






CSO Interchange London

December 4th, 2008

The Lansdowne Club

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

1. Pressures from the current economic climate
 41.7%
2. Security threats from disgruntled employees
 37.5%
3. Increased attacks from cybercrime
 20.8%



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
6. Exploitation of intellectual property
7. Current economic climate

**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

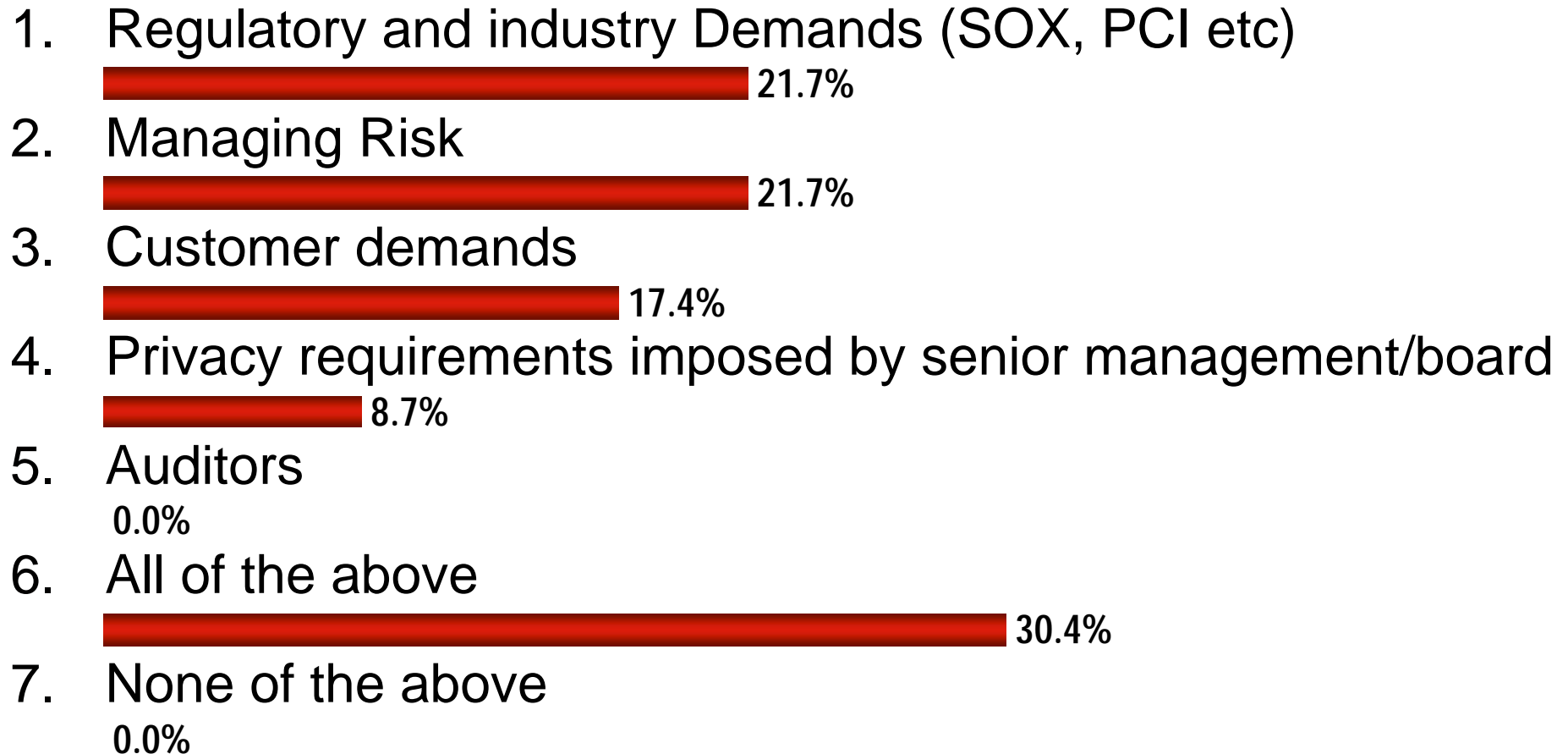
Points

Item

100	7. Current economic climate
97	1. Employees
79	3. Vulnerabilities (systems and/or apps)
78	2. Virtual workers and/or partners
77	6. Exploitation of intellectual property
71	5. Malware
65	4. Web use (eg widgets and gadgets)



What is the main driver for security in your company?



What are the main restraining factors to you in 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
9. Too much tactical versus strategic work

**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

150	2. Time
136	1. Budget
132	3. Personnel
110	9. Too much tactical versus strategic work
93	5. Lengthy hardware/software implementations
79	6. Reporting requirements
71	4. Insufficient technology
39	7. Unhelpful media coverage on security
35	8. My own incompetence



How confident do you feel about your understanding of the risks facing your company?

