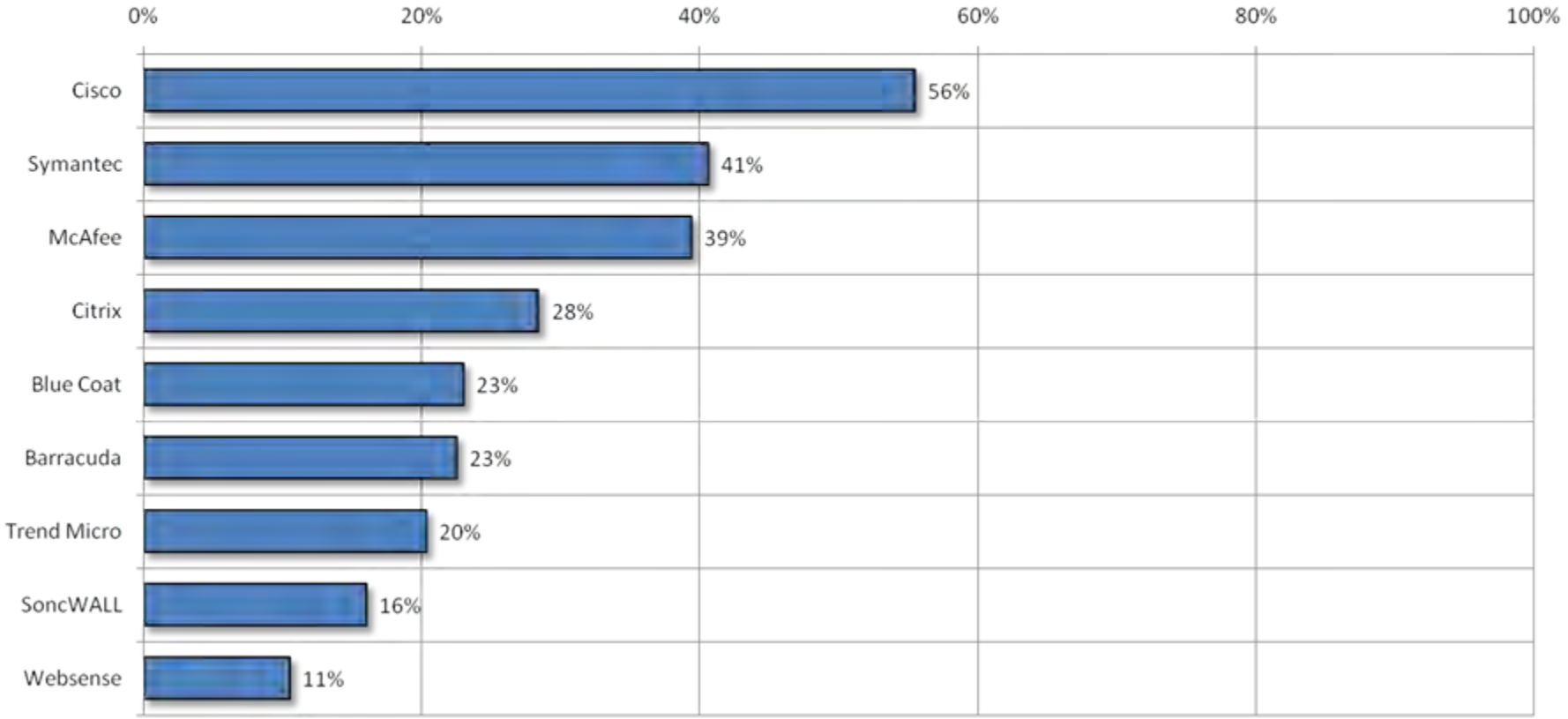
Q96: Do you have a gateway or hosted security product in front of your messaging/collaboration tools?



# Hosted security

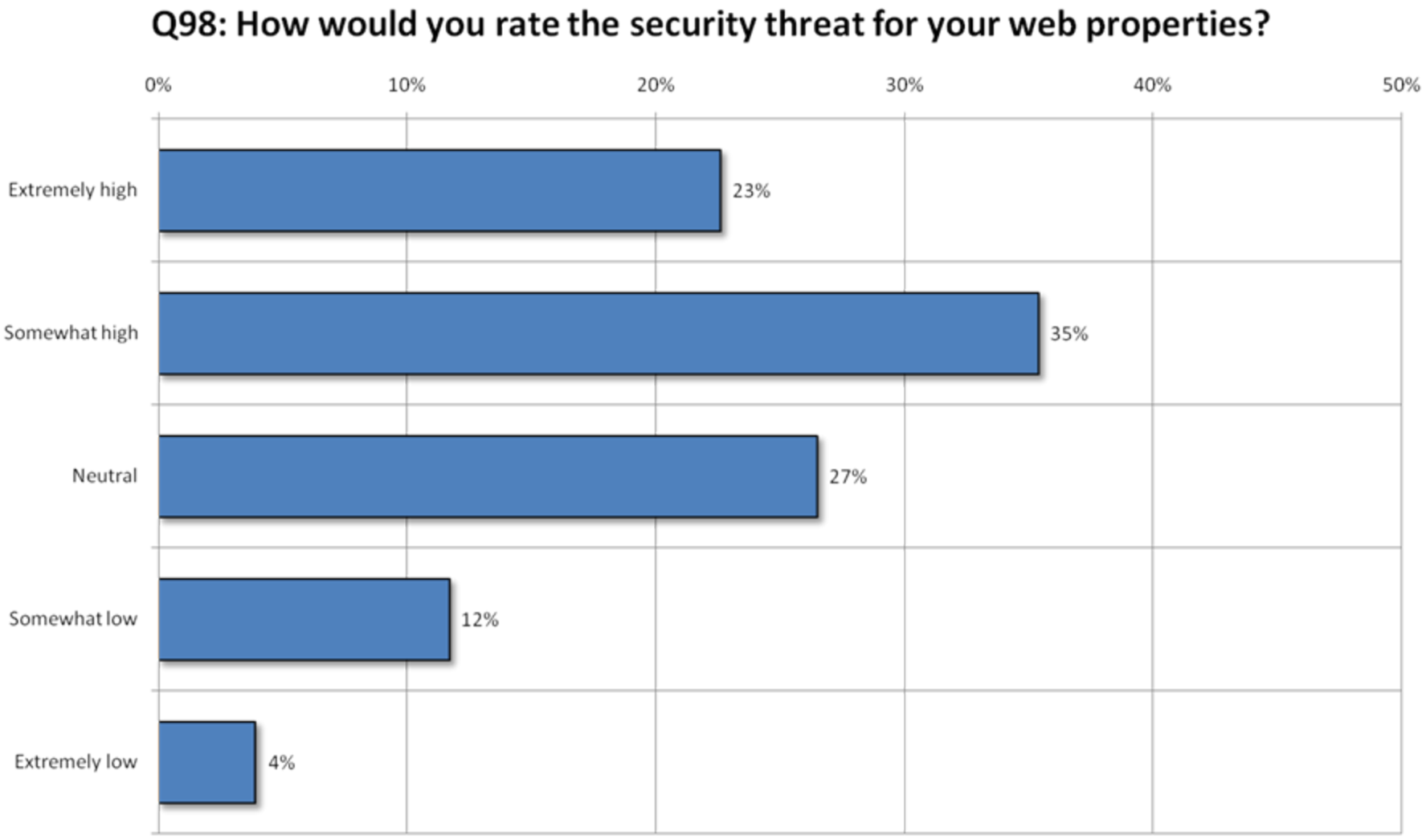
**Q97: Which gateway or hosted security product(s) do you use in front of your messaging collaboration tools? Mark all that apply.**

