




# CSO Interchange London

---

**June 2nd, 2009**

London

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

1. Pressures from the current economic climate  
 29.7%
2. Security threats from disgruntled employees  
 35.1%
3. Increased attacks from cybercrime  
 35.1%



# 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

110	3. Vulnerabilities (systems and/or apps)
108	1. Employees
104	6. Exploitation of intellectual property
90	5. Malware
86	7. Current economic climate
80	4. Web use (eg widgets and gadgets)
70	2. Virtual workers and/or partners



# 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

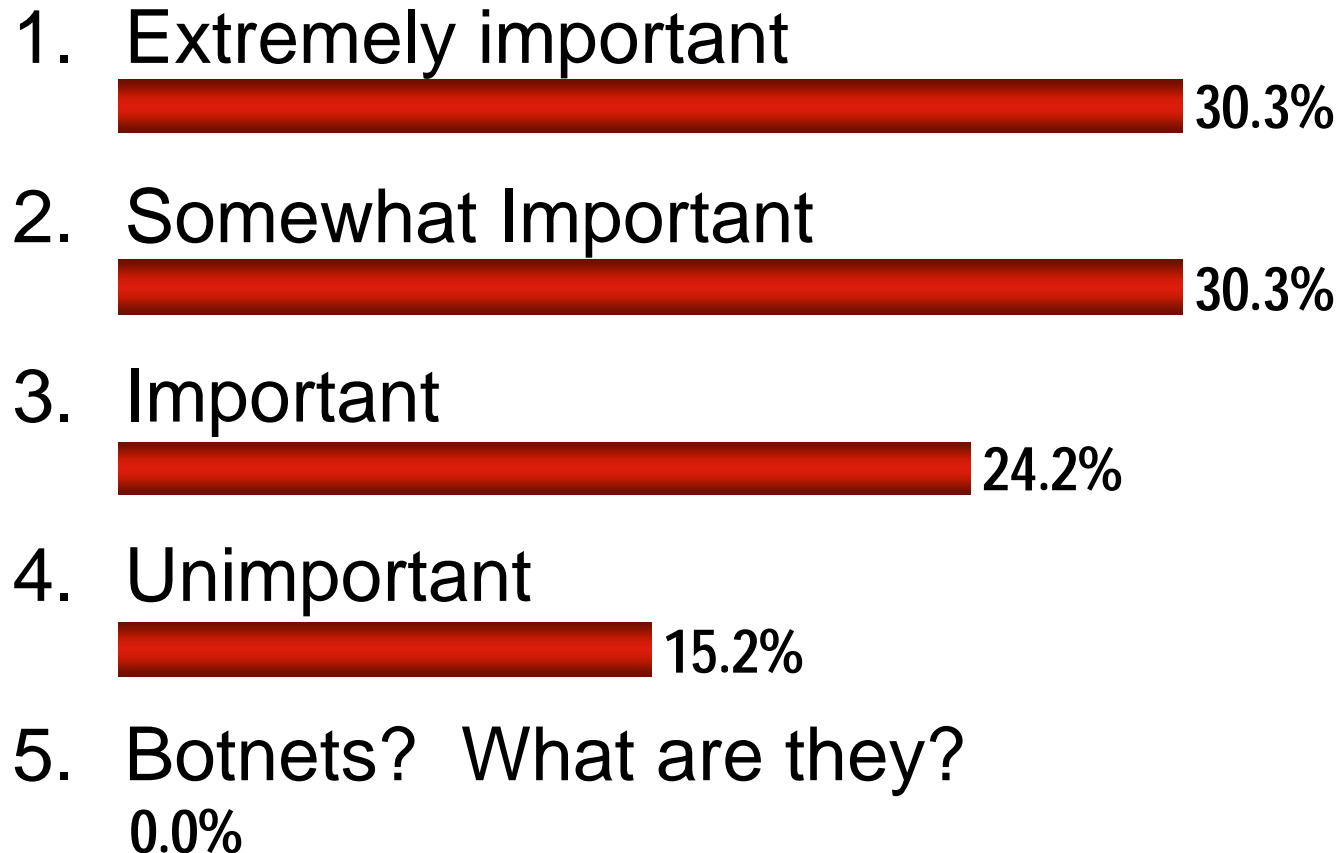
Points

Item

170	2. Time
162	1. Budget
152	9. Too much tactical versus strategic work
149	3. Personnel
98	4. Insufficient technology
95	5. Lengthy hardware/software implementations
94	6. Reporting requirements
53	7. Unhelpful media coverage on security
33	8. My own incompetence



