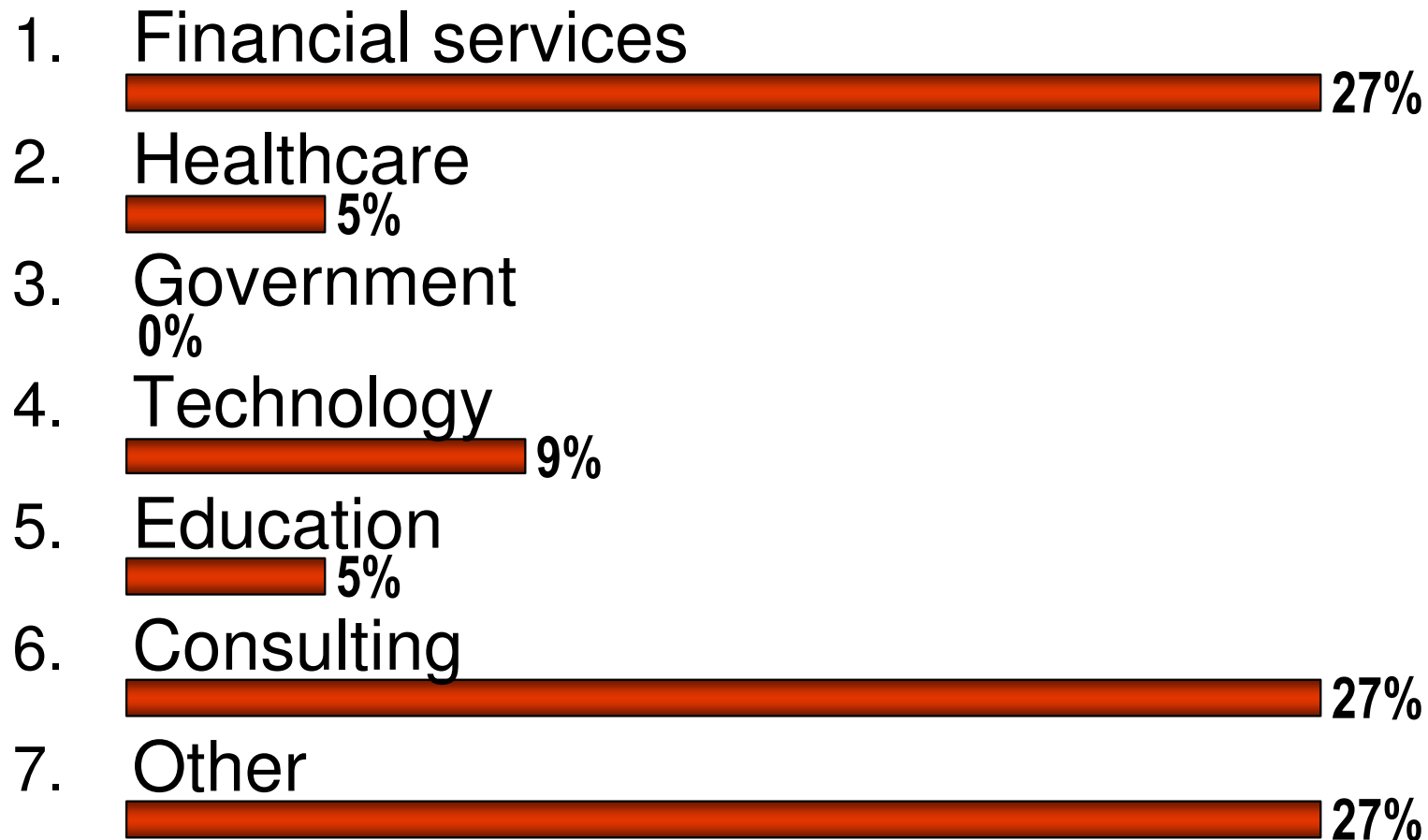




CSO Interchange

CSO Interchange London –
Thursday, 8 December 2005

1. My employer's primary business is in:

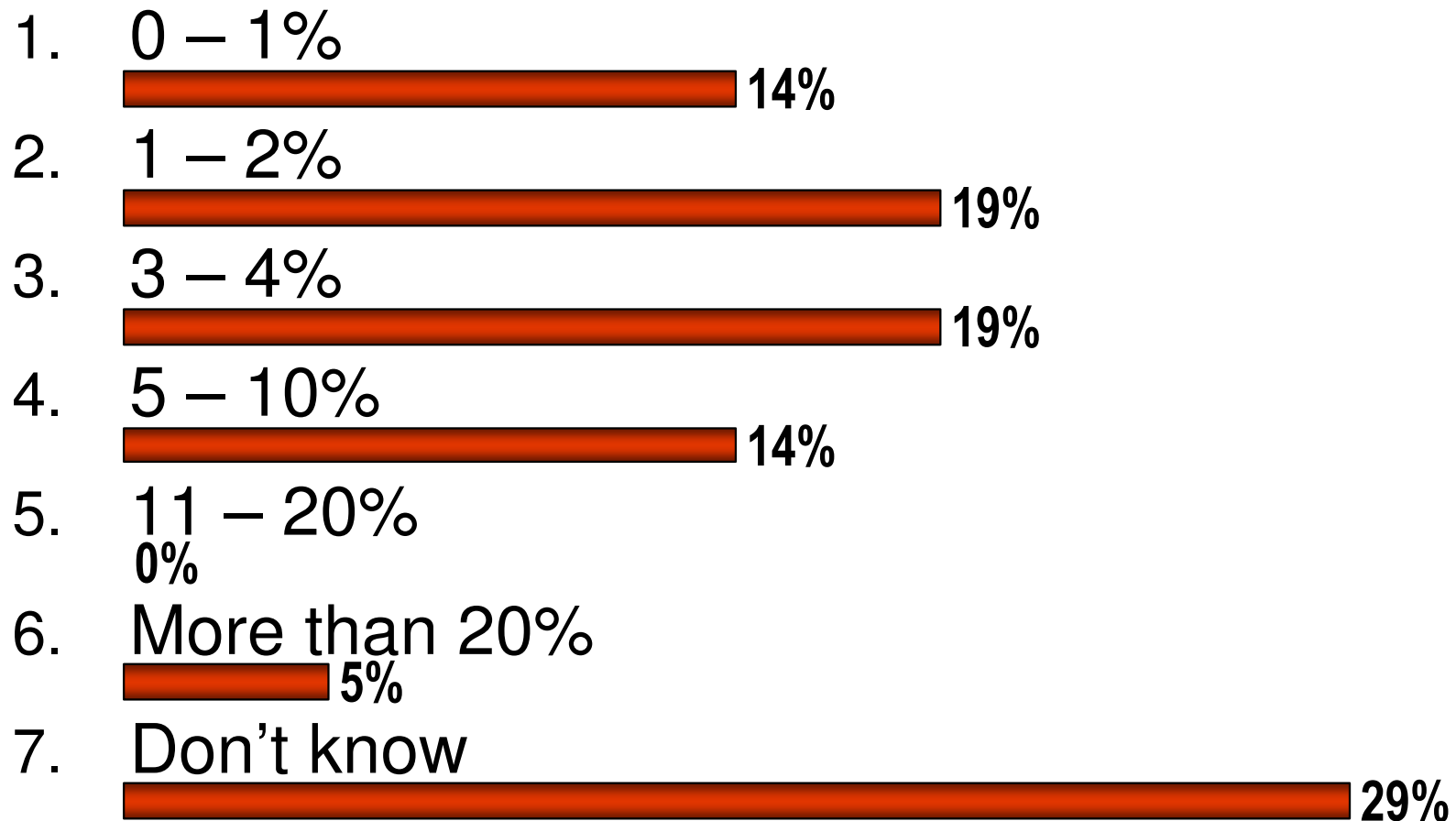


2. I am the...






1. Top ranking security officer in my company
 45%
2. I report to the top ranking security officer
 18%
3. I report to 1-2 levels below the top ranking security officer
 5%
4. Other
 32%



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









4. Over the last year my job has become:

1. Substantially easier
 5%
2. Easier
 5%
3. Has not really changed
 23%
4. More difficult
 45%
5. Substantially more difficult
 23%







5. How are you providing secure remote access to your enterprise?

1. VPN supporting routing (i.e. IPSEC)
 32%
2. Routing VPN using Network Access Control
 20%
3. Web based or thin client over SSL
 12%
4. Remote users can chose either routing VPN or SSL
 20%
