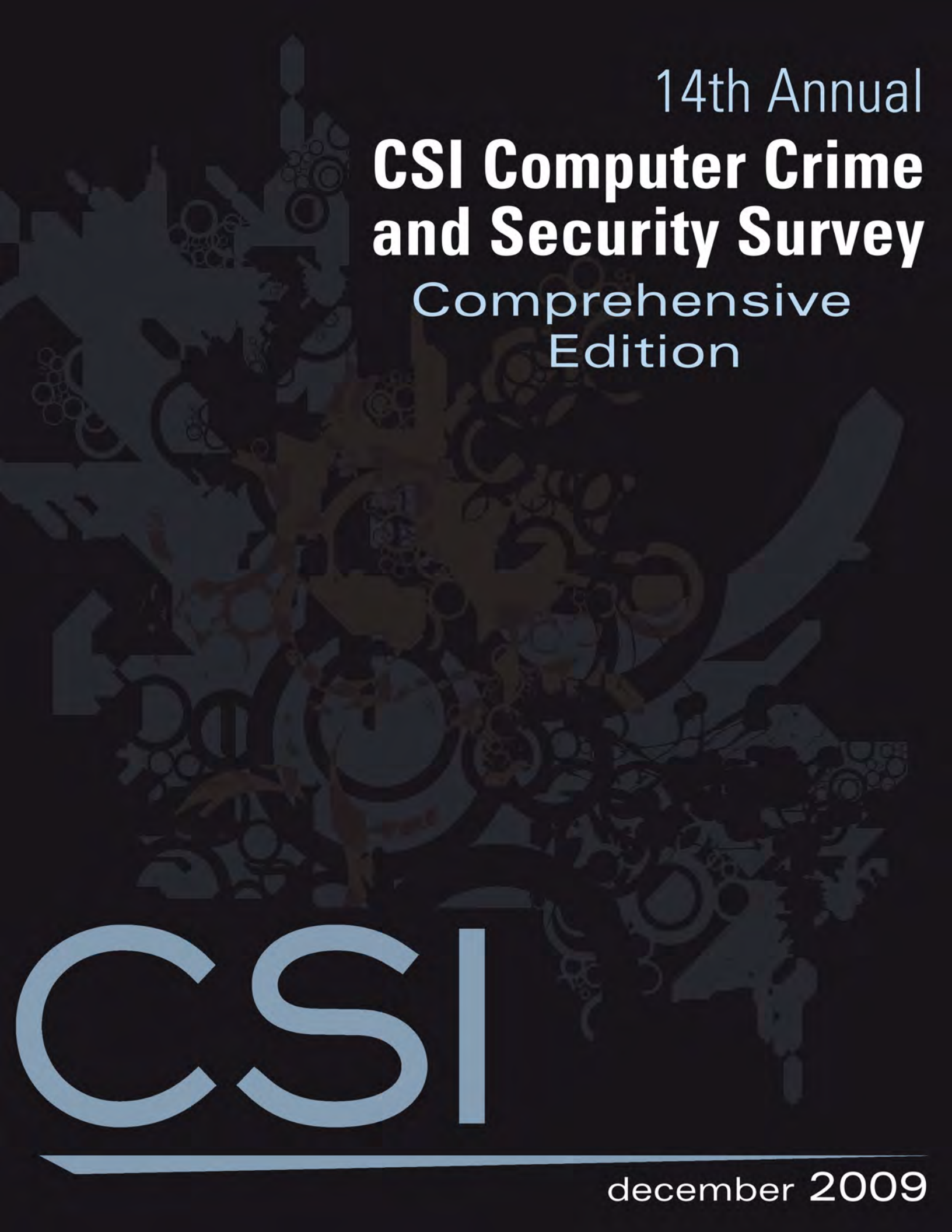


14th Annual

CSI Computer Crime and Security Survey

Comprehensive Edition

CSI

december 2009

The CSI Computer Crime and Security Survey report is the result of independent research conducted solely by the Computer Security Institute. We are proud to have the support of General Dynamics Advanced Information Systems, which sponsored the Webcast we conducted December 1, 2009, during which we briefed the public on this survey's key findings.

This Comprehensive Edition of the CSI Computer Crime and Security Survey is a new benefit exclusively for CSI members. This edition compares CSI's findings to those of the Verizon Business RISK Team 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 polymorphous 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

Comprehensive Edition

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) 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

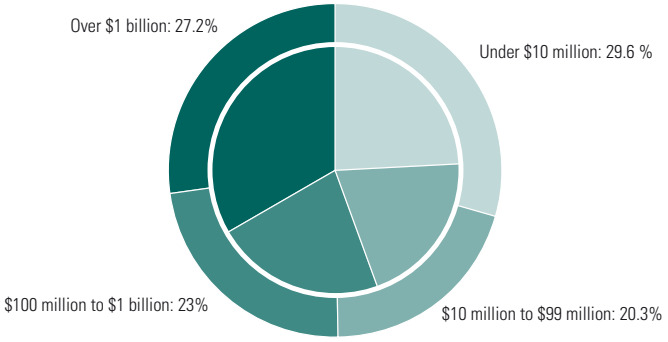
This is an informal survey. As one might expect, this report looks specifically at what the 443 respondents to this year's questionnaire had to say. Two inherent caveats must be borne in mind when interpreting the data.

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.

Respondents by Annual Revenue

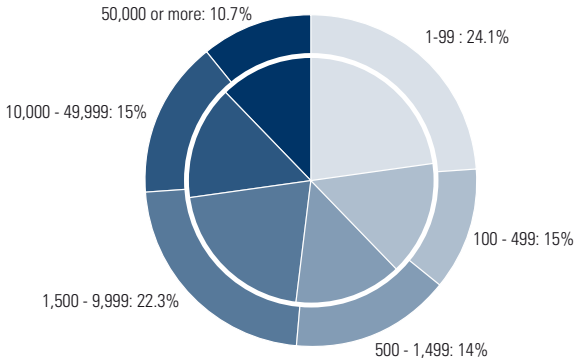
2009 figures on outside, 2008 figures on inside



