14th Annual

CSI Computer Crime and Security Survey

Executive Summary

CSI

This report is the Executive Summary of the CSI Computer Crime and Security Survey. For the first time, CSI has also published a longer Comprehensive Edition of the survey, exclusively for members of the Computer Security Institute. This new comprehensive publication compares CSI's findings to those of the Verizon Business RISK Team's Data Breach Investigations Report, the Ponemon Institute's Cost of a Data Breach report and the Symantec Global Internet Threat Report. It also includes details about respondents' security programs, including policies implemented, tools used, degree of outsourcing, use of metrics and effects of compliance requirements. The expanded report will also include more examination of the attacks respondents experienced, including incident response and deeper speculation about sources of losses.

Information security's history is a series of flawed (sometimes deeply flawed) *successes.* As much as the community bemoans the attacker's inherent tactical advantage, there's no denying that ubiquitous firewalls and a blanket of anti-virus software have made a number of once-devastating attacks largely irrelevant. These are successes and I would argue that they kept the scope of network-vectored crime more or less in stasis as the Internet's size grew exponentially. Crime soared into the first years of this century, but so did Internet use worldwide.

In the meanwhile, cybercrime has gotten less widespread but, at the same time, considerably more devious and malicious. There are seemingly endless variants of the latest polymorphic viruses, but they seem to come from a limited number of sources—and these sources are greatly skilled, well-organized, highly motivated and indisputably criminal.

In this context of a more malicious adversary, the flaws of our previous successes are thrown into sharp relief. No virus scanning tool of the traditional ilk can even pretend to stop the determined, targeted attack of one of today's criminals. The firewall has shifted jobs from rampart to foundation. It's long since cliché to declare that the perimeter is dead, or that it isn't just yet, or that it's migrated to the endpoint. The underlying point is that there are neither stable endpoints nor defensable perimeter boundaries.

My own view is that these flaws are inherent in the solutions themselves. These are solutions that have their uses but that cannot be relied on past a certain point. There's a vaccine for measles but steep hills yet to climb in fighting autoimmune diseases.

As I read through this year's CSI Survey report, I see both clear indications that the work that security professionals do has yielded improved security for organizations and troublesome hints that the will to make the next march may be lacking. Respondents report losses that are within the lower ranges we've seen over the past few years. They report moderate satisfaction with their toolset. Their open-ended responses express a desire more for visibility rather than for ammunition. There's nothing exactly wrong with this, but it's not the kind of environment that makes the fundamental changes to identity management, access control, and software development that could, with luck, lead to a less flawed sort of success.

Robert Richardson,
Director, CSI

by Sara Peters, Senior Editor, Computer Security Institute

2009 CSI Computer Crime and Security Survey
Executive Summary

One sign of maturity, perhaps, is knowing what one does not know. If the 443 responses to this survey, now in its 14th year, are any indication, the security industry is reaching that level of maturity. Generally speaking, respondents did not seem to feel that their challenges were attributable to a lack of investment in their security programs or dissatisfaction with security tools, but rather that, despite all their efforts, they still could not be certain about what was really going on in their environments, nor whether all their efforts were truly effective.

For the first time, we asked respondents not only what security technologies they use, but how satisfied they are with those technologies. On a scale of 1 to 5, *all* technologies received between a 3.0 and a 3.6—meaning that, on average, respondents were satisfied (though not overjoyed) with every single security technology they've deployed. Nonetheless, it's worth noting that the technologies that scored lowest in this range were *not* those that *provide* security per se, but rather those that provide some indication of *how secure an organization is* at any given moment—log management tools claimed the dishonorable position of last place, followed closely by DLP, content monitoring and intrusion detection systems. (Some identity management solutions also made the bottom of the list, but that's a discussion for later.)

Although most of the survey questions produce numbers and figures detailing the types and severity of respondents' security incidents and the particular components of their security programs, some of the most enlightening discoveries were found in the open-ended questions about respondents' hopes and fears. Here again the answers indicated respondents' yearning for greater understanding. When asked what solutions—either existing or imagined—ranked highest on their wishlists, they named better log management, security information and event management, security data visualization, security dashboards and the like—and they wanted these tools to be thoroughly interoperable so that they could show what was happening on an organization's entire environment, not just a few devices. When asked to identify the most critical computer security issues their organization or the security industry at large will face in 2010, they mentioned (among other things) that cloud computing and increased outsourcing will wrest from security professionals some key knowledge about their organization's security practices and incidents. They further mentioned that increasing regulatory compliance requirements will make it even more essential to know what all their data and computing assets are, where they are, who has access to them, when they are accessed and how they are secured.