5. Remote user forced to use one of routing VPN or SSL
 12%
6. No remote access provided
 4%



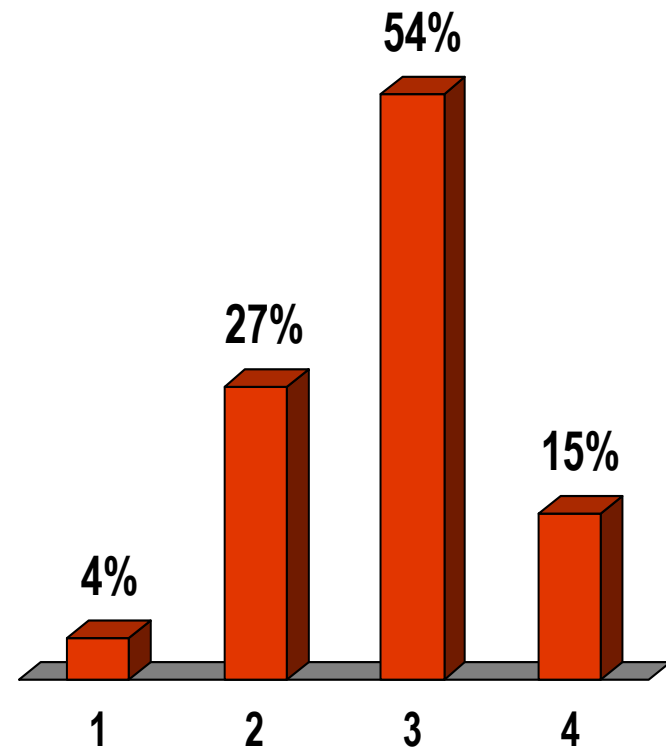
6. In our organization, security is perceived primarily as:

1. A necessary evil
 48%
2. A cost centre
 4%
3. A profit centre
0%
4. A business enabler
 28%
5. None of these
 20%



7. What statement best characterizes your organisation's approach to risk analysis?

1. We almost never do anything
2. Informal - a few people chat about the really big things but nothing much is written down
3. Consistent - we have a procedure for doing it and most of the time it is followed
4. Thorough - we have a formal process which is routinely complied with and there's a large paper-trail







8. The single greatest attribute required of a successful CSO is

1. Technical knowledge
0%
2. People management
8%
3. Influencing and communication skills
92%
4. Project management
0%
5. Other
0%