1. Not very confident



2. Reasonably confident



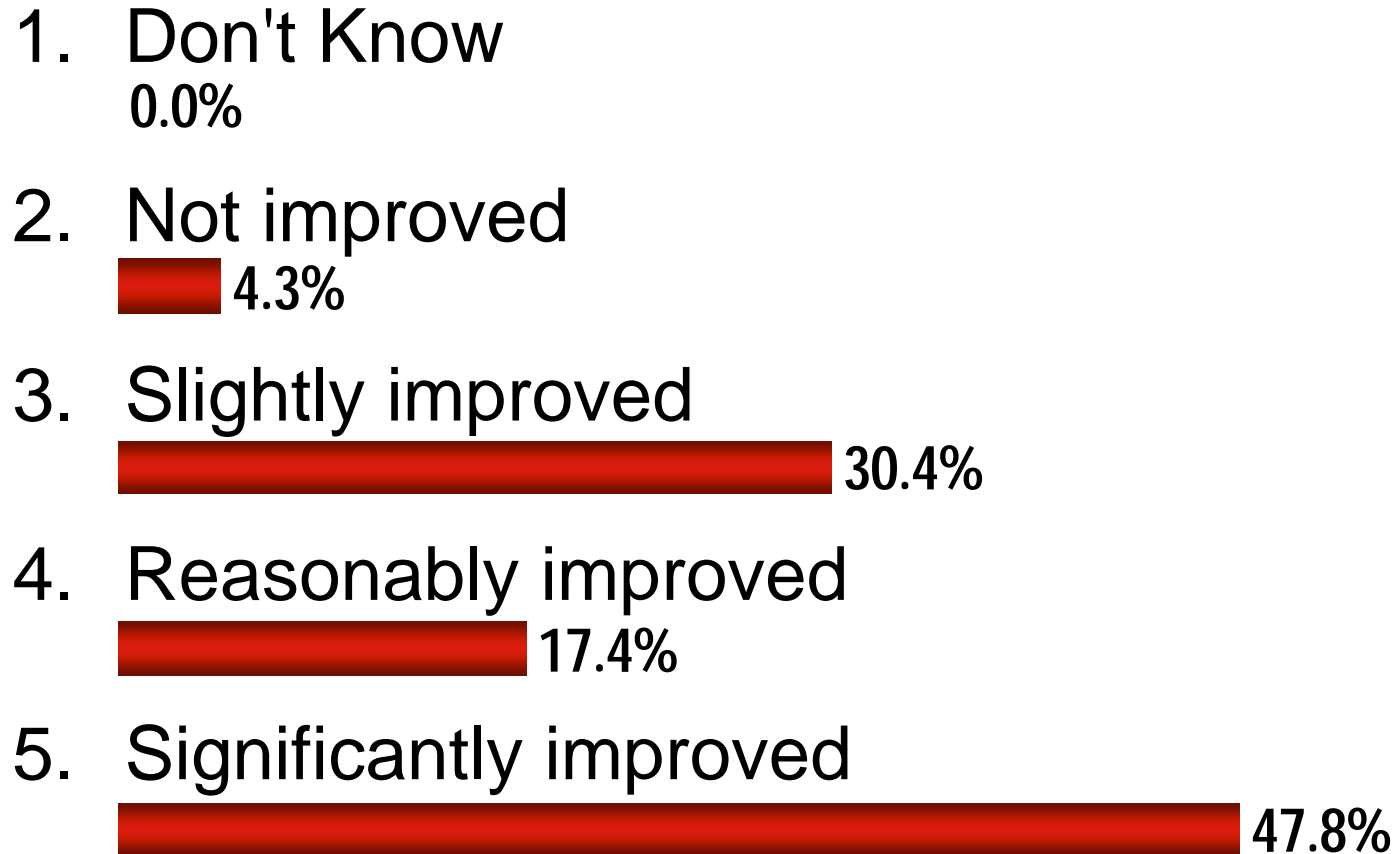
3. Largely confident



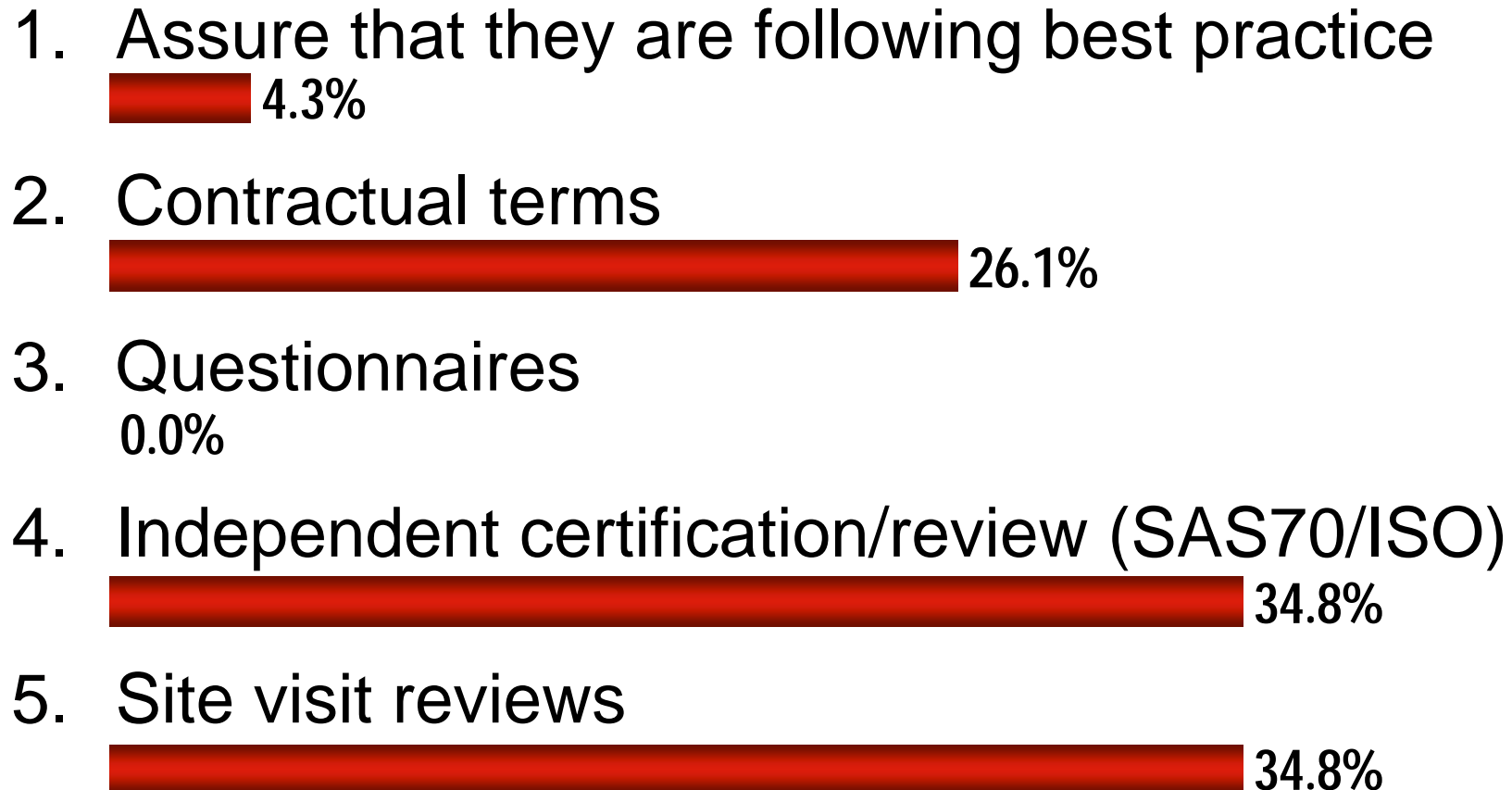
4. Completely confident



How much do you think your corporate awareness of Privacy requirements has increased in the last six months?