Nonetheless there's much to be learned from what respondents *do* know (and what their best guesses are for everything else). This survey report will describe what attacks they're experiencing, what countermeasures they're taking, what other factors are influencing their security programs, and how things have changed since last year.

If you don't know where you are going, any road will take you there. —Lewis Carroll
You don't know what it is, but it's there, like a splinter in your mind, driving you mad. —Morpheus, The Matrix
If you don't know where you are going, you might end up somewhere else. —Yogi Berra

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) they 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 secu-rity technologies increased; the largest increases were in anti-spyware software and encryp-tion 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 respond-ents 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.
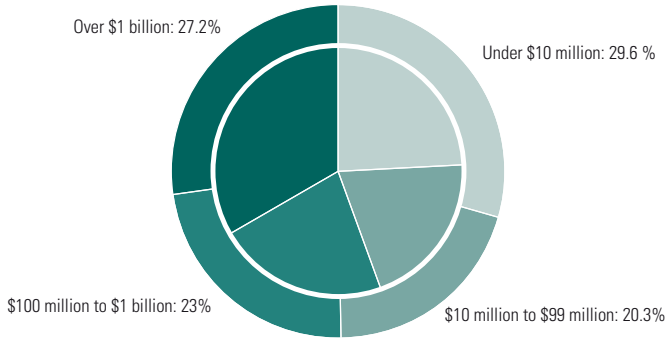
About the Respondents

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 responsibile for the security of their networks. The survey question-naire 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 com-munity 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.

Respondents by Annual Revenue
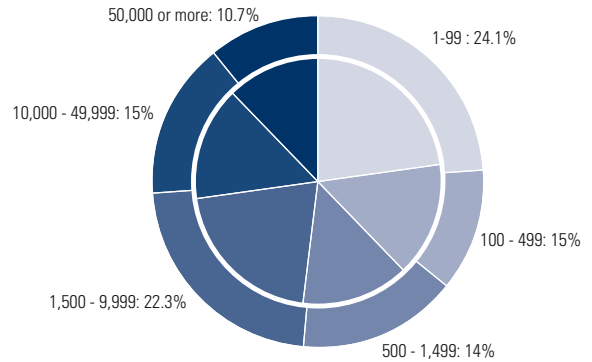2009 figures on outside, 2008 figures on inside

Over $1 billion: 27.2%

Under $10 million: 29.6 %

$100 million to $1 billion: 23%

$10 million to $99 million: 20.3%

2009 CSI Computer Crime and Security Survey · 2009: 335 Respondents

Respondents by Number of Employees
2009 figures on outside, 2008 figures on inside

50,000 or more: 10.7%

1-99 : 24.1%

10,000 - 49,999: 15%

100 - 499: 15%

1,500 - 9,999: 22.3%

500 - 1,499: 14%

2009 CSI Computer Crime and Security Survey · 2009: 439 Respondents

Respondents by Job Title

CEO: 8.8%
CIO: 6.6%
CSO: 3.2%
CISO: 12.9%
Other: 38.9%
Security Officer: 22.9%
System Administrator: 6.6%
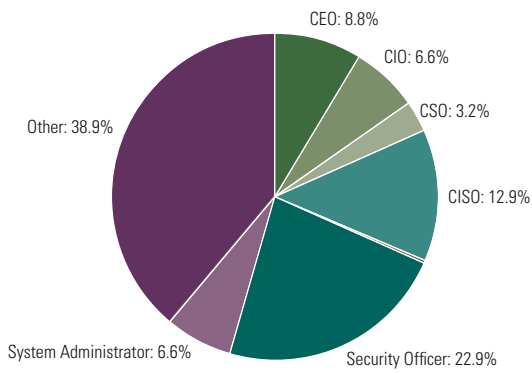
2009 CSI Computer Crime and Security Survey · 2009: 442 Respondents

The 2009 survey respondents are largely the same as the 2008 respondents. The most significant change is that the portion of respondents from the financial services sector dropped from 22 percent to 15 percent. This gap was almost entirely filled by a sizeable increase in the number of respondents from educational institutions (from 7 percent to 13.2 percent).