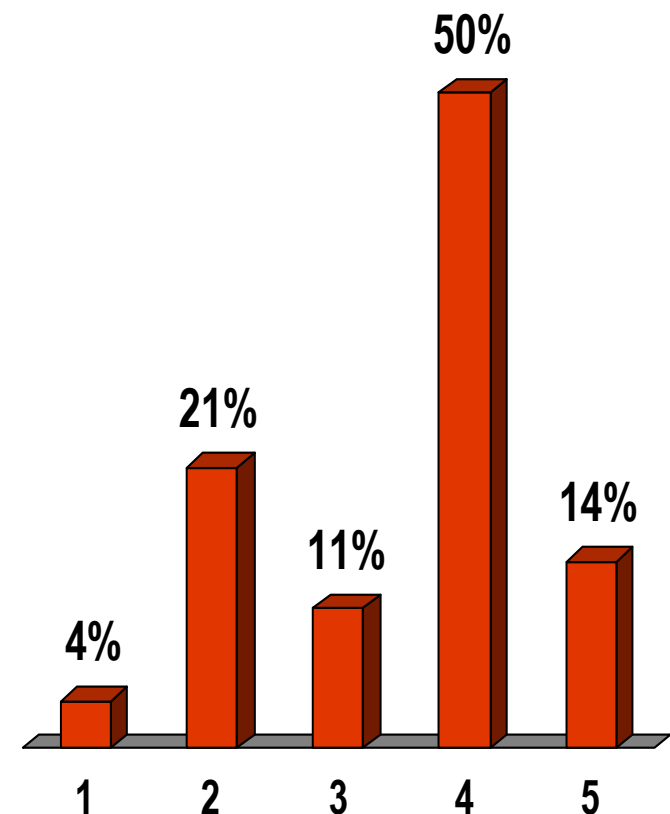
9. Does your current IT Security architecture contains the topic of application security and secure coding standards?

1. Application Security & Secure Coding is included
 44%
2. Application Security only is included
 33%
3. Secure Coding only is included
 4%
4. Not included at all
 19%



10. To what extent do external regulatory, statutory, audit or compliance requirements affect your security strategy?

1. Not at all
2. There are some non-specific requirements we interpret as compliance – but they have no real affect on strategy
3. There are many non-specific requirements we interpret as compliance - with strong influence over our strategy
4. There are some specific requirements with which we must comply but we control the rest of our strategy
5. There are many specific requirements with which we must comply and this dominates our strategy



