



# CSO Interchange

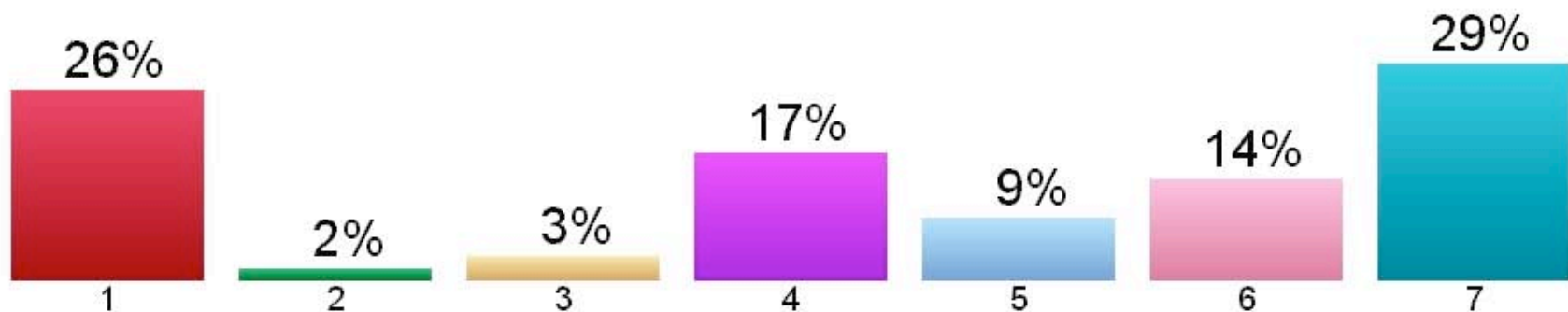
**New York, NY**

December 7, 2004

sponsored by  
 **QUALYS**

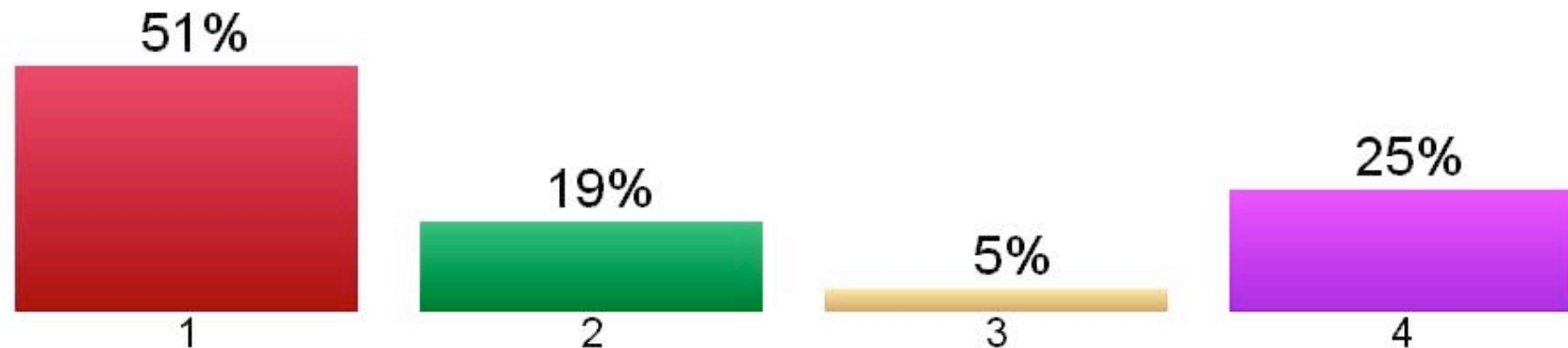
## 1. My employer's primarily business is in:

1. Financial services
2. Healthcare
3. Government
4. Technology
5. Education
6. Consulting
7. Other



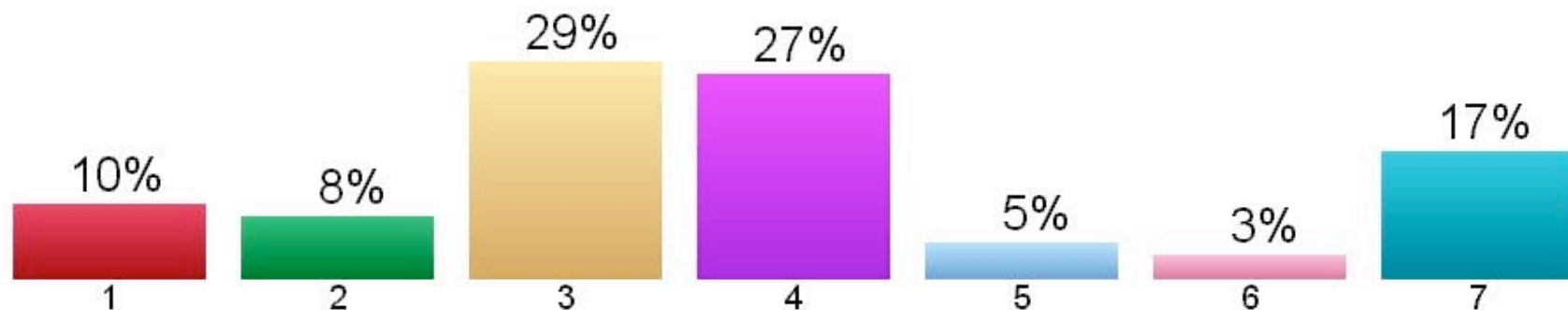
## 2. I am the...

1. Top ranking security officer in my company
2. I report to the top ranking security officer
3. I report to 1 - 2 levels below the top ranking security officer
4. Other



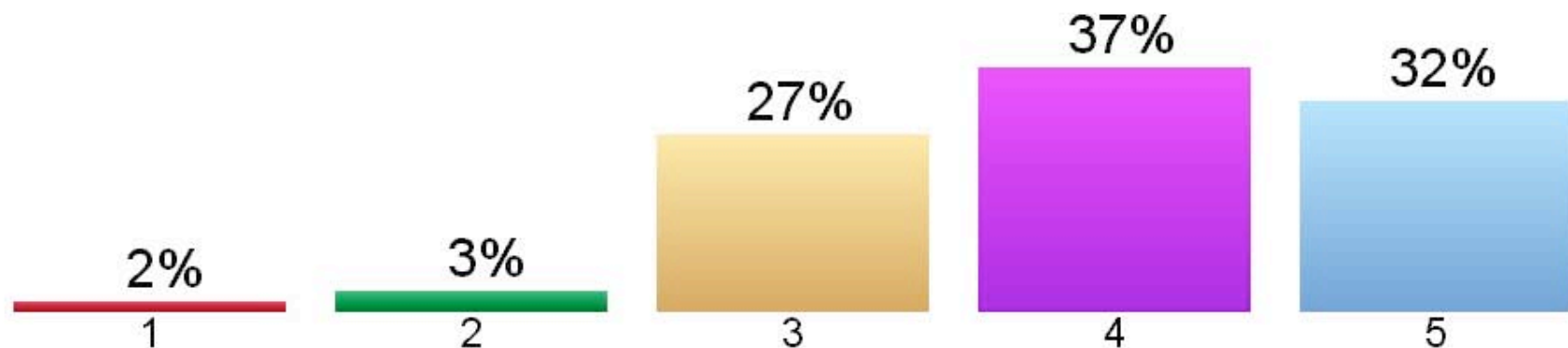
### 3. Our company's security budget is X% of our IT budget

1. 0 - 1%
2. 1 - 2%
3. 3 - 4%
4. 5 - 10%
5. 10 - 20%
6. More than 20%
7. Don't know