Respondents by Industry Sector
2009 figures on outside, 2008 figures on inside

Other: 11.4%
Utilities: 1%
Transportation: 0.5%
Telecommunications: 1.6%
State Government: 1.8%
Retail: 1.6%
Military: 1%
Manufacturing: 5.9%
Local Government: 1.8%
Legal: 1.6%
Law Enforcement: 1%
Information Technology: 12.3%
Health Services: 7.7%
Consulting: 15.7%
Financial Services: 15%
Education: 13.2%
Federal Government: 7.7%
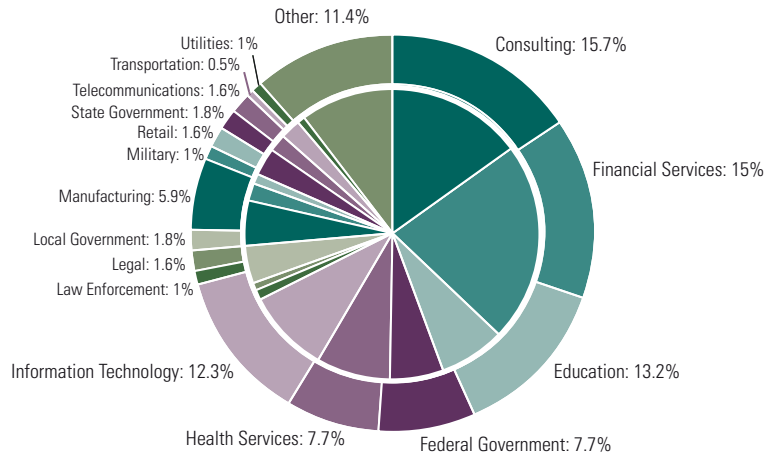
2009 CSI Computer Crime and Security Survey · 2009: 440 Respondents

One must also question whether those who choose to reply to the survey are markedly different in some way from those who do not. (For example, are they more likely to respond to the survey if they have more data or more accurate data at hand; and if so, is that indicative of a better overall security program? Are they more likely to respond if they have or have not experienced a significant security incident?)

Even if you imagine that those not answering the survey are altogether different in some way from those who do, it's interesting to note that the demographics of the respondents have remained very stable over the years, as has the basic make-up of the CSI community as a whole.

As the figures on page 4 show, organizations covered by the survey include many areas from both the private and public sectors. There's a fair degree of consistency in the number of respondents by industry sector. For several years, financial services made up the largest chunk of respondents, but this year finance (15 percent of respondents) was inched out by consulting (15.7 percent). This shuffle is due to the fact that the number of respondents from financial institutions dropped significantly, from 22 percent in last year's survey, to 15 percent this year. The gap was mostly filled by a significant increase (in fact, a near doubling) in the number of respondents from education (from 7 percent last year to 13.2 percent this year).

The portion coming from the IT industry also showed a notable increase—from 9 percent to 12.3 percent. Health services and federal government tied for fifth place, each claiming 7.7 percent of respondents. Government as a whole—combining federal, state and local agencies, as well as military and law enforcement—grabbed roughly 13 percent collectively.

For the Comprehensive Edition of this year's CSI survey* we compared our findings to those of some of the other major security studies released this year, including for example, the Ponemon Institute's Cost of a Data Breach study and Verizon Business' Data Breach Investigations Report. Thus, it is important to note here that only a sliver of our survey pool—a mere 1.6 percent, to be exact—comes from retail. This is in stark contrast to Verizon's data breach case load, 31 percent of which came from retail organizations, and to Ponemon's survey pool, 16 percent of which consisted of retail organizations.

The CSI survey pool continues to lean toward respondents from large organizations. Once again in 2009, organizations with 1,500 or more employees accounted for a little less than half of the respondents. Further, half of the respondents from commercial enterprises reported an annual revenue of $100 million or more. This number is notably slimmer than it was last year, but this is likely indicative of the economic recession's general effect on American businesses' revenues overall, as opposed to a significant difference in the survey pool from last year to this. The main takeaway here is that the survey pool breakdown clearly favors large organizations, when compared to the U.S. economy as a whole, in which there is a preponderance of small businesses.

* The Comprehensive Edition of the survey is given to members of the Computer Security Institute. Membership can be purchased at GoCSI.com/membership.

The survey also categorizes respondents by job title. As the graph shows, 31.5 percent of the respondents are senior executives—chief executive officer (8.8 percent), chief information officer (6.6 percent), chief security officer (3.2 percent) and chief information security officer (12.9 percent). These amounts are consistent with those from recent years. One lone respondent identified themselves as chief privacy officer, which is also consistent over time.

System administrators made up 6.6 percent of respondents, and 22.9 percent of respondents identified themselves as security officers. This left a sizeable 38.9 percent of respondents (over 34 percent last year) labeling themselves as "other." When examining the titles these "others" wrote in for themselves, it seemed that a significant portion of them could be logically reclassified into the "security officer" category. However the "other" category also contained a variety of job roles that fell outside of information technology entirely, which may be evidence that the security function continues to expand into more business segments.