11. Are you more concerned about compliance this year than you were last year?

1. More concerned



2. Less concerned
0%






3. Same level of concern as last year



4. Not concerned at all about compliance

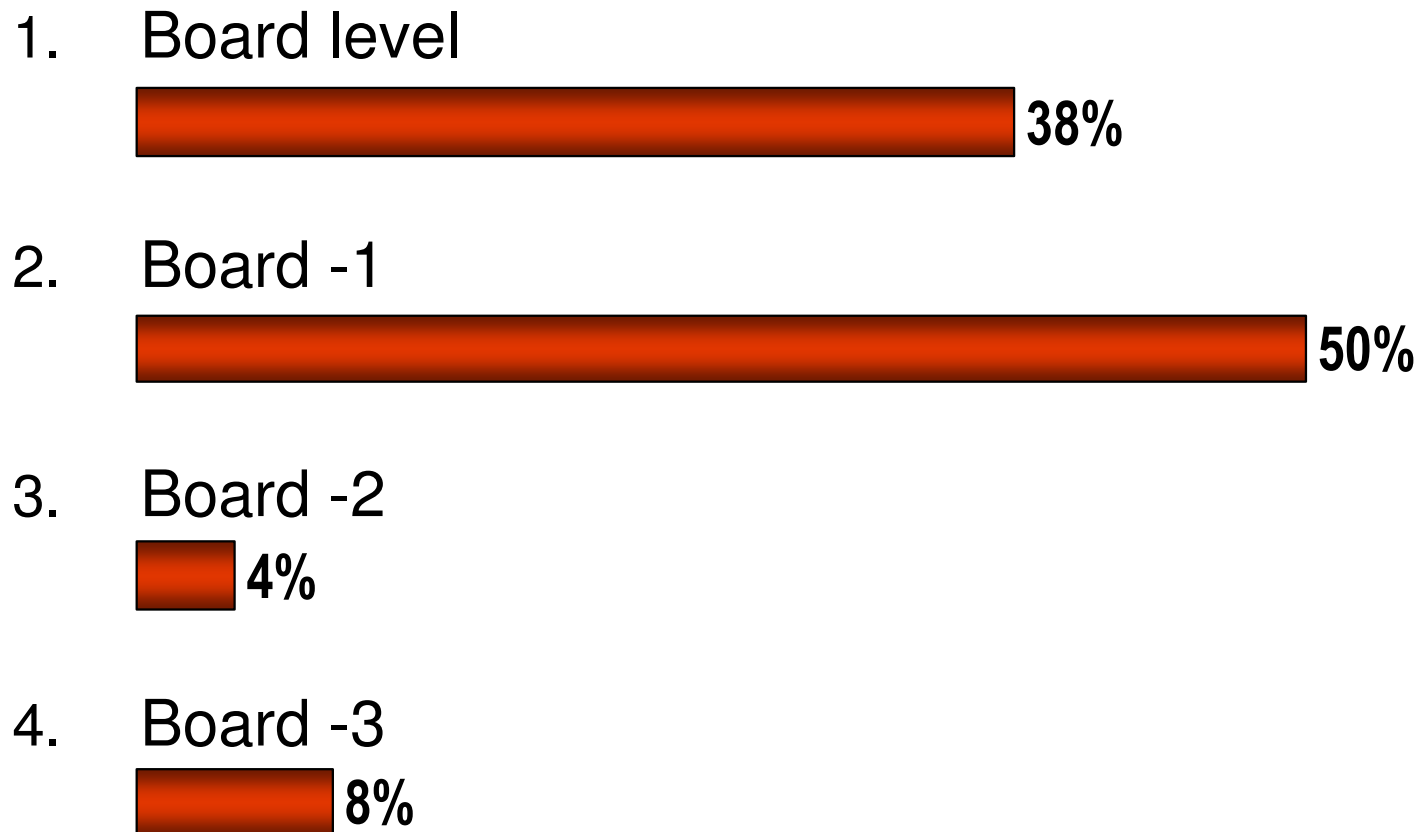


12. Has your budget for compliance solutions changed in the last year?




1. It grew significantly
 19%
2. It grew by a small amount
 31%
3. It stayed the same
 15%
4. It shrank by a small amount
 4%
5. It shrank significantly
0%
6. We don't track our compliance budget separately
 31%



13. Which organizational level takes care of compliance in your company?

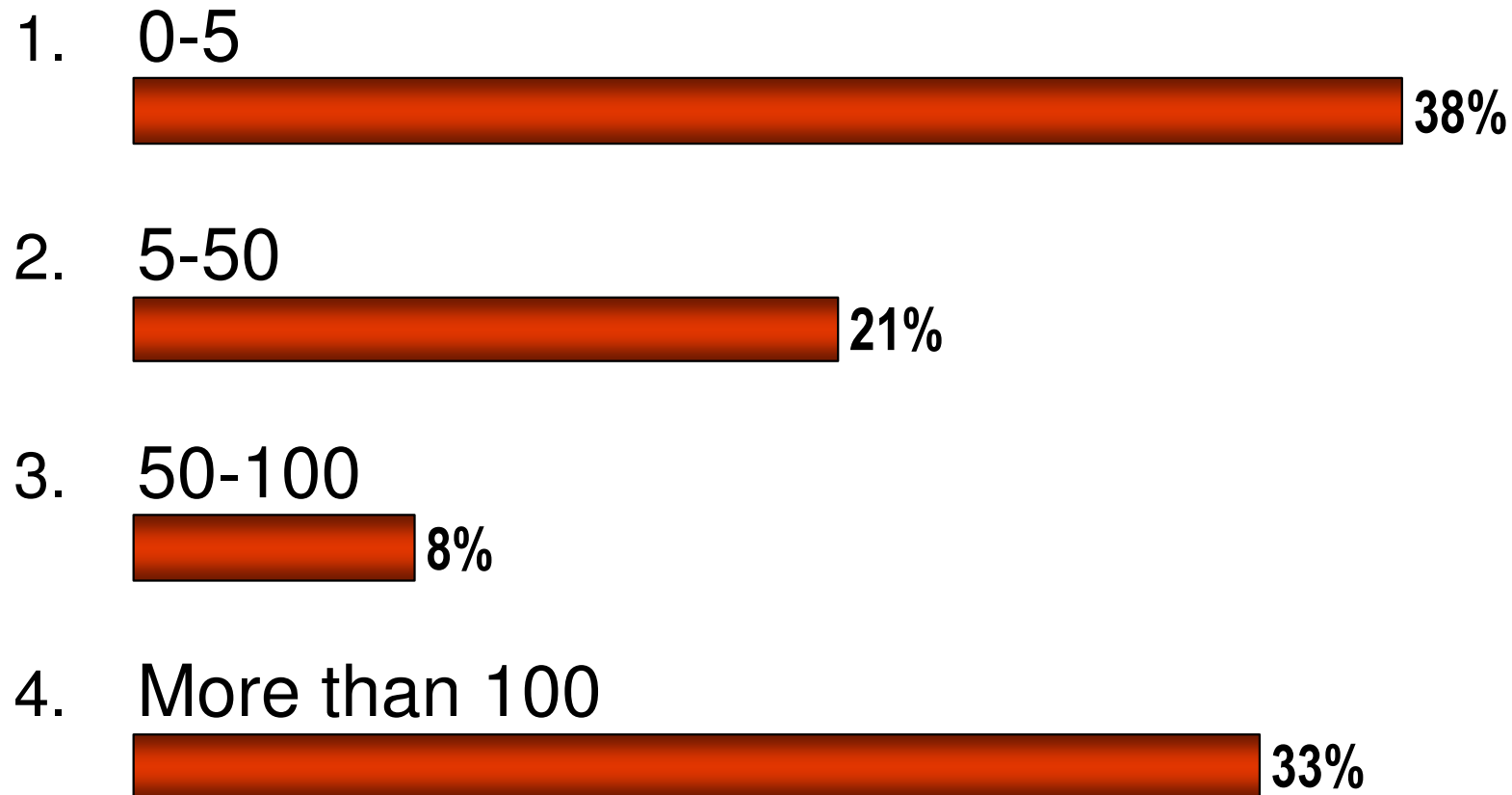


14. Which of the following devices do you currently allow to access your enterprise remotely:

1. Corporate-provided laptops
 73%
2. Employee-owned PCs & laptops
 14%
3. PDAs
0%
4. Laptops belonging to contractors working in your facility
 14%
5. Public kiosks
0%