What method should you use to ensure third parties (and their suppliers) meet your Privacy requirements?



What action should be taken in the event of a data breach?

1. No action
0.0%
2. Fining company
0.0%
3. Fining company proportionately to seriousness of breach
40.0%
4. Fining company proportionately to annual revenue
12.0%
5. Action taken against senior management
4.0%
6. Action taken against board level
8.0%
7. Prison sentence
0.0%
8. All except 1. above
36.0%



Will SaaS replace mission critical enterprise applications software?

1. Within one year



2. Within 2 to 4 years



3. Within 5 years



4. Never



Will SaaS make information easier to secure?

1. Yes



2. No



Has your company deployed or is considering deploying an SaaS solution?

1. Has already deployed









2. Is considering



3. Is not considering






What are the barriers to introducing SaaS in your organisation?

1. fit within existing security strategy
 20.0%
2. perceived lack of right skills within your organisation
 15.0%
3. your own understanding of benefits of SaaS
 10.0%
4. senior management's understanding of benefits of SaaS
 30.0%
5. poor understanding of the SaaS cost model
 5.0%
6. perception that SaaS is less secure
 20.0%






The arguments for or against Security SaaS revolve around the perceived risks associated with trusting an external third party: Do you feel that:

1. A SaaS provider specialising in security technology has better risk mitigation in place than most enterprises
 **55.0%**
2. Your enterprise is much more successful in securing data than any other external provider ever could be
 **10.0%**
3. You are neutral on this one
 **35.0%**






Are you addressing the risks posed by outsourcing to third parties?

1. Comprehensive approach to risk management for outsourcing being developed/implemented
 68.4%
2. Ad hoc approach adopted as and when
 26.3%
3. No risk management approach in place
 5.3%
4. Not seen as an issue
0.0%



Are you addressing the risks posed by Information Leakage to your organisation?

1. Strategic risk mitigation programme being developed/implemented
 43.5%
2. Tactical approaches being undertaken
 47.8%
3. Doesn't concern us
0.0%
4. Can't say
 8.7%



Have you done anything which, if data mined, could be used by the authorities to discredit you?

1. Broken some rules and could be fined



2. It could affect my marriage or other personal relationships

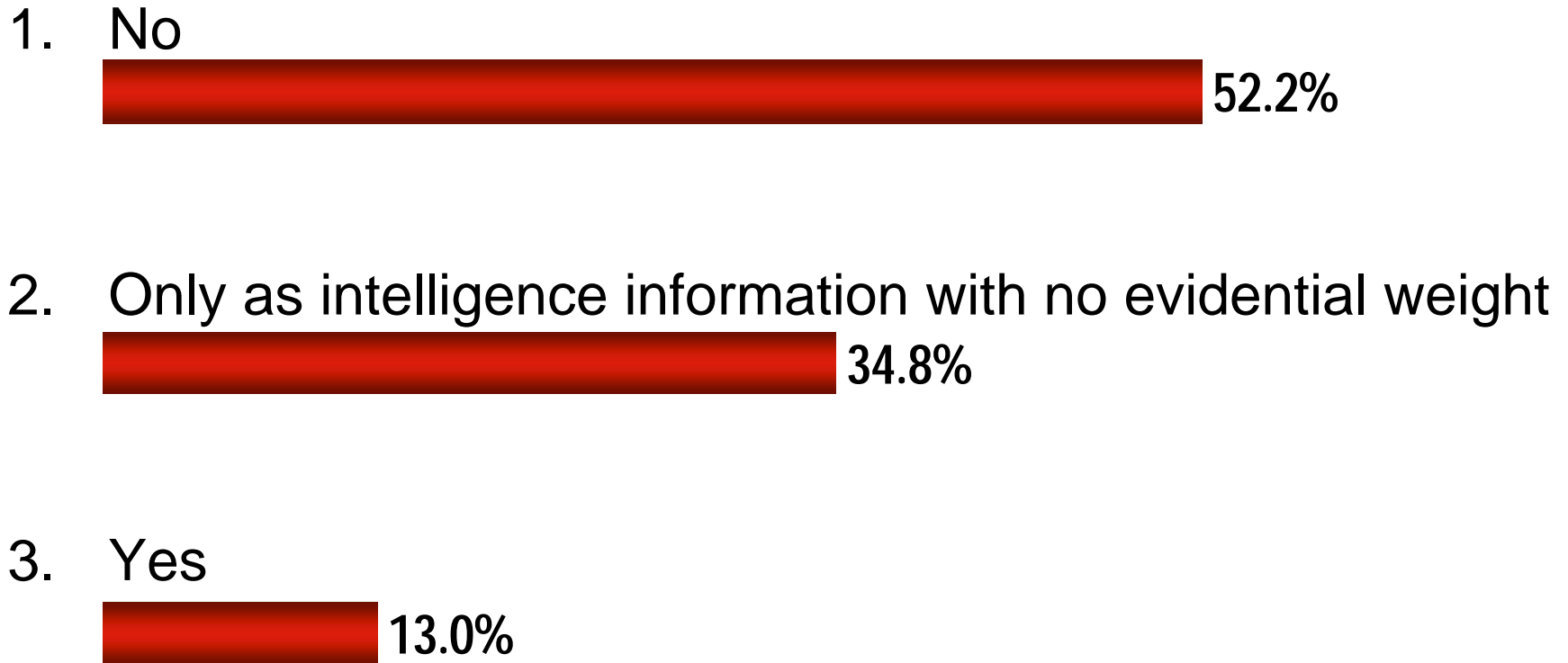


3. I belong to a club organisation that would surprise people
0.0%

4. More than one of the above




Are you happy that your centrally held biometrics data might be used to assist in clearing up general crimes?