"Others" aside, it is clear that at least 39 percent of respondents (CSOs, CISOs, and security officers combined) have full-time security responsibilities. Additionally, as noted earlier, the survey pool is drawn from the CSI community, and thus are assumed to be more "security savvy" than would be a survey pool of randomly selected information technology professionals.
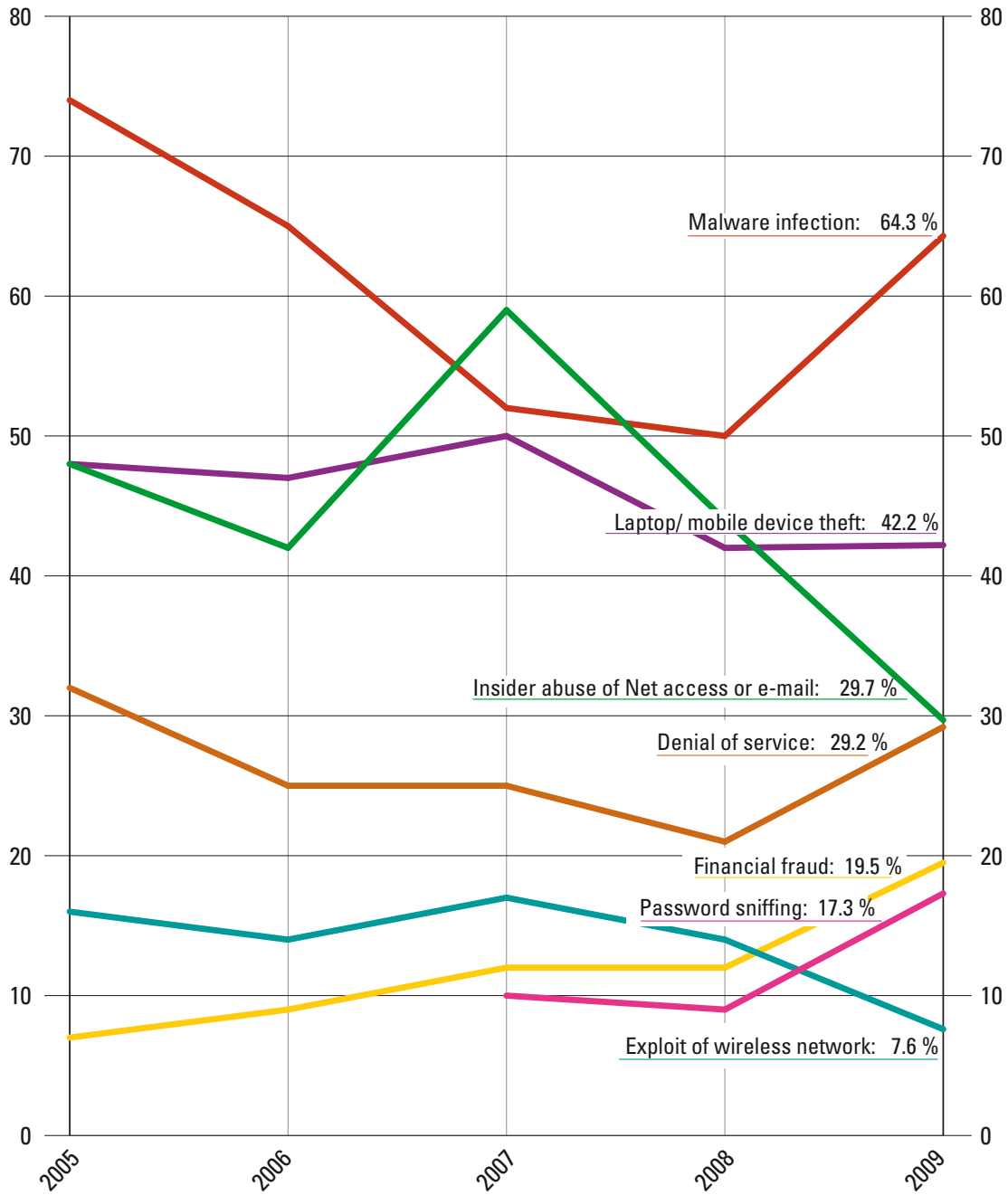
Attacks and Losses

For 14 years we've been asking respondents what types of attacks they've experienced. Each year before distributing the survey questionnaire we reevaluate the list of attack types, to make sure it adequately reflects the current attack landscape and to clarify the meaning of any attack types that might be misunderstood by respondents. Some categories are dropped, others are added, others are changed.

