CSO Interchange London

November 27th, 2007

Lanesborough Hotel

Results

0. Compared to a year ago, has it become easier or harder to secure your networking environment?

1. Easier

2. Harder

3. The same

1. In your organisation, which do you consider the greater security risk…?

1. Insiders (those within the organisation)

75.0%

2. Outsiders (external threats)

25.0%

2. What is the greatest risk to your organisation today? (Rank in order of importance: highest to lowest)

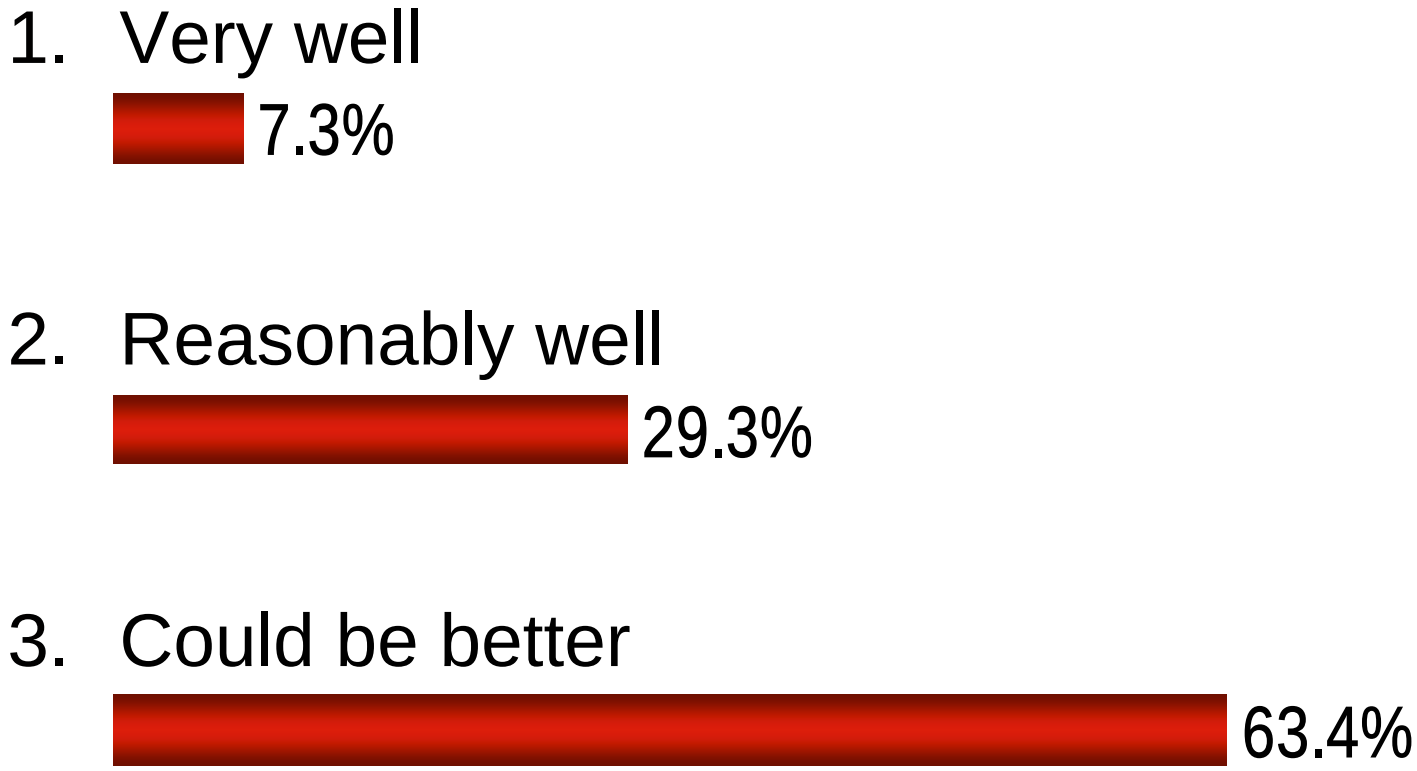
1. Employees
2. Virtual workers and/or partners
3. Vulnerabilities (systems and/or apps)
4. Web use (eg widgets and gadgets)
5. Malware

Enter ALL your choices in order of importance and then press SEND
If you wish to correct your choices press CLEAR and re enter

Ranked Results

Points	Item
145	1. Employees
143	2. Virtual workers and/or partners
127	3. Vulnerabilities (systems and/or apps)
93	5. Malware
91	4. Web use (eg widgets and gadgets)