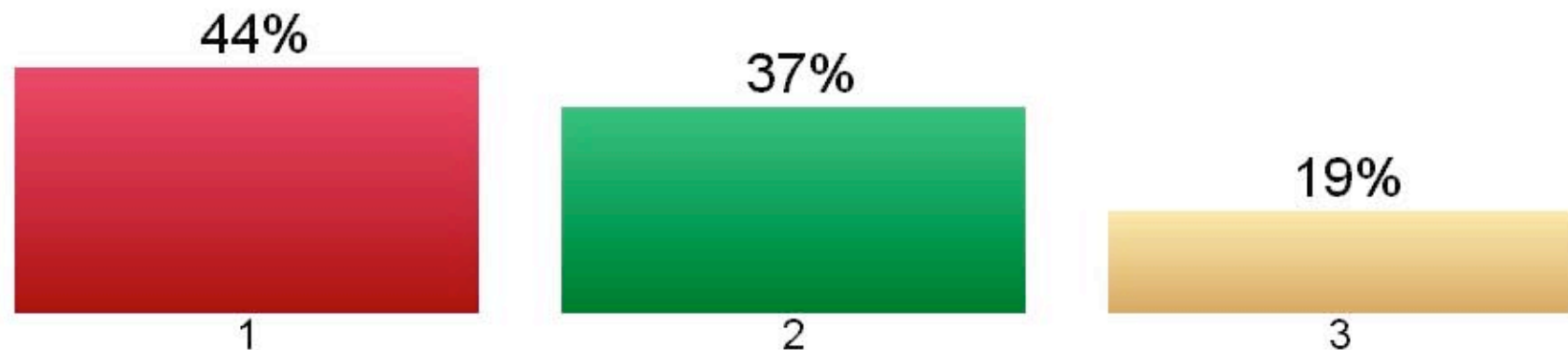
## 4. Over the last year my job has gotten:

1. Substantially easier
2. Easier
3. Hasn't really changed
4. More difficult
5. Substantially more difficult



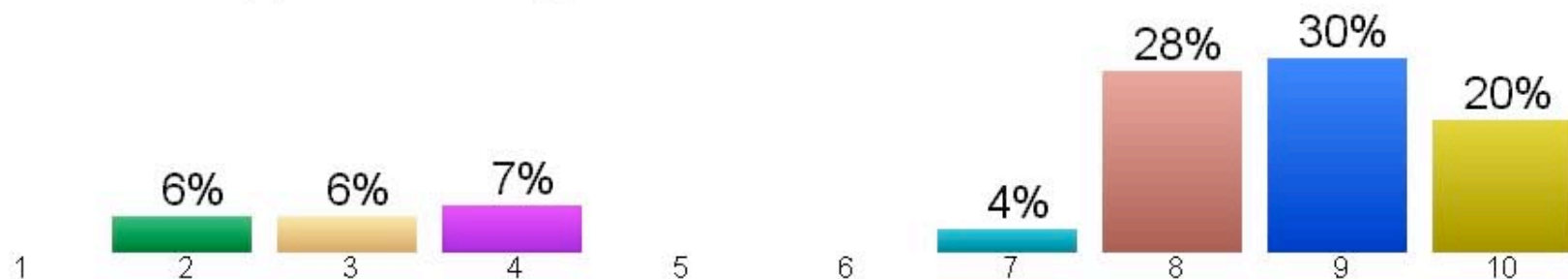
5. November 15th was the deadline for companies to comply with Sarbanes-Oxley. Was security part of your company's Sarbanes-Oxley compliance discussions and resulting activities?

1. Yes, in a significant way
2. Yes, in a limited way
3. No



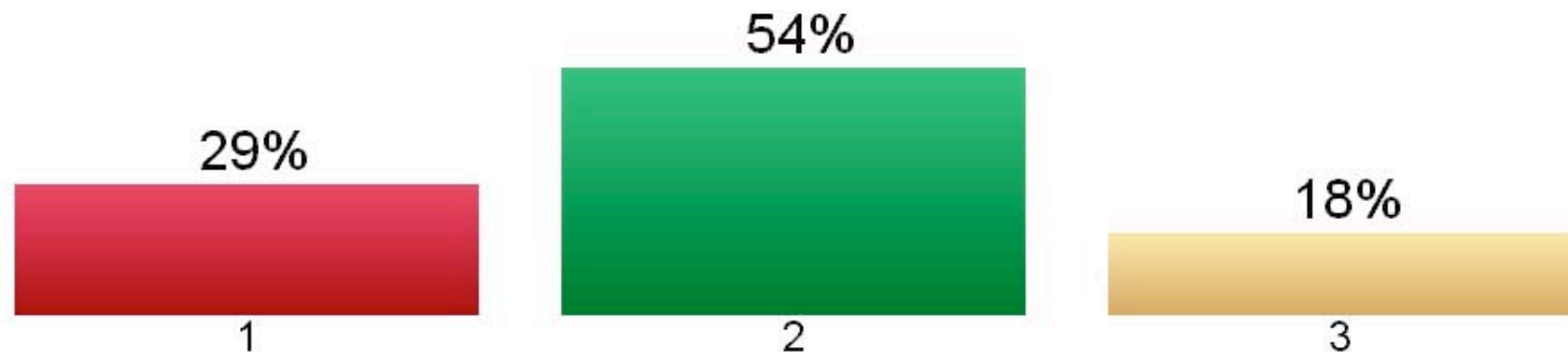
## 6. The security area I'm most concerned about is:

1. Phishing
2. Identity theft
3. Wireless network security
4. Spyware
5. Spam
6. Instant messaging security
7. Cyberterrorism
8. Worms, viruses, and Trojan horses
9. Regulatory compliance
10. End user sloppiness or outright malicious behavior



7. Has your organization rolled out additional defenses, either technical or administrative, to avoid phishing scams, both internally and externally