2009 CSI Computer Crime and Security Survey 2009: 335 Respondents

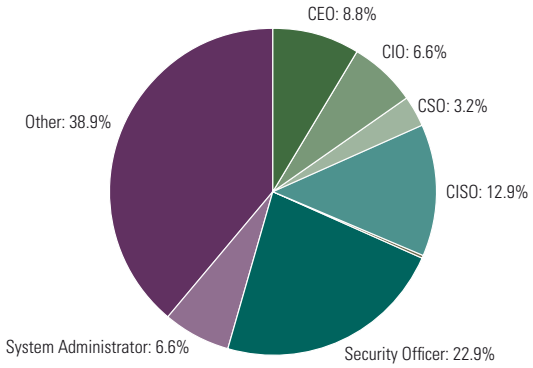
Respondents by Number of Employees

2009 figures on outside, 2008 figures on inside



2009 CSI Computer Crime and Security Survey 2009: 439 Respondents

Respondents by Job Title

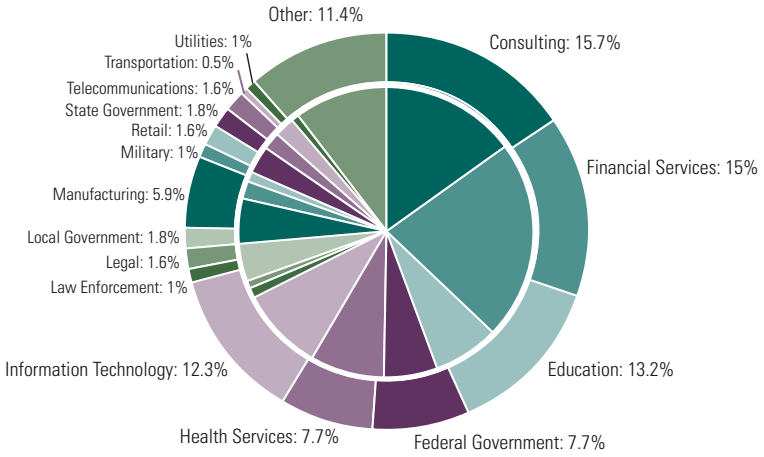


2009 CSI Computer Crime and Security Survey 2009: 442 Respondents

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



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.

In this Comprehensive Edition of the CSI survey report we will compare 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 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 respondents are assumed to be more "security savvy" than would be a survey pool of randomly selected information technology professionals.

As we lay out the detailed findings of our survey we will compare some of our survey results with the findings of other studies. Thus it is imperative to first recognize the differences in each study pool.

The Ponemon Institute's study (sponsored by PGP Corporation) examined the costs incurred by 43 organizations that had experienced data breaches. According to the report, "breaches covered in the survey ranged from less than 4,200 records to more than 113,000 records." As Dr. Larry Ponemon, chairman and founder of the Ponemon Institute explained to us, they purposely aimed at having a relatively homogenous study pool, specifically going after breach cases in which between 1,000 and about 100,000 records were disclosed. The breached organizations cover 17 different industry sectors—the most heavily represented industry sectors were financial services, which accounted for eight of the 43 breaches, and retail, which accounted for seven. Four breaches were from the healthcare industry, three from "technology," three from education, and one from "defense." (Based on the information Ponemon presents, this one from "defense" appears to be the only representative of the government or military.) Ponemon also told us that the Institute's report is best reviewed as a synthesis of 43 case studies of confirmed data breaches, as opposed to a more sweeping survey.

Verizon Business' Data Breach Investigations Report compiles information about 90 confirmed data breaches that Verizon Business' Investigative Respose Team (or "RISK team") was called in to investigate in 2008. Together these 90 breaches were accountable for the compromise of 285 million records—on average this is 3,167,000 records per breach, which is 28 times greater than Ponemon's biggest breach. Since Verizon itself investigated and responded to these breach cases,

we can assume that the data on attack methods and sources is very reliable. Due to the facts that the entire study pool consisted of organizations that had experienced confirmed breaches and that the overall severity of these breaches is quite high, the Verizon study probably best represents the average of the extreme (rather than the average of the whole). Put another way, the Verizon's study's greatest value perhaps is that it tells us how the *worst* breaches actually happen.

Most of the 90 breach cases the Verizon study covers occurred in the United States, but over one-third of the RISK team's 2008 caseload were investigations outside the United States. (As we specified before, although the "CSI community" extends across the globe, our survey pool was restricted to individuals and organizations located in the United States). Thirty-one percent of those breaches were from retail, 30 percent from financial services, 14 percent from food and beverage, 6 percent from business services, 6 percent from hospitality, 3 percent from technology and 4 percent were categorized as "other." You'll notice there are no cases from government agencies, healthcare organizations or educational institutions. Thus, the demographics by industry sector are also quite different from ours.

The data collected by Symantec for their Global Internet Threat Security Reports do not derive from surveys, interviews or investigations of individual security incidents, but rather from malicious activity detected by Symantec systems across the globe. As Symantec states in the most recent Global Internet Security Threat Report, "Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. More than 240,000 sensors in over 200 countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight Threat Management System, Symantec Managed Security Services and Norton consumer products, as well as additional third-party data sources. Symantec also gathers malicious code intelligence from more than 130 million client, server and gateway systems that have deployed its anti-virus products."

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 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 regulations.

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 10.

As the graph on page 9 and the chart on page 10 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).