3. How well integrated is your view of risk in the overall enterprise risk landscape?



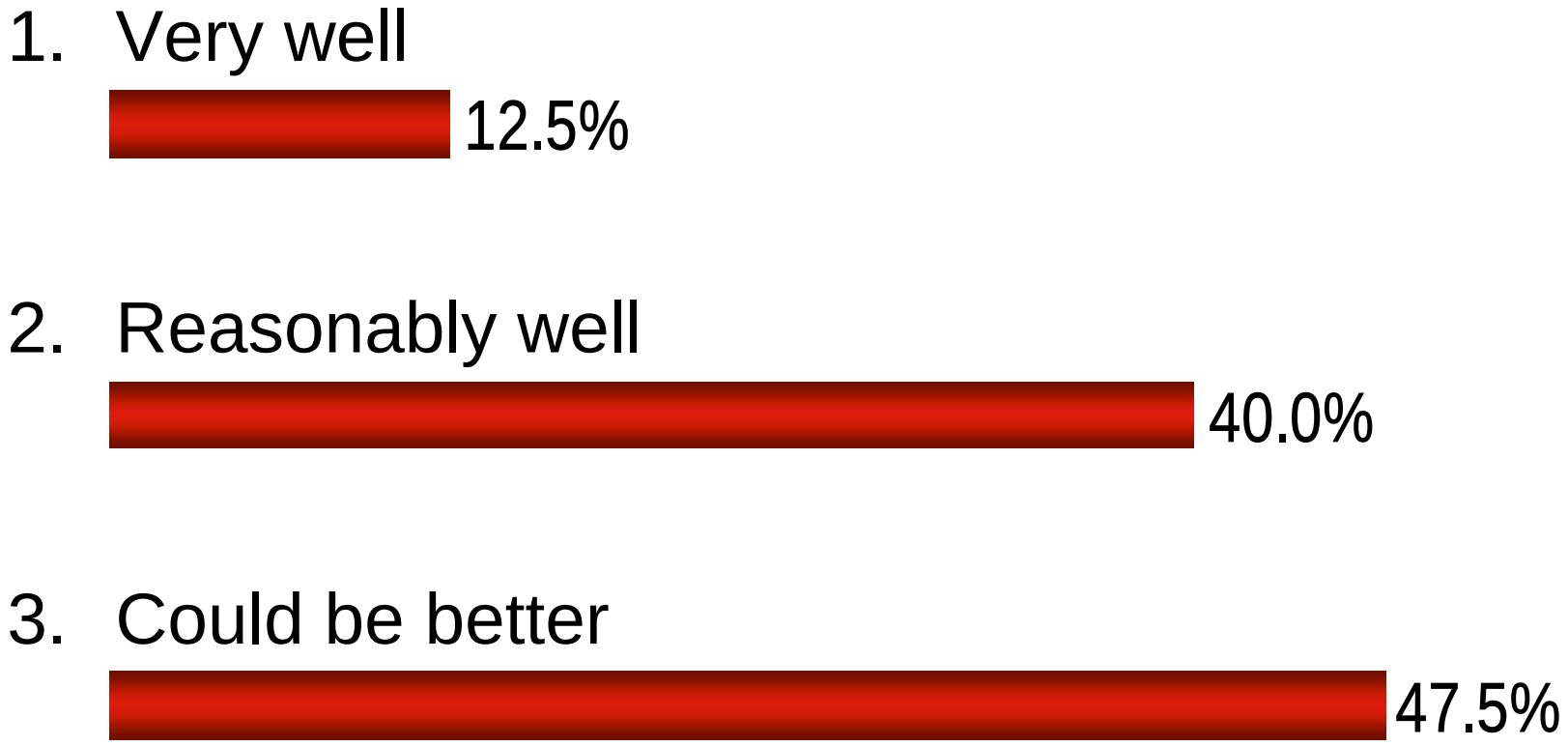
4. How easy is it for you to articulate the impact of these risks and the impact of mitigation financially?