This year we added two entirely new incident types to the list: exploit of client Web browser and exploit of user's social network profile. Also, while we've kept "Web site defacement," which has been an option on the survey since 2004, we've swapped out "misuse of public Web application" (also added in 2004) for "other exploit of public-facing Web site or Web application."

Last year we decided to separate "laptop or mobile hardware theft" from the associated data breaches, so that we could get a better picture of how many laptops, USB drives and the like are actually holding sensitive data, distinguish between the monetary losses attributable to the loss of the device itself and the losses attributable to the breach of the data, and determine whether or not the near-paranoic fear of lost laptops was well-placed or whether in fact more data breaches were happening via other vectors. So, in addition to "laptop or mobile hardware theft" we added four new categories last year: theft or loss of customer data from mobile devices, theft or loss of proprietary information (intellectual property) from mobile devices, theft or loss of customer data from all other sources, and theft or loss of proprietary information from all other sources. We've

Types of Attacks Experienced
By Percent of Respondents

Malware infection: 64.3 %

Laptop/ mobile device theft: 42.2 %

Insider abuse of Net access or e-mail: 29.7 %

Denial of service: 29.2 %

Financial fraud: 19.5 %

Password sniffing: 17.3 %

Exploit of wireless network: 7.6 %

Types of Attacks Experienced
By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization	added in 2007		21%	20%	23%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%
Password sniffing	added in 2007		10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%
Web site defacement	5%	6%	10%	6%	14%
Other exploit of public-facing Web site	option altered in 2009				6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server	added in 2007		6%	8%	7%
Exploit of client Web browser	option added in 2009				11%
Exploit of user's social network profile	option added in 2009				7%
Instant messaging abuse	added in 2007		25%	21%	8%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%
System penetration by outsider	option altered in 2009				14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%

kept all those new categories, but this year we made a clarification: instead of "customer data" we specified "personally identifiable information (PII) or personal health information (PHI)." This change was made because what we were truly interested in were the breaches of data that would be covered by privacy regulation.

Also, we made clarifications to the categories "system penetration" and "unauthorized access." System penetration has been changed to "system penetration by outsider," and unauthorized access has been changed to "unauthorized access or privilege escalation by insider." Although these were intended as clarifications, we feel that the potential changes in respondents' interpretations are significant enough that any comparison to previous years' figures would be too flawed, and thus we've taken those pre-2009 figures out of the "Types of Incidents Experienced" chart on page 8.

As the graph on page 7 and the chart on page 8 show, several of these incident types showed notable changes from the 2008 survey to the 2009 survey (which covers the period of July 2008 to June 2009).

Malware infection leapt from 50 percent of respondents to 64.3 percent of respondents, making it easily the most prevalent incident; and specifically "bots in the organization" increased modestly from 20 percent of respondents to 23 percent. These increases may not be very surprising, considering that the study period coincided with the proliferation of Conficker, Koobface, and Storm variants, and these were arguably the most sophisticated pieces of malware ever to reach the wild. Considering the rapidly increasing sophistication of malware—and the not-so-rapidly-increasing sophistication of anti-malware solutions—it would not be altogether surprising if malware infection makes another big jump next year.

The second-most prevalent incident is laptop and mobile hardware loss or theft, holding steady at 42 percent of respondents. The number of respondents that experienced data breaches that occurred as a result of these hardware losses and thefts held level at 12 percent. Specifically: breach of PII or PHI dropped from 8 percent to 6 percent, and breach of proprietary information or intellectual property rose from 4 percent to 6 percent.

Although mobile devices gone astray did lead to data breaches for 12 percent of respondents, 18 percent of respondents suffered data breaches for entirely different reasons—10 percent reported theft of or unauthorized access to PII or PHI due to other causes, and 8 percent reported theft of or unauthorized access to proprietary information or intellectual property due to other causes.

The third-most prevalent incident—reported by over one-third of respondents—was phishing fraud, in which a victim organization is fraudulently represented as the sender of phishing messages. Fourth place was earned by insider abuse of Internet access or e-mail—by which we principally mean pornography, pirated software and the like—which was reported by 30 percent of respondents.