Do you believe that the government really will restrict the use of personal communications data for intelligence purposes only?

1. Yes
0.0%

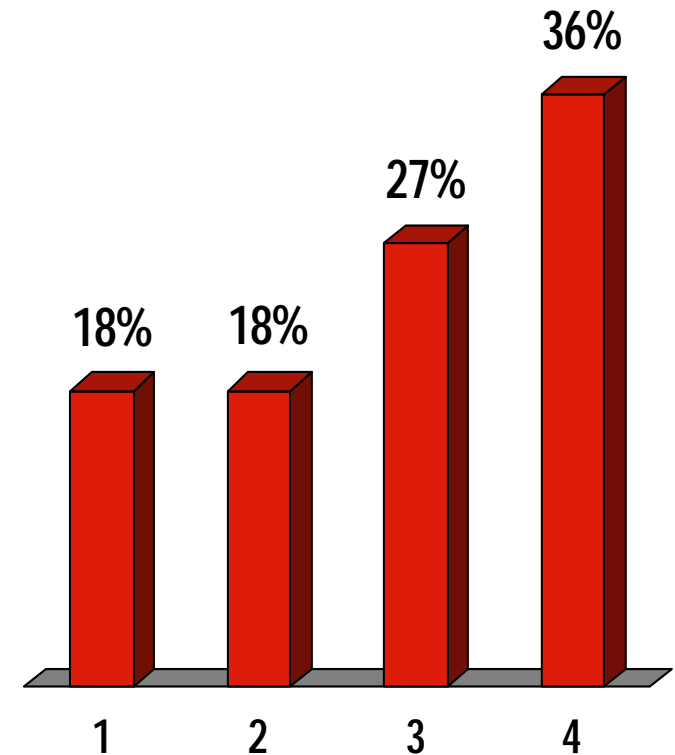
2. No
 95.8%

3. I'm not sure that these responses are truly anonymous and would rather not commit myself!
 4.2%

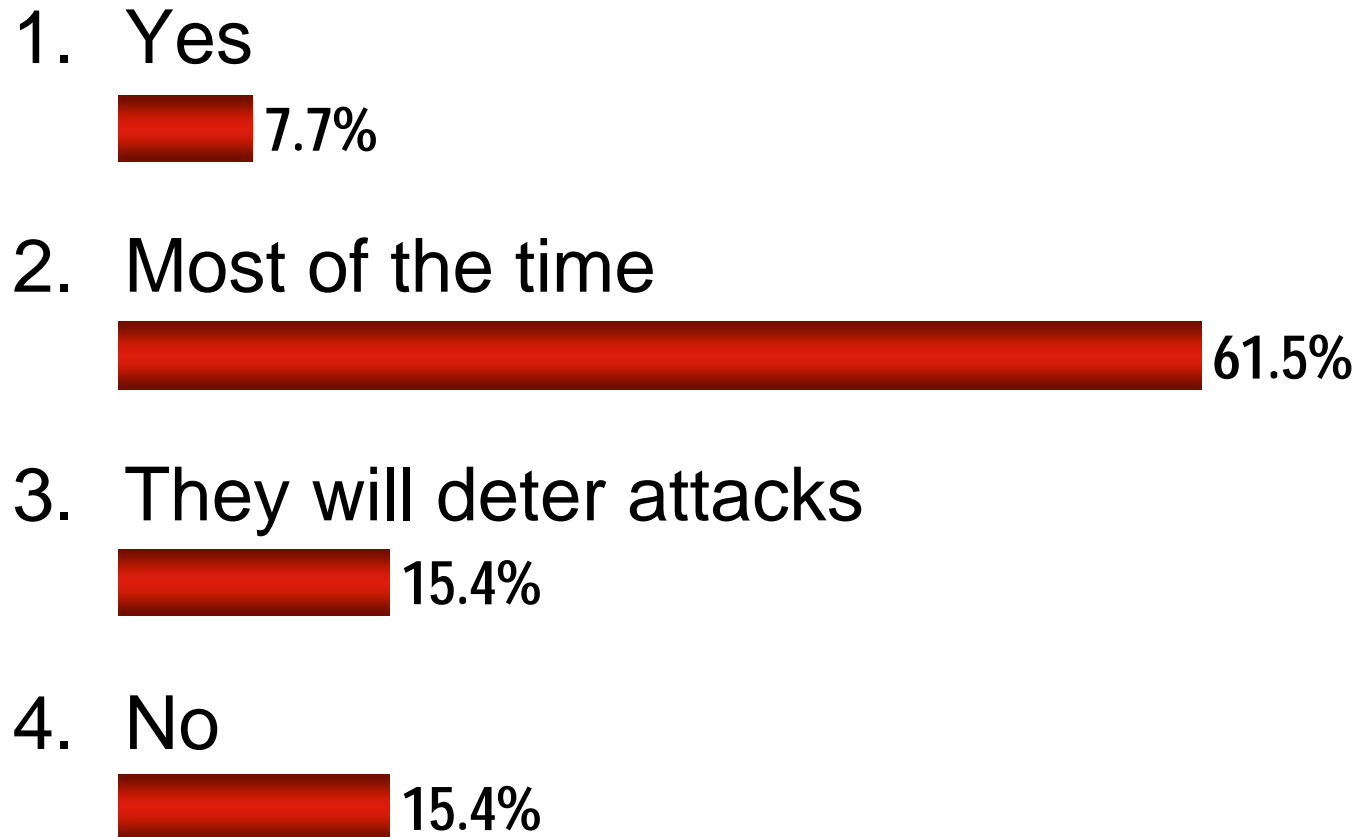


Are you happy with the current proposals for a National ID Card?