1. Very well

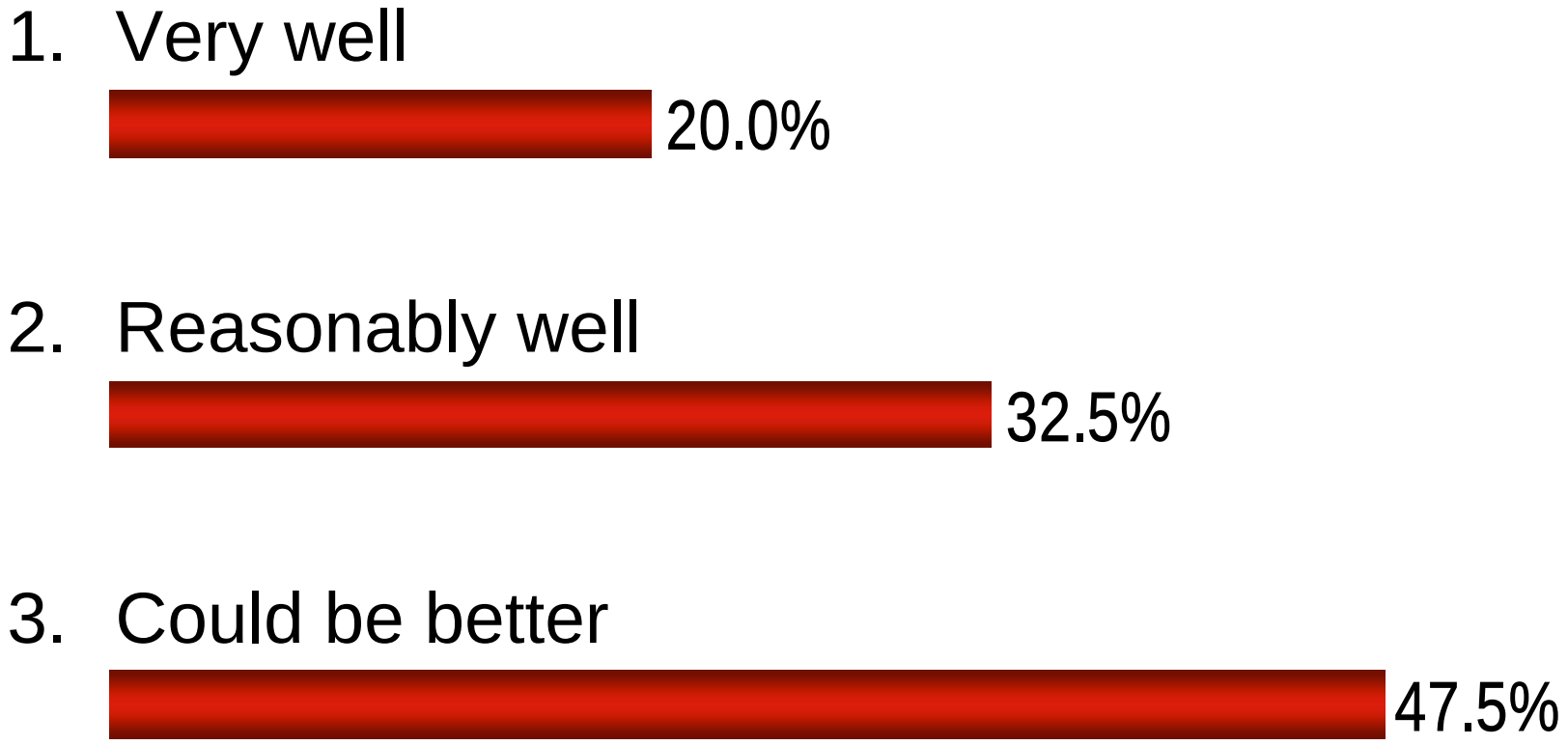
2. Reasonably well

3. Could be better

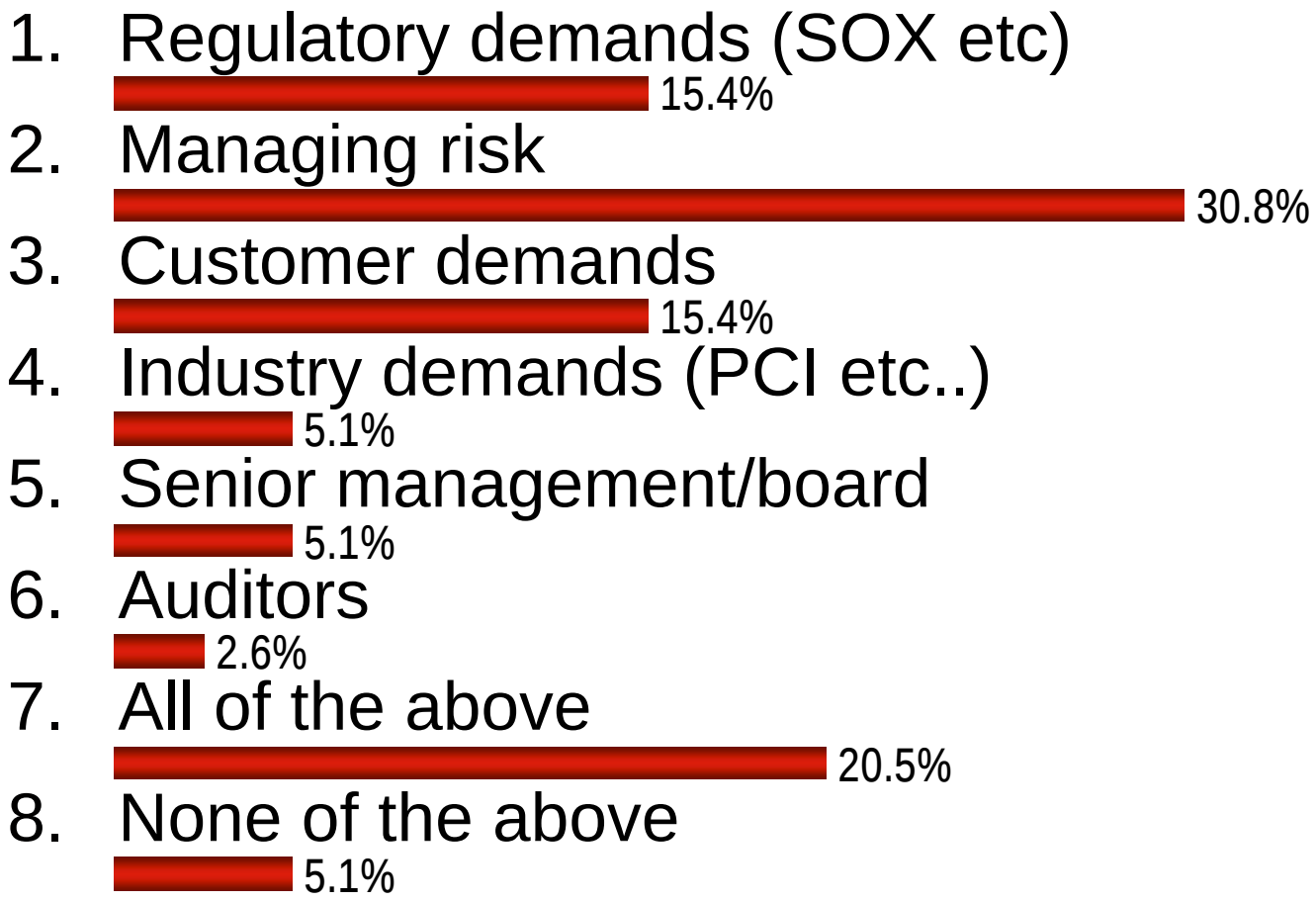
5. How well do you think that you demonstrate to the business the value of what you do?