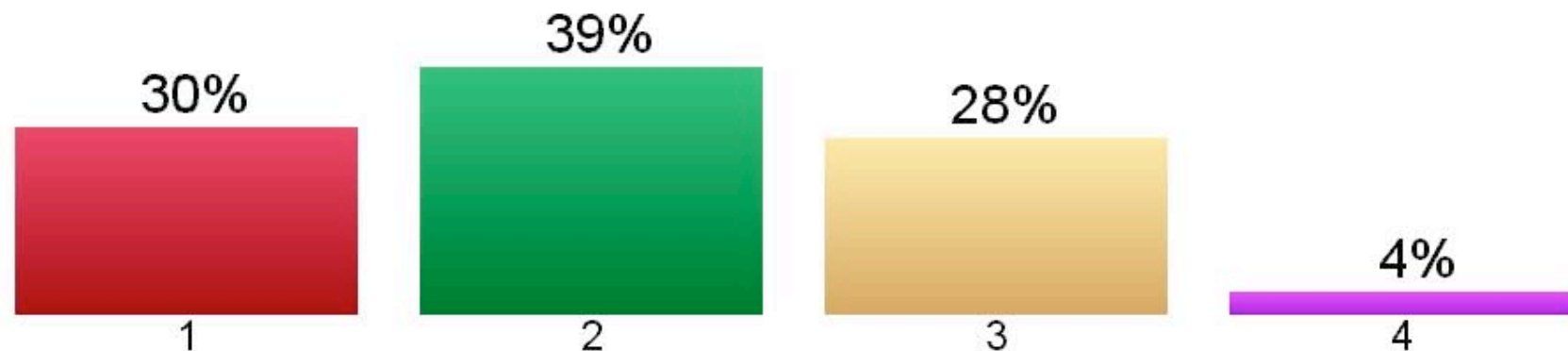
- 1. Yes
- 2. No
- 3. In process



## Online fraud prevention

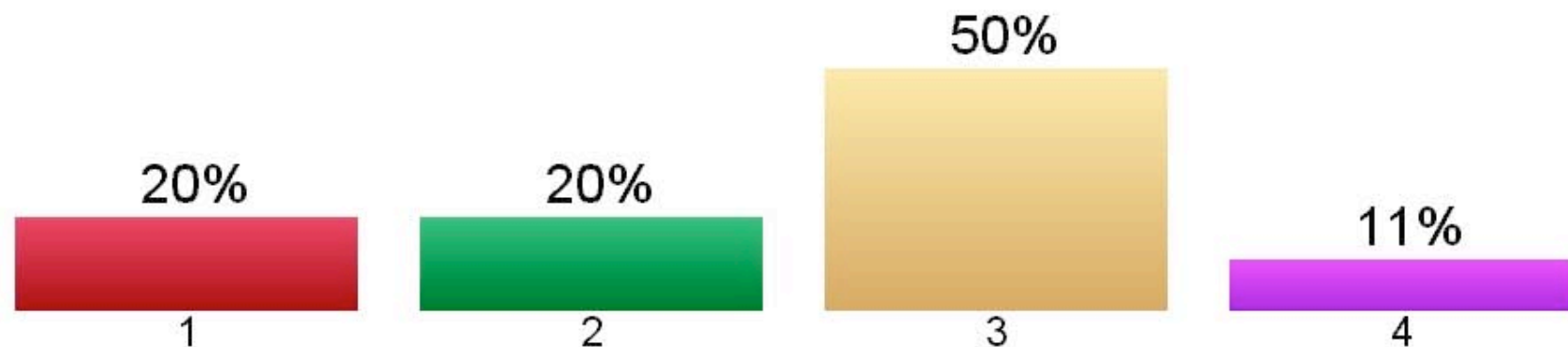
8. How concerned are you about online fraud at your organization?

1. Extremely concerned
2. Somewhat concerned
3. Not very concerned
4. You mean, you can commit fraud online?



## 9. How much does your organization do to prevent online fraud?

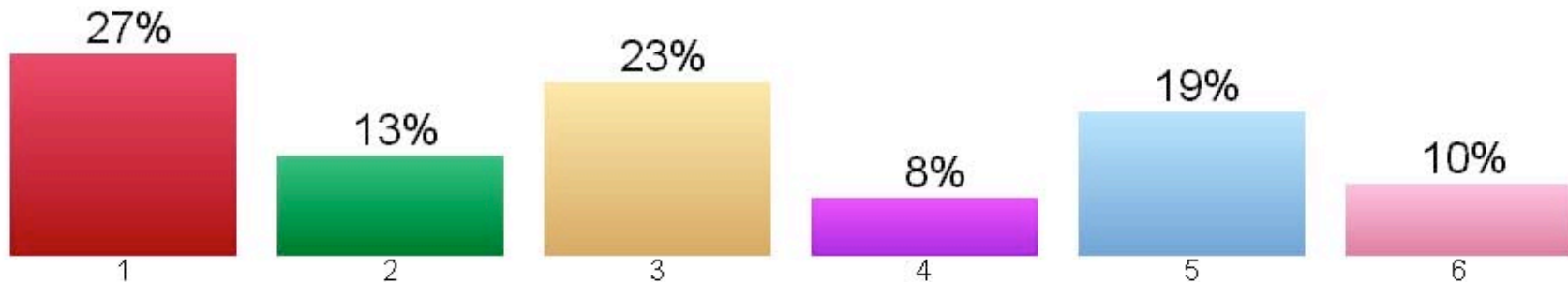
1. Everything in our power
2. We meet industry standards
3. We do our best but we could do a lot more
4. Nothing



## The Role of the CSO

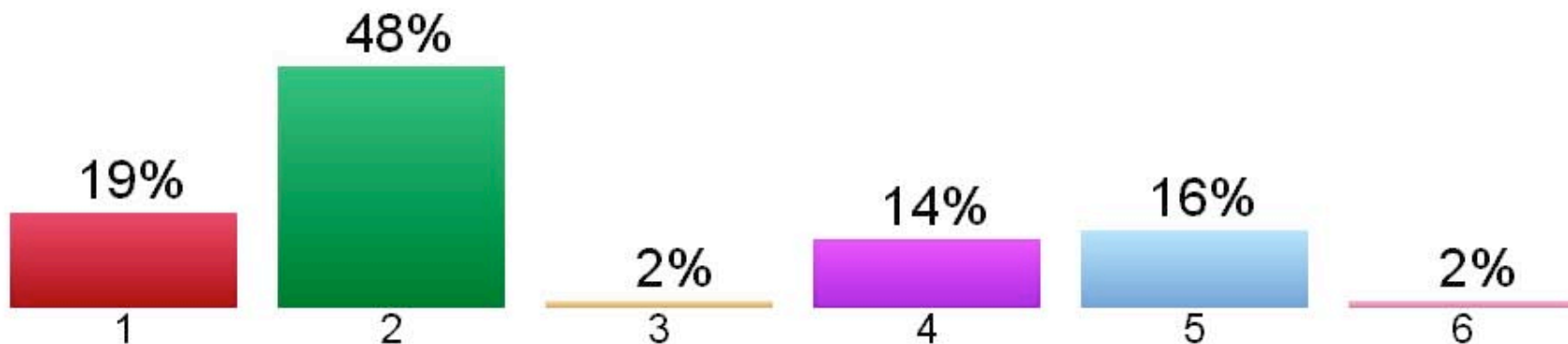
### 10. What portion of your job takes the bulk of your time?

1. Aligning security with business requirements
2. Compliance to regulations and legislation
3. Establishing and following standards of good practice
4. Establishing security controls in business partner relationships and contracts
5. Overall risk management
6. Managing security technology such as firewalls and IDS



## 11. The top security person within my company reports to the:

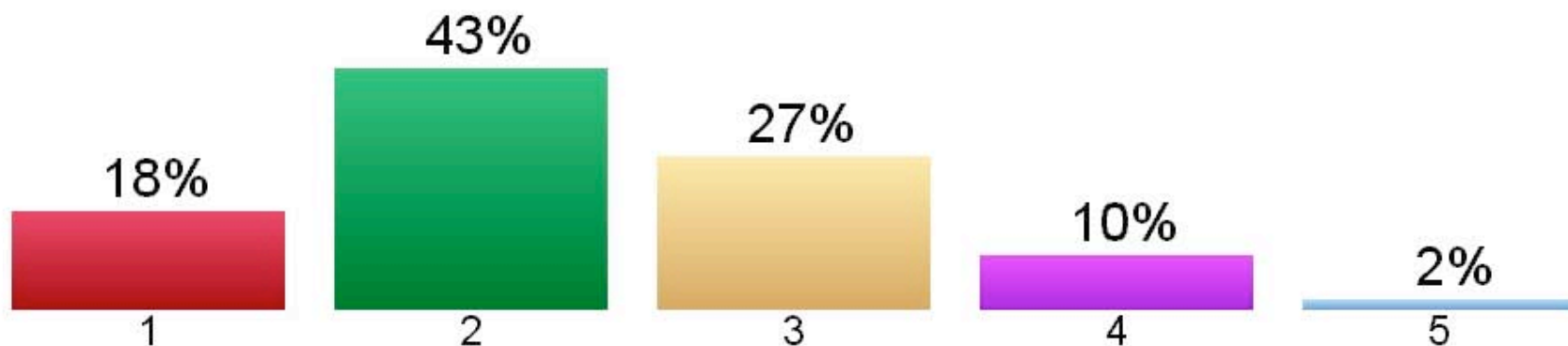
1. CEO
2. CIO
3. CFO
4. VP/EVP, Operations
5. Other
6. Don't know