Average Losses Per Respondent

$345,000

$300,000

$289,000

$234,000

$204,000

$168,000
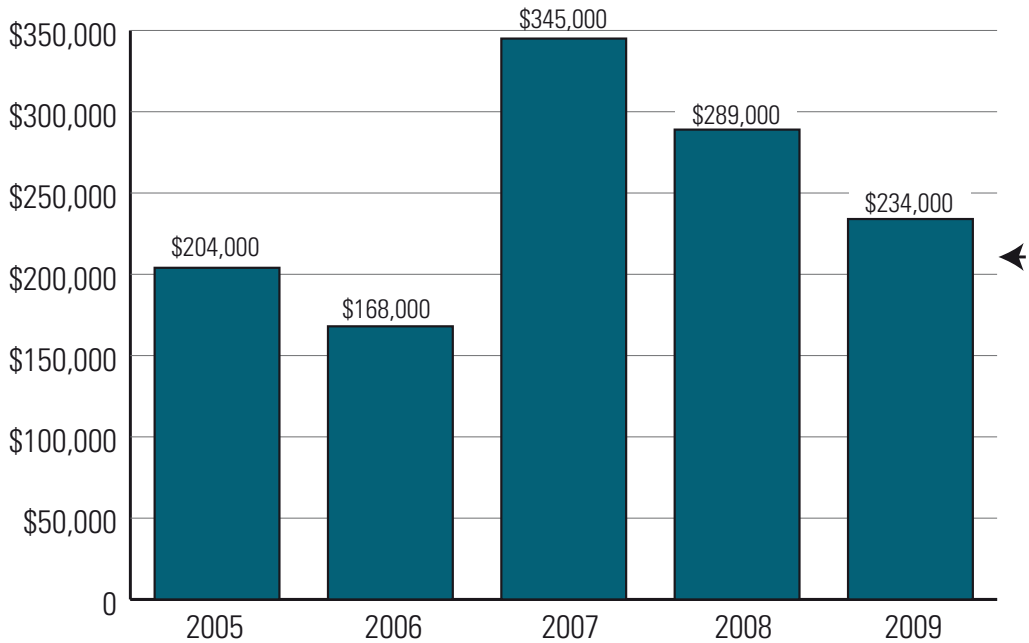
In 2005, respondents' reported losses dropped beneath the $500,000 mark. Losses haven't come anywhere near that amount, since then.

← highest average losses ever reported: 2001: $3,149,000
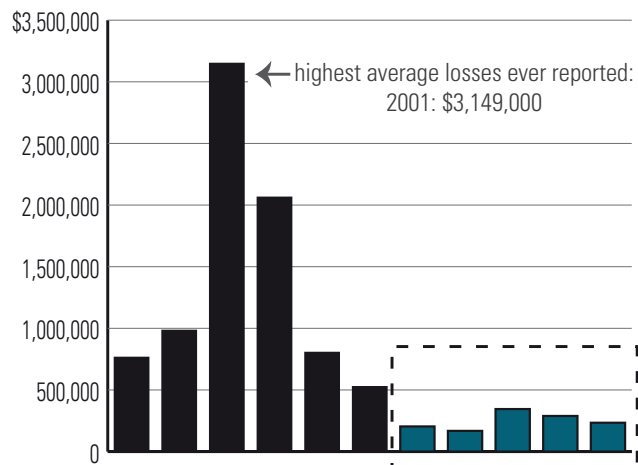
2009: 102 Respondents

Though still a hefty number, this is a big decrease. Last year 44 percent of respondents reported insider abuse, and insider abuse was the most prevalent incident in 2007, when it was reported by 59 percent of respondents.

Next in line are denial-of-service attacks, which jumped from 21 percent last year to 29 percent this year. This number is somewhat surprising, since DoS attacks are presumed to be far less profitable for attackers than data breaches are, and that DoS attacks receive far less press and attention than data breaches do (unless of course the DDoS is experienced by a high-profile Web service). It might be easier to understand if there'd been a sudden surge in the amount of blackmail or extortion associated with the threat of a DDoS, but this number was once again only infinitessimal—reported by only 3 percent of respondents.

Perhaps the change of greatest concern is that financial fraud increased from only 12 percent of respondents to 19.5 percent of respondents. This is reason for concern because financial fraud consistently causes victim organizations huge losses—almost $450,000 per victim organization this year.

Other notable changes: password sniffing almost doubled, leaping from 9 percent to 17 percent, while wireless exploits were nearly sawed in half, dropping from 14 percent to 8 percent.

So, how did these attacks affect target organizations? As the graphs on page 10 show, respondents suffered, on average, $234,000 in losses due to security incidents between July 2009 to June 2008. This is a 19 percent drop from last year's average of $289,000; which was a 16 percent drop from 2007's average of $345,000.

In 2005, respondents' reported losses dropped beneath the $500,000 mark for the first time, and haven't come anywhere near that line since. (This year's losses are 15 percent higher than 2005's average loss of $204,000.)