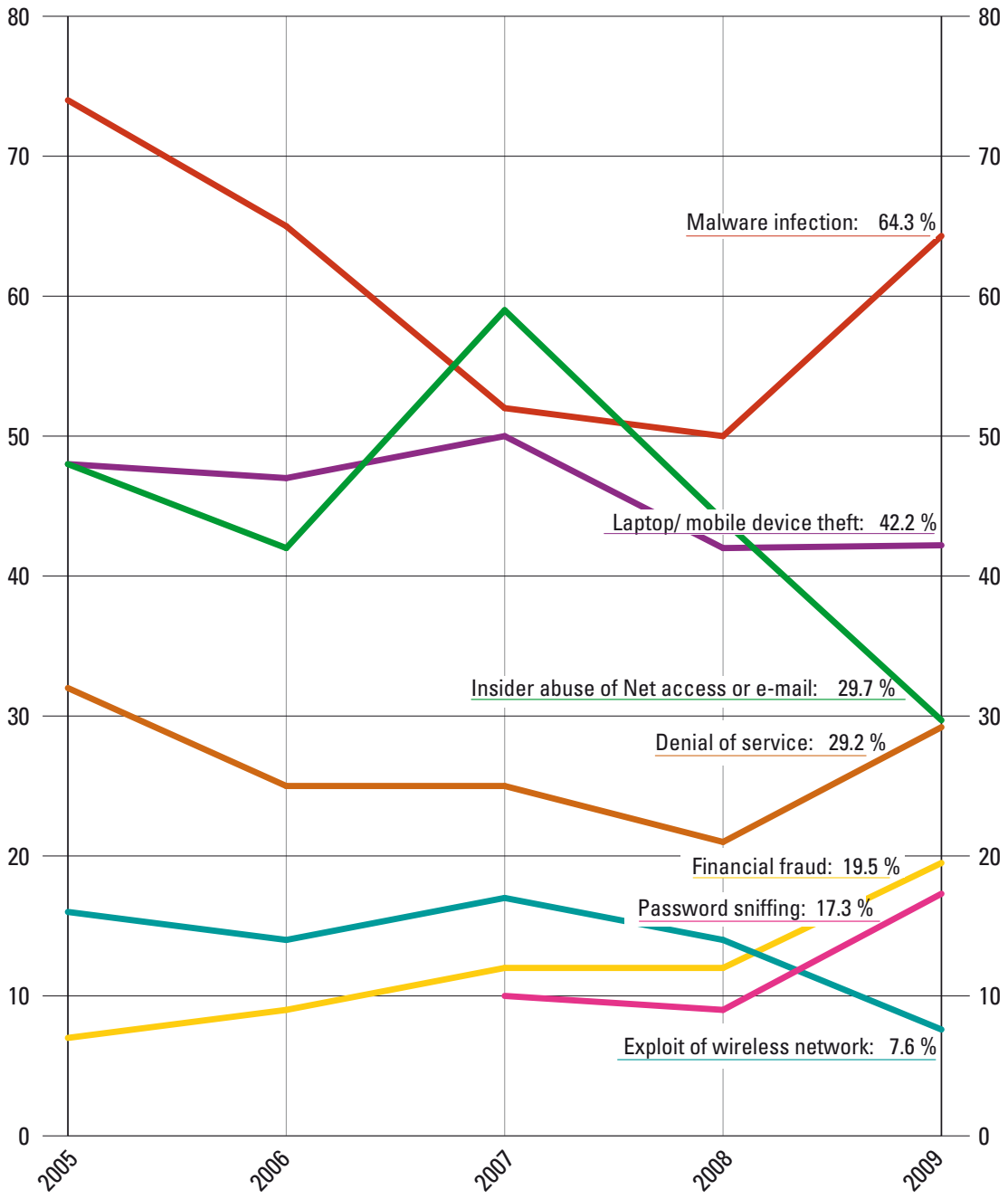
Malware infection leapt from 50 percent of respondents to 64.3 percent of respondents, making it easily the most prevalent incident; and specifically, "bots in the organization" increased modestly from 20 percent of respondents to 23 percent. These increases may not be very surprising, considering that 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. According to Dean Turner, Symantec's Director of the Global Intelligence Network Security Technology and Response, many malware attacks were mutli-stage attacks, in which the malware would download separate obfuscation tools (or tools to otherwise enhance the effectiveness of the malware attack).

Not only did malware improve, it increased in number. In their last Internet Global Security Threat Report (published in April 2009), Symantec reported that they detected 1,656,227 *new* malicious code threats in 2008. Those new threats alone accounted for over a whopping 60 percent of the approximately 2.6 million malware threats that Symantec has detected in total over time.

Considering the rapidly increasing number and sophistication of malware—and the not-so-rapidly-increasing sophistication of anti-malware solutions—it would not be altogether surprising if malware

Types of Attacks Experienced

By Percent of Respondents



2009 CSI Computer Crime and Security Survey

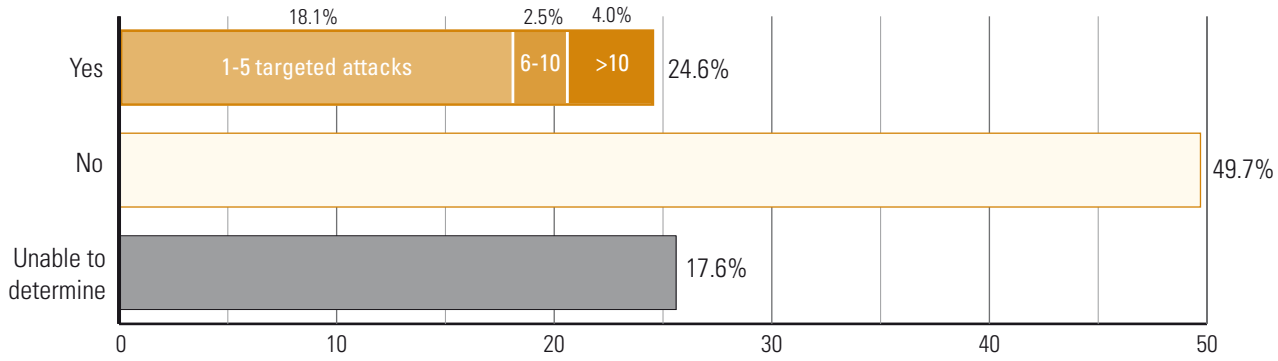
2009: 185 Respondents

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%
2009 CSI Computer Crime and Security Survey					2009: 185 Respondents

Did Any of These Security Incidents Involve Targeted Attacks?



2009 CSI Computer Crime and Security Survey

2009: 199 Respondents

infection makes another big jump in our survey next year. Turner said he is not surprised that our respondents reported a significant jump in malware infection, and agrees that another increase next year is likely.

There's also evidence that attackers are spending more energy customizing malware to make it more effective in targeted attacks. The Verizon report states that, of the breaches they investigated that involved malware in some fashion, 59 percent involved highly customized malware. Turner told us that many of the pieces of malicious code Symantec detected were actually just variants of other malware (as opposed to totally unique code), and the number of incidents attributable to each variant was relatively small, because these variants were each crafted for narrower, more specifc groups of attack targets. Twenty-five percent of CSI survey respondents told us that at least some of their security incidents involved targeted attacks—4 percent told us they experienced more than 10 targeted attacks.

The second-most prevalent incident experienced by CSI survey respondents was 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 proprietary information or intellectual property rose from 4 percent to 6 percent, and breach of PII or PHI dropped from 8 percent to 6 percent. (We might be twisting the numbers up a bit more than adviseable, but put another way, only about 14 percent of lost or stolen mobile devices led to breaches of protected data like PII and PHI.)

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.

Put another way, CSI respondents told us that approximately 40 percent of data breaches were a result of lost or stolen mobile devices. This number is a bit lower than what Symantec found and what The Ponemon Institute found, but nonetheless in the same ballpark.