## Budgets, priorities and cost-cutting

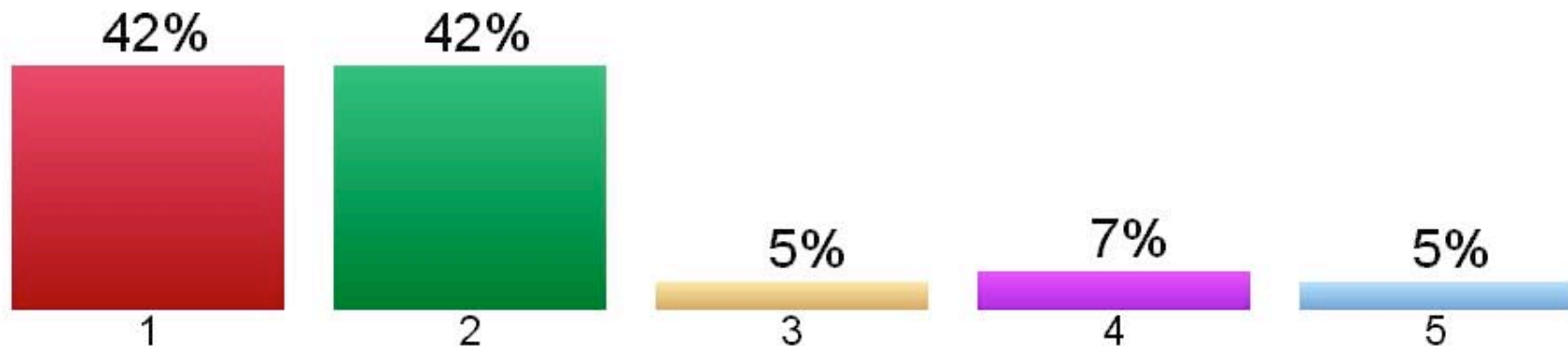
### 12. What happened to your company's security budget in 2004 v. 2003?

1. It grew significantly
2. It grew by a small amount
3. It stayed the same
4. It shrank by a small amount
5. It shrank significantly



13. How strongly do you agree or disagree with the following statement:  
The information security program in my organization is under funded.

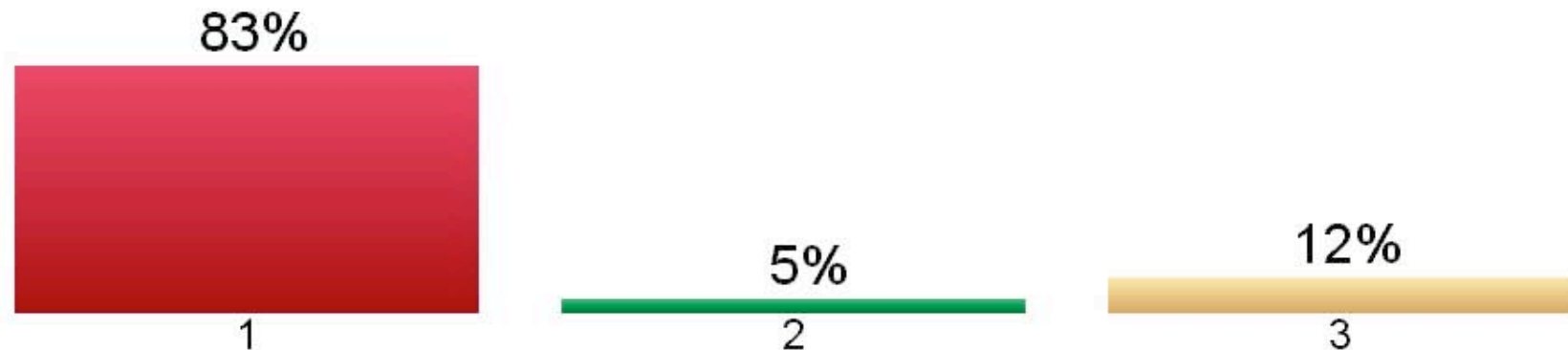
1. Strongly agree
2. Agree
3. Neither agree or disagree
4. Disagree
5. Strongly disagree



## Cybersecurity in a distributed business unit environment

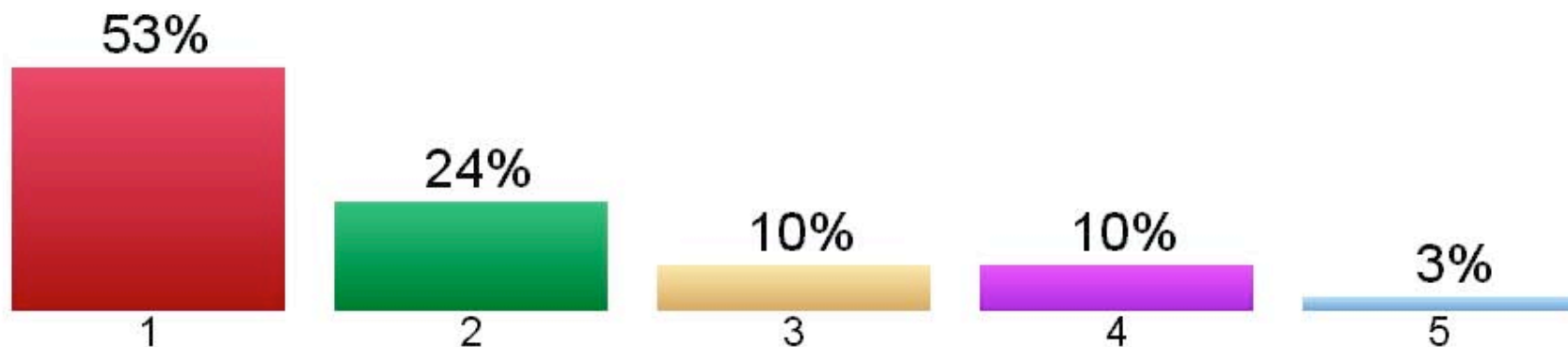
14. Do you manage security in a distributed environment -- either multiple offices in one country, or offices in multiple countries?

1. Yes
2. Not now, but I will in the near future
3. No



15. How strongly do you agree or disagree with the following statement: Network security will eventually have to evolve to accommodate a perimeter-less environment

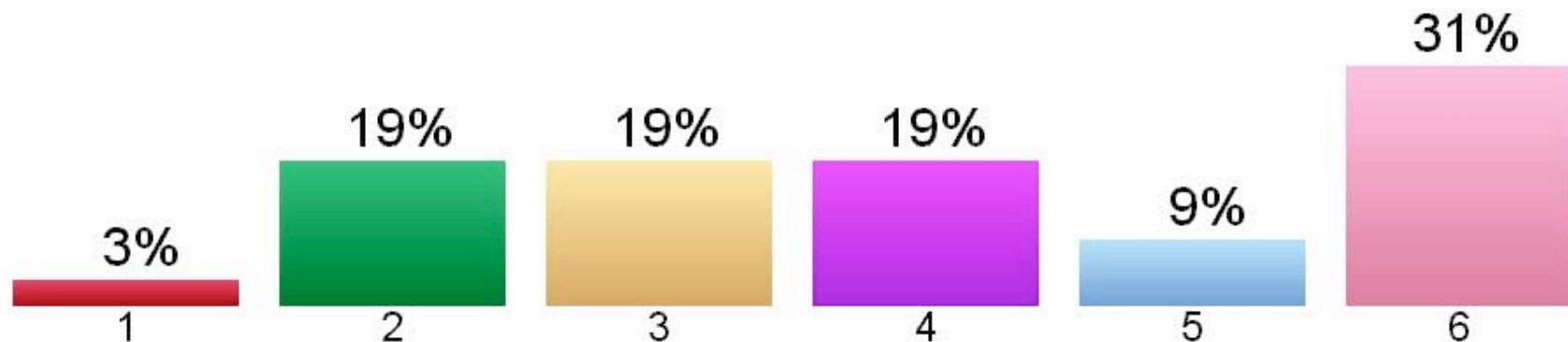
1. Strongly agree
2. Agree
3. Neither agree or disagree
4. Disagree
5. Strongly disagree



## Managing zero hour exploits

16. How strongly do you agree or disagree with the following statement: My organization has the appropriate defenses in place to protect itself against zero hour exploits.