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

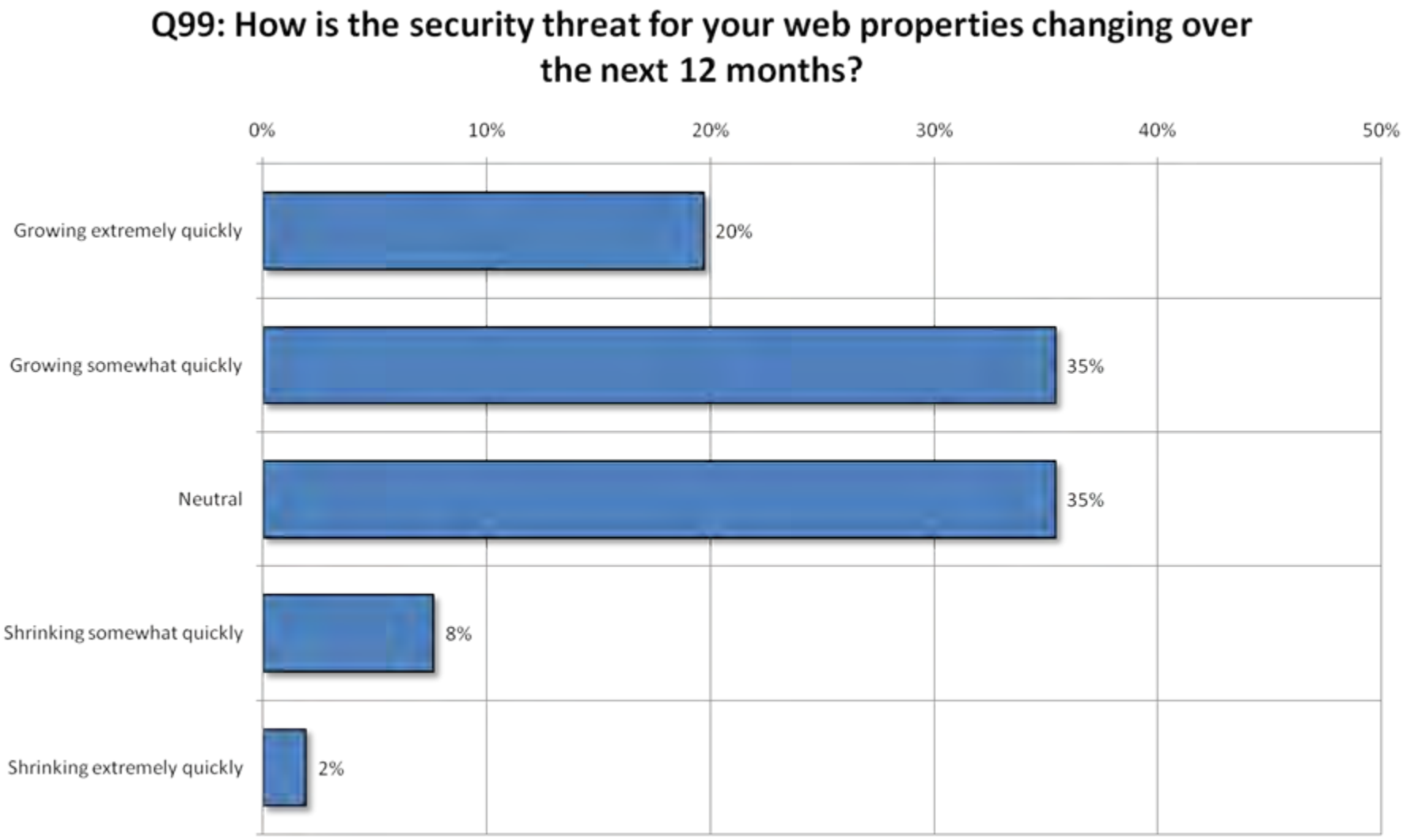


# Web Security

# Web property security



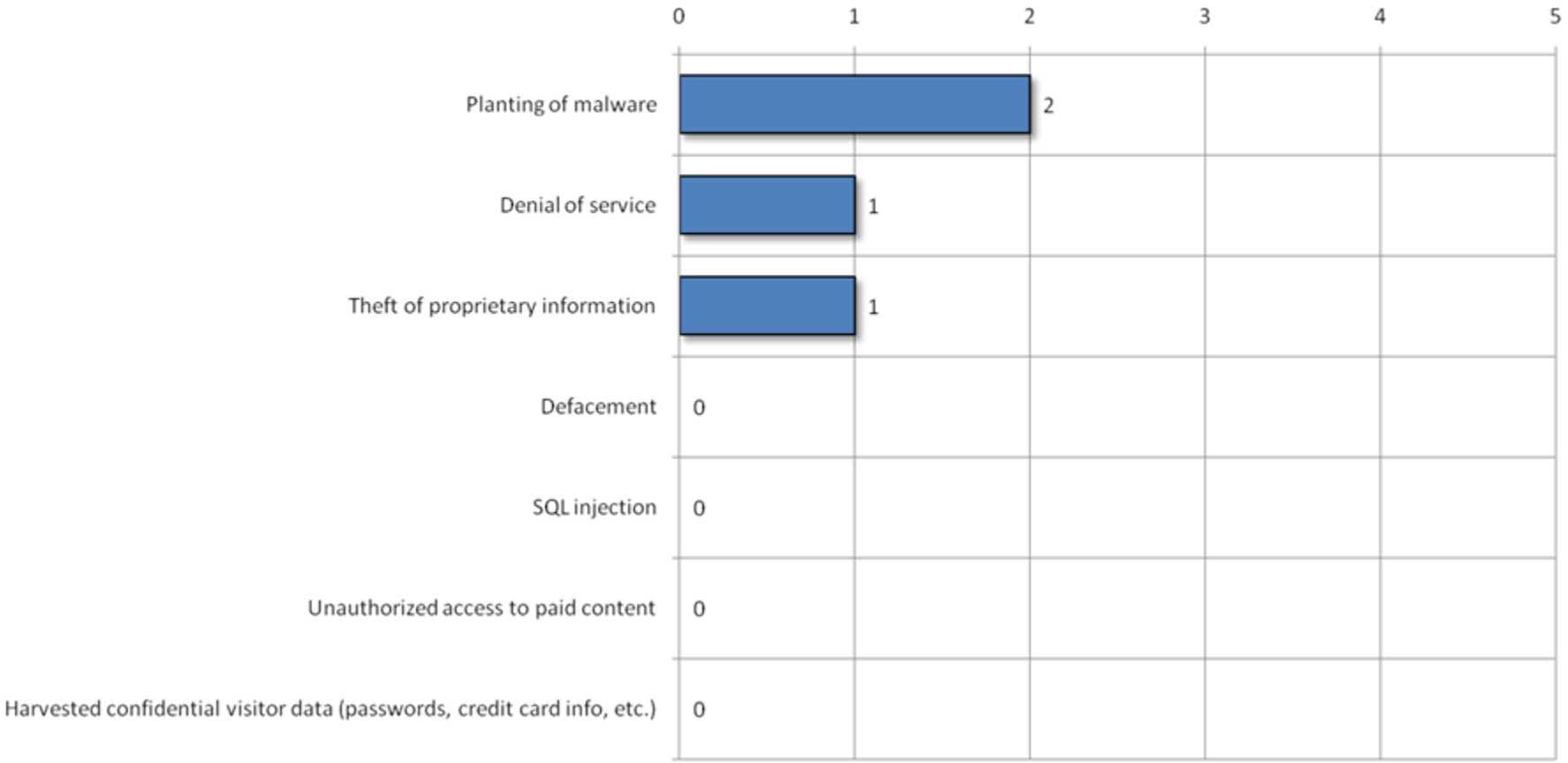
# Web property security



# 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?

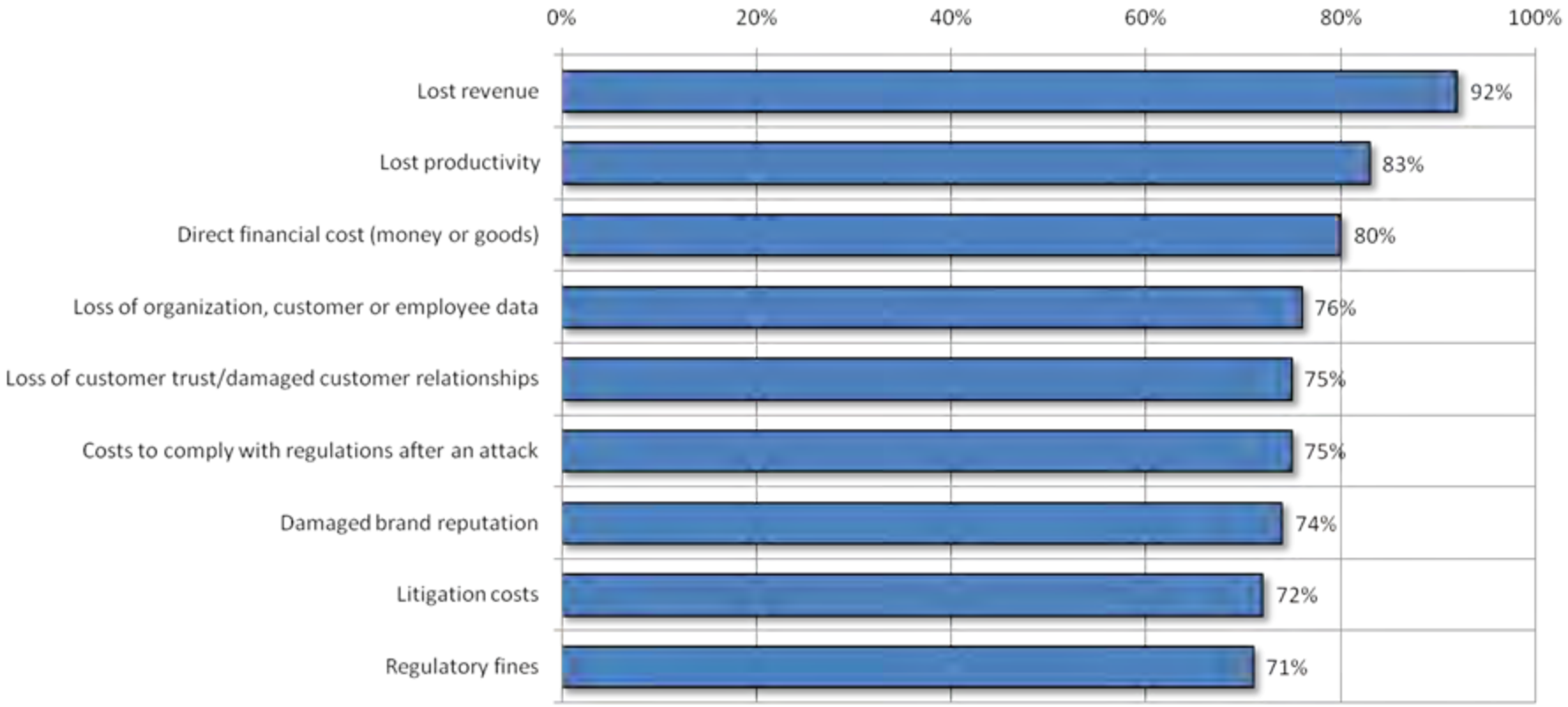
(Medians shown)