6. How well do you think that you measure the impact of incidents on your organisation?



7. What is the main driver for security in your company?



8. What are the main obstacles in doing your job? (Rank in order of importance: highest to lowest)

1. Budget
2. Time
3. Personnel
4. Insufficient technology
5. Lengthy hardware/software implementations
6. Reporting requirements
7. Unhelpful media coverage on security
8. My own incompetence

Enter ALL your choices in order of importance and then press SEND
If you wish to correct your choices press CLEAR and re enter

Ranked Results

Points	Item
214	2. Time
212	3. Personnel
209	1. Budget
144	5. Lengthy hardware/software implementations
136	4. Insufficient technology
109	6. Reporting requirements
75	7. Unhelpful media coverage on security
68	8. My own incompetence

9. What is your view on software as a service? Will it displace enterprise software?

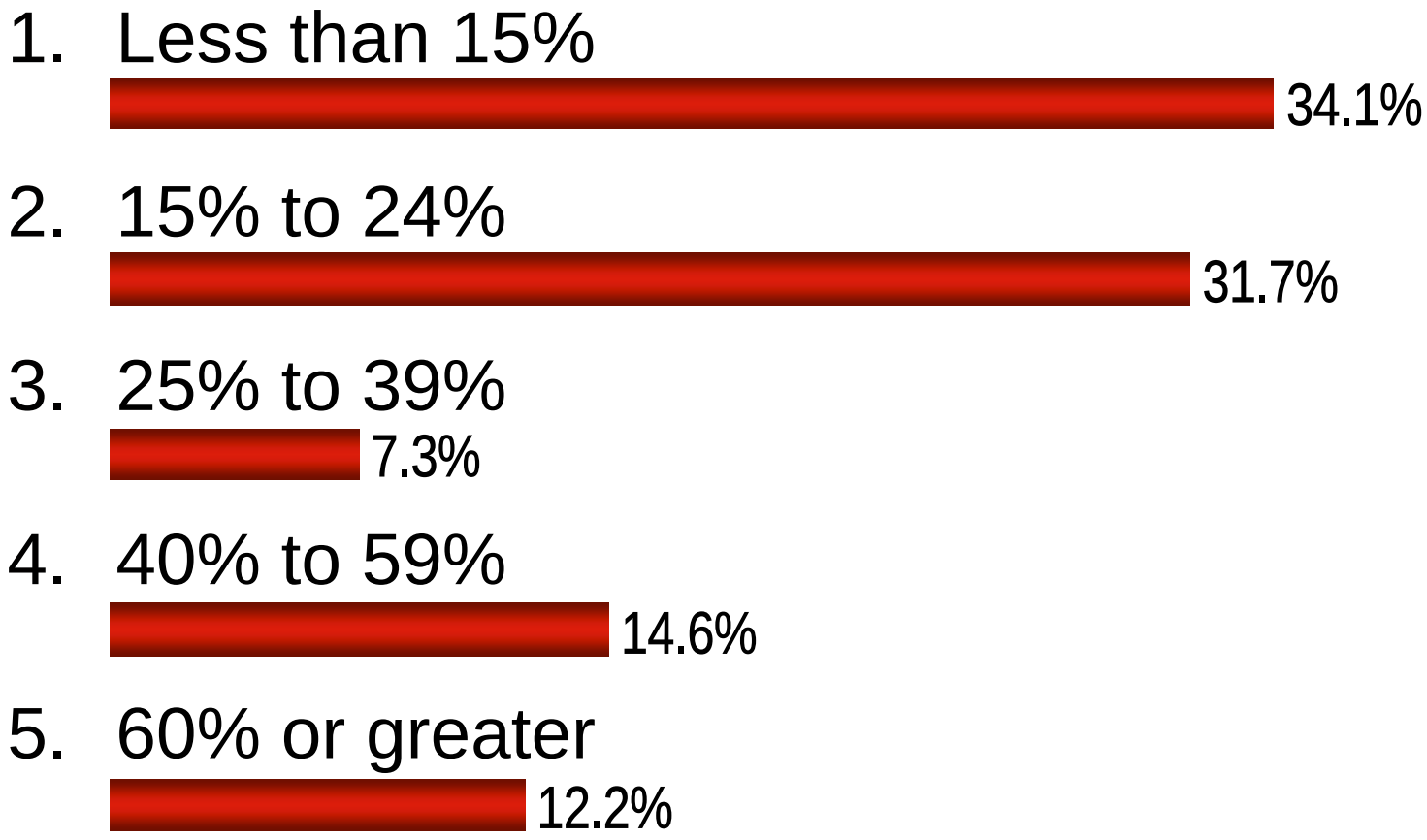
1. Yes

50.0%

2. No

50.0%

10. What proportion of your team's time is dedicated to meeting security compliance requirements?



11. The greatest consequence of a card data security breach is to….

1. Brand reputation

72.5%
2. Company finance

5.0%
3. Customer finance and identity

2.5%
4. My job

2.5%
5. All of the above

17.5%

12. What does security convergence mean to you?

1. Physical Security and Information Security


16.7%

2. Audit & Compliance Business Continuity & Information Security


40.5%

3. Network/IT Security and Information Security


16.7%

4. Financial crime

0.0%

5. All of the above


26.2%

13. What is your approach to Business Continuity Planning for your organisation?

1. Integrated plan led by the CSO
   
   28.2%
2. Integrated plan led by another unit
   
   25.6%
3. Separate plans by organisational responsibility
   
   38.5%
4. Only an IT Disaster Recovery plan
   