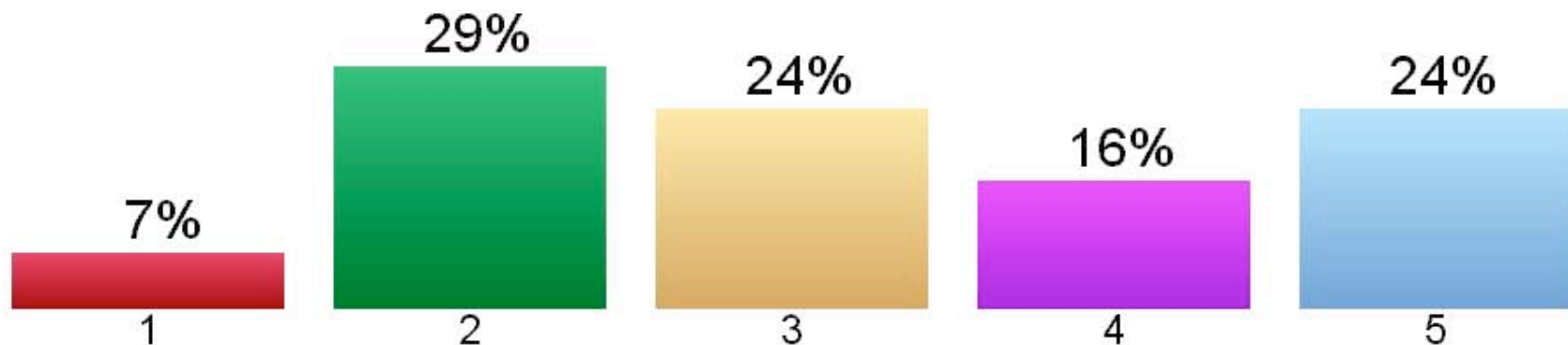
1. Strongly agree
2. Agree
3. Neither agree or disagree
4. Disagree
5. Strongly disagree
6. There are no defenses that could truly protect us from zero hour exploits



## Data privacy regulations

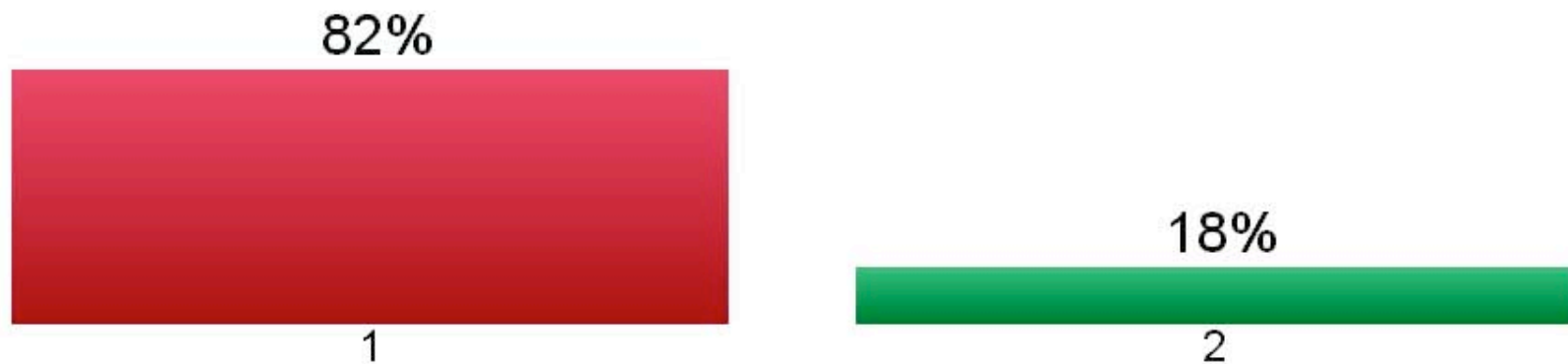
17. In my organization, data privacy is the primary responsibility of:

1. IT department
2. CSO
3. Chief privacy officer
4. CIO
5. Someone else



## 18. My top executives are concerned about data privacy

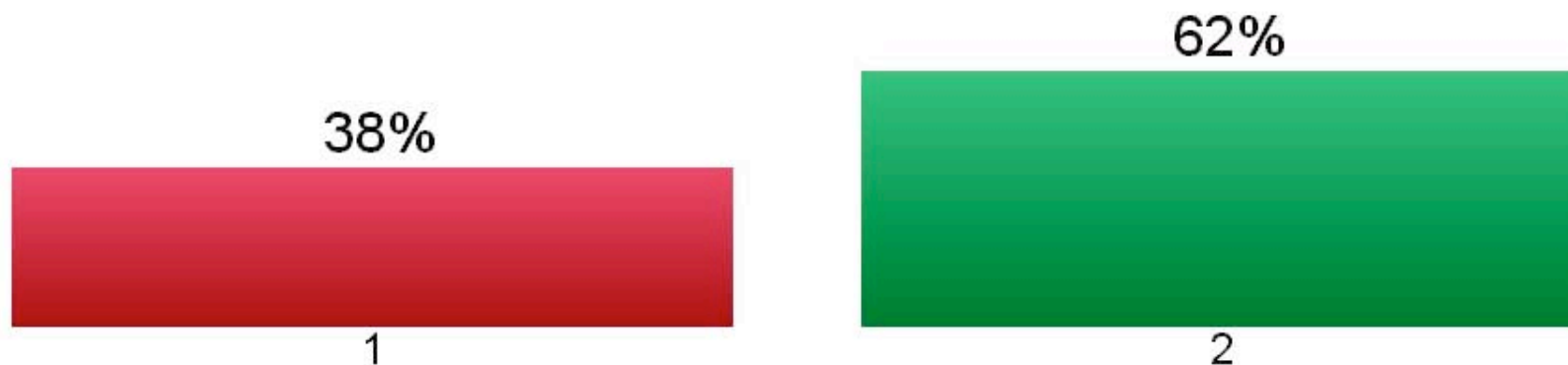
1. True
2. False



## Early warning for cyberattacks

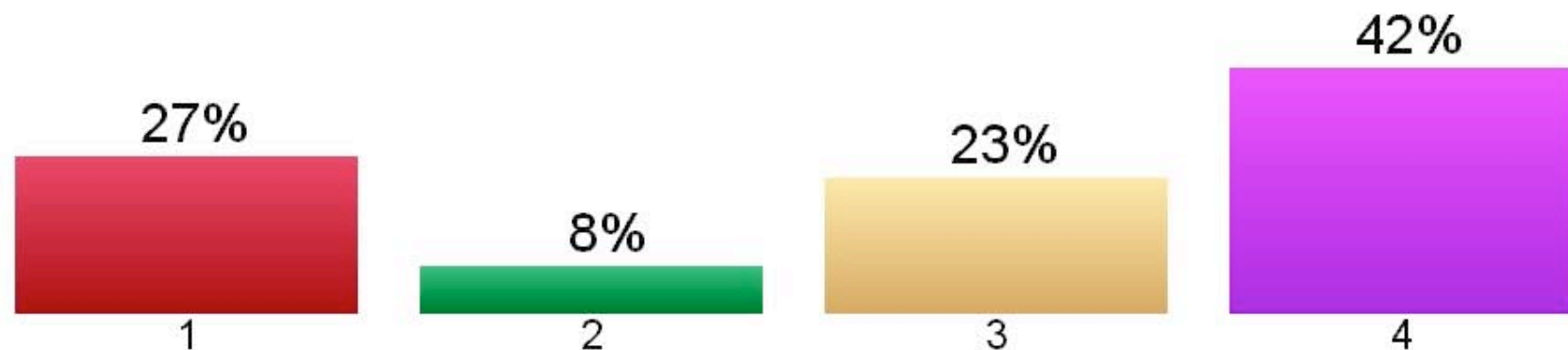
19. Do you feel you currently receive sufficient “early warning” for major cyberattacks?

