SECURITY PROS & ‘CONS’:
IT professionals on confidence, confidential data, and today’s cyber-cons

Based on an independent study of 1,000 international IT security managers and 1,000 employees

Over-confidence among security professionals

82% of IT security managers feel CONFIDENT that their IT security protects their company against modern malware

YET only 48% protect themselves against company-confidential data being uploaded to the web

Misperception of risk

40%+ believe they have DLP in place to protect their data in rest, use, and motion. In reality, only 2% are using a solution capable of this

50%+ believe they have real-time detection of malware. In reality, the majority are using AV not designed to protect against advanced attacks.

False sense of security leads to data leaks

- 37% report data had been lost by employees
- 24% say their CEO or other executives’ confidential data had been breached
- 20% state data affected by regulatory compliance was compromised
- 20% have seen confidential information posted on a social networking site
- 19% of companies have fallen victim of an advanced persistent threat (APT)

©2011 Websense, Inc. All Rights Reserved.
**Employees’ right to security**

- Both IT security managers and employees place IT security as the third most important employee ‘right’ following a proper lunch break and coffee breaks.

<table>
<thead>
<tr>
<th>Activity</th>
<th>IT security managers</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal web browsing</td>
<td>23%</td>
<td>23%</td>
</tr>
<tr>
<td>Protection against accidental data leaks</td>
<td>47%</td>
<td>53%</td>
</tr>
<tr>
<td>Protection against internet security threats</td>
<td>53%</td>
<td>62%</td>
</tr>
<tr>
<td>A proper lunch break</td>
<td>71%</td>
<td>91%</td>
</tr>
<tr>
<td>Coffee breaks</td>
<td>70%</td>
<td>71%</td>
</tr>
<tr>
<td>Cigarette breaks</td>
<td>37%</td>
<td>18%</td>
</tr>
<tr>
<td>Accessing social networking sites</td>
<td>22%</td>
<td>16%</td>
</tr>
</tbody>
</table>

**Data breaches put IT jobs on the line**

86% say their job would be at risk if a security incident were to occur, including:

- 36%  CEO or other executive’s confidential data was breached
- 34%  Losing data needed for compliance
- 34%  Confidential information posted on a social networking site
- 30%  A serious security breach happening more than once
- 28%  Losing customer-confidential information
- 28%  Failing to pass a third-party compliance security audit
Data talk at the top

91% of IT security managers report new levels of management have engaged in data security conversations in the last year.

Stress of security

72% say an incident such as a minor car accident, managing personal debt, or divorce is LESS stressful than being responsible for protecting their company’s confidential data.

Including 14% that say losing their job would be LESS stressful than staying in their current role!

43% Head of IT
38% Managing Director
33% CEO
29% Head of Legal
27% Head of Compliance

Download the full report ‘Security Pros and ‘Cons’: IT professionals on confidence, confidential data, and today’s cyber-cons’ to find out more about the State of Security today. www.websense.com/prosandcons