Symantec found that "the primary cause of data breaches that could facilitate identity theft was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium." Such theft or loss was responsible for 48 percent of data breaches according to Symantec.

Ponemon's respondents told them that 35 percent of the breaches were due to lost laptop computers, 5 percent to lost media backups and 14 percent to "other data-bearing devices." However, in our conversations with Dr. Ponemon, he theorized that these last two figures may be rather low; and we're rather inclined to agree. "Users may be less likely to report the loss or theft of something like a USB thumb drive than they are to report a laptop or phone," he said. As he noted, smartphones and laptops are computing devices, not just storage devices, and thus they are essential to an employee's work, and an employee would therefore be compelled to report the loss or theft of such devices, and report them promptly. The same rule probably does not apply to portable storage devices that may serve solely as back-ups.

So, roughly speaking, these three stufies agree that the loss or theft of mobile devices account for between 40 to 60 percent of data breaches. Verizon's figures, however, are vastly different. Only 9 percent of Verizon's breaches—and only 2 percent of compromised records—were due to "physical" attacks, which include, among other things, theft or loss of mobile devices.

Perhaps this then means that, although mobile devices are responsible for a relatively large number of data breaches, they do not cause the most severe breaches. This is what we cautiously believe and Ponemon tells us he agrees with this assessment as well.

However, Symantec's numbers do not support that view. Although 48 pertcent of data breaches that could result in identity theft were due to lost mobile devices, 66 percent of the breached records were due to mobile devices—more than their fair share. Not only does this conflict with the findings and interpretations of Verizon, Ponemon and CSI, it is also somewhat counterintuitive, because one would generally assume that mobile devices cannot carry as much sensitive data as something like a back-end server; plus there'd be fewer essential reasons for users to store that data on mobile devices. However, as Turner points out, modern mobile devices now have the memory capacity to store plenty of sensitive databases, and that just because storing sensitive data on something like a smartphone or a USB stick is against corporate security policy doesn't mean that it doesn't happen. This is certainly a valid argument. We'll discuss security policy in greater depth later in this report.

The third-most prevalent incident experienced by CSI Survey respondents—reported by over one-third of respondents—was phishing fraud, in which a victim organization is fraudulently represented as the sender of phishing messages. Although Symantec found that 79 percent of "brands" used in phishing messages were from financial services organizations, our numbers weren't nearly so one-sided, but rather evenly spread across industries.

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. 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 a DDoS is experienced by a high-profile Web service). It might be easier to understand this increase 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 infinitesimal—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.

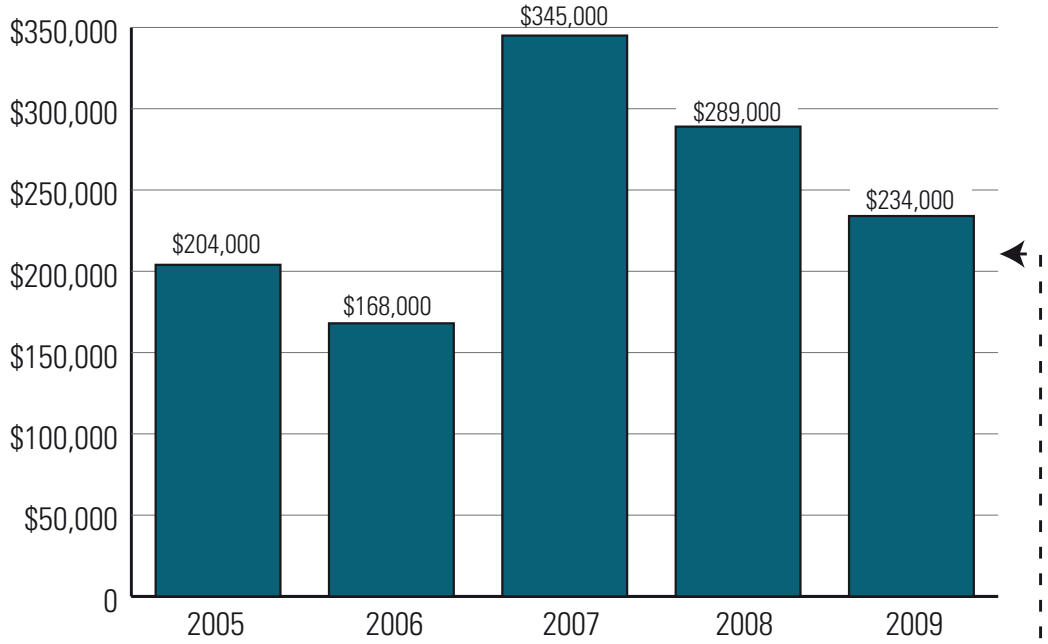
Other notable changes: password sniffing almost doubled, leaping from 9 percent to 17 percent, while wireless exploits were nearly sawed in half, dropping from 14 percent to 8 percent.

So, how did these attacks affect target organizations? As the graphs on page 14 show, respondents suffered, on average, $234,000 in losses due to security incidents between July 2008 to June 2009. 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.

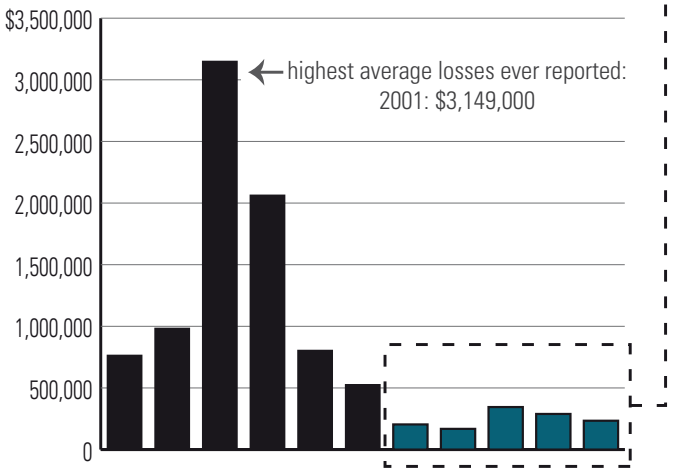
In 2005, respondents' reported losses dropped beneath the $500,000 mark for the first time, and haven't come anywhere near that line since. (This year's losses are 15 percent higher than 2005's average loss of $204,000.)

Our numbers, thus are drastically different from those reported by the Ponemon Institute, which found that the average total cost incurred by an organization was $6.6 million per data breach, or $202 per compromised record, and had increased since last year.