1. Yes
2. No



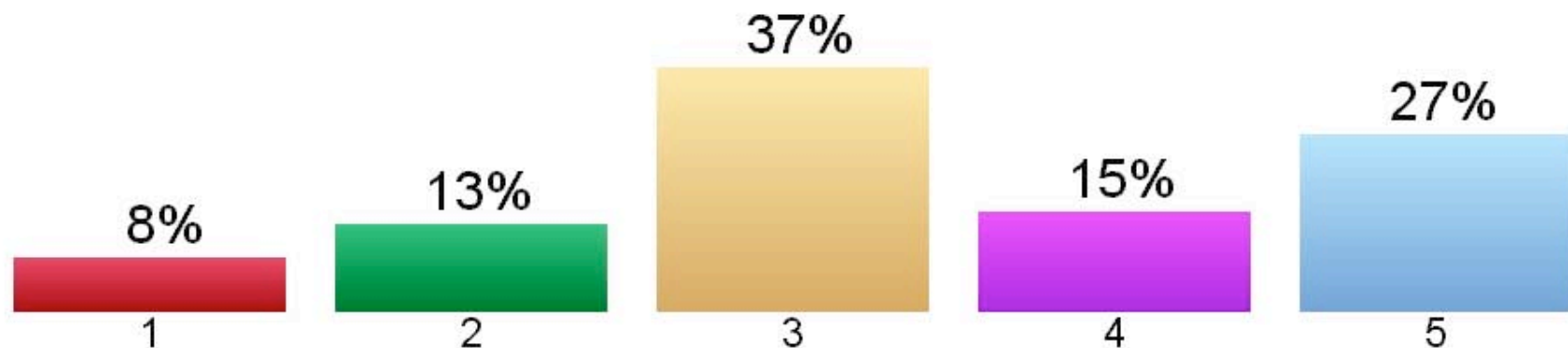
## 20. What would be the desirable level of early warning for new attacks?

1. One hour
2. One day
3. One week
4. Any warning at all would be nice



21. How strongly do you agree or disagree with the following statement: It is the government's responsibility to provide early warning for cyberattacks.

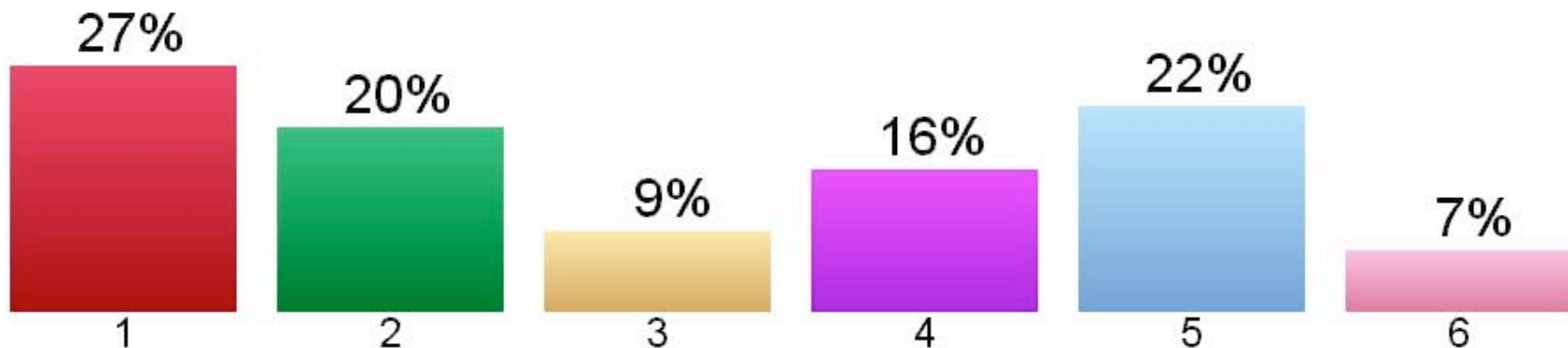
1. Strongly agree
2. Agree
3. Neither agree or disagree
4. Disagree
5. Strongly disagree



## Mobile devices and wireless LANs: worms, viruses and system intrusions

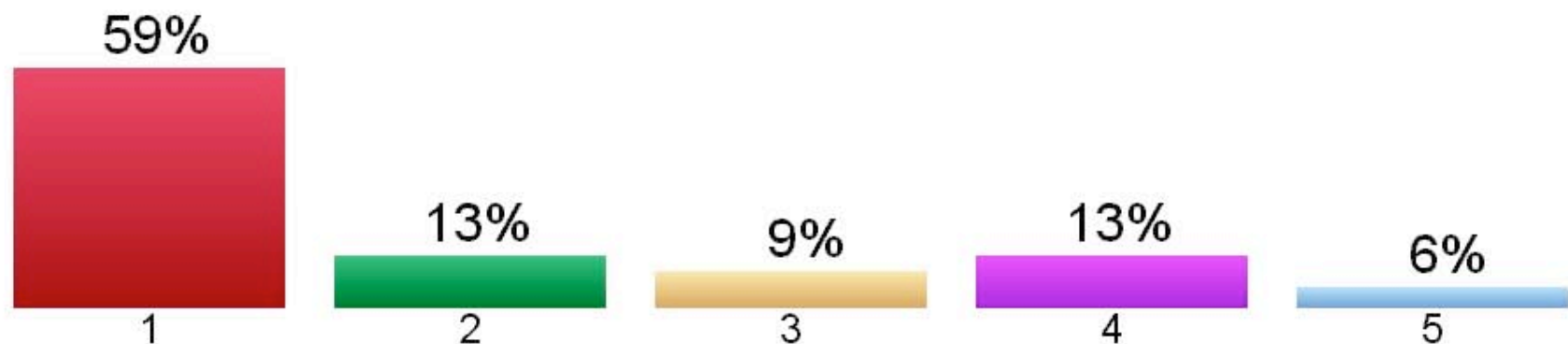
22. How are you currently securing the mobile devices connected to your network?

1. Encryption (WEP or other)
2. Forced authentication
3. MAC address filtering
4. Other
5. We have not deployed any wireless network
6. We do not currently employ any form of wireless security



## 23. Does your organization have a specific policy regarding the security of wireless devices on your network?

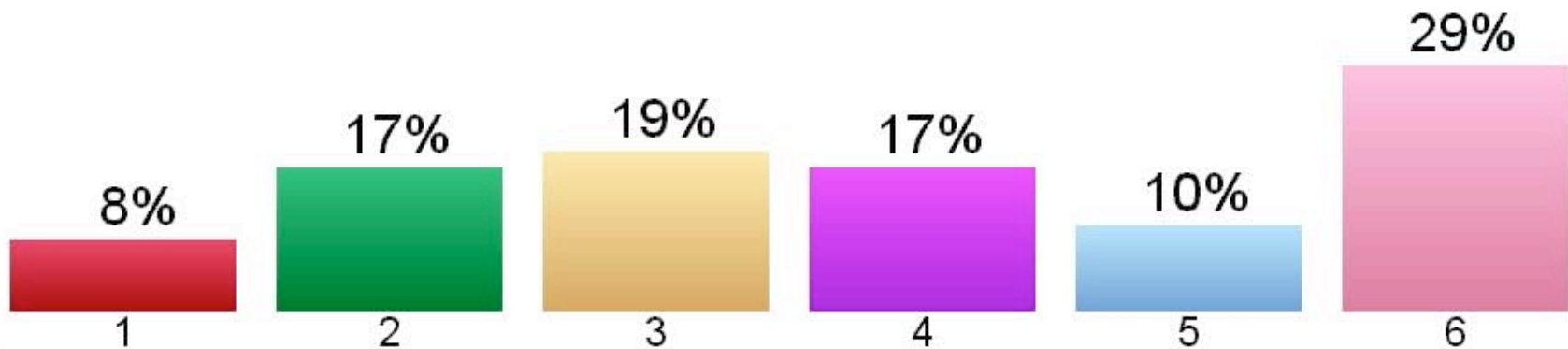
1. Yes
2. Yes, but nobody really follows it
3. No, but the security team keeps their eye on it
4. No, it is not at the top of our priority list
5. I am in denial that there are any wireless devices connected to my network