   7.7%
5. Nothing formal
   0.0%

14. Does Software as a service help make information more secure?

1. Yes

34.9%

2. No

65.1%

15. How would you assess Information leakage for your organisation?

1. A serious problem

45.2%

2. A problem but not an immediate concern

45.2%

3. Not an Issue

4.8%

4. Can’t say

4.8%

16. Do you believe there are adequate controls in your organisation to deal with data theft?

1. There are controls but they are not robust

67.4%

2. We have an effective control process in place to counter this risk

9.3%

3. We have no controls in place

14.0%

4. We have not assessed this as an issue

9.3%

17. Do you know where your customer data is stored and can you protect it from being stolen?

1. We know where are data is and have controls to prevent its theft

32.5%

2. We have some idea where are data is and limited controls

60.0%

3. We have no idea where are data is and no controls

0.0%

4. We are working on this

7.5%

18. Has your company deployed or considering deploying a Software as a service solution?

1. Has already deployed

42.9%

2. Is considering

31.4%

3. Is not considering

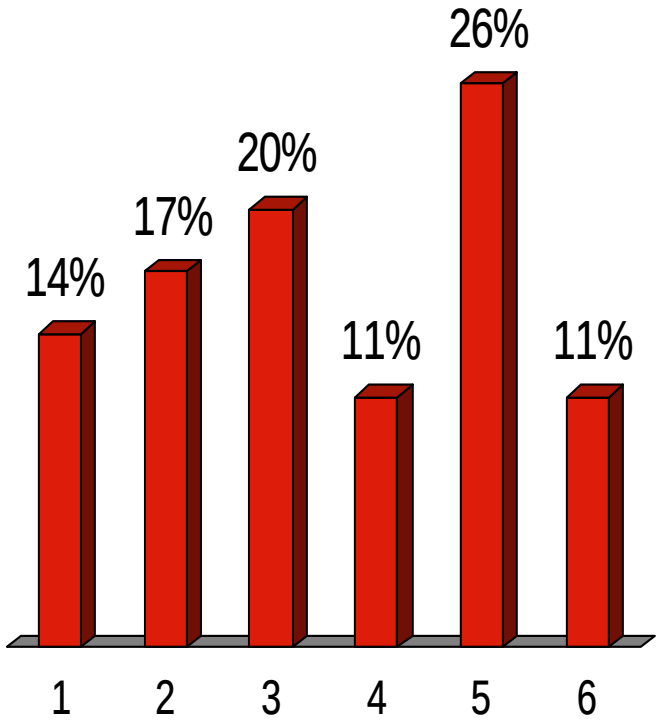
25.7%

19. How mature is your IT Security budgeting and accounting process?

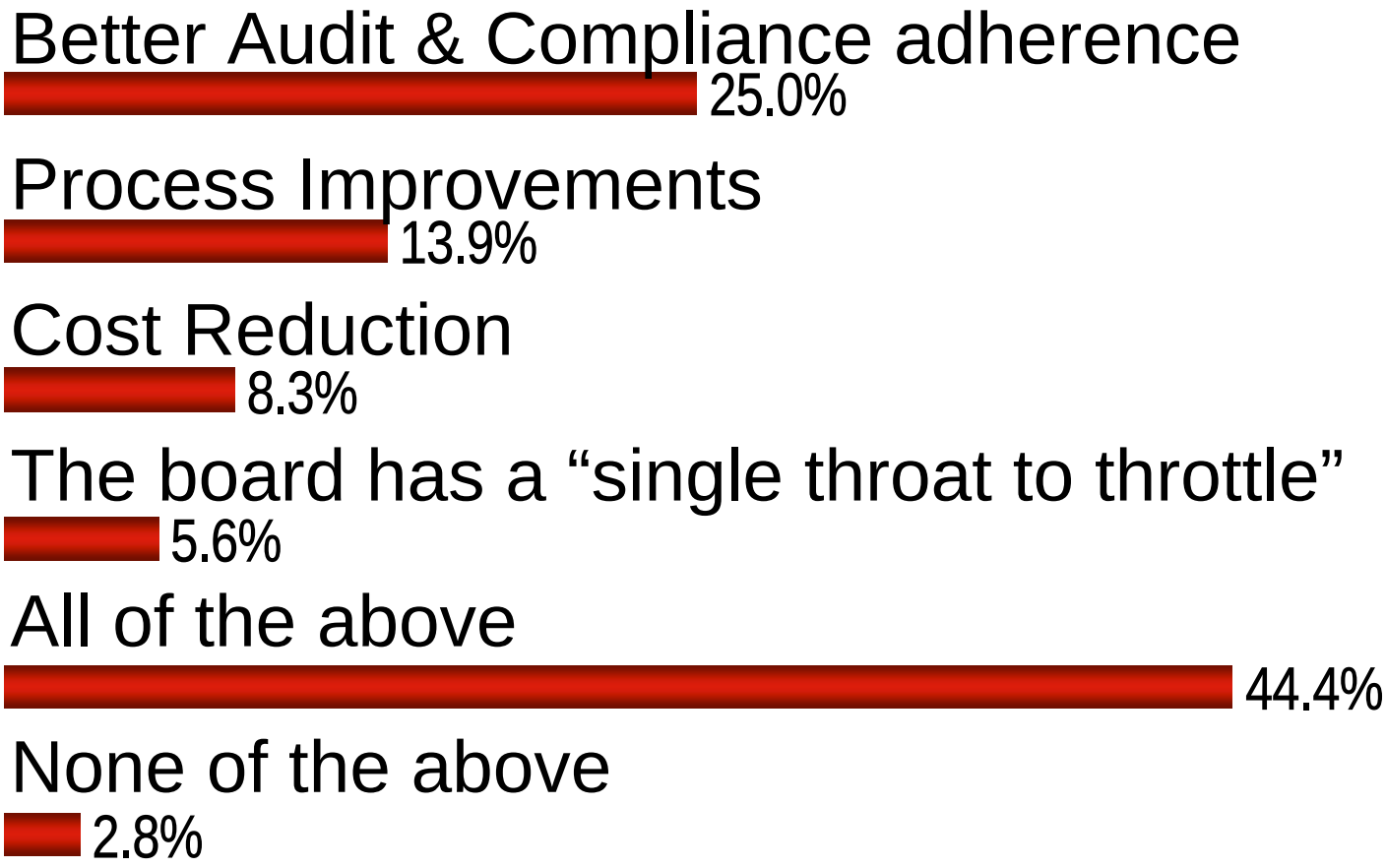
1. Very mature – we budget for everything in detail and measure ROI
   5.7%
2. Mature – we budget for everything but in broad-brush terms, but do not really have an accurate ROI
   37.1%
3. Growing – we recognise the need for accurate budgets and to prove value for money, and we are developing a process
   37.1%
4. Scarce – we just throw money at the latest fire and live from day to day!
   20.0%

20. How well have the card schemes, acquirers and the PCI Security Standards Council publicised the Data Security Standard and its implications?