This sounds like good news for CSI survey respondents, but it must be noted that, despite anonymity, only 102 respondents (less than 25 percent) were willing to share details of their financial losses, thus continuing a troublesome downward trend. Because of the relatively small number of loss numbers reported, it is dangerous to pay too much heed to which attacks caused what financial damage. Thus, we will not tread that slippery ground here; that ground will be cautiously explored in the lengthier comprehensive edition of this survey report.
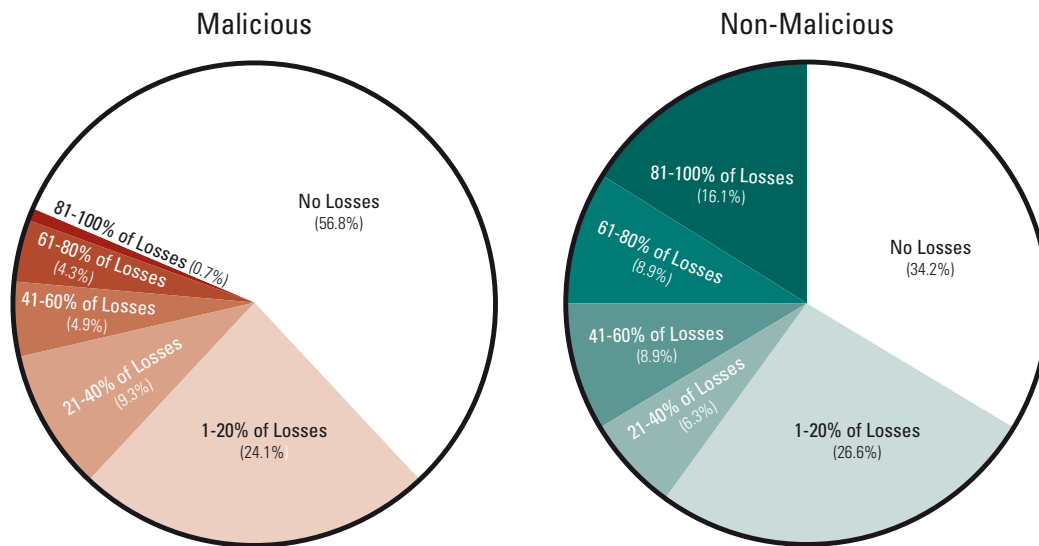
Why, you might rightly ask, are our respondents' numbers so small, in comparison to some numbers posited by other sources? Simply put, our study skews to a more security-aware study pool than others and, more importantly, other studies report solely on the experiences of organizations that suffered confirmed data breaches, while we sent our questionnaire to a wide survey pool without any knowledge of whether or not they'd experienced any security incidents whatsoever.

More in-depth discussion and comparison of these respective loss numbers will also be left for the lengthier comprehensive edition of this survey report.

The CSI survey historically has also asked respondents to estimate what percentage of monetary losses were attributable to actions (or, presumably, inactions) by individuals within the organization. Much is made of "the insider threat," but this "threat" really includes two very different types of threats—those posed by the malicious employee who leverages their inside information to conduct a highly targeted attack with a big payoff and those posed by the average well-meaning user who discloses data to a social engineer because they just don't know any better. This year, for the first time, we asked survey respondents to specify between malicious insiders and non-malicious insiders. The graphs below show their responses. (Before you look too closely at the numbers, look at the pies from a distance and get a feel for the amount and richness of the pies' overall color. The richer the overall color, the greater the losses.)

It's interesting to note that 43.2 percent of respondents stated that at least some of their losses were attributable to malicious insiders; but clearly non-malicious insiders are the greater problem.

Percentage of Losses Due To Insiders

Malicious

81-100% of Losses (0.7%)
61-80% of Losses (4.3%)
41-60% of Losses (4.9%)
21-40% of Losses (9.3%)
No Losses (56.8%)
1-20% of Losses (24.1%

2009 CSI Computer Crime and Security Survey

Non-Malicious

81-100% of Losses (16.1%)
61-80% of Losses (8.9%)
41-60% of Losses (8.9%)
21-40% of Losses (6.3%)
No Losses (34.2%)
1-20% of Losses (26.6%)

2009: 163 Respondents

The fact that 16.1 percent of respondents estimated that nearly *all* their losses were due to the non-malicious, merely careless behavior of insiders drives home the point that security awareness training for end users plays an important role in organizations' security programs.

Unfortunately 43.4 percent of respondents stated that less than 1 percent of their security budget was allocated to awareness training. Of course it's reasonable to consider that effective awareness training is inherently less expensive than the arsenal of security technology that most enterprises use to employ defense-in-depth. Nevertheless, 55 percent of respondents stated that the investment made in awareness training was inadequate.