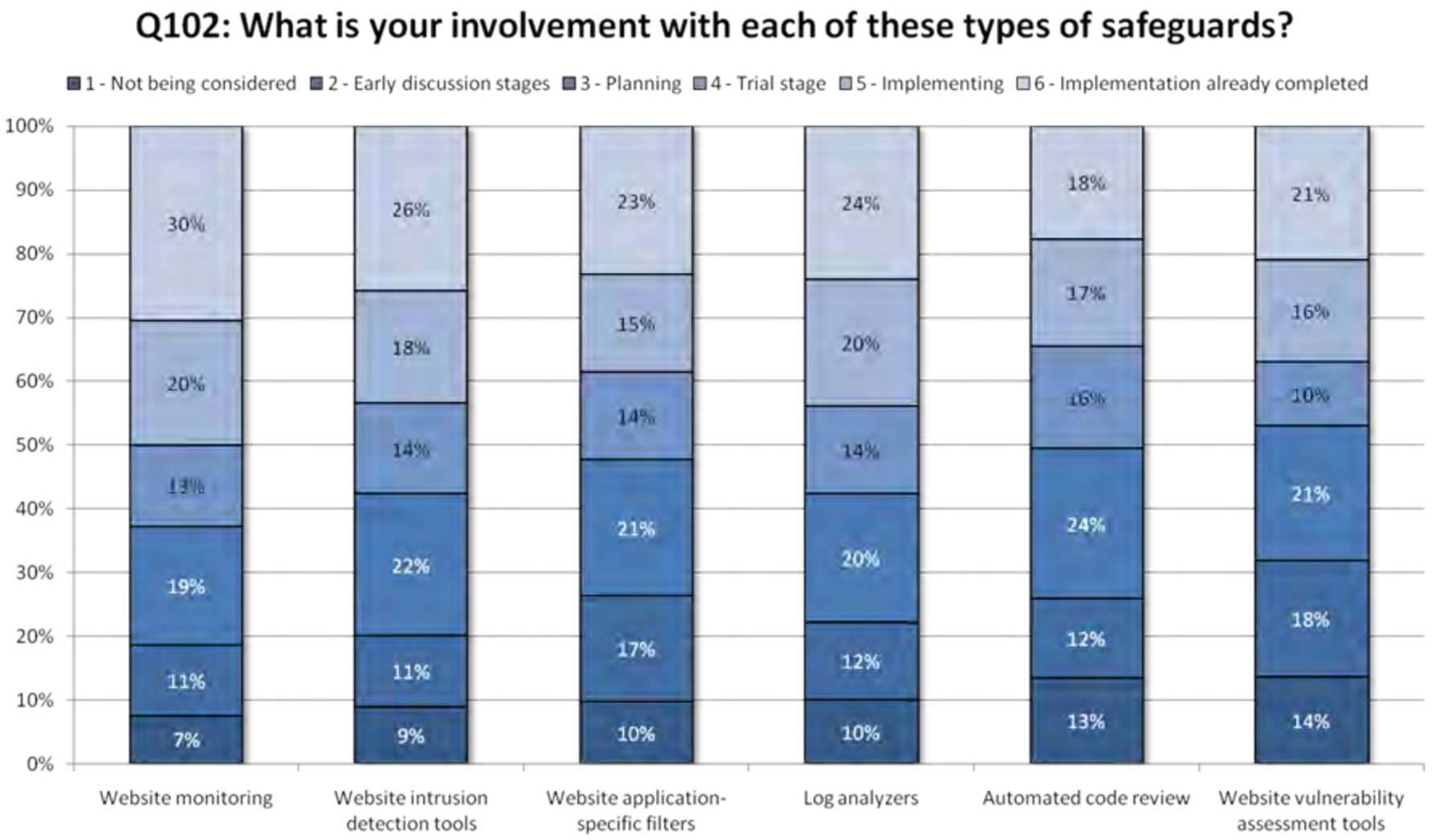
# Web property attack costs

**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)**

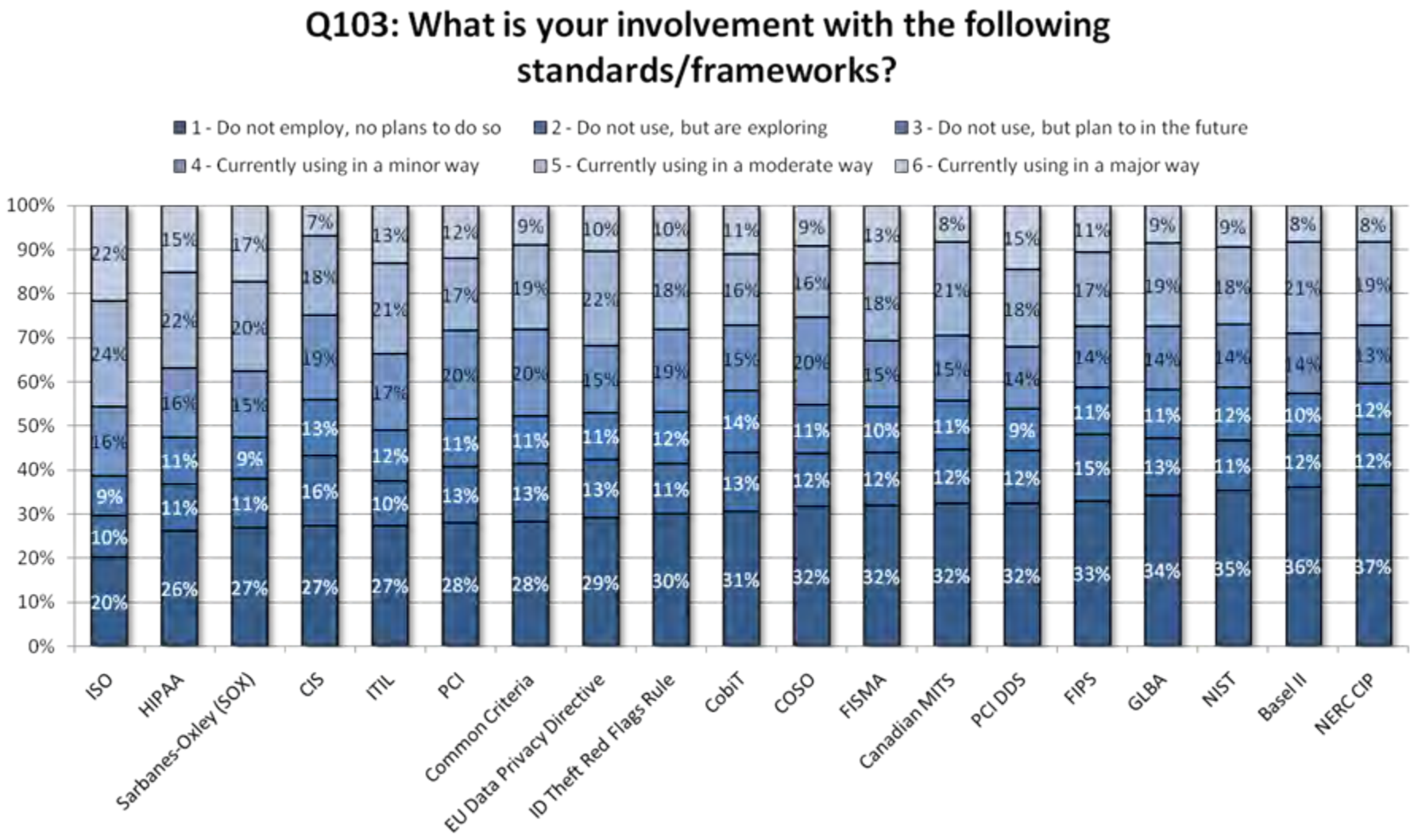


# Safeguards


Q102: What is your involvement with each of these types of safeguards?
1 - Not being considered
2 - Early discussion stages
3 - Planning
4 - Trial stage
5 - Implementing
6 - Implementation already completed
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
30%
20%
13%
19%
11%
7%
26%
18%
14%
22%
11%
9%
23%
15%
14%
21%
17%
10%
24%
20%
14%
20%
12%
10%
18%
17%
16%
24%
12%
13%
21%
16%
10%
21%
18%
14%
Website monitoring
Website intrusion detection tools
Website application-specific filters
Log analyzers
Automated code review
Website vulnerability assessment tools

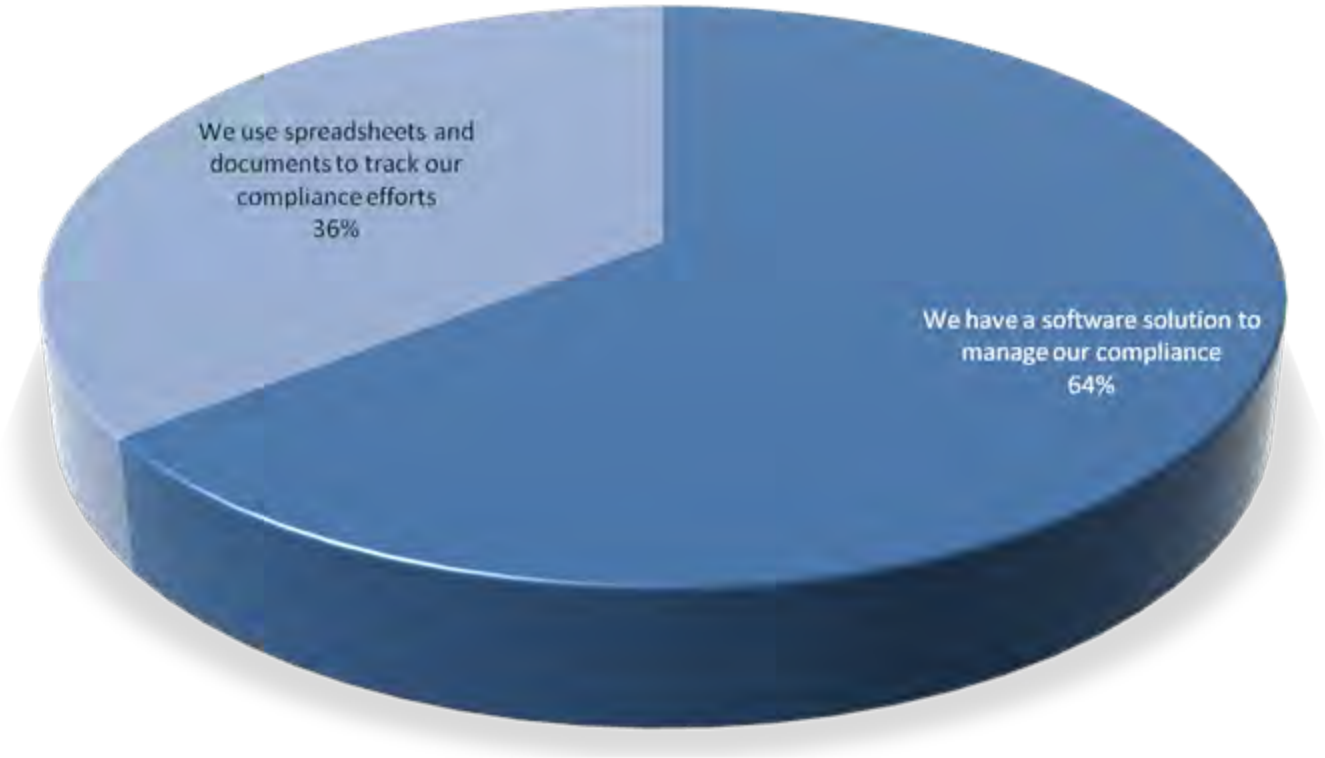
# Compliance

# Standards and frameworks



# Standard compliance

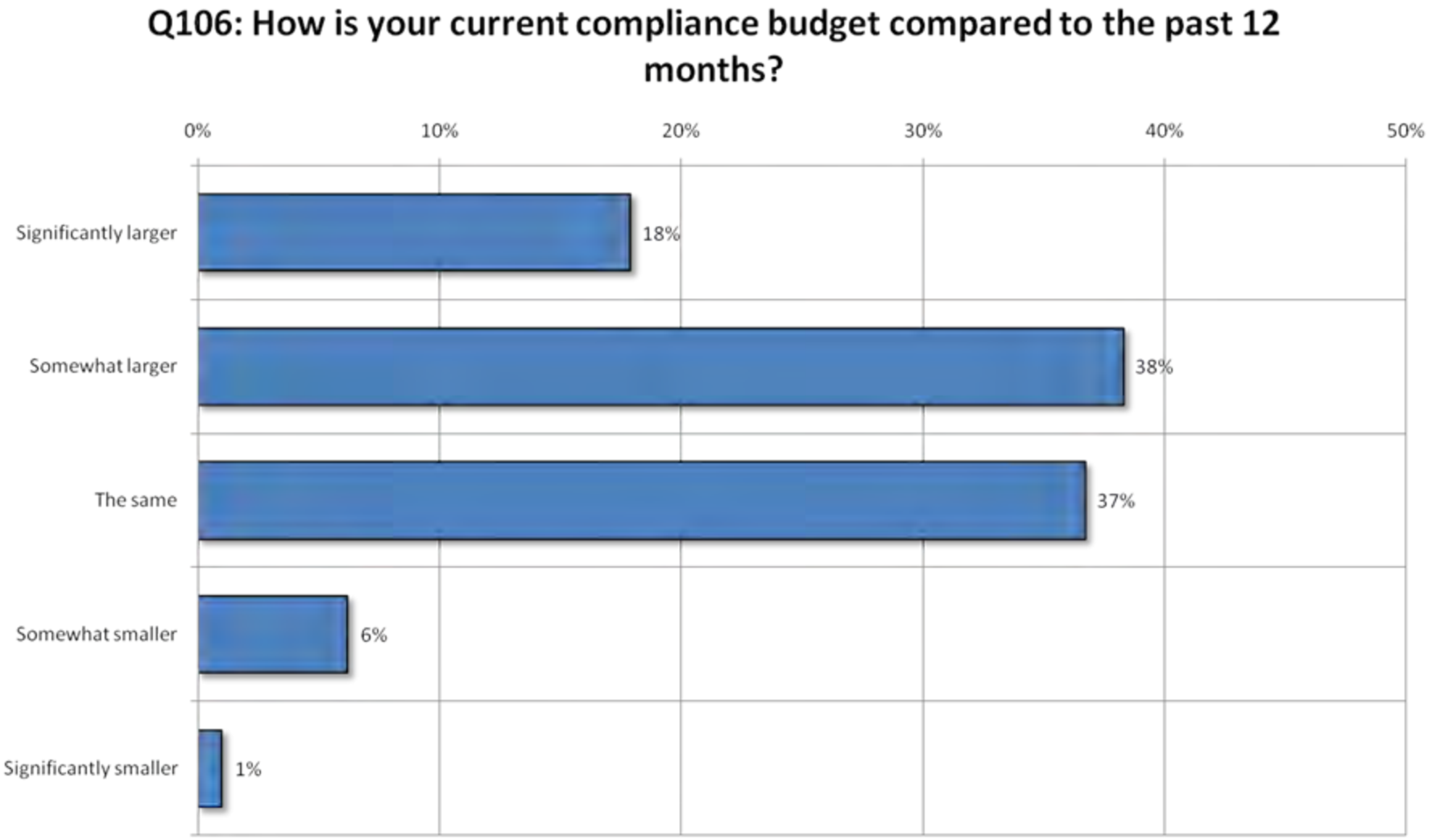
**Q104: How automated are your efforts to comply with the various standards, frameworks, and regulations?**



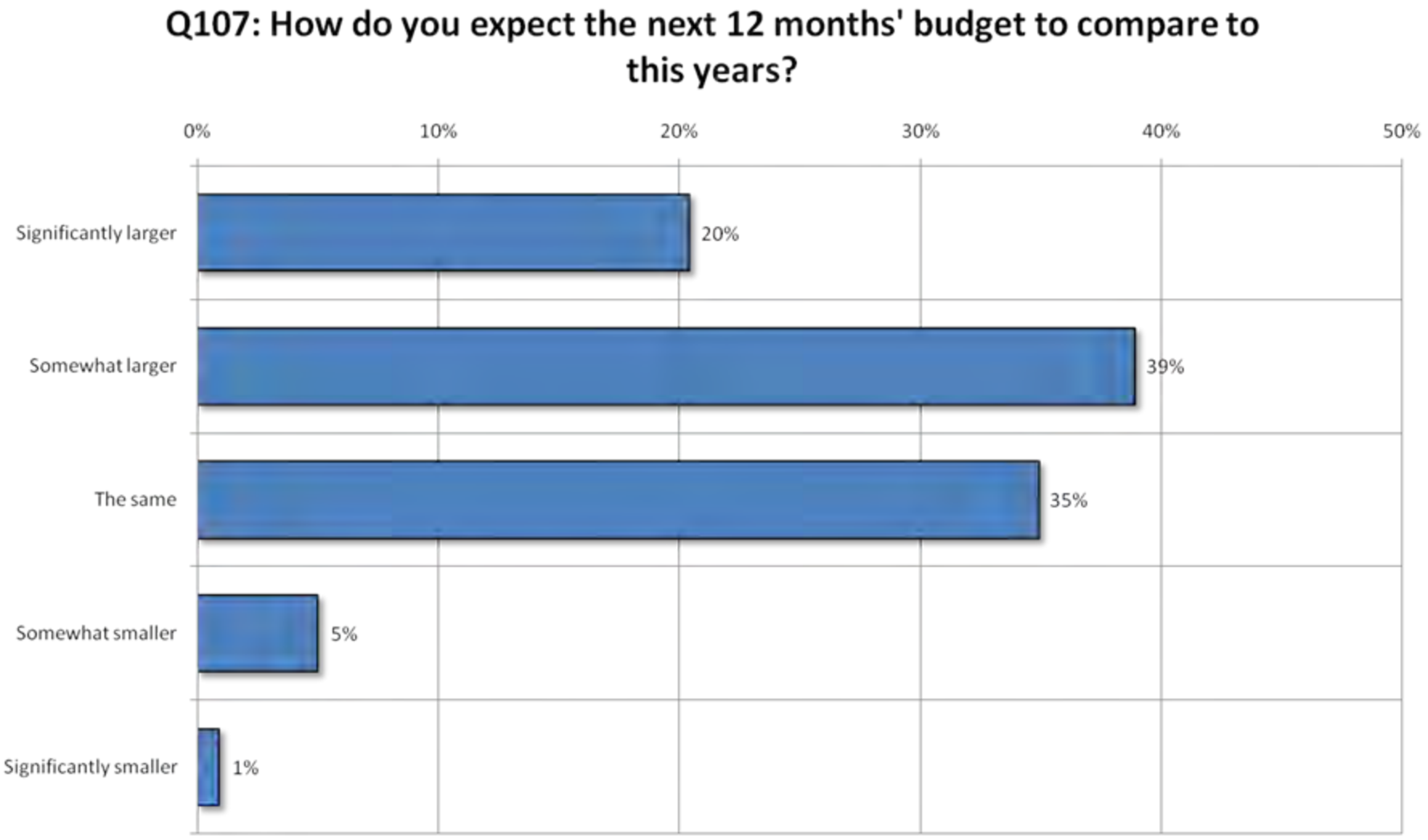
# Compliance budget

| Q105: What is your total budget for compliance efforts worldwide? | |
|---|---|
| Median | $200,000 |