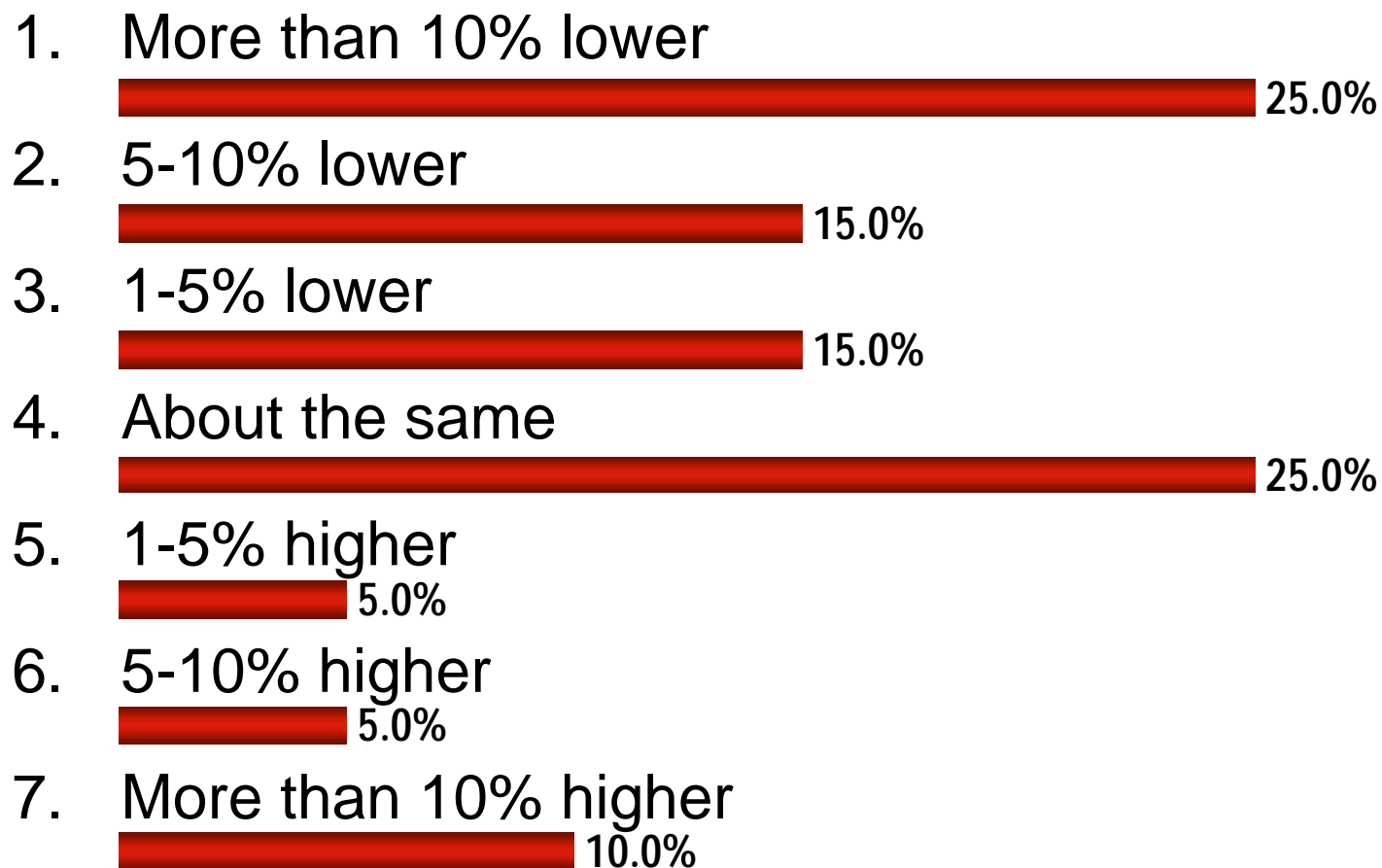
1. I am happy to carry one and think it should be universal
2. I would carry one for a purpose that enabled me to assert my identity or authority when transacting business with a government system
3. I am concerned about some aspects of the proposals
4. I am against any centrally managed national ID card system



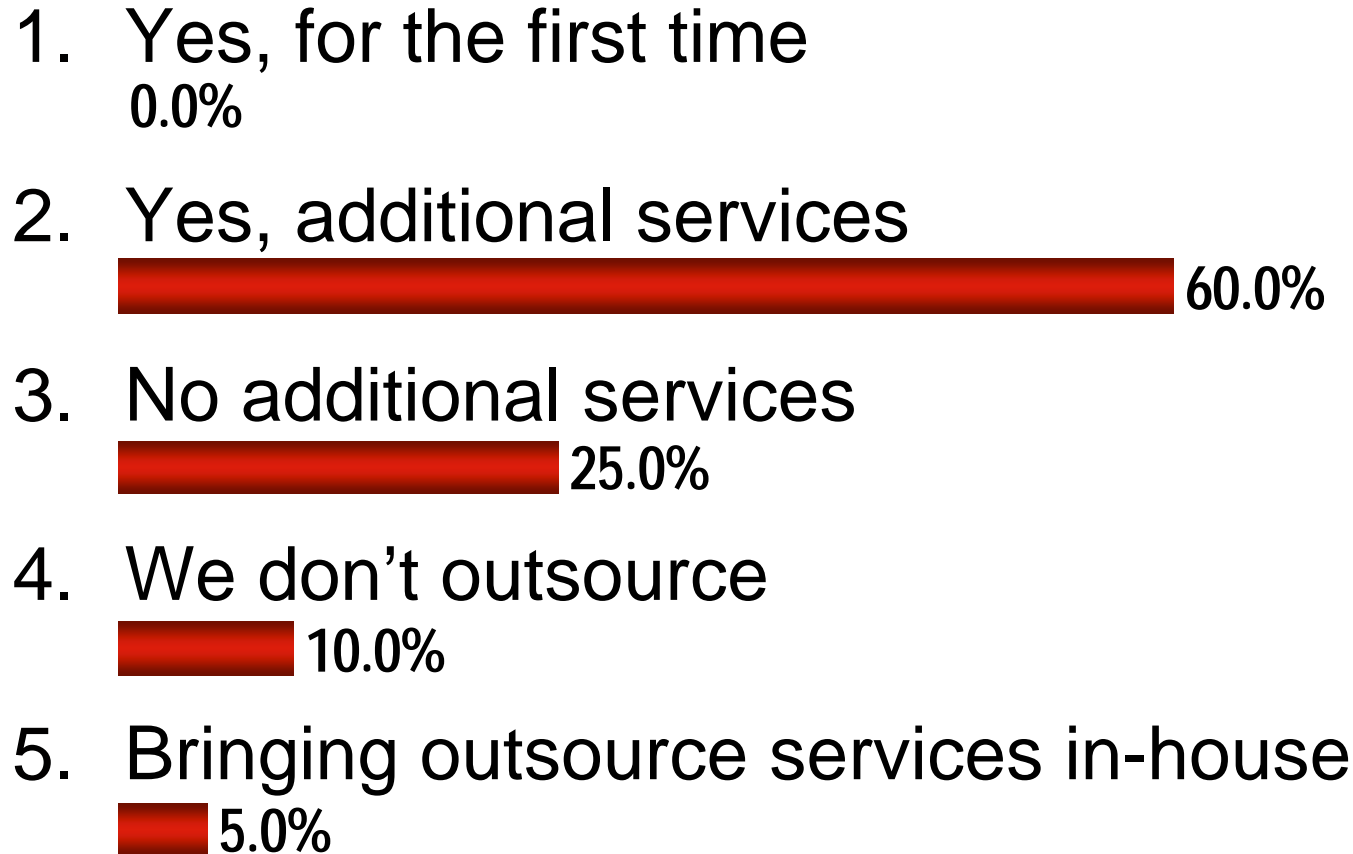
Do you think that the correct and comprehensive procedures can properly protect a system?