1. Not at all: what's PCI?
2. Poorly: my acquirer sent me one letter
3. Well: I have had detailed information from my acquirer and the PCI Security Standards Council
4. Excessively: I am fed up of them going on about it
5. Not relevant
6. Don’t know



21. What are the intended benefits that go along with security convergence?



22. How often do you conduct a practice of the Business Continuity Plan?

1. Complete practice once a year

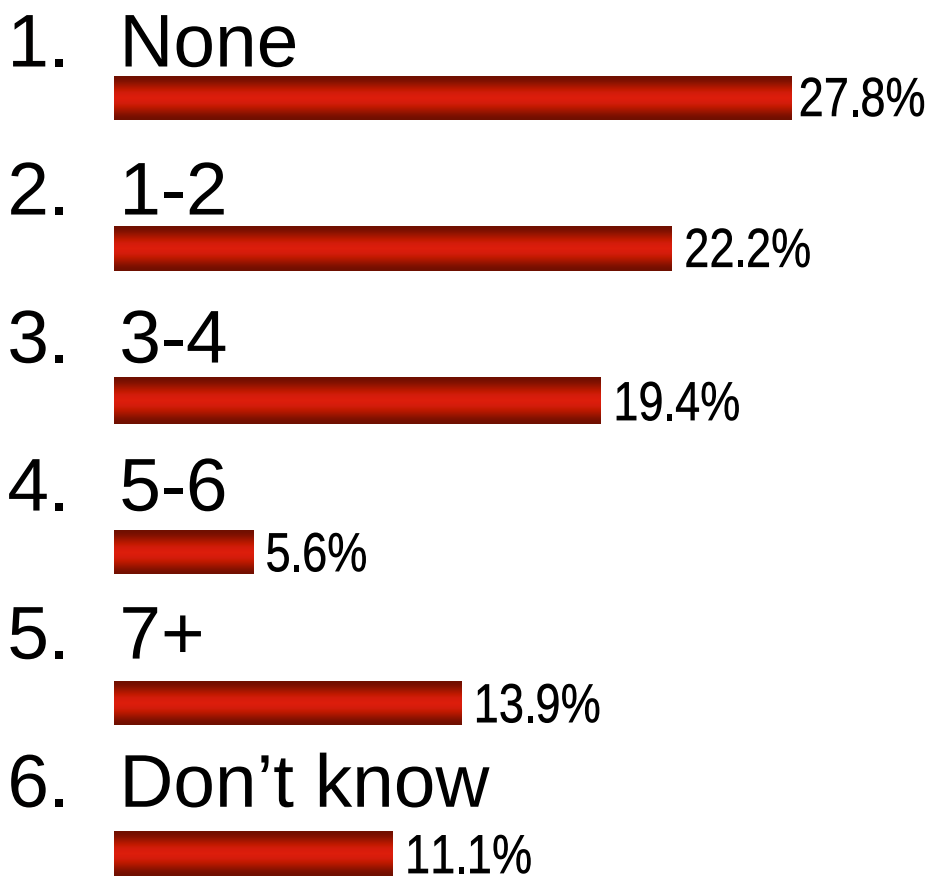
20.0%
2. Partial practice once a year

25.7%
3. Complete practice every 5 years
0.0%
4. No complete practice

34.3%
5. No practice at all

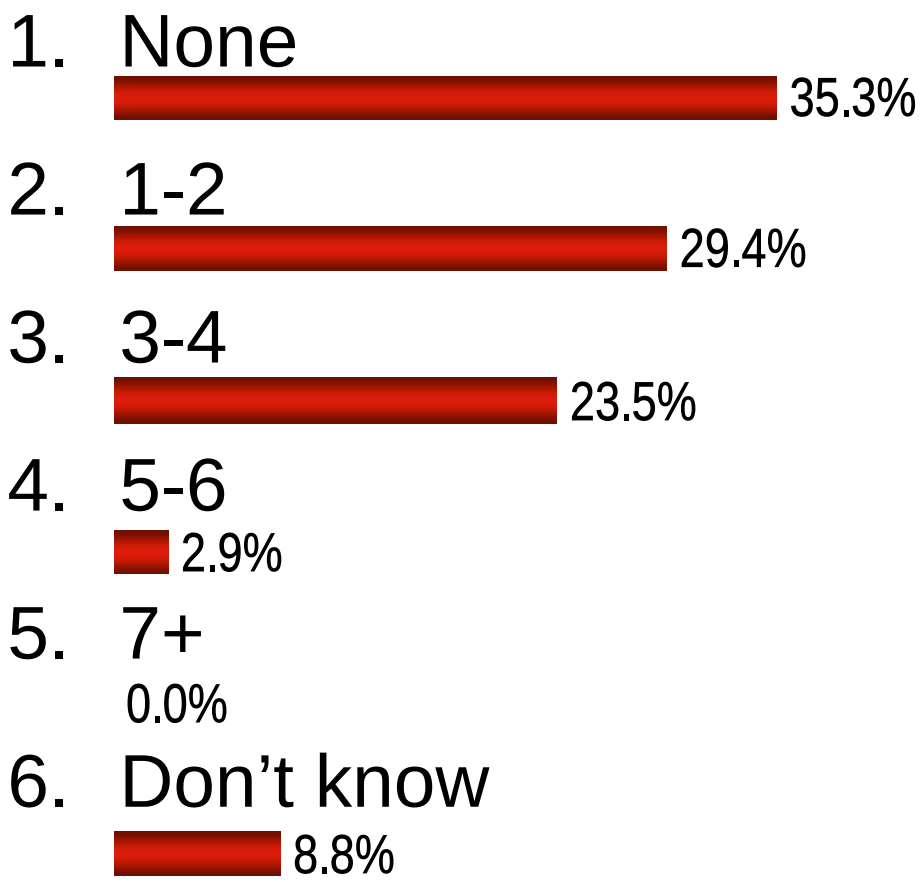
20.0%

23. How many types of collaborative Web 2.0 applications are hosted in your organisation for internal use?



Examples
Blogs
Wikis (Twiki, Wikipedia)
Social software (like Facebook)
Web service APIs
Podcasts