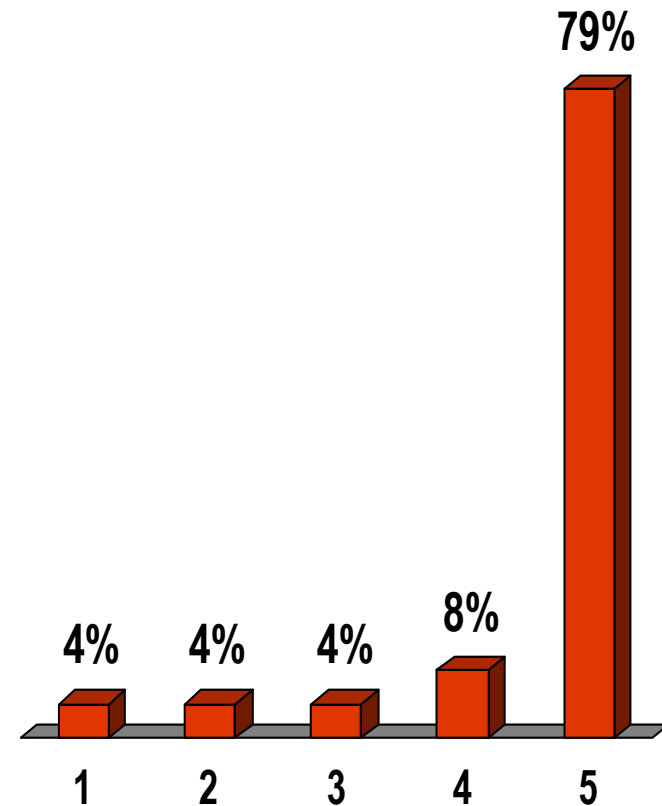


15. How many individuals are there within your security organization?



16. Who does Risk Analysis in your organisation?

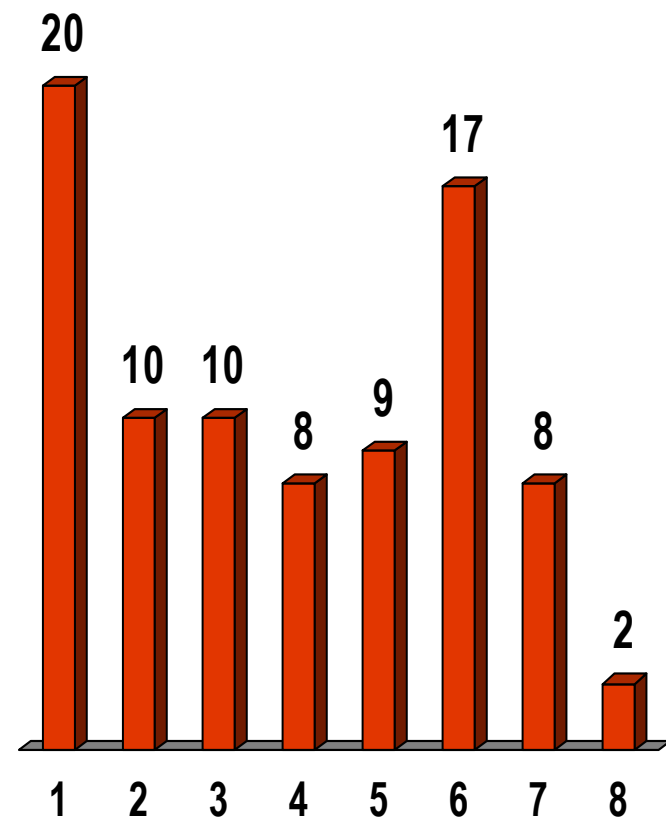
1. Whoever was sleeping in the meeting when the job was handed out
2. The Risk Manager
3. Technical staff
4. Managerial staff
5. A combination of the above



17. Does your current role include organization-wide responsibility for the following

1. Information security
2. Physical security
3. Disaster recovery
4. Business continuity
5. Broader IT risks, such as project risk
6. IT legislation and regulatory compliance
7. Fraud prevention and detection
8. Anti-money laundering

Enter your choices and press SEND






17. Does your current role include organization-wide responsibility for the following

1. Information security
0%
2. Physical security
0%
3. Disaster recovery
0%
4. Business continuity
0%
5. Broader IT risks, such as project risk
100%
6. IT legislation and regulatory compliance
0%
7. Fraud prevention and detection
0%
8. Anti-money laundering
0%



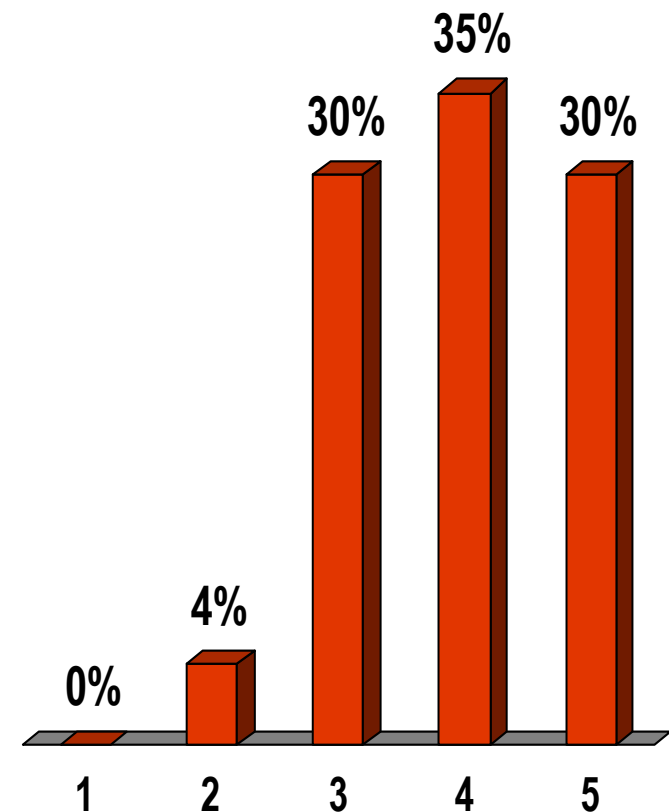
18. Does your company educate and train your developer (internal & external) around secure coding and secure application design?