# Compliance budget

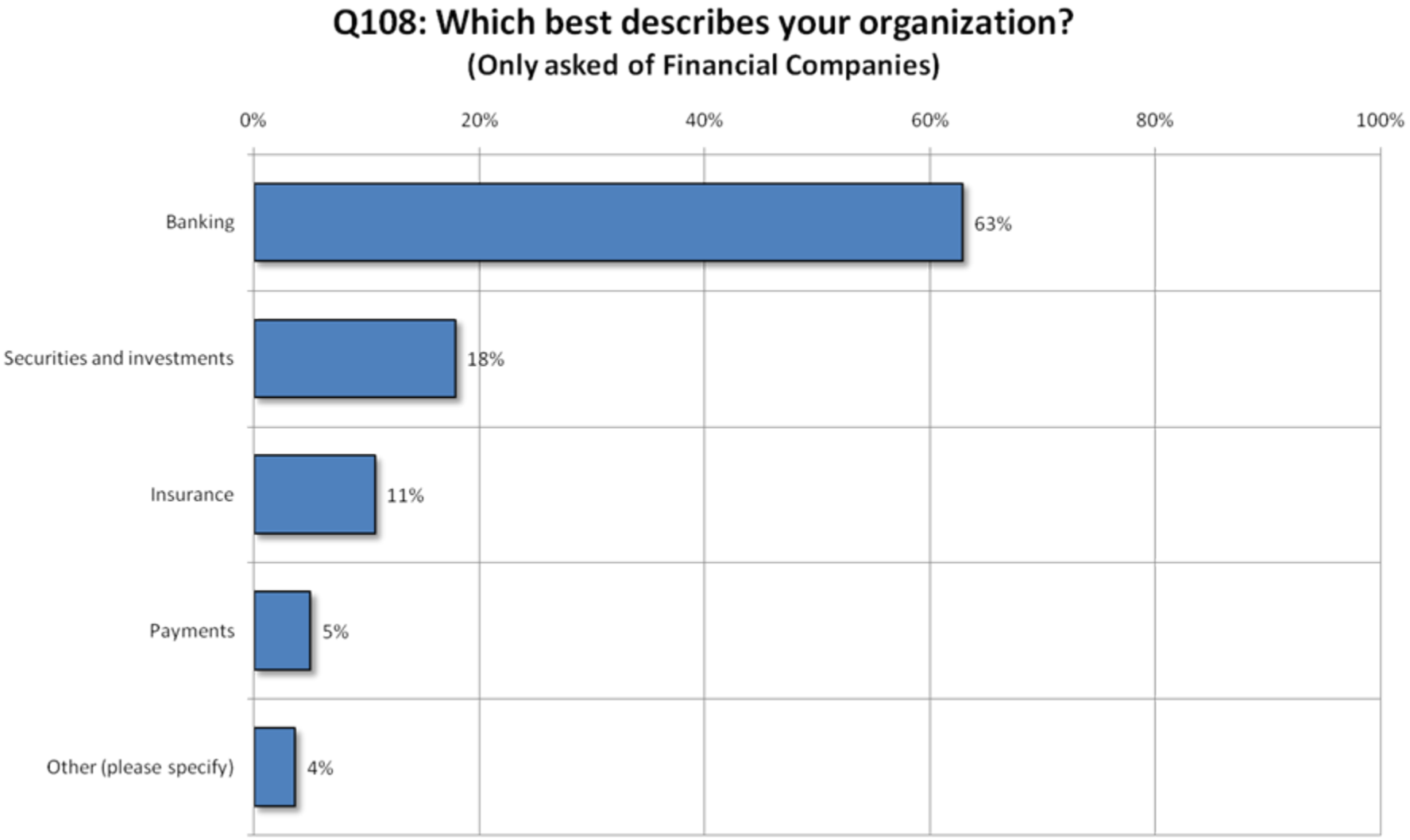


# Compliance budget



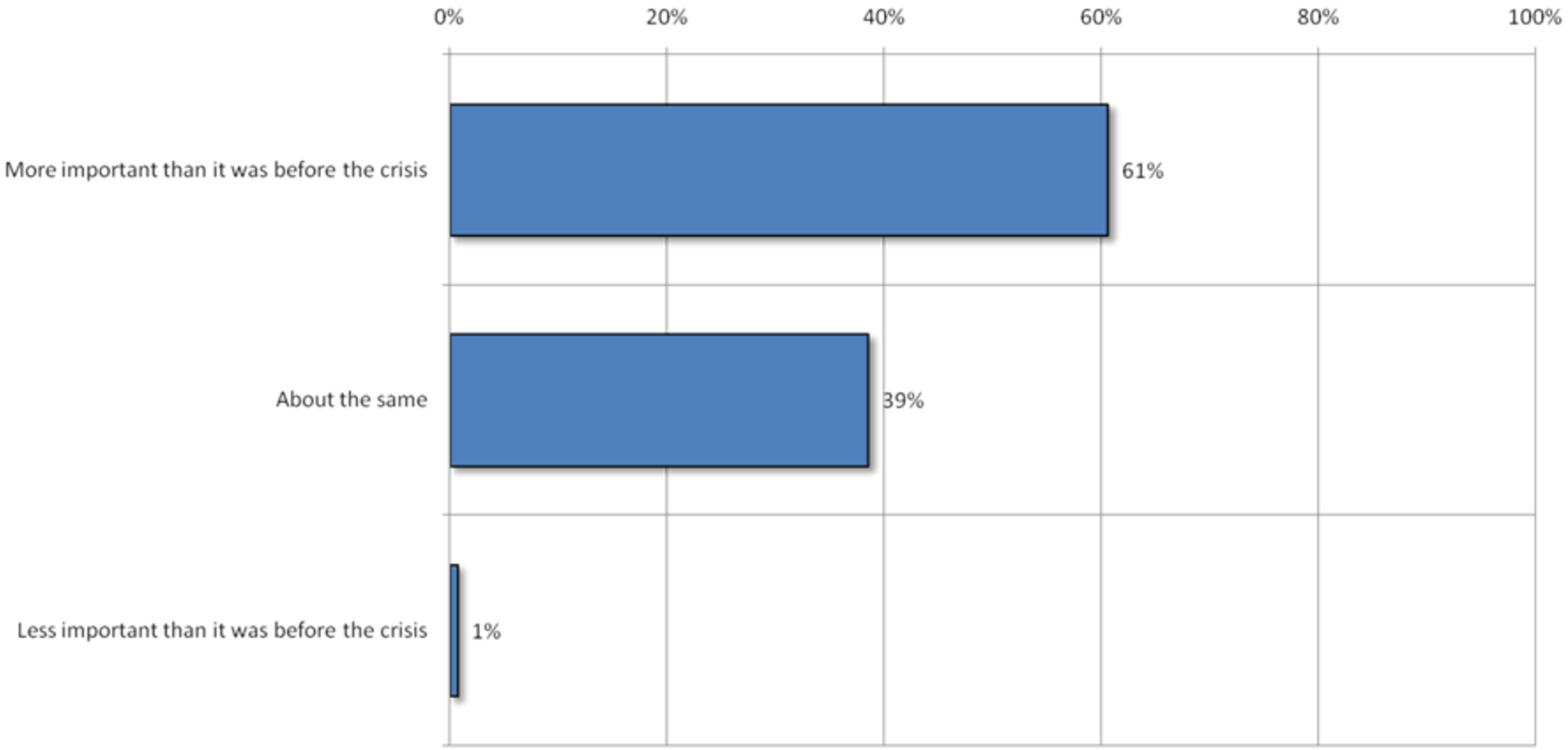
# Industry Verticals: Financial

# Industry Verticals: Financial



# Industry Verticals: Financial

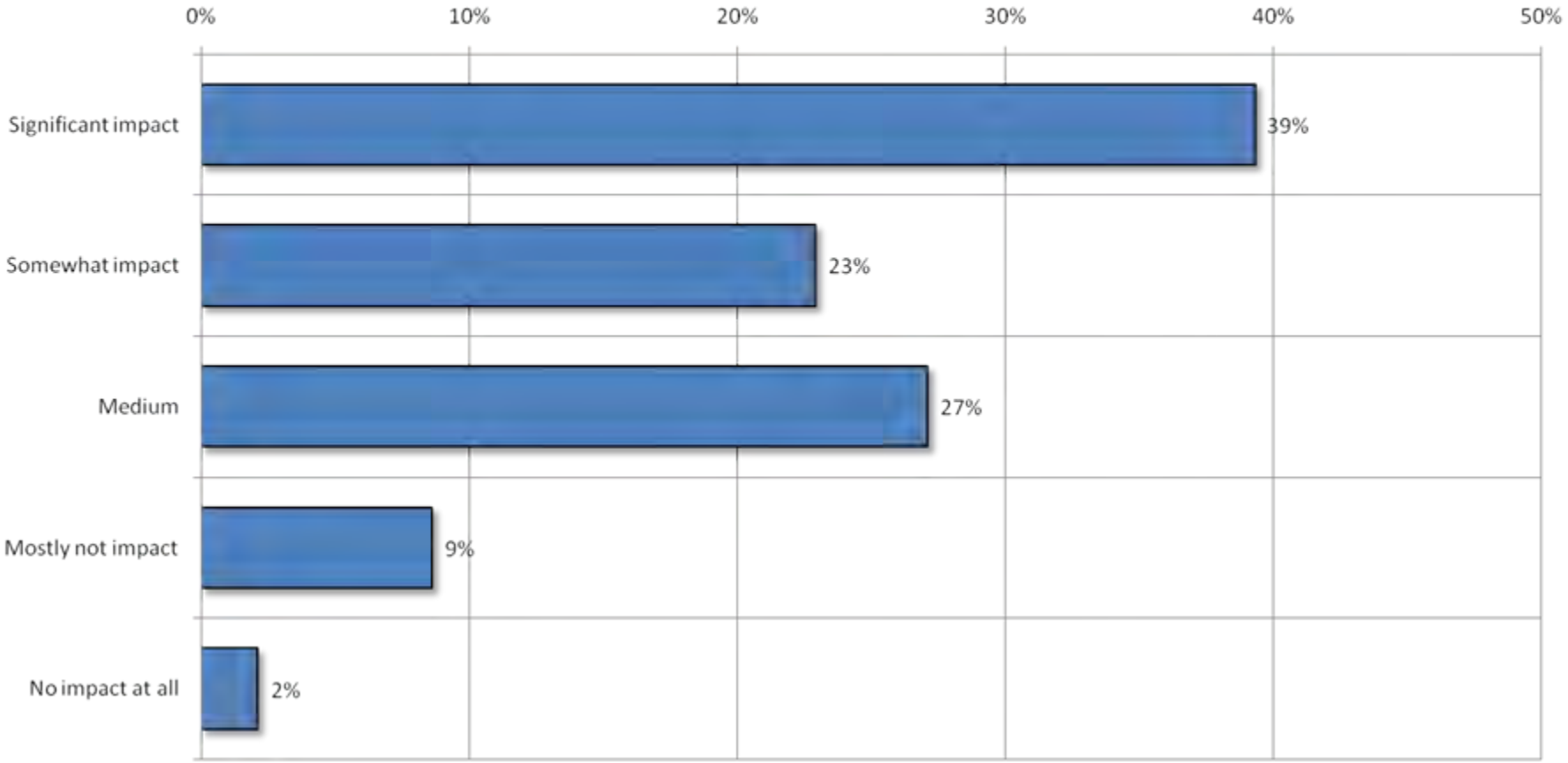
**Q109: Considering the financial crisis of the past year, do you find your IT security to be...?**
**(Only asked of Financial Companies)**