Average Losses Per Respondent



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



2009 CSI Computer Crime and Security Survey

2009: 102 Respondents

Why, you might rightly ask, are our respondents' numbers so small, in comparison? There are several reasons, but first let's be clear: We don't dispute the fact that security incidents can cause organizations $6 million or more. Several of our respondents told us that security incidents cost them multiple millions of dollars. Why, though, was the *highest* monetary loss reported by our respondents ($6 million) lower than Ponemon's *average* loss ($6.6 million)?

Mainly it's because of the differences in our survey pool. All of Ponemon's data comes from organizations (43 of them) that were known to have experienced data breaches and who agreed to share their estimated losses with the researchers. Meanwhile, only a portion of our 443 respondents experienced data breaches, because we sent our questionnaire to a wider survey pool without any knowledge of whether or not they'd experienced any security incidents whatsoever.

Further, as mentioned earlier, our survey pool skews toward those with a demonstrated, active interest in and understanding of information security. There's reason to believe that organizations that are taking security seriously are, if not avoiding, then at least mitigating the impact of cyber attacks. Some of the organizations that suffered data breaches (or other incidents) reported that while they might have lost track of some data, they didn't lose any money at all.

This certainly *sounds* like good news for CSI survey respondents—and we think it actually is. Dr. Ponemon agrees. His institute's data breach study contains some related data. It states that organizations experiencing a breach for the first time spend and lose more money than organizations experiencing their second or third breach. The report states that "the per-victim cost for a first-time data breach is $243, versus $192 for experienced companies." Dr. Ponemon said "Organizations do seem to get better at security as they become more experienced and more knowledgeable."

We would be remiss if we did not note that, despite anonymity, only 102 respondents to the CSI survey (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. It's slippery ground we will now tread here, so we explore it cautiously and ask that you do the same.

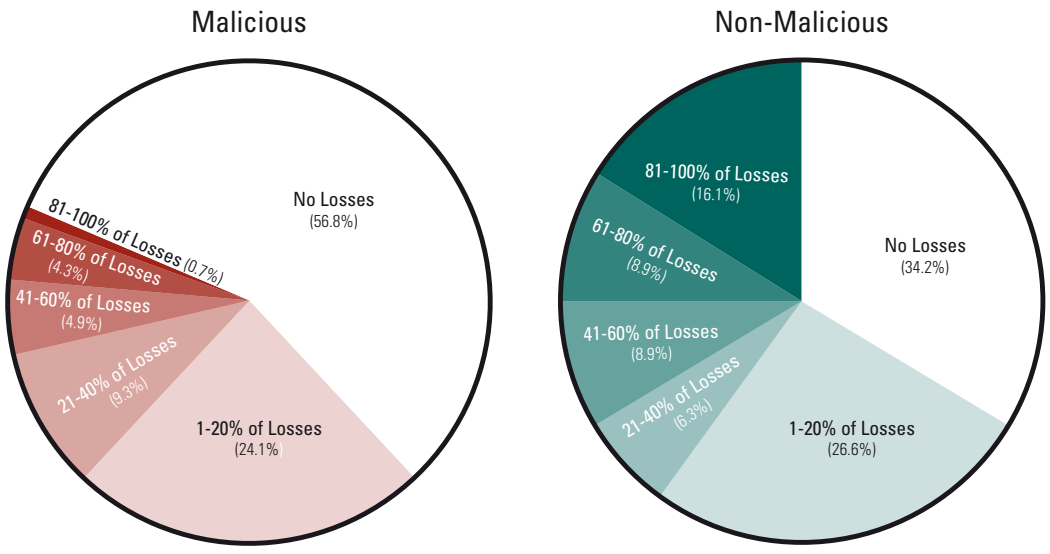
Financial fraud continues to consistently be a highly expensive attack, averaging almost $450,000 in losses, per organization that suffered fraud. However, this year, isolated incidents pushed financial fraud down to number three on the most-expensive incident list, behind wireless exploits ($770,000) and theft or loss of personally identifiable or personal health information through all causes other than mobile device theft ($710,000). Loss figures were only offered by three respondents who'd experienced wireless exploits, and nine respondents who'd experienced theft or loss of PII or PHI through all causes other than mobile device theft.

Web application exploits (excluding Web site defacement) were the fourth-most expensive security incident, costing $115,000 on average, followed by unauthorized access or privilege escalation by an insider, which cost, on average, $95,400.

Of the 21 respondents who told us how much a data breach cost them, the only two who reported losses in the multiple millions of dollars said that their breaches were ***not*** due to lost or stolen mobile devices. In a roundabout sort of way, that brings us back to what we earlier inferred: that data breaches via lost or stolen mobile devices may well be frequent, but not necessarily as severe as data breaches through other vectors.

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, or leaves their corporate smartphone in a taxi, or some other act of negligence. This year, for the first time,

Percentage of Losses Due To Insiders



2009 CSI Computer Crime and Security Survey

2009: 163 Respondents

we asked survey respondents to specify between malicious insiders and non-malicious insiders. The graphs on page 16 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. 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. (More on that later.)

It's also essential to note that there is plenty of white space on both those graphs—meaning that "the insider threat," however you define it, does not negate the danger of the outsider threat (which accounts for about half of CSI respondents' estimated monetary losses).

Other studies do not approach the question of insiders in quite the same way we do, but some data can be cautiously correlated. According to Ponemon's reckoning, the average cost per record of a breach caused by "negligence" was $199, which was cheaper than the cost of a breach caused by a "malicious act" ($225 per record). Nevertheless, Ponemon's subjects found that negligence was much more expensive *overall*, because 88 percent of breaches were attributed to negligence.

So only 12 percent of the Ponemon's study's breaches were from malicious acts, which seems quite small, particularly when compared to Verizon's numbers. Verizon splits the "source of breach" into three categories—external, internal and partner—but one breach could be associated with multiple sources. In their report they state that only 20 percent of the breaches were at least partially caused by an "internal" source. (Their definition of "internal" generally is narrower than Ponemon's "negligence," and generally matches our definitions of malicious and non-malicious insider action combined. By "internal" they include actions like succumbing to a phishing message and unwittingly downloading malicious code, but do not include inactions or oversights.) Meanwhile 32 percent were at least partially caused by a partner, and 74 percent were at least partially caused by an "external" source like organized crime. Put another way, Verizon stated that: 39 percent of breaches came from multiple sources, 7 percent from only partner sources, 11 percent from only insider sources, and 43 percent from only external sources.