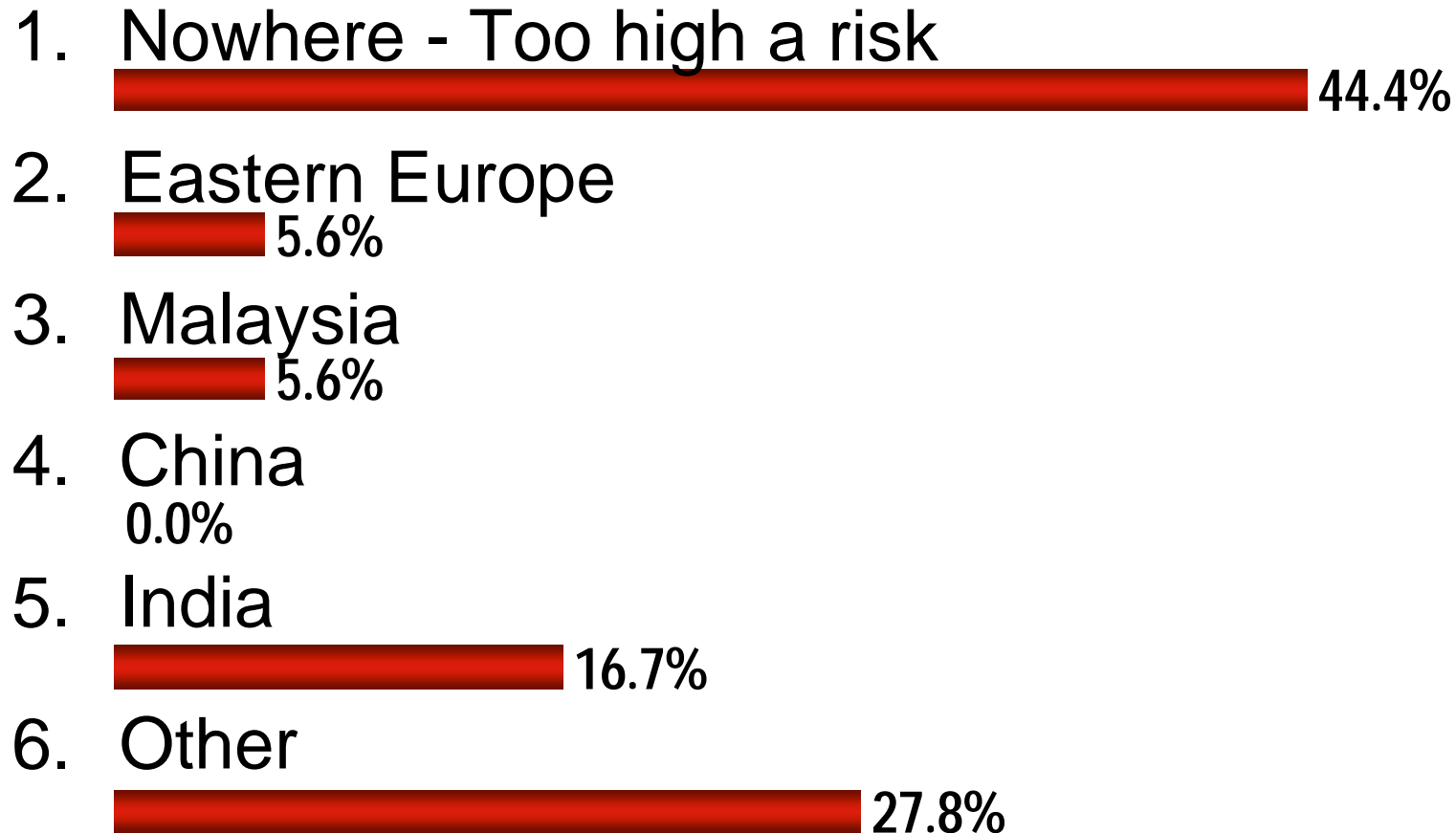
Is your security budget in 2009 relative to 2008 likely to be:



Are you considering outsourcing any security services?



What is the best location to offshore security services?



How do you measure cost performance?