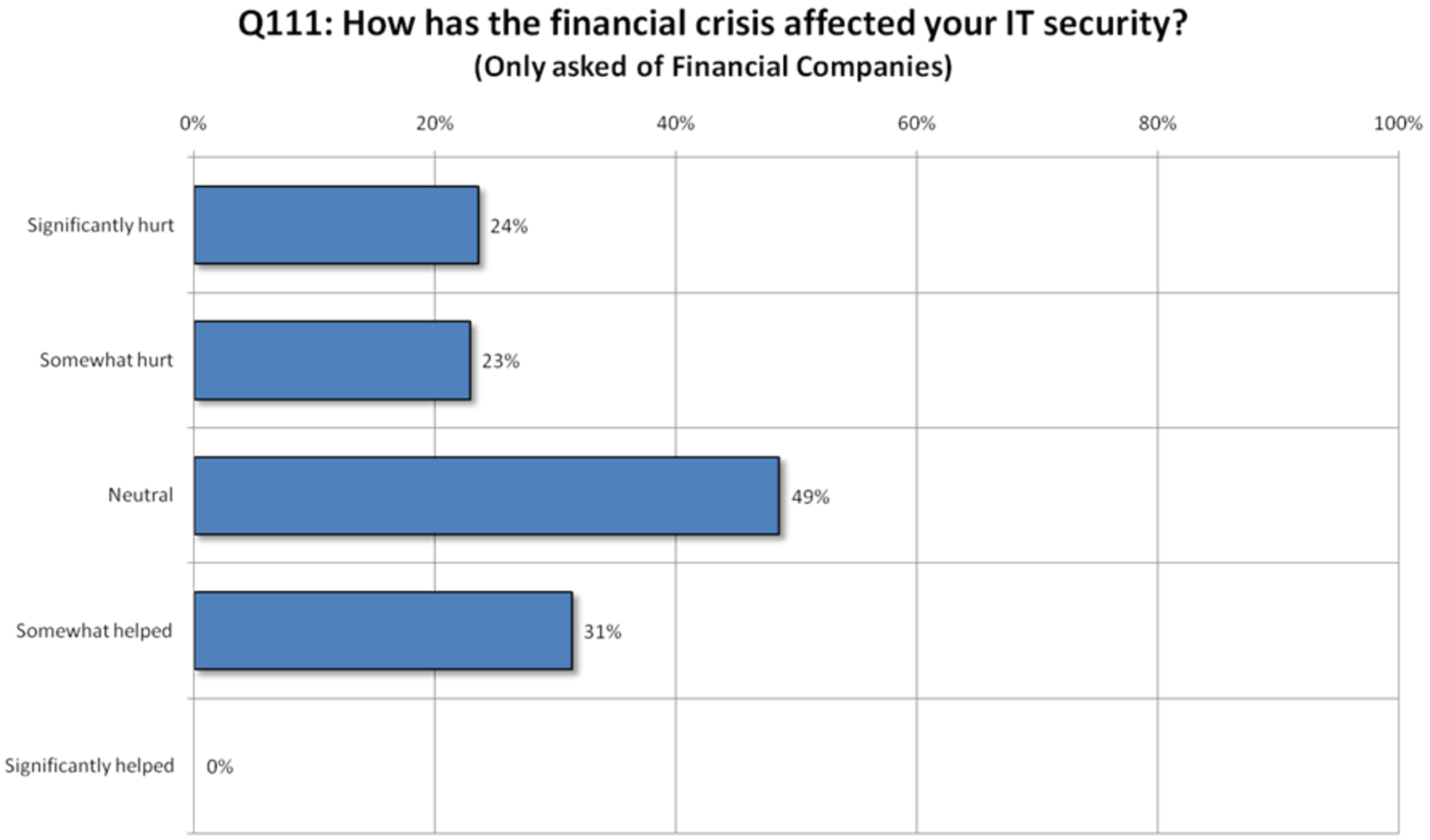
# Industry Verticals: Financial

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

(Only asked of Financial Companies)