Verizon states: "It is true that these results are based upon our caseload—which is consumer data-heavy—and may not be reflective of all data breaches. Perhaps insiders are more apt to target other types of data, such as intellectual property. It is also true that many insider crimes may never be detected, though one would think any breach causing material harm would eventually be noticed. It is also feasible that they are more likely handled internally [instead of by a third party like the Verizon RISK Team]. At any rate, results from 600 incidents over five years make a strong

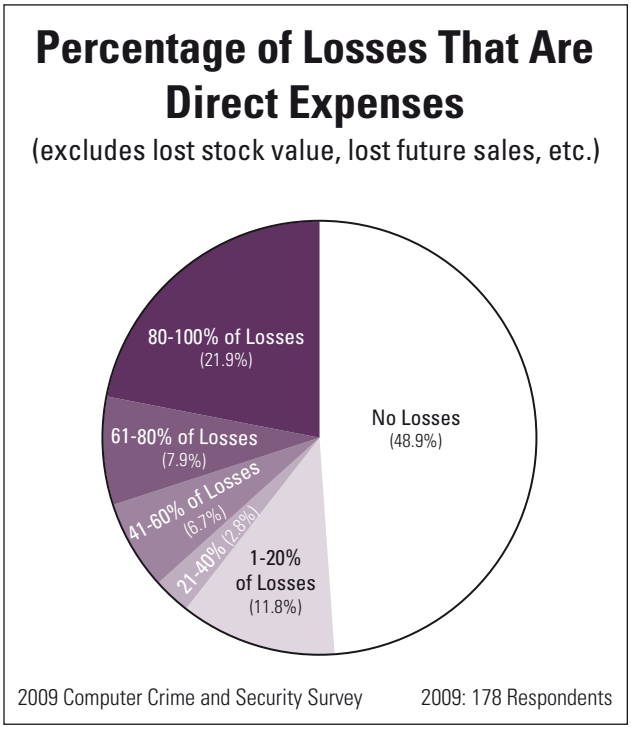
case against the long-abiding and deeply held belief that insiders are behind most breaches." Both Dr. Ponemon and we at CSI are inclined to agree.

Though this is a bit tangential to the insider threat discussion, it's worth pointing out another of Verizon's findings. They classified the attacks they investigated by attack difficulty. "None" meant that there were no special skills or resources required and that an average user could have done it. "Low" meant "basic methods, no customization, and/or low resources required. Automated tools and script kiddies." "Medium" meant "skilled techniques, some customization, and/or significant resources required." "High" meant "advanced skills, significant customization, and/or extensive resources required." Although only 17 percent of attacks that caused breaches were classified as "high difficulty," they were responsible for 95 percent of the records breached.

Putting aside the questions of who caused a security incident and how they caused it, let's turn to the question of how all that "lost" money was spent. We split up losses into "direct" and "indirect." Direct losses would include costs of things like responding to an incident, hiring a forensic investigator, sending out data breach notification letters and the like. Loss of customers, potential loss of future business, or drop in stock prices would fall into the "indirect losses" category.

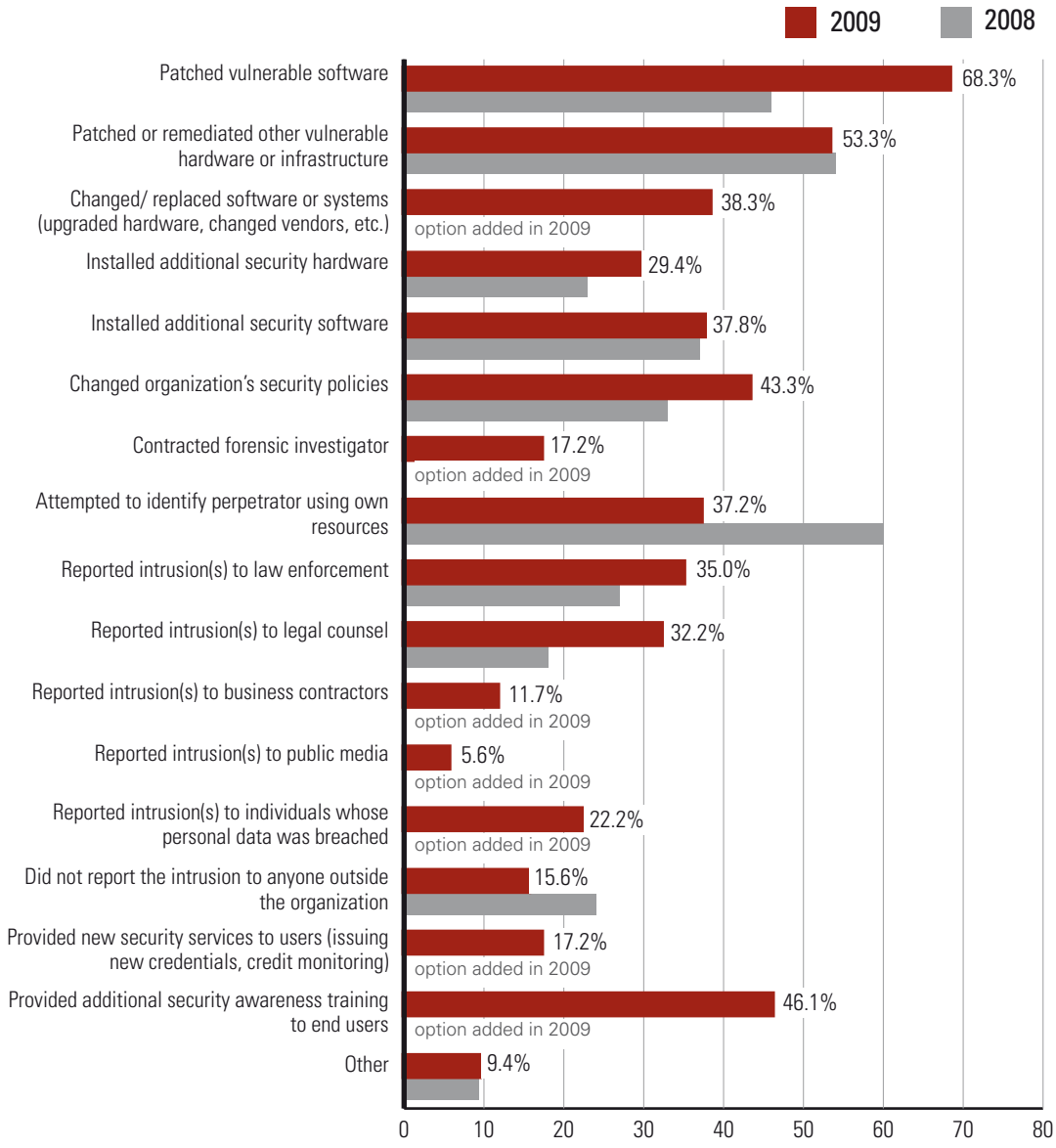
Nearly half of our respondents (48.9 percent) reckon that all losses were indirect. Although not an apples-to-apples comparison, Ponemon's respondents seem to agree that lost business is where the costs add up. They divide costs into four categories: detection and escalation, notification, ex-post response (which would include things like giving breach victims discounts or credit monitoring services) and lost business. By their measurements, 69 percent of losses fell into that fourth category.