24. How many types of collaborative Web 2.0 applications are hosted in your organisation for external use?



Examples
Blogs
Wikis (Twiki, Wikipedia)
Social software (like Facebook)
Web service APIs
Podcasts

25. What is your company's position on green IT?

1. We do not really have one

2. We are addressing in our data centres only

3. We are addressing in all areas of our organisation

26. What is you view of third party IT resources such as co-location and software as a service?

1. They make our use of IT more reliable and secure

2. They make no difference to IT security and reliability

3. They make our use of IT less reliable and secure

27. What is you view of using the internet for critical business communications?

1. It is good for our business and we can make internet communication secure

54.3%

2. We have to use, but consider to be inherently insecure

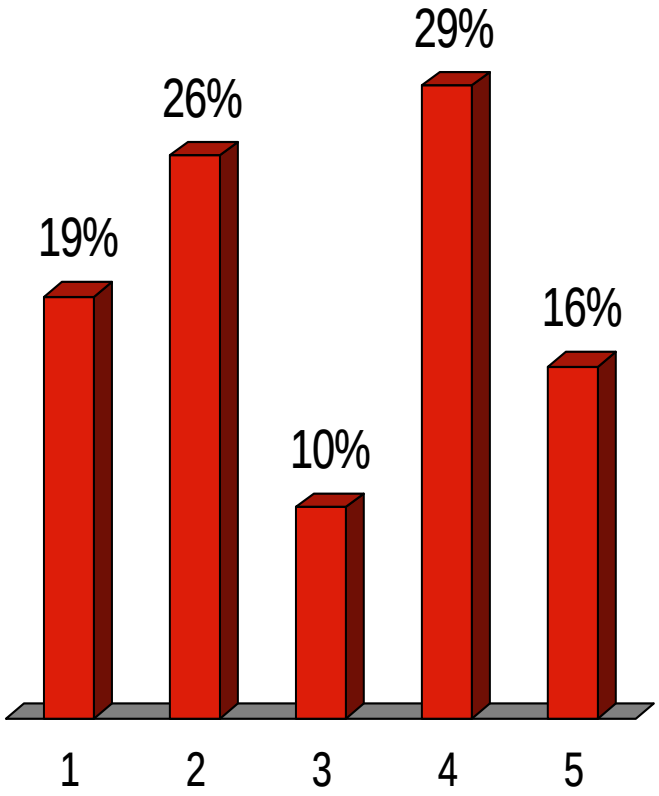
37.1%

3. We avoid use as it is unreliable and insecure

8.6%

28. Which of the following measures do you use or consider valid when presenting the business case for IT Security?

1. Reduction in theft, loss and fraud
2. Avoidance of breaches of law or regulation with associated fines and adverse publicity
3. Increased availability of business-critical information and business efficiency
4. Avoidance of harm to reputation
5. Use of secure business environment as positive marketing differentiator



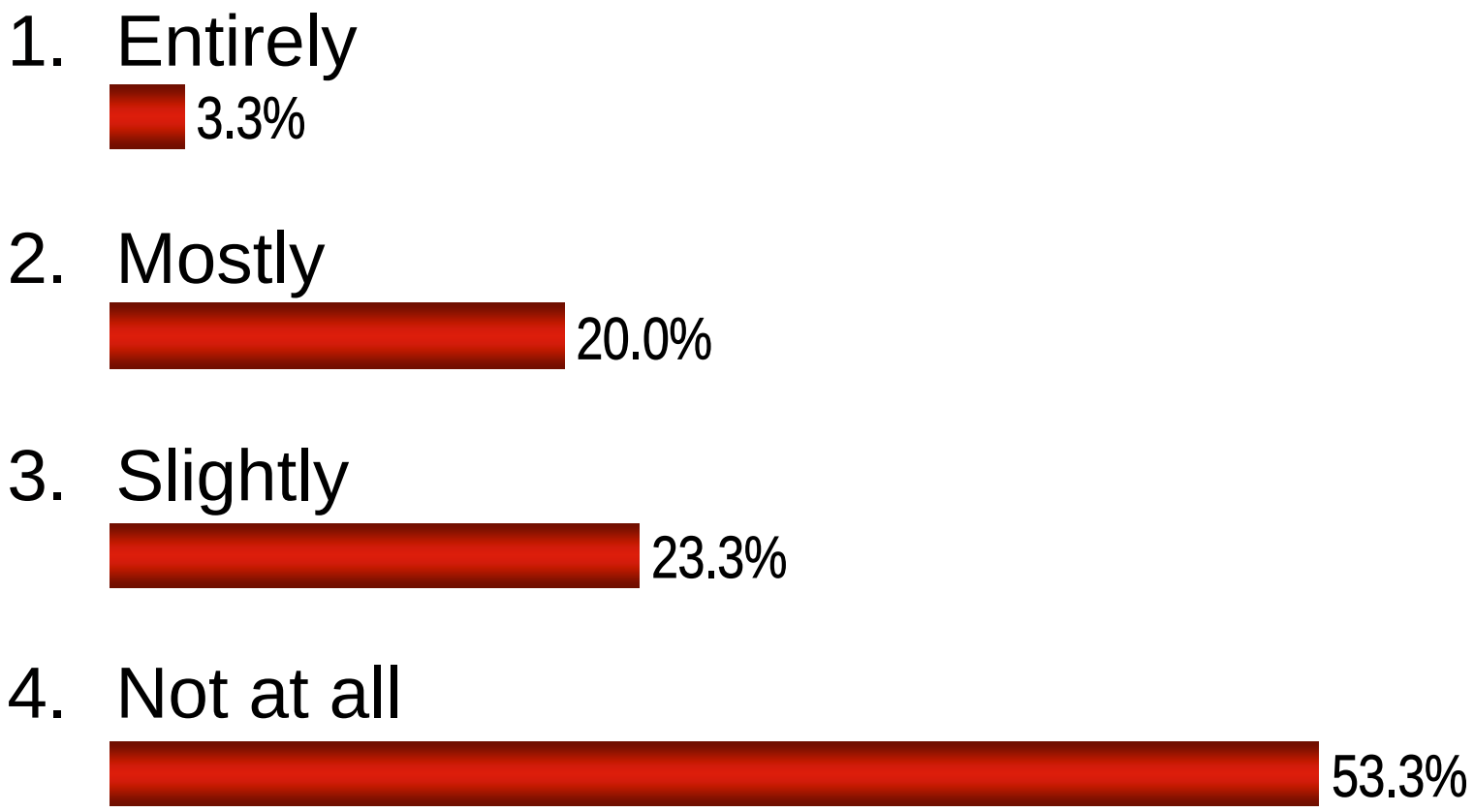
29. How reasonable are the requirements of the PCI Data Security Standard?

