

Key Findings

This year's survey results are based on the responses of 443 information security and information technology professionals in United States corporations, government agencies, financial institutions, educational institutions, medical institutions and other organizations. Their responses cover the security incidents they experienced and security measures they practiced from the period of July 2008 to June 2009. This is the 14th annual edition of the CSI Computer Crime and Security Survey, making it the longest-running project of its kind in the security industry.

- Average losses due to security incidents are down this year (from \$289,000 per respondent to \$234,244 per respondent), though they are still above 2005 and 2006 figures.
- One-third of respondents' organizations were fraudulently represented as the sender of a phishing message.
- Respondents reported big jumps in incidence of financial fraud (19.5 percent, over 12 percent last year); malware infection (64.3 percent over 50 percent last year); denials of service (29.2 percent, over 21 percent last year), password sniffing (17.3 percent, over 9 percent last year); and Web site defacement (13.5 percent over 6 percent last year). Respondents reported significant dips in wireless exploits (7.6 percent, down from 14 percent in 2008), and instant messaging abuse (7.6 percent, down from 21 percent).
- Financial fraud continues to consistently be a highly expensive attack, averaging almost \$450,000 in losses, per organization that suffered fraud. However, this year, isolated incidents pushed financial fraud down to number three on the most-expensive incident list, behind wireless exploits (\$770,000) and theft of personally identifiable or personal health information through all causes other than mobile device theft (\$710,000).
- When asked what actions were taken following a security incident, 22 percent of respondents stated that they notified individuals whose personal information was breached and 17 percent stated that they provided new security services to users or customers (i.e. credit monitoring, issuing new credentials).
- Twenty-five percent of respondents felt that over 60 percent of their financial losses were due to non-malicious actions by insiders.
- Most respondents felt their investment in end-user security awareness training was inadequate, but (somewhat surprisingly) most felt their investments in other components of their security program were adequate.
- Respondents reported a notable reduction in the amount of security functions outsourced. This year 71 percent of respondents stated that they do not outsource any security functions at all; last year only 59 percent of respondents made this statement.
- Respondents are satisfied, but not overjoyed with security technology. Use of almost all security technologies increased; the largest increases were in anti-spyware software and encryption of data at rest (in storage).
- When asked what security solutions ranked highest on their wishlists, many respondents named tools that would improve their visibility—better log management, security information and event management, security data visualization, security dashboards and the like.
- Respondents reported a big increase in the use of Return on Investment (ROI) as a security metric—67.8 percent this year, over 44 percent last year. On the other hand they reported sharp declines in the use of Net Present Value (NPV) and Internal Rate of Return (IRR).
- Despite the fact that only 7.7 percent of respondents categorized their organizations as being in the "health services" industry, 57.1 percent of respondents said their organization had to comply with the Health Insurance Portability and Accountability Act (HIPAA). More respondents said that HIPAA applied to their organization than any other law or industry regulation.
- Respondents generally said that regulatory compliance efforts have had a positive effect on their organization's security programs.

About the Respondents

This is an informal survey. As one might expect, this report looks specifically at what the 443 respondents to this year's questionnaire had to say. Two inherent caveats must be borne in mind when interpreting the data.

First and foremost, there is a definitive skew towards individuals and organizations that have actively demonstrated an interest in security. This isn't a random sample of all the people in the country who are ostensibly responsible for the security of their networks. The survey questionnaire was sent—thrice via e-mail, thrice through the post—to 6,100 U.S.-based members of the CSI community. By "CSI community" we mean members of the Computer Security Institute and people who have attended CSI live events and Webcasts. CSI caters to security professionals on the front lines, so it goes without saying that the respondents to this survey come from a community that is actively working to improve security. This pool, in short, doesn't stand in for the organizations in the United States that are simply not paying attention to security (and there are, unfortunately, all too many such organizations).

Second, this is a self-response study. Respondents fill out the questionnaire voluntarily, all on their own, without any help from us. All responses are submitted anonymously in order to encourage candor. This anonymity introduces a limitation in comparing data year over year, because of the possibility that entirely different people are responding to the questions each time they are posed.