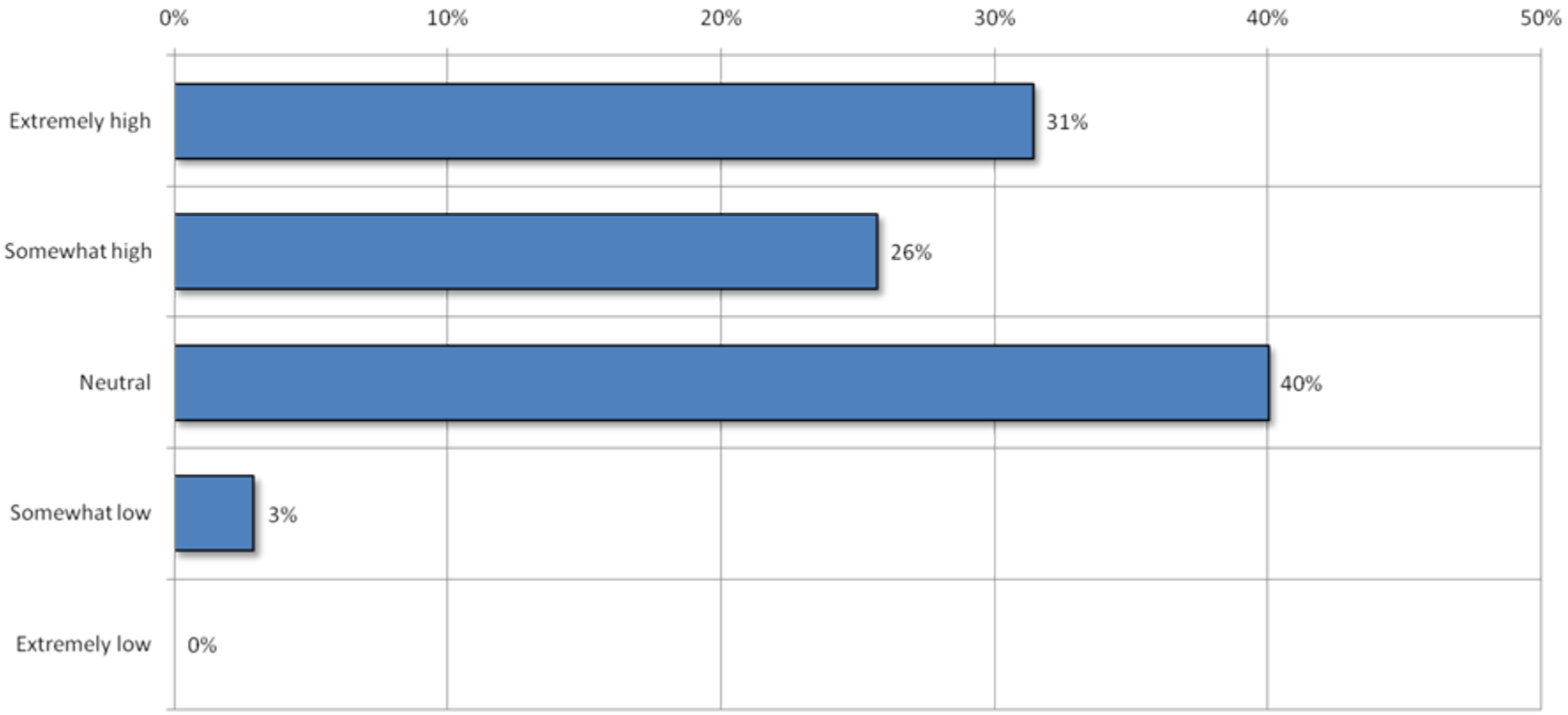


# Industry Verticals: Financial

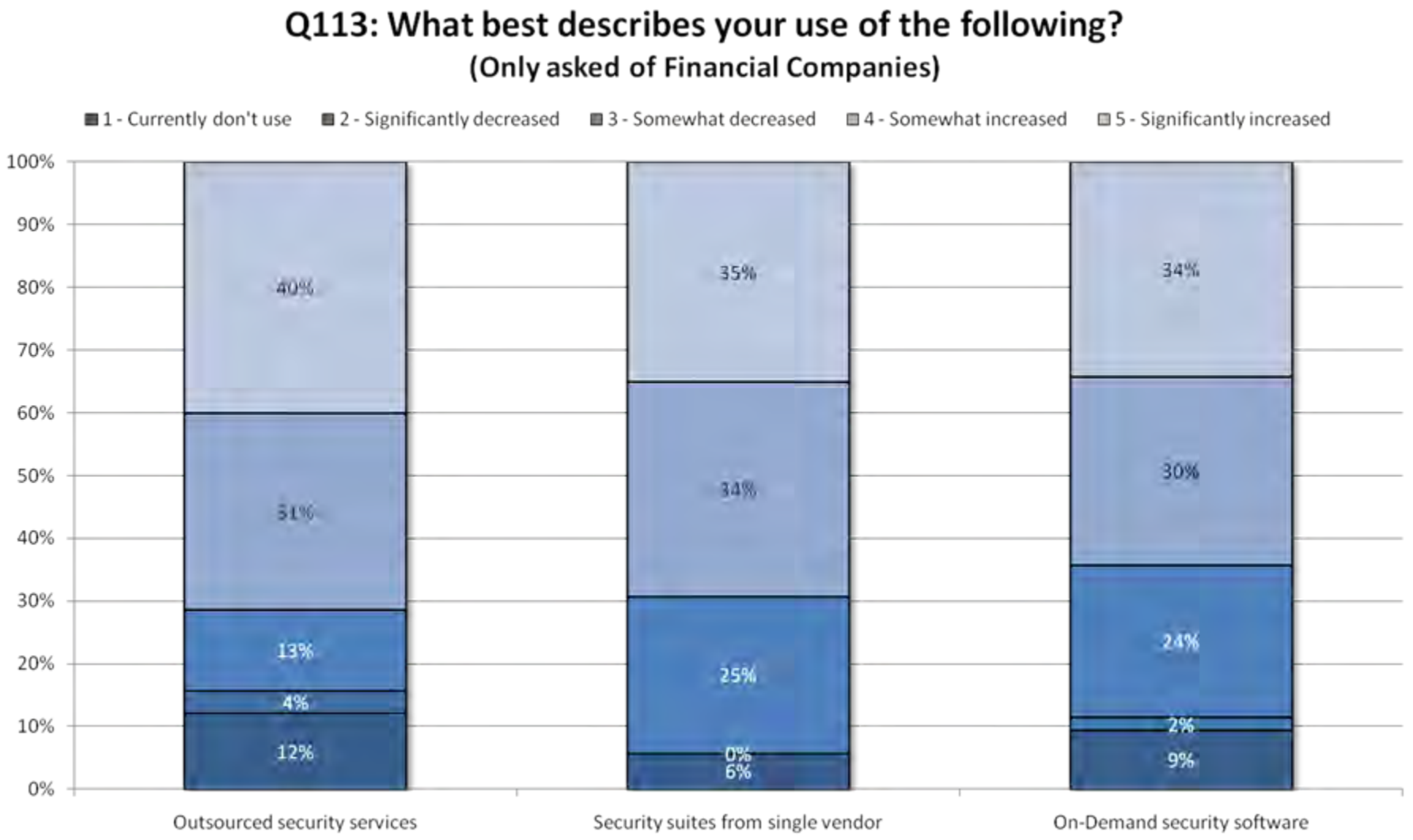


# Industry Verticals: Financial

**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)**

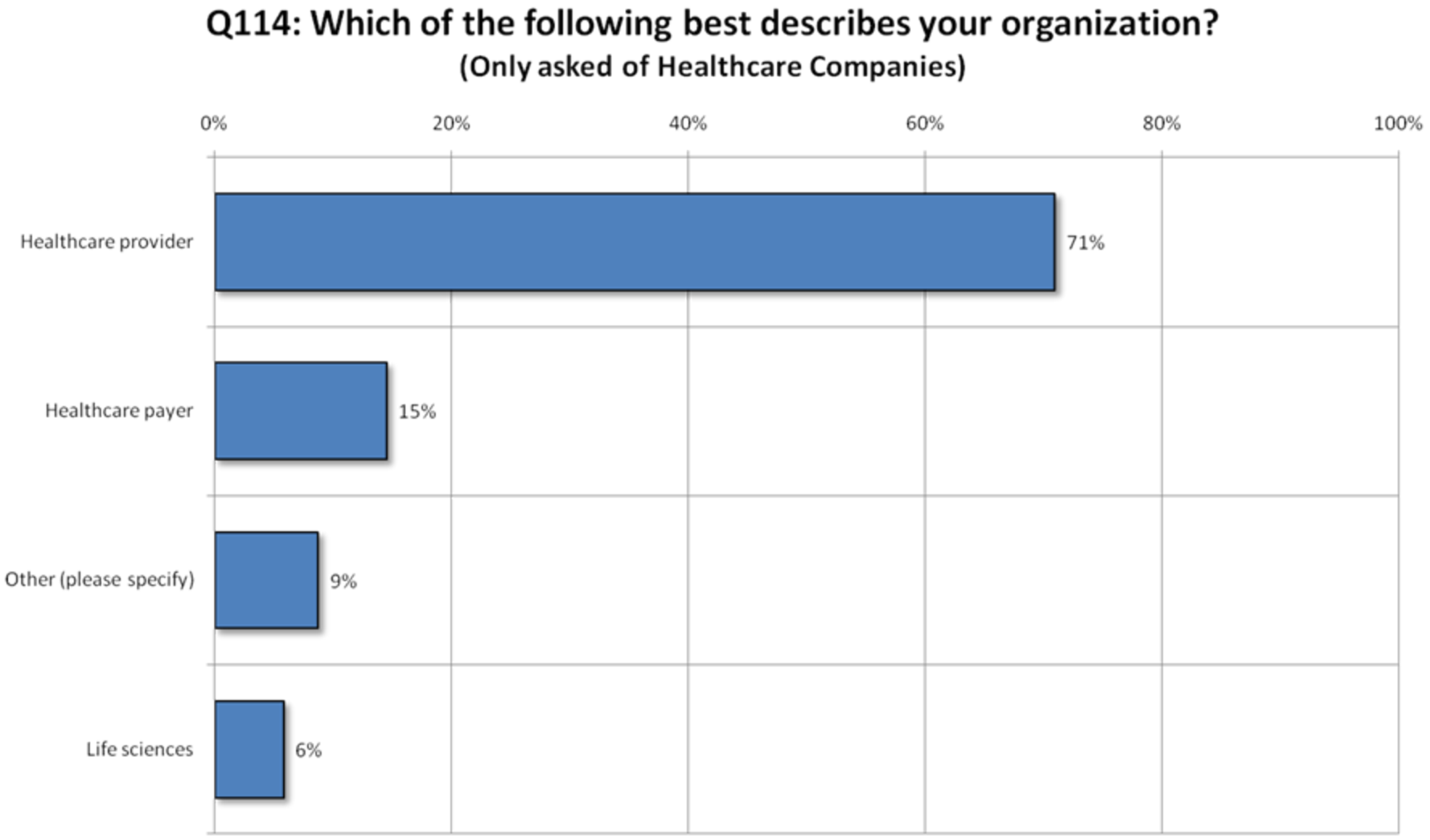


# Industry Verticals: Financial

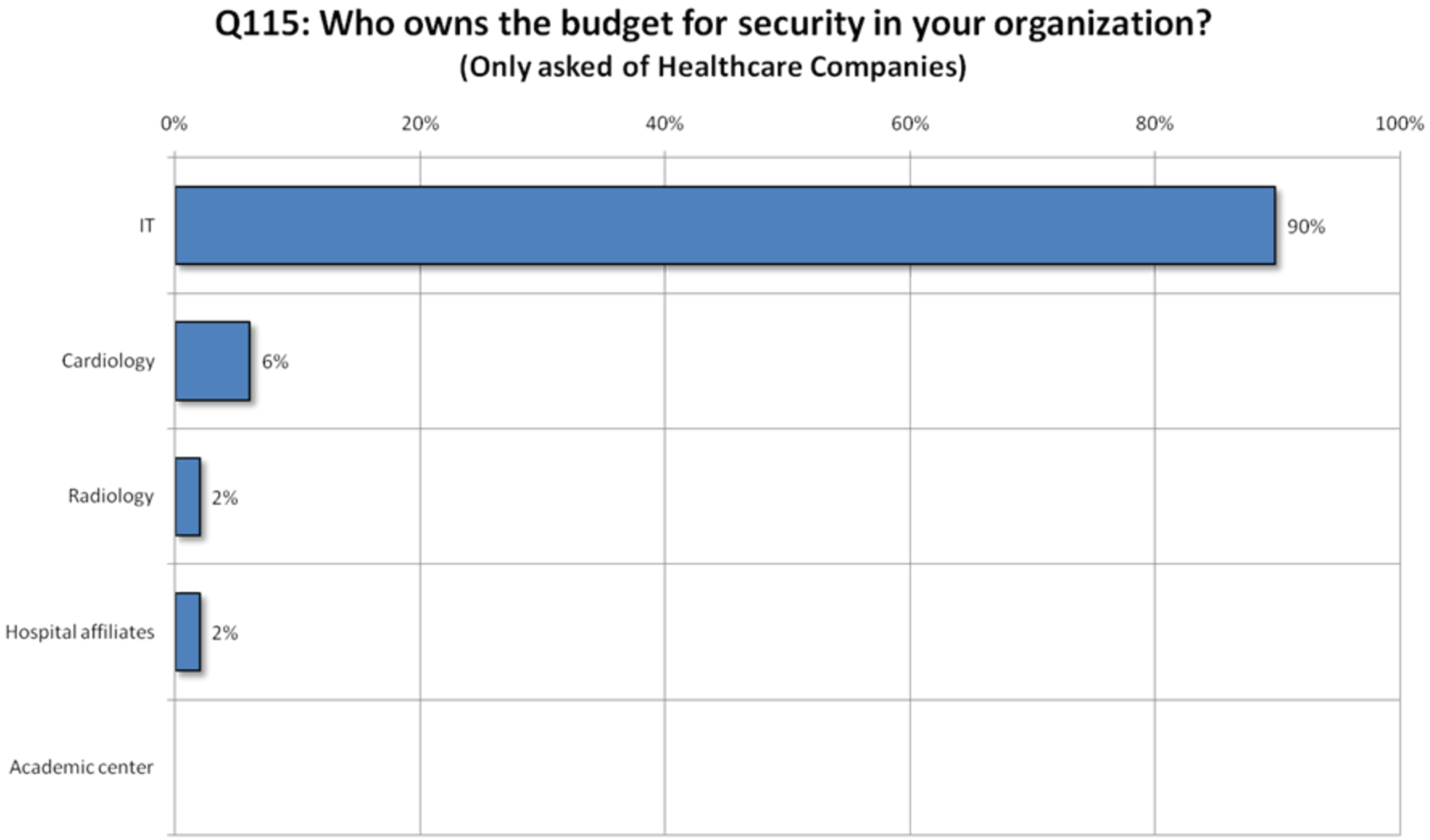


# Industry Verticals: Healthcare

# Industry Verticals: Healthcare

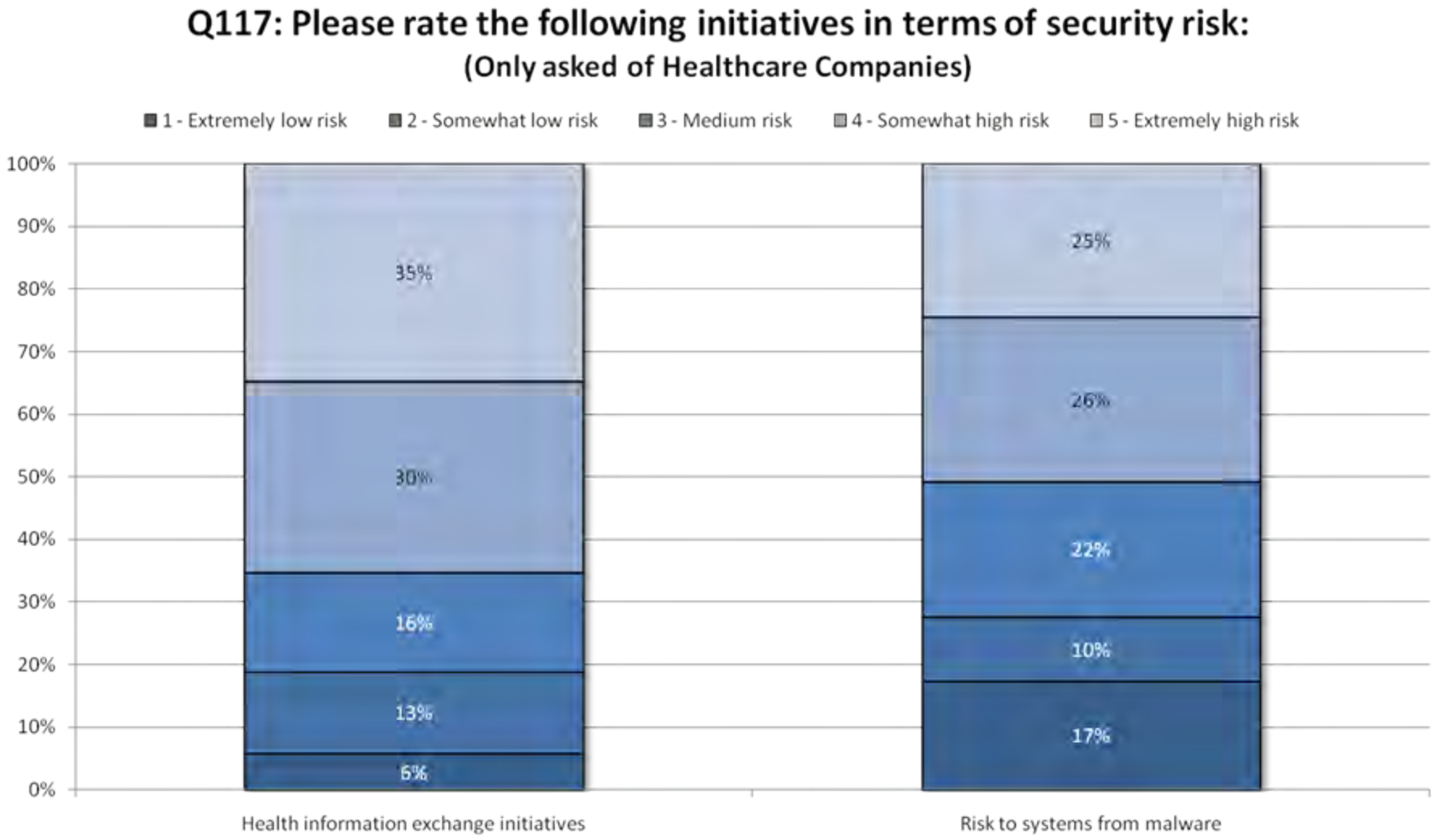


# Industry Verticals: Healthcare



# Industry Verticals: Healthcare

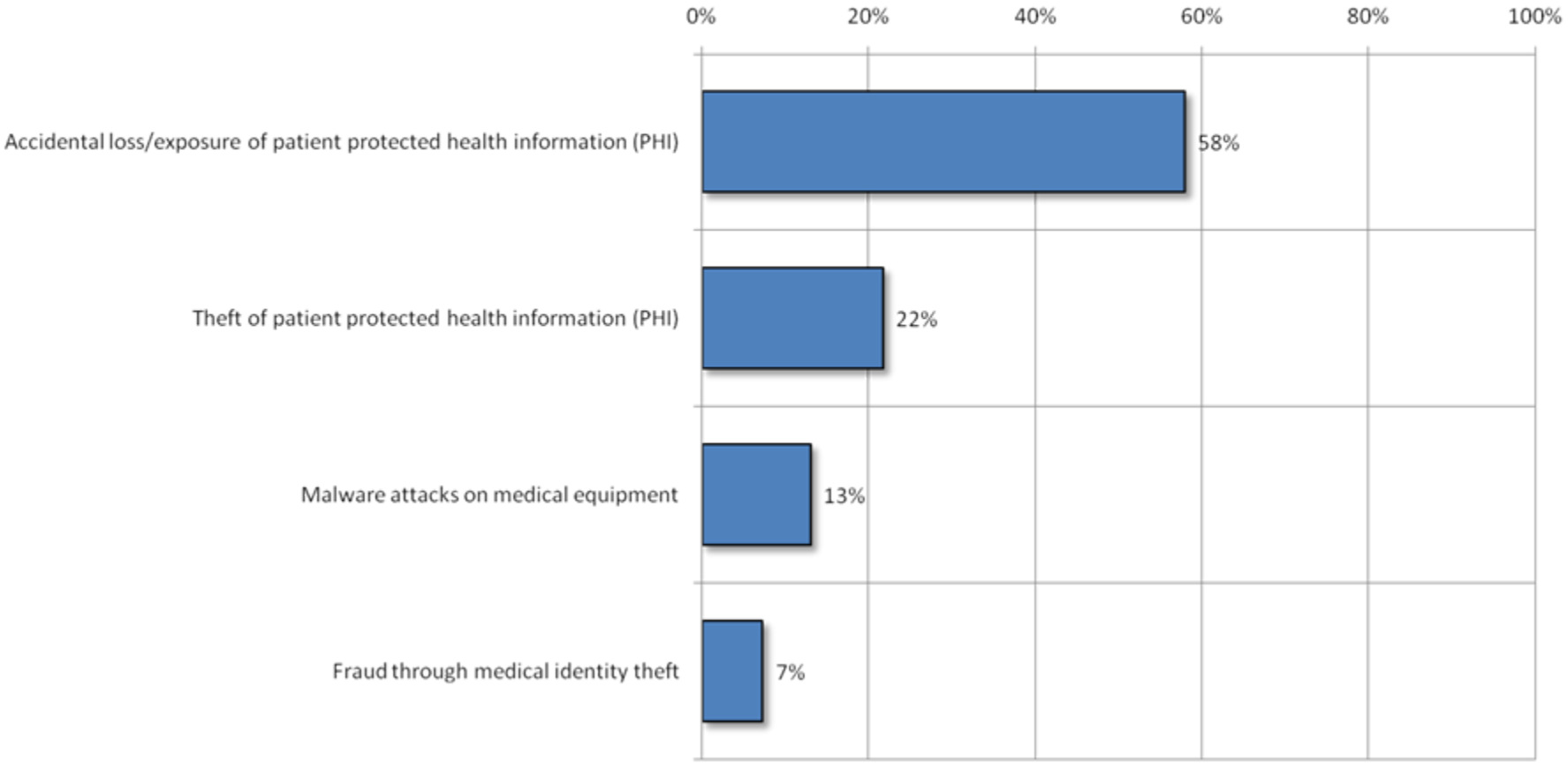
# Industry Verticals: Healthcare



# Industry Verticals: Healthcare

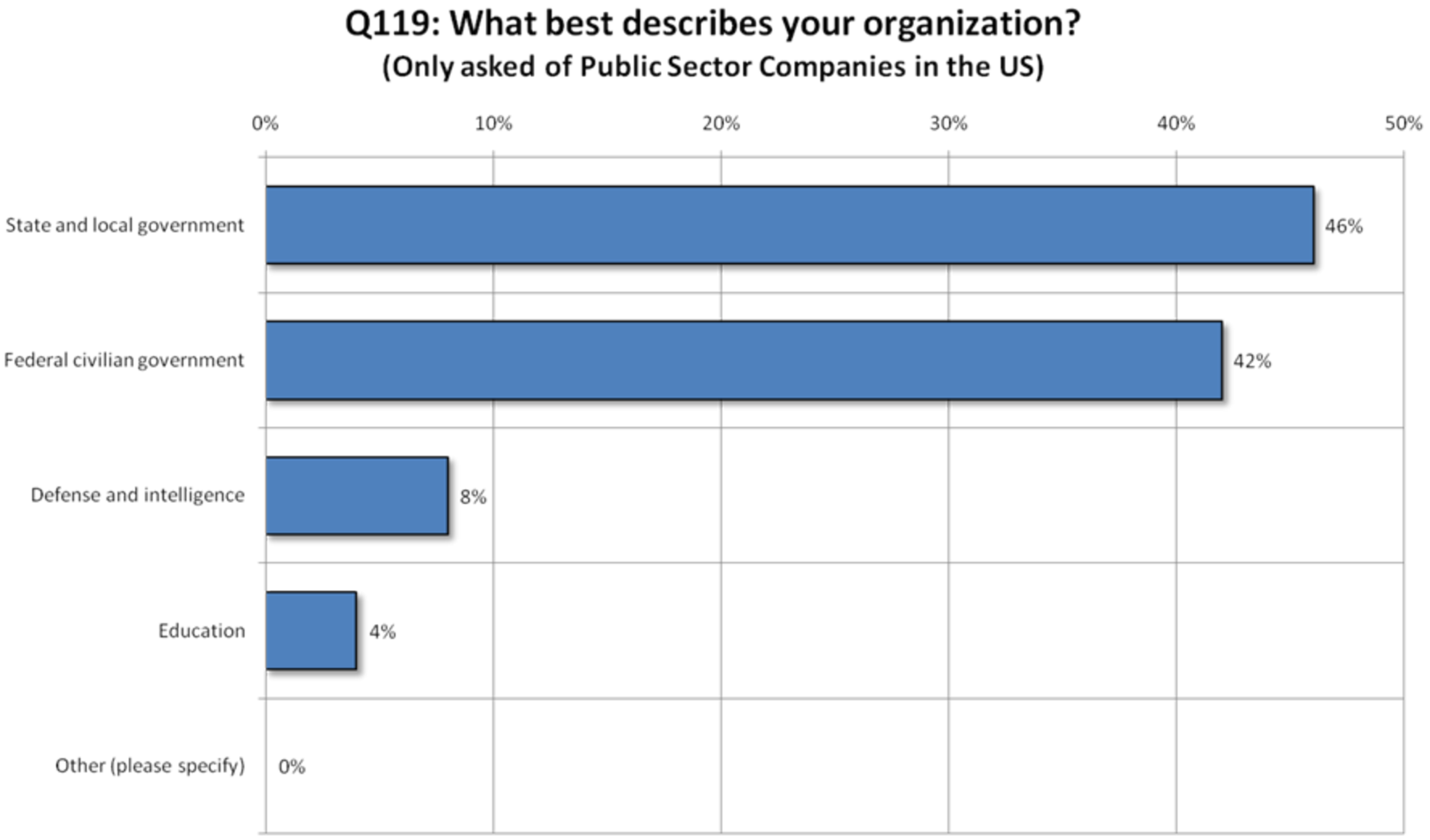