1. We train internal & external programmers
 17%
2. We train only internal programmers
 25%
3. We train only external programmers
0%
4. We do not train at all
 58%



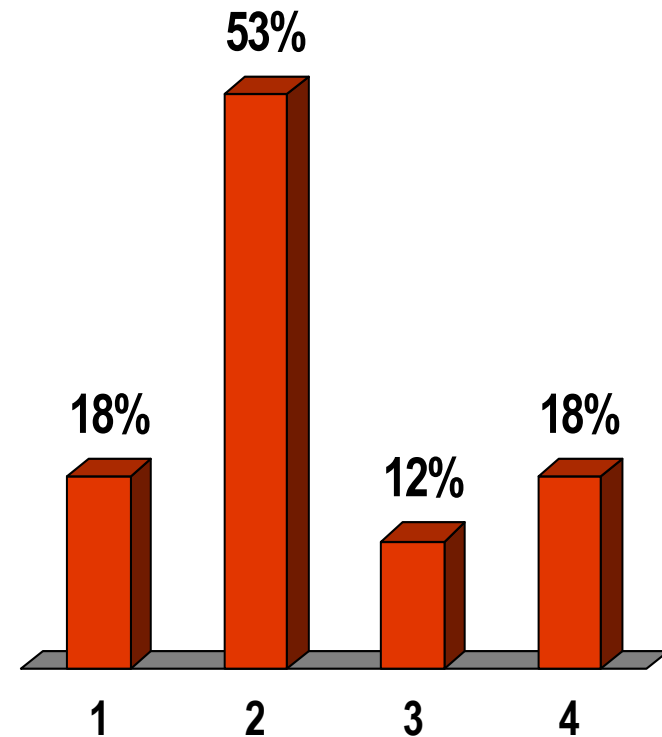
19. How do you decide what to do when you have to comply with external regulatory/statutory/audit/compliance requirements?

1. No need for compliance
2. We retain third-party help (eg auditors, consultants) to interpret & action requirements
3. We ask a third-party (eg regulators, auditors, consultants) to interpret requirements & identify actions & implement them ourselves
4. We interpret the requirements, identify specific actions & implement them ourselves
5. We determine our security strategy, take necessary action, & then compare results with requirements, addressing any gaps



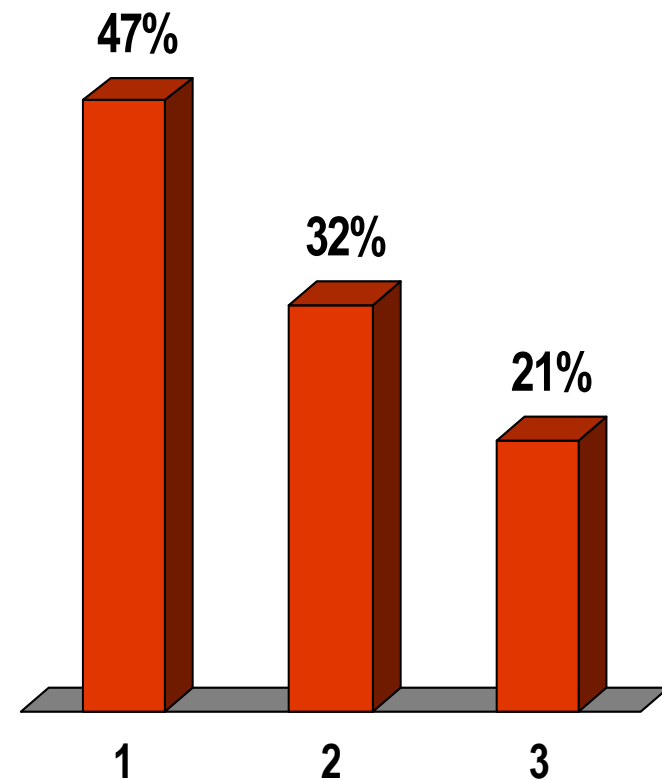
20. If you compare e-commerce to other more traditional retail channels such as in-store shopping, do you think e-commerce is

1. prohibitively risky
2. significantly more risky
3. the same
4. less risky



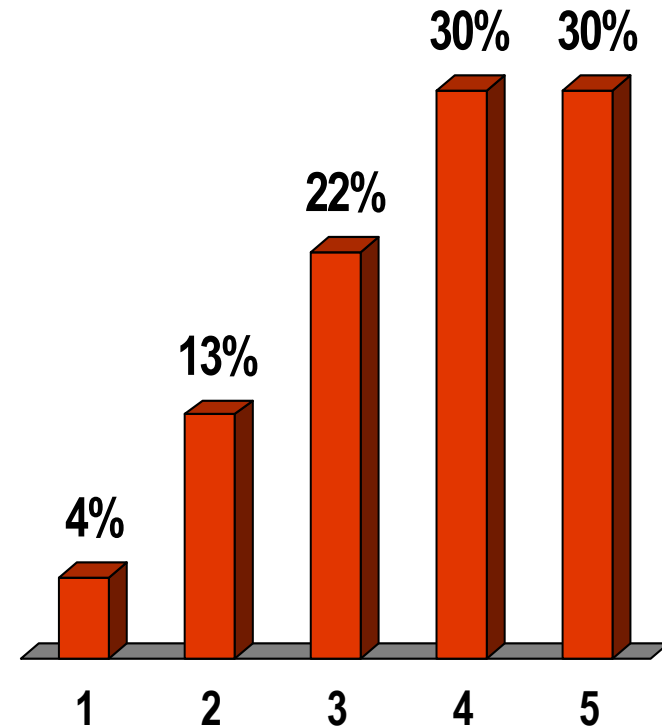
21. How adequate do you think current commercial law is in dealing with e-commerce risks?