# How relative do you think the Botnet threat is to your organisation?



# Were you aware that Botnets are such a substantial money maker?

1. Yes



2. No



3. I had some idea, but did not know that they were worth over a Billion Euros a year



# Were you aware that Anti-Virus and IPS/IDS systems were not 100% effective against the threat of Botnets?

1. Yes



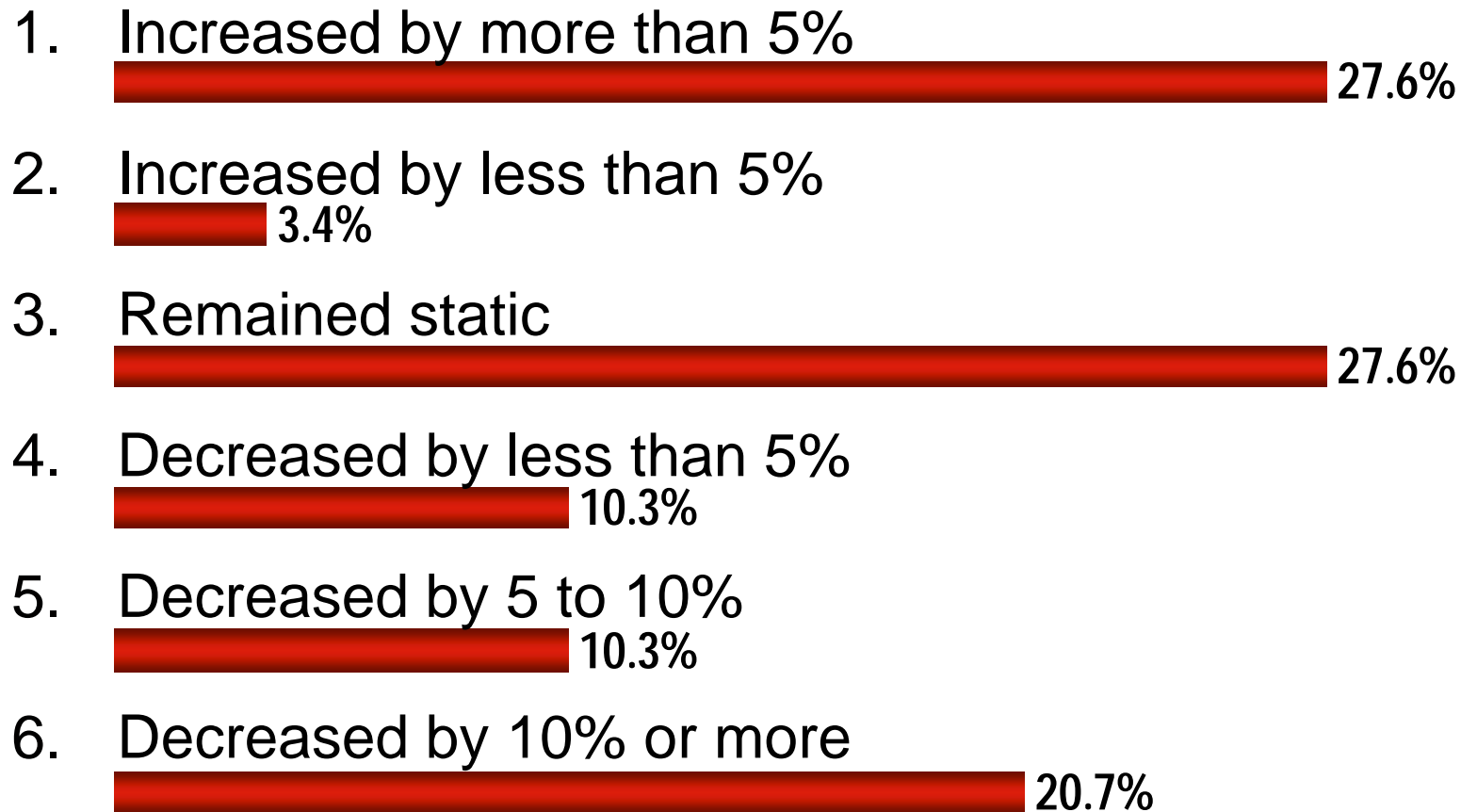
2. No



3. I had some idea



# For the current financial year, has security budget in your organisation:



# What are your priorities in terms of capital spend on security. Rank the following security disciplines highest to lowest.

1. Identity and Access Management
2. Data Leakage Prevention
3. Vulnerability Management
4. Firewall
5. Intrusion Detection.
6. Fraud Prevention.

**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

138	1. Identity and Access Management
128	2. Data Leakage Prevention
108	3. Vulnerability Management
78	4. Firewall
78	6. Fraud Prevention.
69	5. Intrusion Detection.






# What drives you to comply with regulatory requirements?

1. Need to improve risk profile and level of security  
 16.0%
2. Risk of penalties, reputational damage and/or loss of license to operate  
 64.0%
3. There is no strong drive. Regulations have no real influence  
 16.0%
4. We are not regulated  
 4.0%







## Regulatory requirements are:

1. Appropriate, fit for purpose and pragmatic to implement  
 3.4%
2. Overly complex, burdensome and costly to implement  
 31.0%
3. Ill defined and leave us at the mercy of expensive consultative interpretation  
 65.5%
4. No opinion  
0.0%



## More regulation will prove to be:

1. A positive contributor to effective risk management  
 6.9%
2. Distracting and a hindrance to furthering effective risk management  
 69.0%
3. A complete waste of time with little if no effect  
 13.8%
4. Of no relevance to my organisation  
 10.3%



# Do you have a policy on the use of social networks in your organisation?

1. Yes



