
Robert Richardson
Director, Computer Security Institute
Code: CSI200
CSIannual.com
More material at: GoCSI.com
Respondents by Industry Segment

- Consulting: 15.15%
- Education: 7.07%
- Federal Government: 6.06%
- Financial Services: 5.05%
- Health Services: 4.04%
- Information Technology: 3.03%
- Law Enforcement: 2.02%
- Legal: 2.02%
- Local government: 2.02%
- Manufacturing: 1.01%
- Military: 1.01%
- Retail: 1.01%
- State government: 9.09%
- Telecommunications: 8.08%
- Transportation: 22.22%
- Utilities: 10.10%
- Other (please specify): 1.01%
Respondents by Size of Organization

- 50,000 or more: 12.00%
- 1-99: 23.00%
- 9,999-49,999: 15.00%
- 100-499: 15.00%
- 500-1499: 14.00%
- 1500-9999: 21.00%
- 1-99
- 100-499
- 500-1499
- 1500-9999
- 9,999-49,999
- 50,000 or more
Respondents by Organization Revenue

- Over $1 billion: 33%
- Under $10 million: 24%
- $10 to $99 million: 20%
- $100 to $1 billion: 22%

Legend:
- Under $10 million
- $10 to $99 million
- $100 to $1 billion
- Over $1 billion
Respondents by Title

- Other: 34%
- CEO: 7%
- CIO: 10%
- CSO: 3%
- CISO: 12%
- Security Officer: 25%
- System Administrator: 8%

521 respondents
Percentage of IT Budget for Security

- Unknown: 15%
- More than 10%: 12%
- 8-10%: 11%
- 6-7%: 8%
- 3-5%: 24%
- 1-2%: 18%
- Less than 1%: 11%

2008: 518 Respondents
Percentage of IT Budget for Security

Awareness Training as a Percentage of Security Budget

- Unknown: 13%
- More than 10%: 5%
- 8-10%: 5%
- 6-7%: 3%
- 3-5%: 12%
- 1-2%: 19%
- Less than 1%: 42%

This answer added in 2008 survey.

2008: 519 respondents
Security Technologies Used

- Endpoint / NAC
- App firewalls
- File encryption (storage)
- Encryption in transit
- Anti-spyware
- VPN
- Firewalls
- Anti-virus

2008: 530 Respondents
Awareness Training Metrics

2008: 460 Respondents
Formal Policy

Information Security Policy w/n Your Organization

- Formal Policy Established: 68%
- No Policy: 1%
- Other: 2%
- Informal Policy: 12%
- Formal Policy Being Developed: 18%

2008: 512 Respondents
Data Policy

Data Retention Policy within Your Organization

- Formal Policy Established: 54%
- Informal Policy: 17%
- Formal Policy Being Developed: 24%
- Other: 1%
- No Policy: 5%

2008: 510 Respondents
Software Development Process

2008: 489 Respondents

Formal Process Established - 29%
Other - 1%
Don't Know - 8%

Formal Process Being Developed - 19%
Informal Process - 22%
Formal Process - 29%
Percentage Experiencing Incidents

Experienced Security Incidents

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>43</td>
<td>10</td>
</tr>
<tr>
<td>45</td>
<td>44</td>
<td>13</td>
</tr>
</tbody>
</table>

2008: 517 respondents
Percentage of Key Incident Types

Percentages of Key Types of Incident

- Virus
- Insider Abuse
- Laptop
- Unauth acc
- Bots
- Financial Fraud
- DNS

2008: 433 Respondents
Actions Taken Following Incident

- Attempted to identify perpetrator: 60% in 2007, 54% in 2008
- Did your best to patch security holes: 54% in 2007, 46% in 2008
- Installed software patches: 37% in 2007, 33% in 2008
- Installed additional security software: 24% in 2007, 27% in 2008
- Changed organization's security policies: 23% in 2007, 18% in 2008
- Did not report outside the organization: 15% in 2007, 15% in 2008
- Reported to law enforcement agency: 13% in 2007, 13% in 2008
- Installed additional hardware: 13% in 2007, 13% in 2008
- Reported to legal counsel: 13% in 2007, 13% in 2008
- Other: 13% in 2007, 13% in 2008
Figure 21: Reasons for Not Reporting

Average response on a 1 to 7 scale, with 1 “of no importance” and 7 “of great importance”.

- Unaware of Law Enforcement Interest: 2.66
- Civil Remedy Pursued: 2.78
- Competitors Would Use to Advantage: 3.14
- Other: 3.21
- Negative Publicity: 3.71
- Believed Law Enforcement Couldn't Help: 4.07
- Incidents Too Small to Bother Reporting: 4.33

2008: 233 Respondents
Incidence of ID Fraud

Identity Fraud Continues to Decline
Year Over Year ID Fraud and Victimization Rates

- Millions of victims in the last 12 months
- 12-month incidence rate

© 2008 Javelin Strategy & Research
“This year’s report reinforces a three-year trend that criminals mostly obtain the majority of information from stolen personal belongings, and through telephone calls, rather than online.”
Figure 2. Active bot-infected computers per day

Source: Symantec Corporation
Figure 3. Active bot-infected computers by day
Source: Symantec Corporation
Percentage of Key Incident Types

Percentages of Key Types of Incident

- Virus
- Insider Abuse
- Laptop
- Unauth acc
- Bots
- Financial Fraud
- DNS

2008: 433 Respondents
Average Losses Per Respondent

Losses in Thousands of Dollars
2008: 144 Respondents
Success at the Perimeter Meets Its Boundary
Success at the Perimeter Meets Its Boundary
Percentage of Losses Due to Direct Costs

- None: 38.00%
- Up to 20%: 28.00%
- 21 to 40%: 4.00%
- 41 to 60%: 4.00%
- 61 to 80%: 9.00%
- 81 to 100%: 17.00%
TJX Three-Year Chart
Success at the Perimeter Meets Its Boundary
In the opening years of this century, our legacy includes two very high security products and the community knowledge to deploy them wisely. One could argue that we are in a much better situation now than in the early 1980’s. The general feeling, however, is that computer and network security is in decline.

-- David Bell
The sellers can't explain what they're selling to the buyers, and the buyers don't buy because they don't understand what the sellers are selling. There's a mismatch between the two; they're so far apart that they're barely speaking the same language.

Bruce Scheier, blogging about RSA 2008
What we’re really lacking is imagination. There is plenty of existing academic research to underpin dozens of new security product concepts that would deliver value to customers. I can think of several that are easy to build and that customers would buy. But we keep seeing variations of the same solution.

--David Lacey, ComputerWeekly.com, blogging about Bruce’s blogging
Troubling Statistics:

8% had Domain Name System incidents
27% experienced targeted attack
Potential Game Changers:

- Trusted Computing
- User-centric identity management
Potential Game Changers:

Data-centric security

Secure Code Development
Potential Game Changers:

Virtualization

Web 2.0
Thank you.
Additional Commentary: GoCSIblog.com

That code again:
CSI200 -- Registration & Info: CSIannual.com

Robert Richardson
Director, CSI
rrichardson@techweb.com
Twitter: twitter.com/cryptorobert