1. completely inadequate
2. somewhat inadequate
3. OK

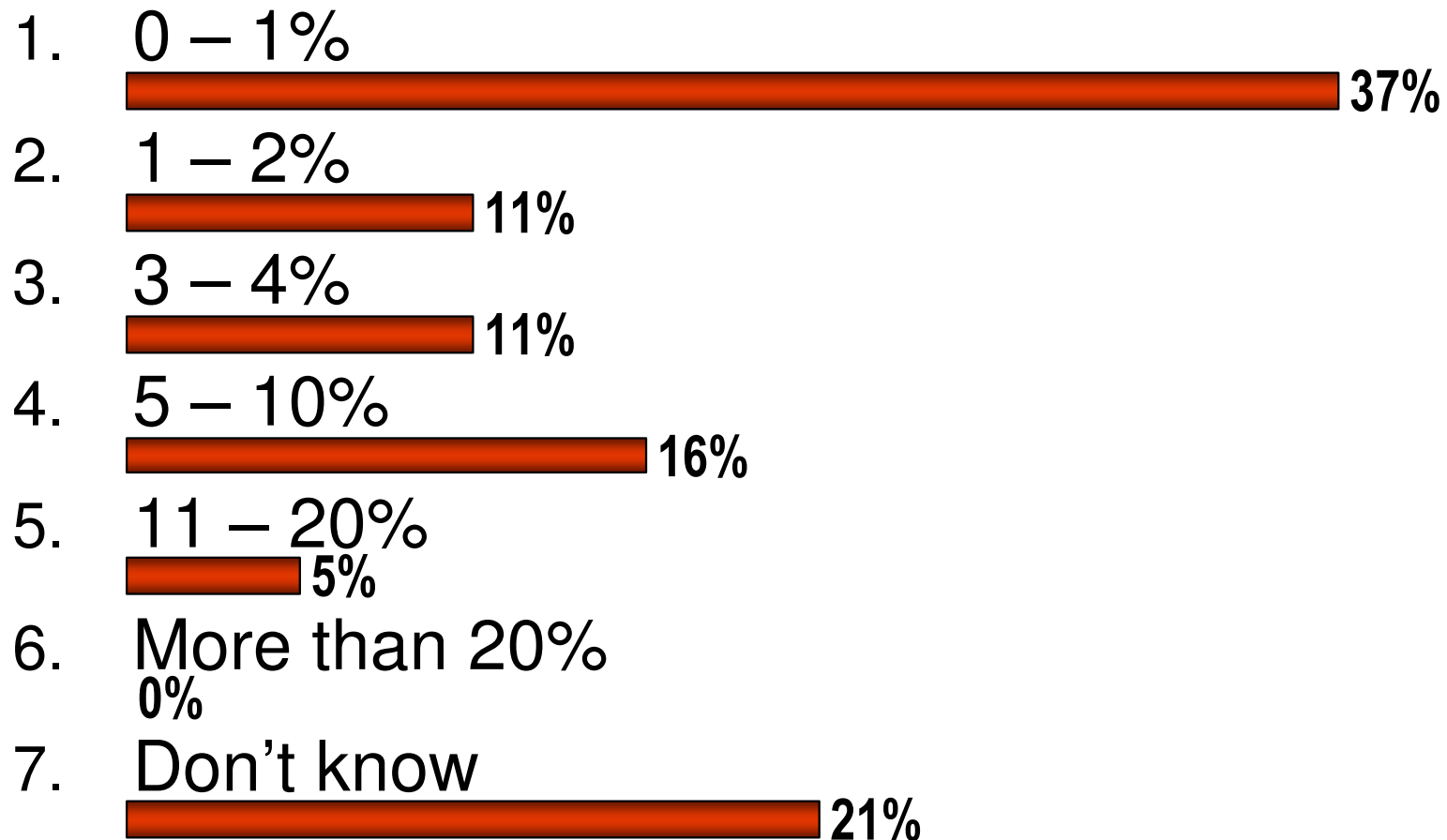


22. How would you feel if you had to carry and use a personal security token?

1. Very put out
2. Mildly inconvenienced
3. Don't mind
4. See it as a plus
5. Don't understand why they haven't been introduced sooner