## Q118: Which of the following have you experienced in the past 12 months?

### (Only asked of Healthcare Companies)



# Industry Verticals: Public Sector (US)

# Industry Verticals: Public Sector (US)



# Industry Verticals: Public Sector (US)

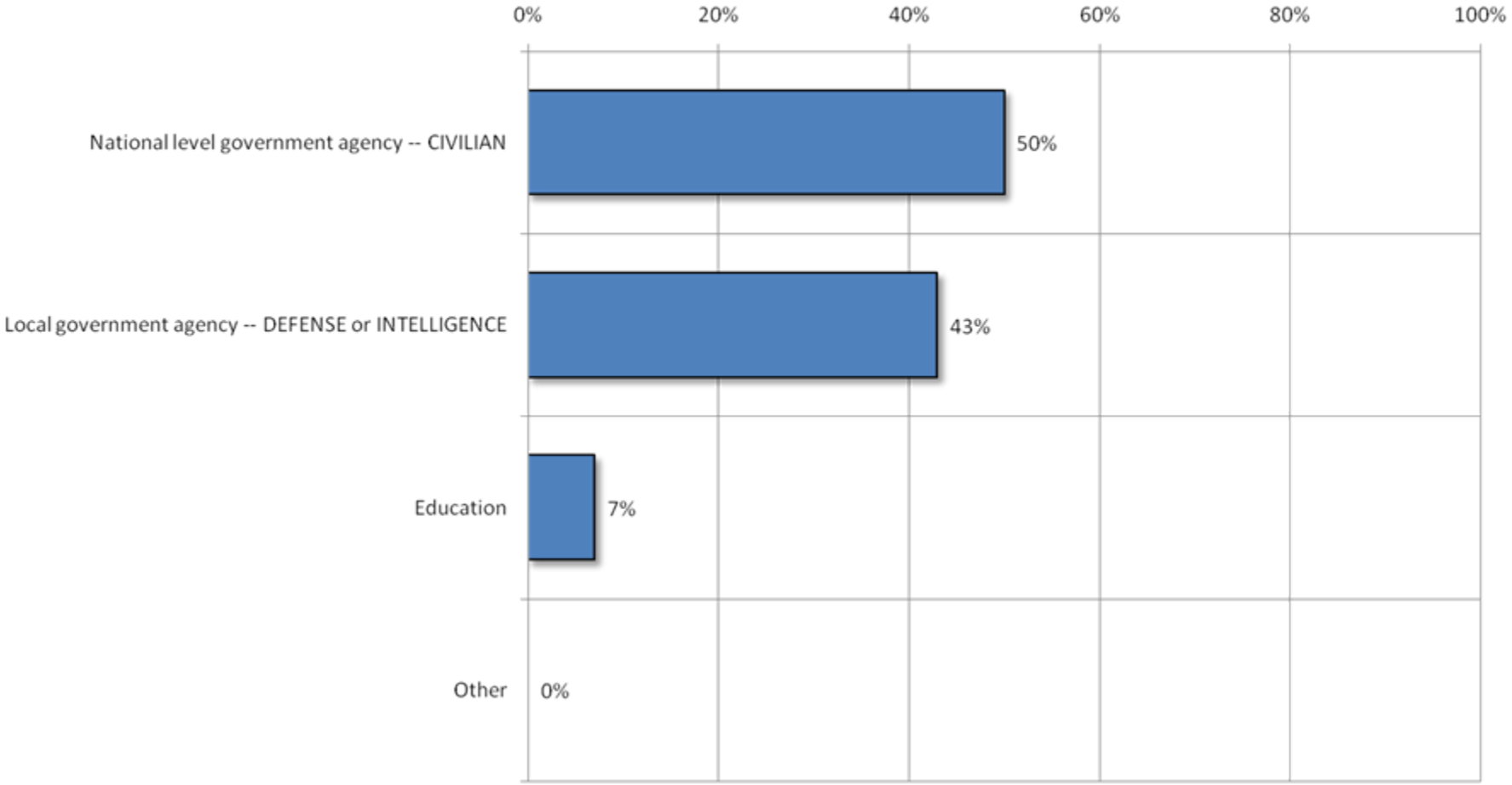
| Q120: What percentage of your *security* funding is coming from national stimulus funding currently? | |
|---|---|
| Median | 0% |

# Industry Verticals: Public Sector (Non-US)

# Industry Verticals: Public Sector (Non-US)

## Q121: Which best describes your organization?

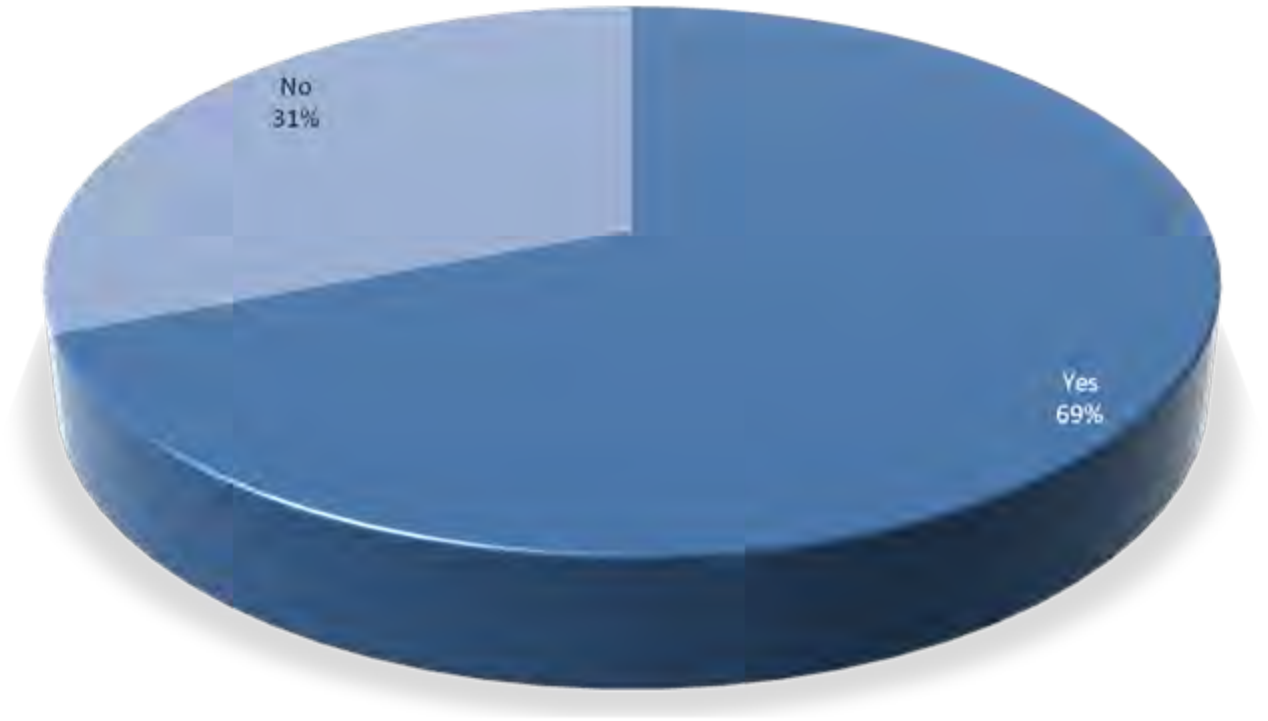
### (Only asked of Public Sector Companies not located in the US)