Of course, before organizations tally all the dollars and cents that were



Actions Taken Following a Security Incident

By Percent of Respondents



2009 CSI Computer Crime and Security Survey

2009: 180 Respondents

lost because of a security incident, they have to respond to the incident itself. The graph on page 19 shows the actions CSI respondents took, following security incidents.

This year CSI respondents were much more active and communicative following security incidents than they were in last year's survey. In this survey 68.3 percent of respondents stated that they patched vulnerable software following a security incident, while last year only 46 percent of respondents made this statement. This year 43 percent of respondents changed their organization's security policy (over 33 percent last year), 29.4 percent installed new security hardware (over 23 percent last year) and 37.8 percent installed additional security software (over 37 percent last year).

For the first time we asked whether or not respondents contracted a forensic investigator—17.2 percent stated that they had. One thing that respondents did far less of was attempting to identify the perpetrator by themselves—this dropped from 60 percent of respondents last time to 37.2 percent of respondents. This is a good thing, because many security professionals who do their own forensic investigations and e-discovery automatically and unintentionally damage the evidentiary value of forensic data—and thus damage any legal case against the perpetrator of the attack.

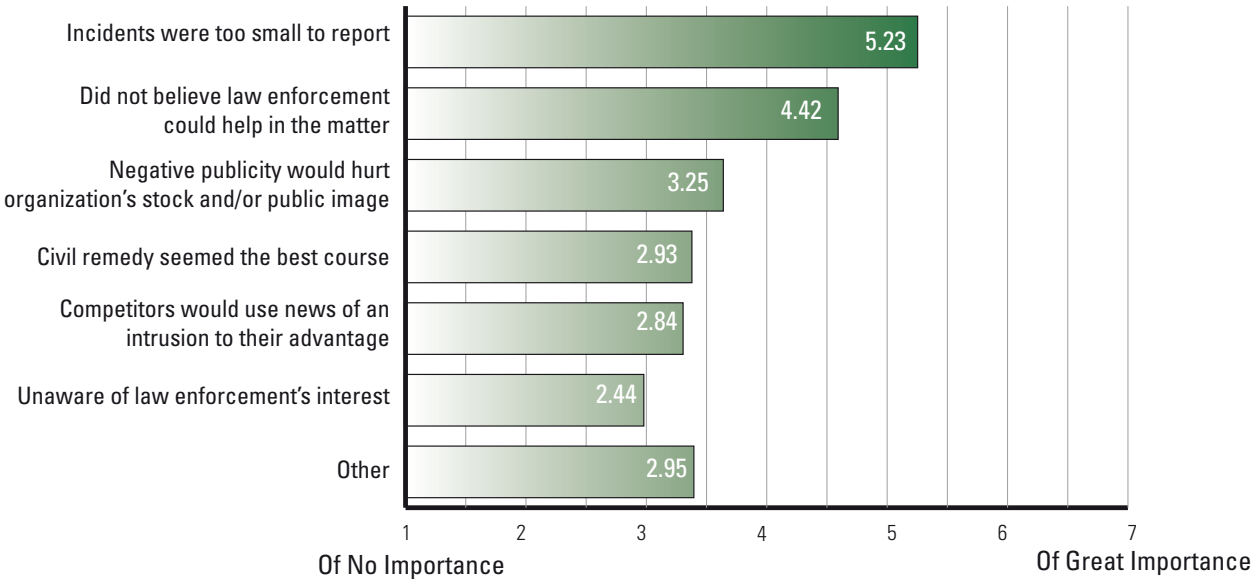
We added several other new options to this question to get a broader picture of how widely organizations were communicating about their security incidents and how they were treating individuals whose personal information was exposed by a data breach. Although 15.6 percent of respondents still did not communicate the breach to anyone outside the organization, 11.7 percent of respondents reported the incident to business contractors, 5.6 percent reported to public media and 22.2 percent reported to individuals whose personal data had been breached. Also, 17.2 percent of respondents provided new security services to users, including issuing new credentials and offering credit monitoring services.

This year, more respondents reported incidents to law enforcement—35 percent, compared to 27 percent last survey—and nearly twice as many reported incidents to legal counsel—32.2 percent, as compared to 18 percent last time. We again asked respondents who did not report the incident to law enforcement why they had chosen not to. As the graph on page 21 shows, the leading reason continues to be that the incidents were too small to report, followed by "did not believe law enforcement could help in the matter."

For the first time we asked respondents whether they provided additional security awareness training to end users—46.1 percent said that they had. (Ponemon asked a similar question, and 53 percent of their respondents said they conducted awareness training after an incident.)

Nonetheless, respondents told us that security awareness training continues to be a weak spot in their organizations' security programs.

If Your Organization Did NOT Report the Intrusion to Law Enforcement, Why Not?