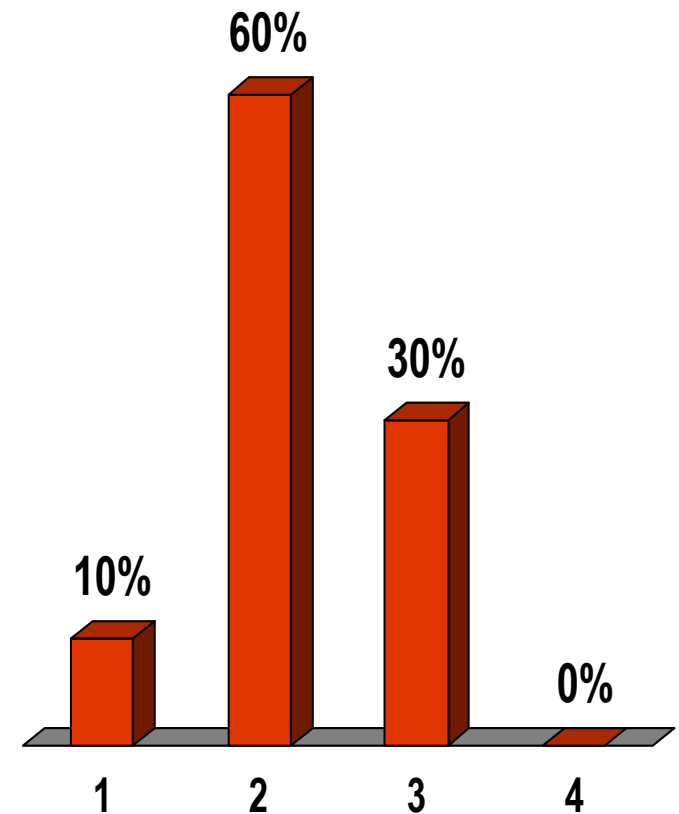


23. Our company spends x% of our security budget on security awareness



24. To what extent does the output of your Risk Management activities inform Senior Management decision making?

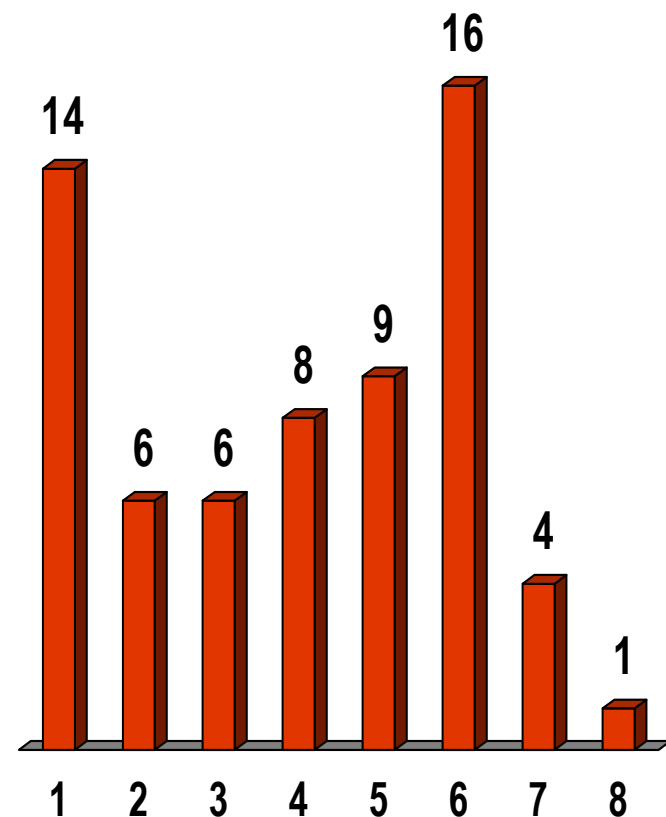
1. There is no communication path between those assessing risks and those taking decisions
2. Senior Management are somewhat aware of risks when making decisions
3. Senior Management are very aware of risks when making decisions
4. Senior Management are constrained from making decisions that exceed defined risk parameters



25. Do you envisage your responsibilities increasing in the following areas in the next two years

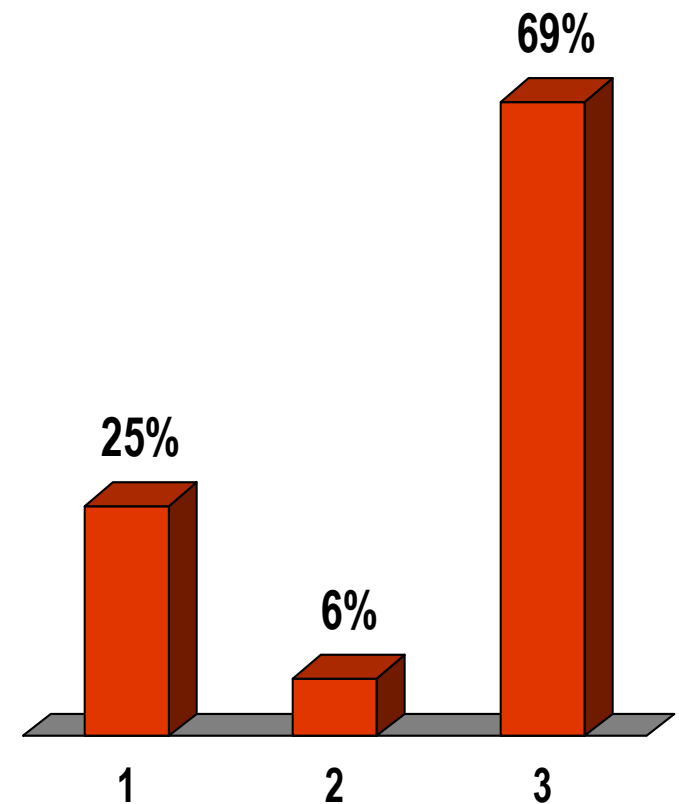
1. Information security
2. Physical security
3. Disaster recovery
4. Business continuity
5. Broader IT risks, such as project risk
6. IT legislation and regulatory compliance
7. Fraud prevention and detection
8. Anti-money laundering

Enter your choices and press SEND






26. Which of the following security services are you providing for your remote access users:

1. Encryption of stored data
2. Automated backup of remotely stored files to an enterprise server
3. Multi-factor user authentication (i.e. hardware token)



27. Does your organisation have any kind of application security related key performance indicators (KPI's)?

1. Yes, on CIO level
 21%
2. Yes, on application project level
 16%
3. Yes, on programmer level
0%
4. No, not at all
 63%



28. How much of your spend on information security requirements is driven by external regulatory / statutory / audit / compliance requirements?