1. Annual budgets



2. Costs per service



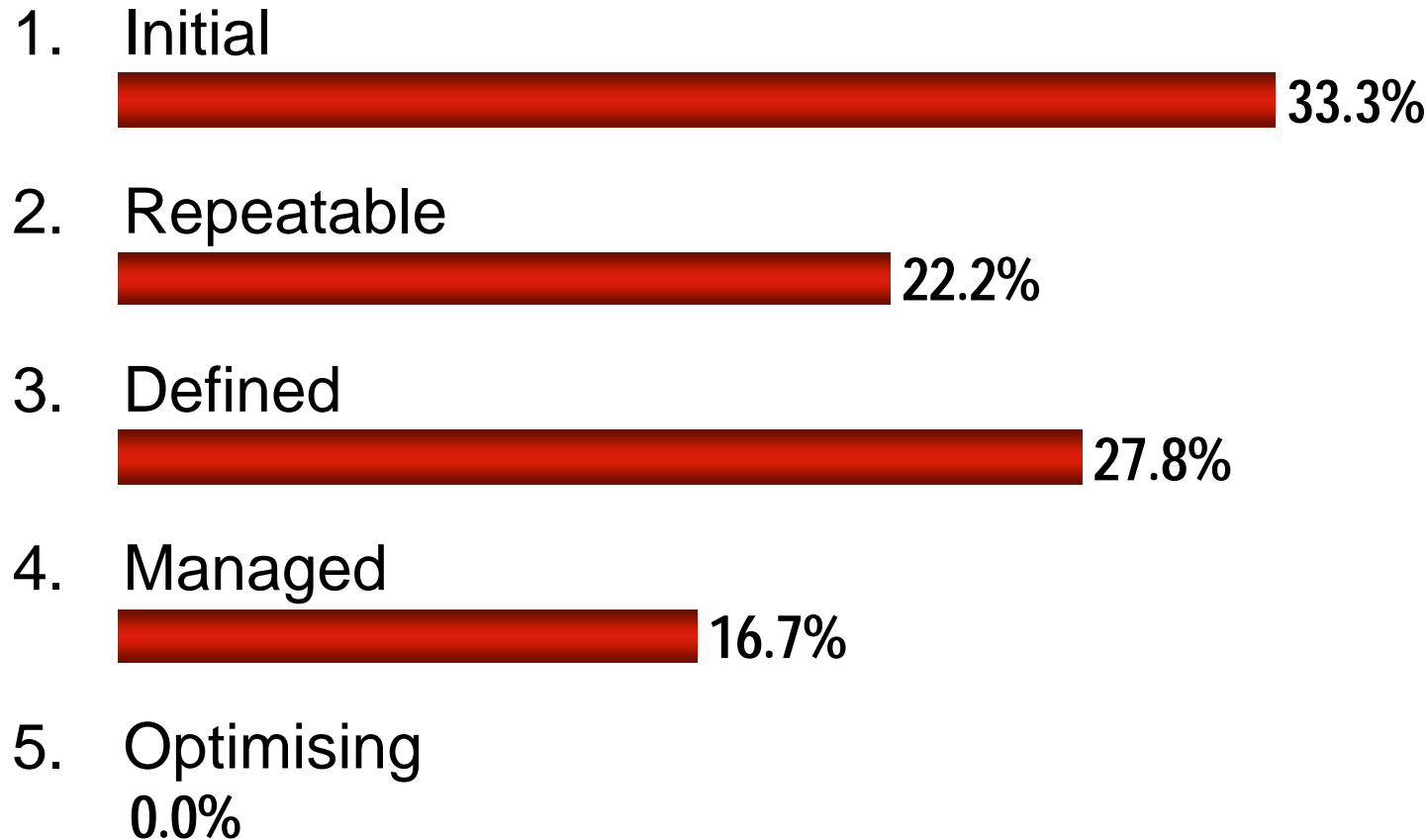
3. Risks managed for investment



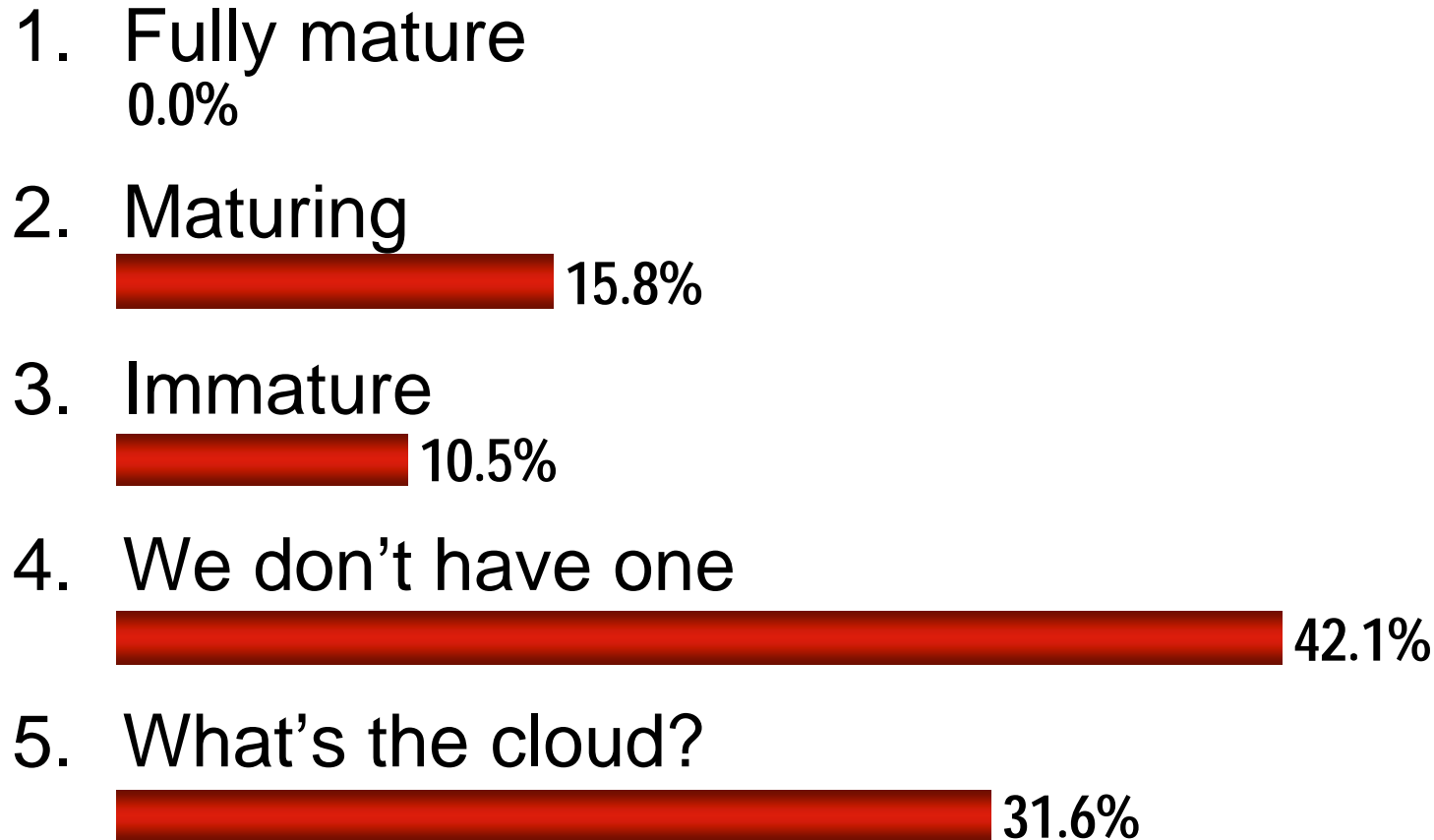
4. We don't measure



On a scale of 1 to 5 how mature do you feel your security metrics are?



How advanced is your organisation's cloud computing strategy?



Has your organisation assessed the risks associated with operating in the cloud?

1. Yes, we have fully evaluated them






2. We have done some initial assessment



3. No, not at all

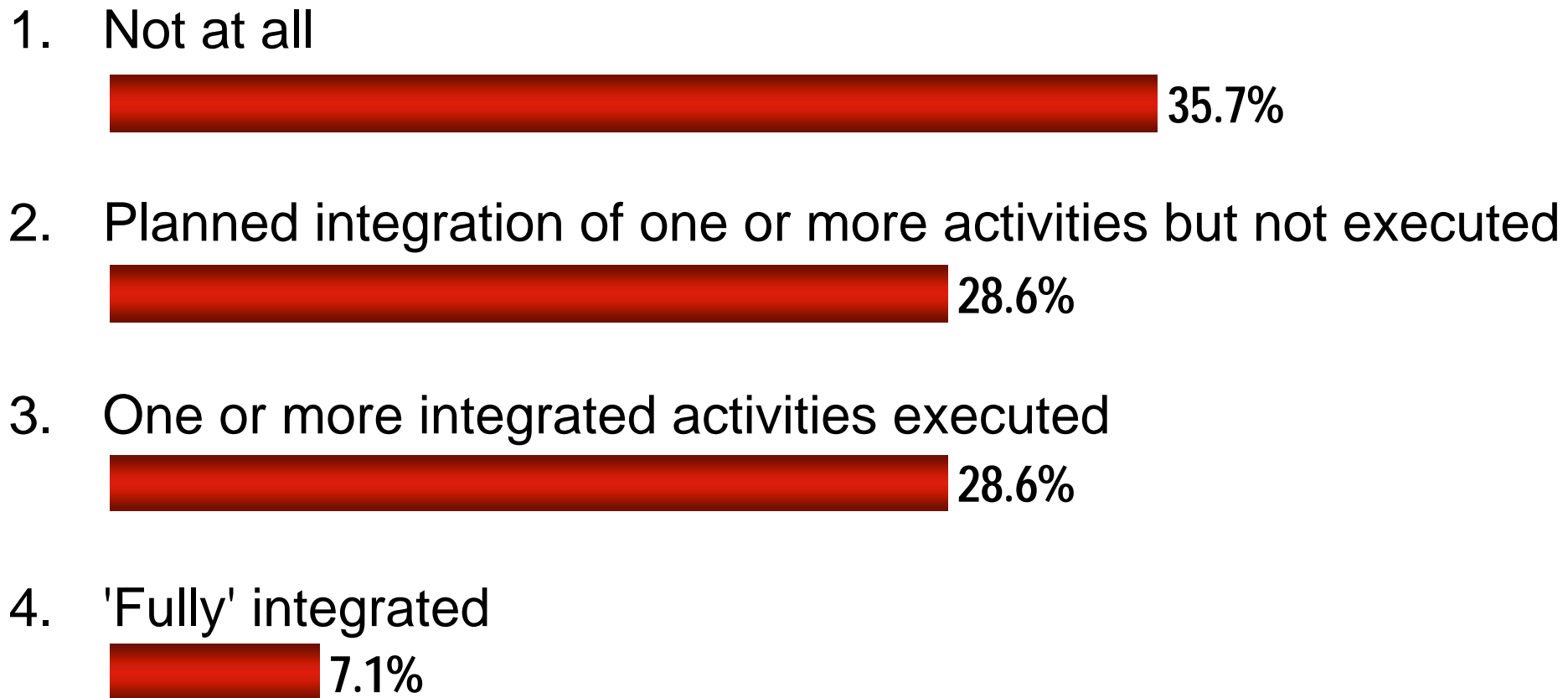


Has your organisation assessed the value of cloud computing?






1. Yes, we have fully assessed the benefits
 10.5%
2. We have done some initial assessment
 63.2%
3. Haven't thought about it yet
 26.3%



To what extent have you integrated physical and IT Security activities?






What are (or have been) the major barriers to integration?

1. Not seen as practical or useful
 12.5%
2. Organisational boundaries and politics
 50.0%
3. Different skills and capabilities
 18.8%
4. Physical Security is handled outside of my organisation
 6.3%
5. Other
 12.5%



Which of the following is most important for pursuing integration activities?

1. Cost saving via synergy
 12.5%
2. Better holistic risk management
 68.8%
3. Better customer experience
0.0%
4. Enhanced career development opportunities
0.0%
5. Better detection and response to blended attacks
 18.8%



Which security activity is most likely to be achievable and successful?