## Hiring/Job Seeking

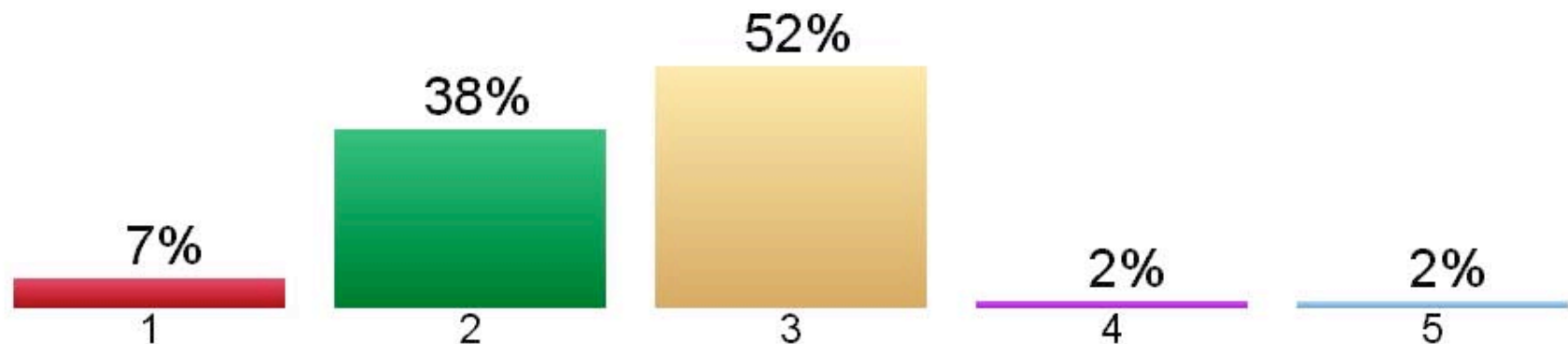
24. What is the size of your company's dedicated security staff?

1. Less than one full-time person
2. 1 - 2 people
3. 3 - 5 people
4. 5 - 10 people
5. 10 - 20 people
6. More than 20 people



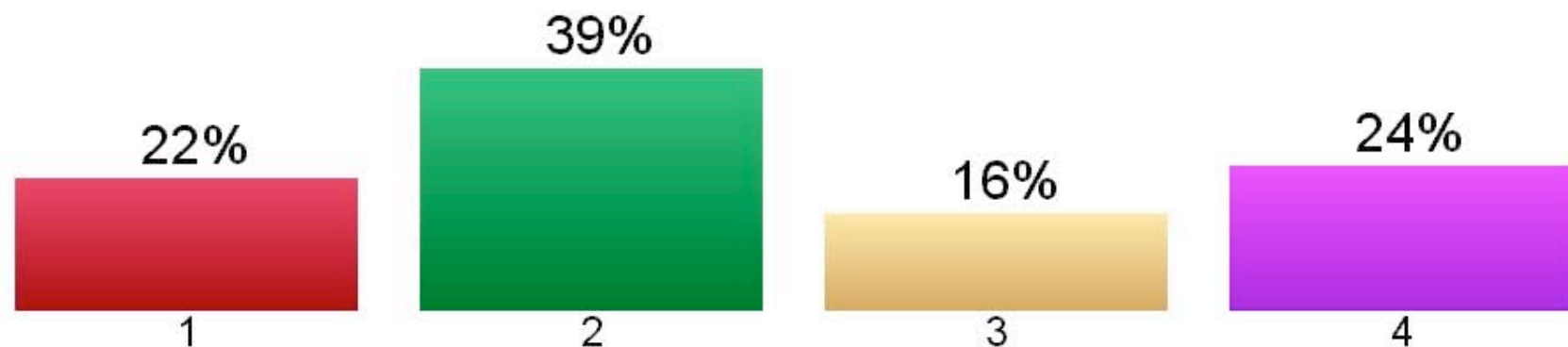
## 25. What happened to the number of dedicated security personnel in your organization during 2004 v. 2003?

1. It grew significantly
2. It grew by a small amount
3. It stayed the same
4. It shrank by a small amount
5. It shrank significantly



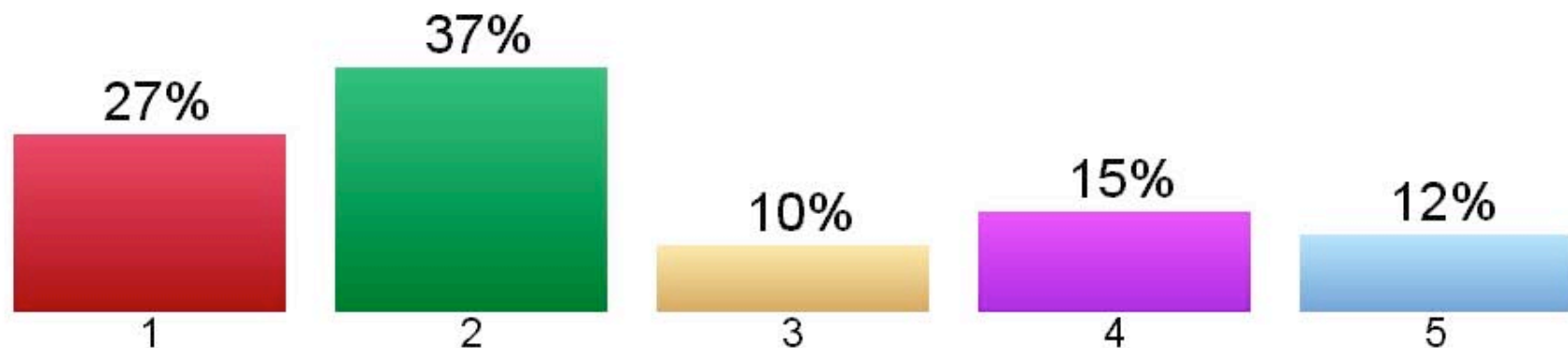
26. A recent Merrill Lynch survey reported that security skills are more in demand than any other IT skill set. How large an issue is finding skilled security personnel?