# 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)**

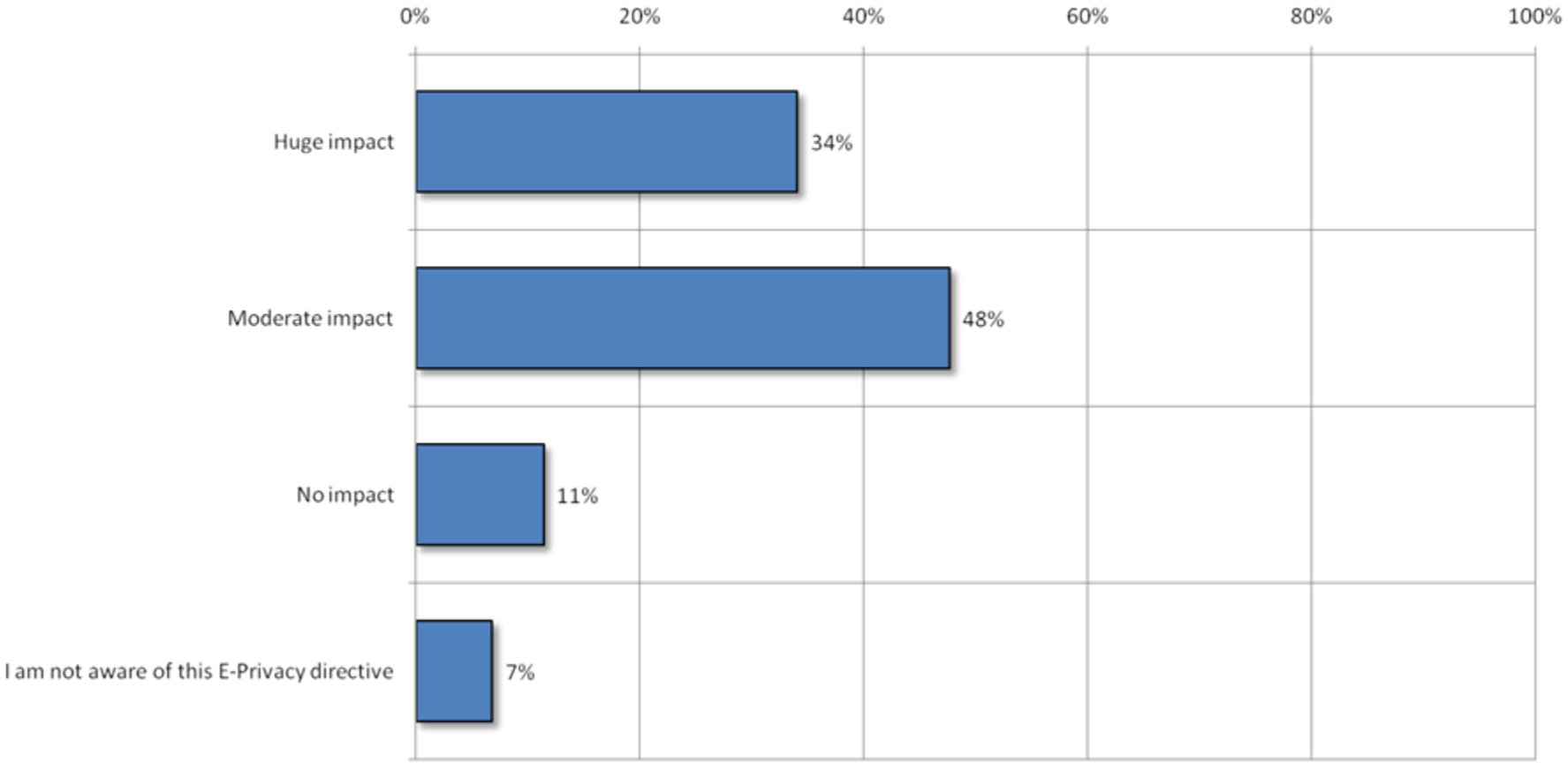


# Industry Verticals: Telecommunications

# Industry Verticals: Telecommunications

## Q123: How do you rate the impact of Data Breach Notification for your security spending in the next coming months?

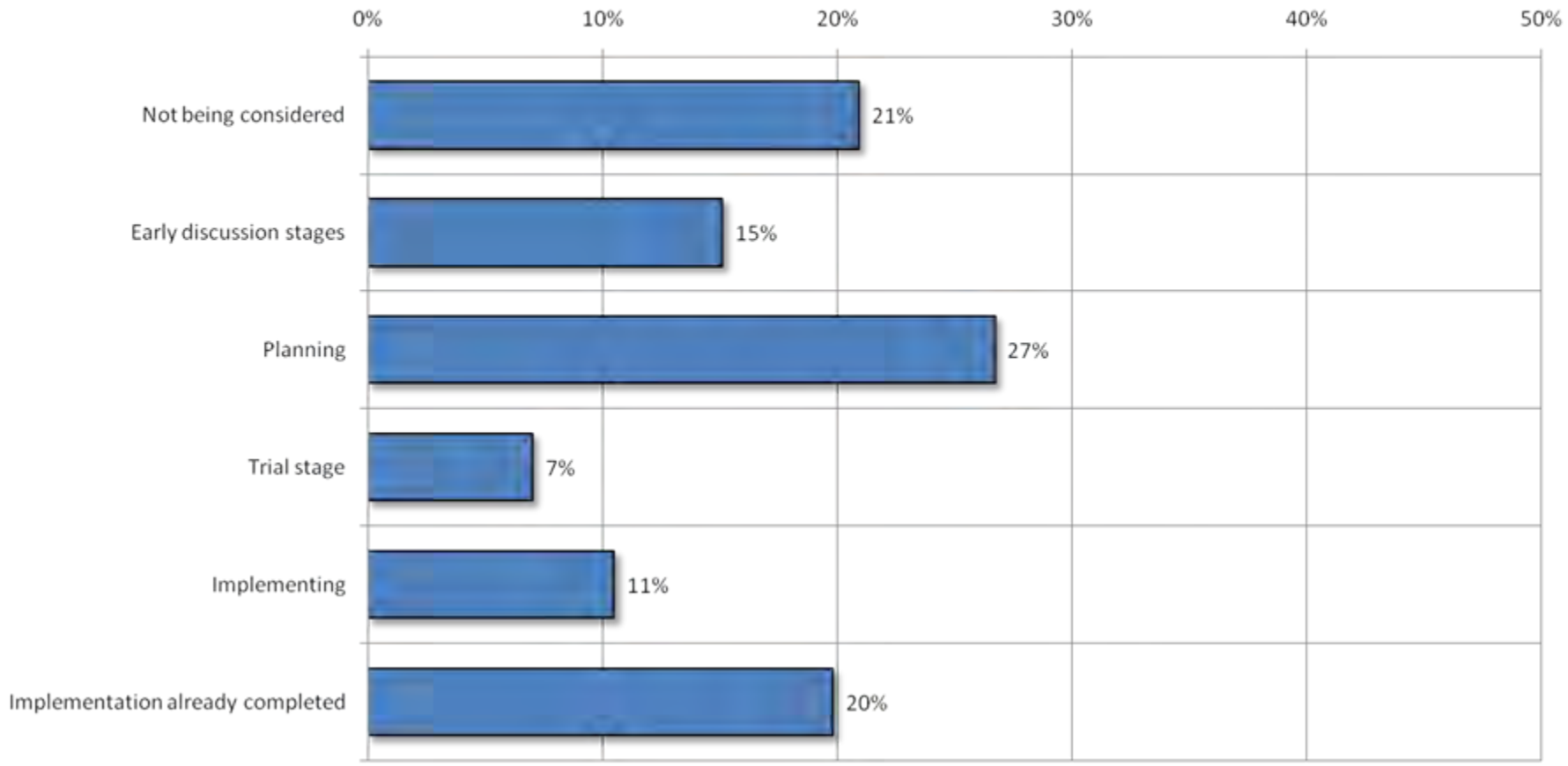
(Only asked of Telecommunications Companies in select countries)



# Industry Verticals: Telecommunications

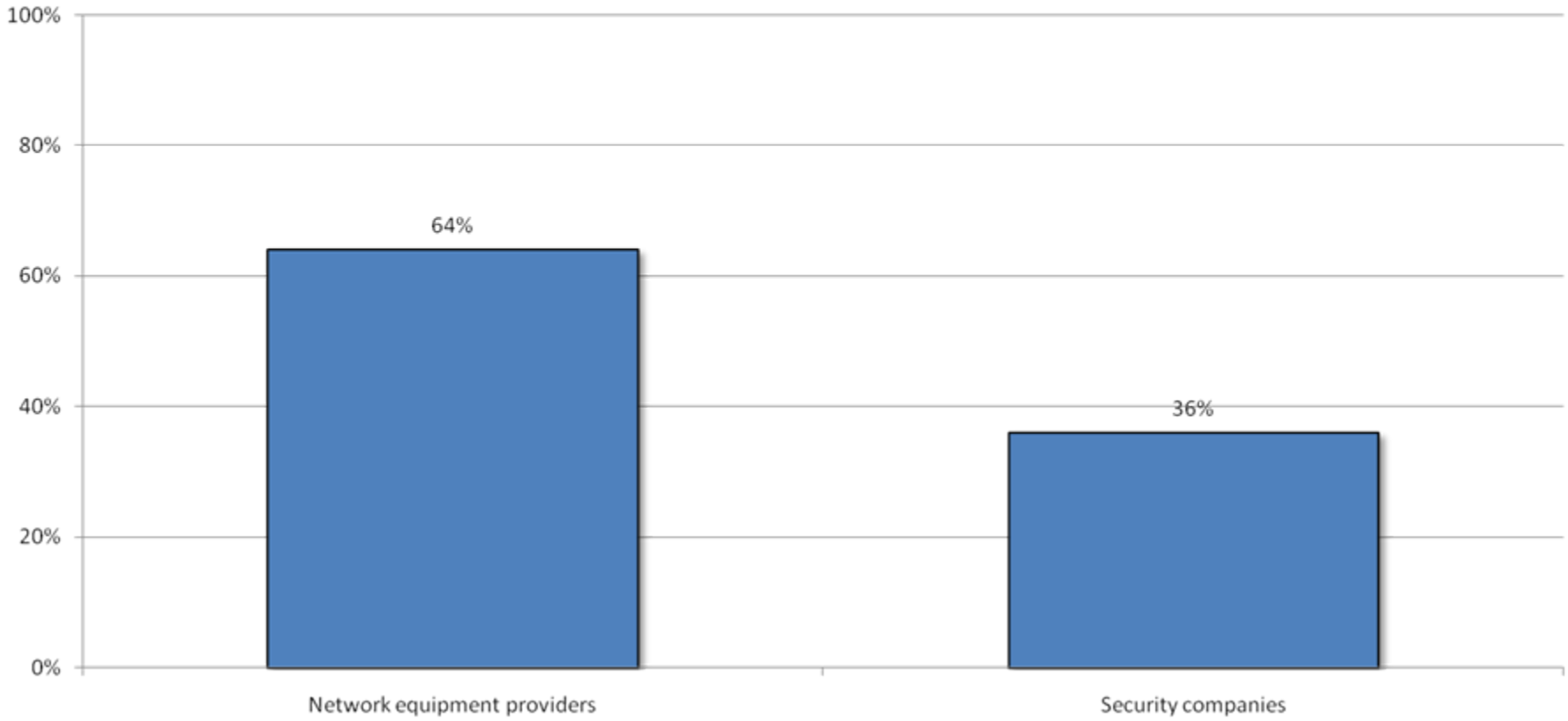
## Q124: Do you plan to offer Managed Security Services to your customers?

(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