1. Not at all: *much too stringent*
   6.5%
2. Fairly: *most are reasonable but a few are excessive*
   25.8%
3. Completely reasonable: *they represent good practice*
   25.8%
4. Too reasonable: *they should be made stronger*
   6.5%
5. Don’t know
   35.5%

30. How clear are the requirements of the PCI Data Security Standard?

1. Not at all: *many are vague*
   3.2%
2. Fairly: *mostly clear but several are vague or irrelevant*
   29.0%
3. Quite: *almost all the requirements are clear*
   16.1%
4. Very: *there are no areas we're not clear about*
   6.5%
5. Don't know
   45.2%

31. To what extent is your Business Continuity Plan driven by regulatory requirements?



32. Do you have staff dedicated to maintaining a Business Continuity Plan?

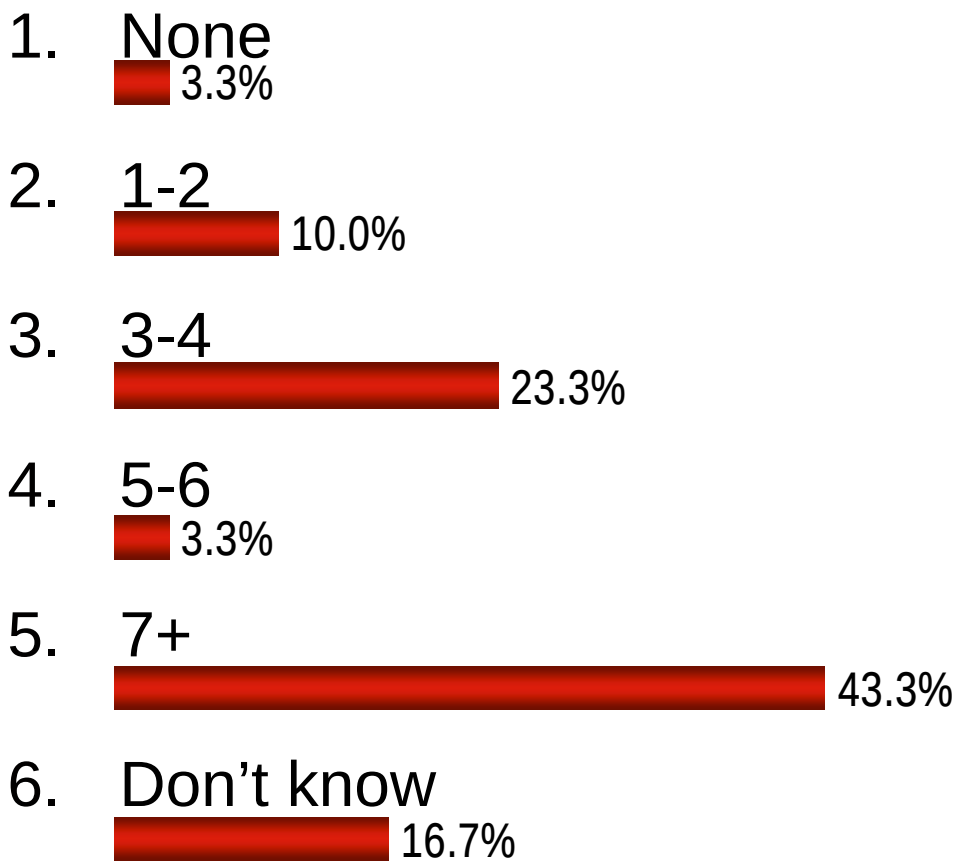
1. Yes

41.9%

2. No

58.1%

33. How many types of collaborative Web 2.0 applications do you allow your employees to access on the Internet?



Examples
Blogs
Wikis (Twiki, Wikipedia)
Social software (like Facebook)
Web service APIs
Podcasts