1. The lack of skilled candidates is slowing our ability to hire the number of people we really need
2. We can find the people we need with some difficulty
3. We can find the people we need without difficulty
4. I wouldn't know; we haven't hired in ages



## 27. How likely is it that you will be looking for a new job during 2005?

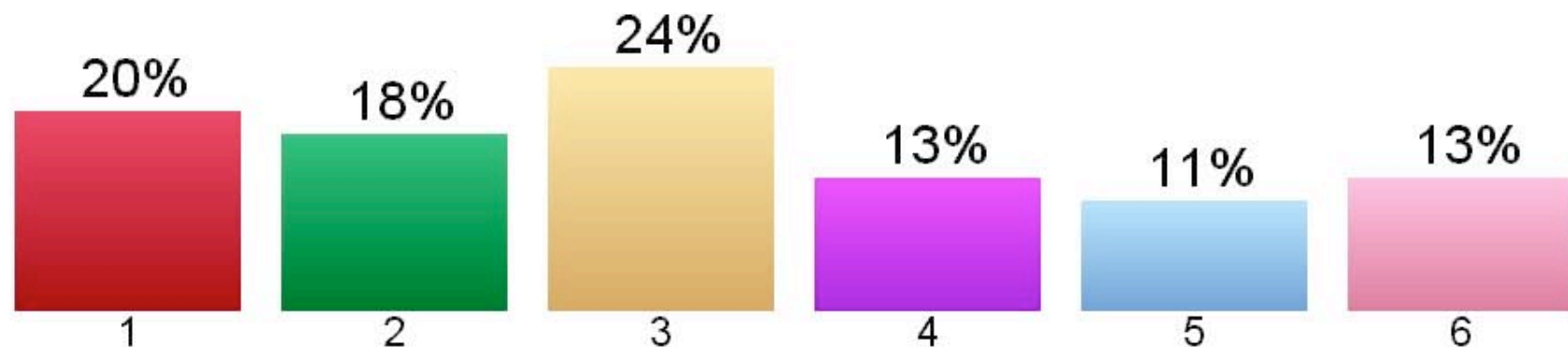
1. Absolutely
2. Possibly
3. Couldn't say one way or the other
4. Probably not
5. Definitely not



## Impact of Cyberattacks

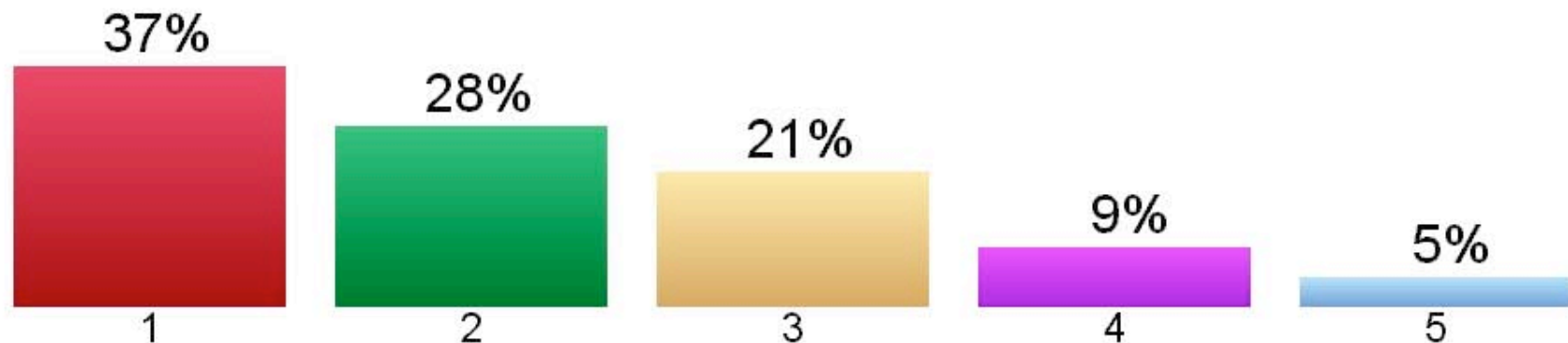
28. Within a range, how much have cyberattacks cost your organization in the past year?

1. zero
2. under \$25,000
3. \$25,000- \$50,000
4. \$50,001-\$100,000
5. \$100,001-\$500,000
6. over \$500,000



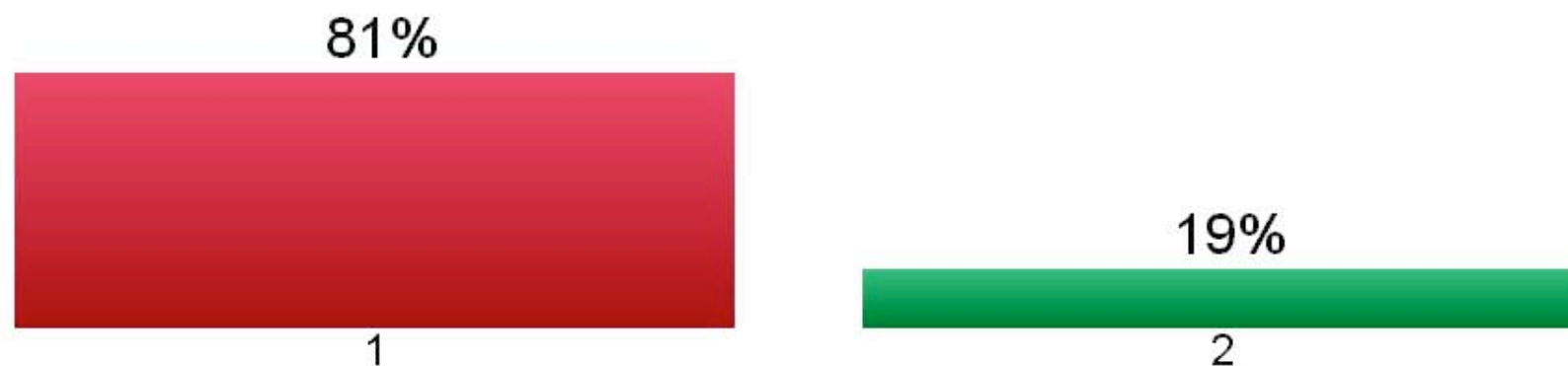
## 29. How much down time have you experienced this year due to a cyberattack?

1. Zero
2. Less than 12 hours
3. Between 12 and 24 hours
4. Between one day and one week
5. More than one week



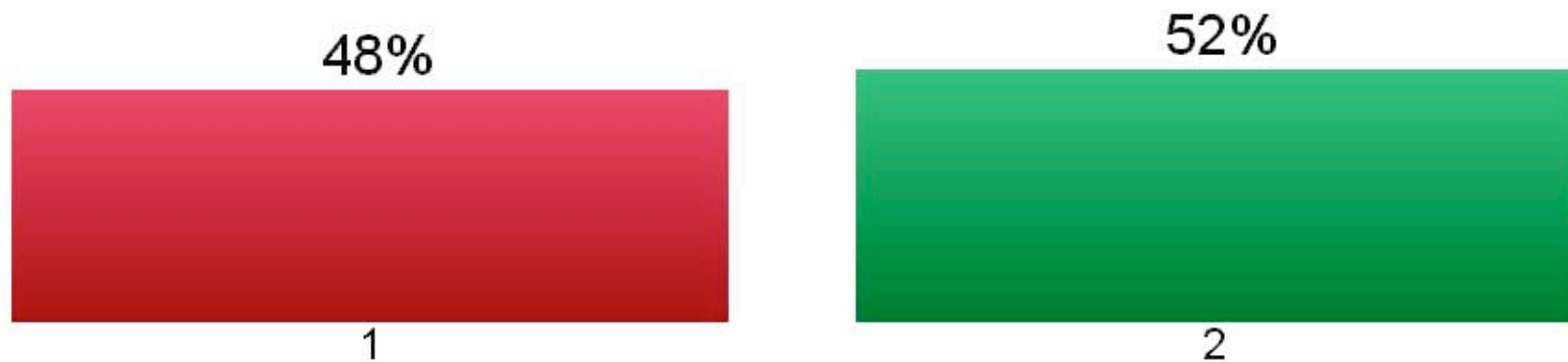
## 30. On a personal level, do you bank electronically?

1. Yes
2. No



## 31. Are you concerned that Congress will regulate cybersecurity?

1. Yes
2. No



## 32. Should the head of the National Cyber Security Division be elevated to an assistant secretary?

1. Yes
2. No