2. No



# If your organisation does have a policy, is it:

1. To block and ban?



2. To allow with controls?



3. To allow it?



# To what extent are you using server virtualisation within your organisation?

1. Not at all



2. Testing and planning underway







3. Already using in Test / Development / QA



4. Already using in production







# Which of the following is the most important driver for pursuing server virtualisation?

1. Reduction of hardware implementation costs  
 50.0%
2. Increase server utilisation  
 25.0%
3. Data centre space / power / cooling efficiency  
 12.5%
4. Speed up server provisioning  
 12.5%
5. Deploy multiple OS on a single hardware platform  
0.0%



# How confident are you about active malware on your network, including botnets and trojans? (Ignore malware that gets blocked at the gateway or by anti-virus)

1. I know I don't have any significant problem  
 34.6%
2. I've not seen any evidence of a problem  
 46.2%
3. I'm just not sure, we can't easily detect such problems  
 15.4%
4. I think I might have a significant problem, but need more evidence  
 3.8%
5. I know I have a significant problem  
0.0%



# Which of these threats are you most concerned about? (rank in order of importance: highest to lowest)

1. Botnets or trojans inside my organisation's network
2. Botnets or trojans in my customers' PCs
3. Social networking threats
4. Consumerisation / use of personally devices
5. Attacks on DNS servers
6. Compromise of my organisations web servers
7. Pandemics
8. Cloud computing
9. Rogue security software

**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

142	1. Botnets or trojans inside my organisation's network
112	4. Consumerisation / use of personally devices
84	5. Attacks on DNS servers
82	3. Social networking threats
80	2. Botnets or trojans in my customers' PCs
80	6. Compromise of my organisations web servers
65	7. Pandemics
40	9. Rogue security software
35	8. Cloud computing