One might expect that security professionals—like all of us—will be keen to say that their budgets are too small. However, when asked whether their organization's investments in compliance efforts, security services and security technology were adequate, the lion's share of respondents stated that they *were* adequate; some even said that too many resources were committed to those components.

Percentage of Security Budget
Spent on End-User Security
Awareness Training
and
Is this investment adequate?
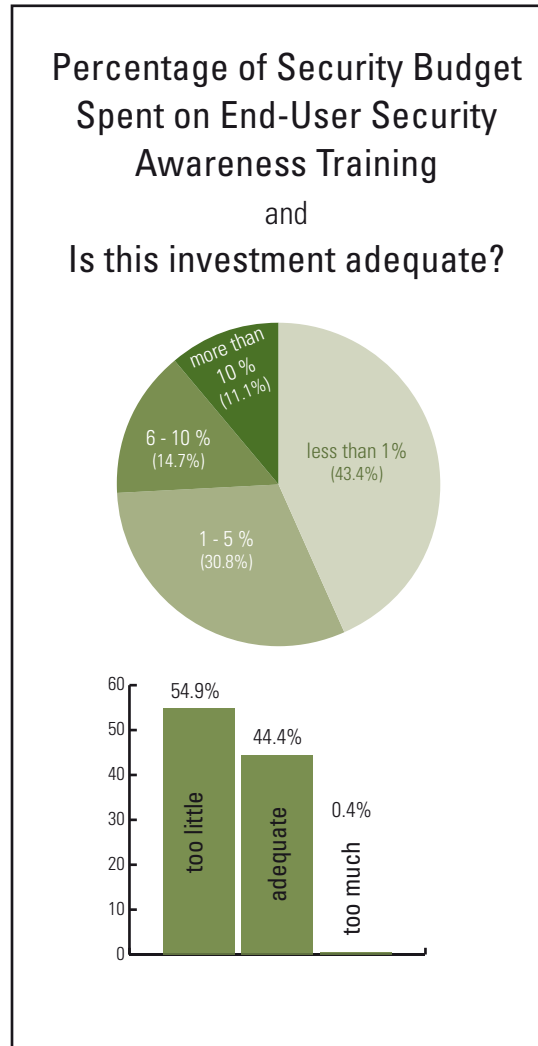
In the Comprehensive Edition:

The Comprehensive Edition of this report goes into greater details about respondents' security programs, including policies implemented, tools used, degree of outsourcing, use of metrics and effects of compliance requirements. The expanded report will also include more examination of the attacks respondents experienced, including incident response and deeper speculation about sources of losses. Further, the report will include respondents' opinions on the future of security. Finally, CSI survey findings will be compared to the findings of similar studies, including Verizon Business' most recent Data Breach Investigations Report, The Ponemon Institute's Cost of a Data Breach study, and Symantec's recent Global Internet Security Threat report. The Comprehensive Edition of the survey is given to members of

Note from Author

For several years now CSI Director Robert Richardson has led survey efforts and written the survey report. This year he passed the torch to me, but was nonetheless an essential part of the process. Many sincere thanks to Robert for his vision, guidance and patience.

Use of Survey Statistics

CSI encourages most uses of the survey. For purely academic, non-profit classroom use, you may use the survey freely. If you are quoting the survey in a research paper for instance, you are hereby granted permission and do not need to contact CSI. For other uses, there are four general requirements you must meet.

First, you should limit any excerpts to a modest amount—if you are quoting more than 800 words or reproducing more than two figures, you need special permission.

Second, you must of course give appropriate credit—state that the material you are excerpting is from the 2009 CSI Computer Crime and Security Survey, used with the permission of the Computer Security Institute.

Third, you may not profit directly from your use of the survey. You may however use survey statistics and the like as part of marketing and advertising programs, or as small parts of larger books or smaller works.

Finally, when the published or broadly distributed work in which you are using the quotation appears, you must send to CSI a copy of the work, link to the work online, or clear indication of how the material was used.

If you can meet these four requirements, you are hereby given permission. If not, please seek additional special permission from the author of this report. Contact:

Sara Peters, Senior Editor, CSI
sara.peters@ubm.com
11 W. 19th Street, Third Floor
New York, NY 10011

About CSI

CSI (Computer Security Institute) leads, informs and connects the security community through face-to-face and online events, in-depth content, research and professional membership. CSI holds two conferences annually: CSI SX in the spring and the CSI Annual Conference in the fall. CSI publishes the CSI Computer Crime and Security Survey and offers webcasts and end-user awareness tools. For information about CSI, visit e-mail csi@ubm.com, visit GoCSI.com, join our LinkedIn group, follow us on Twitter, or become a fan of CSI on Facebook.