2009 CSI Computer Crime and Security Survey

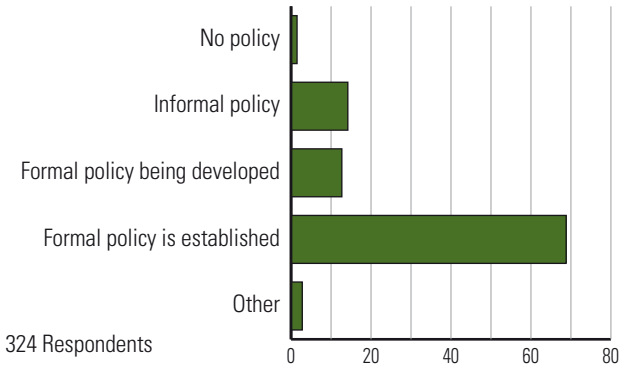
2009: 93 Respondents

Security Program

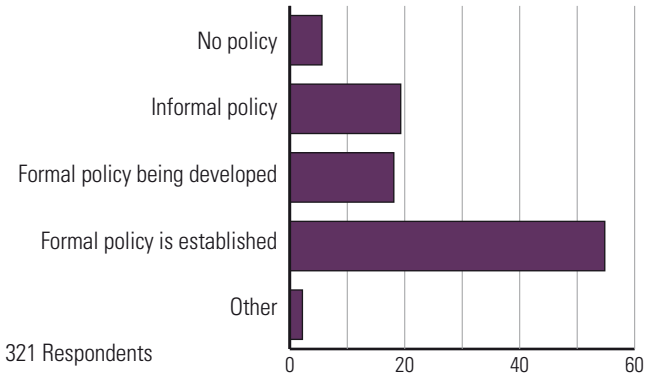
This survey has always contained a number of questions about cyber crime, but for the past six years, it has also explored just how security professionals are combatting this crime. Fewer studies exist that examine security programs in quantitative fashion than those that examine security incidents, so we don't have as many comparisons to make in this part of the report. What this section will definitively show is that respondents to the CSI survey are quite proactive about defending their computing environments. It will also hint at some ways that the economic recession has and has not affected organizations' security strategies.

The graphs on page 22 show the status of security policies in respondents' organizations. The majority of respondents have, in place, formal information security policies (68.8 percent) and formal data retention and destruction policies (54.8 percent), and almost all the rest are developing

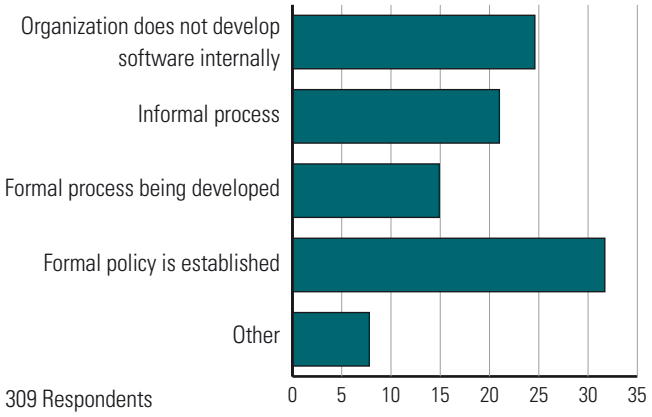
How Would You Describe Information Security Policy Within Your Organization?



How Would You Describe Data Retention / Destruction Policy Within Your Organization?



Does Your Organization Use a Secure Software Development Process?



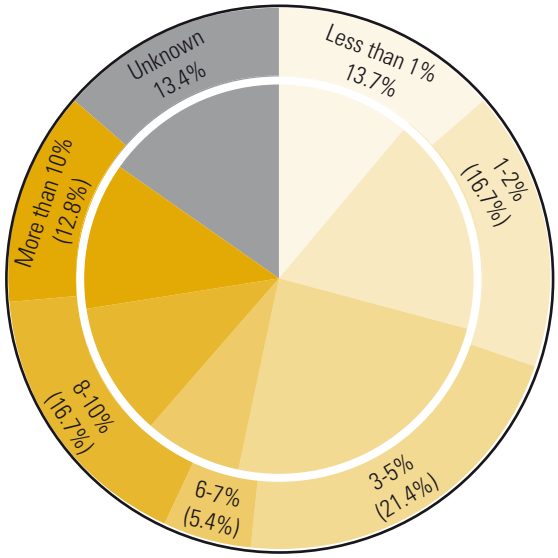
such formal policies or using an informal policy. Only a small number of respondents have no security policy (1.5 percent) or no data retention and destruction policy (5.6 percent).

A few years ago, secure software development was a very hot topic. Although some of the fire has died down, there is still concern over organizations' home-grown applications, which may be just as essential to the business as a commercial off-the-shelf application is, but may not be as appropriately tested, secured, or patched. We asked respondents if their organization uses a secure software development process to see how they were addressing the issue. Although 24.6 percent said they don't develop software internally, almost a third (31.7 percent) of respondents stated that they both develop software and have a formal secure development process in place.

Of course, while policy is all well and good, it isn't worth the paper it's written on unless it can be enforced—but have security professionals been given enough muscle (and enough money) to adequately enforce these policies? To begin answering that question, we ask survey respondents how much of the overall IT budget is allocated to security. It should be noted that some security funding may come from other departments, like perhaps the legal department or physical security budget, but we're confident that the lion's share of the security budget comes as a slice of IT. As the graph on page 23 shows, CSI survey respondents told us that they've gotten a bigger piece of the pie than they did last year. This year 29.5 percent said that security claimed 8 percent or more of the over-

Percentage of IT Budget Spent on Security

2009 Figures on Outside, 2008 Figures on Inside

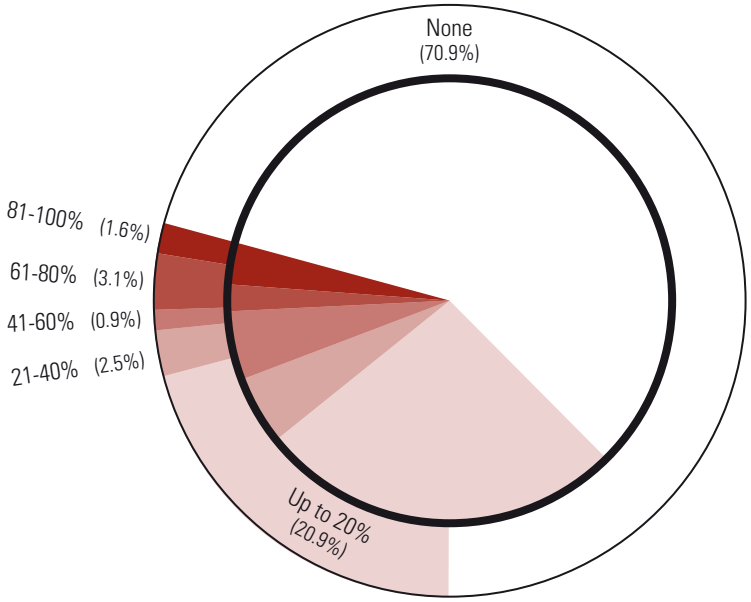


all IT budget, while last year only 23 percent could make that statement. This doesn't necessarily mean, of course, that security departments were given more money to spend this time around. It is perhaps more likely that IT budgets were cut overall, and that security got trimmed a bit less than other IT segments. Regardless of the actual dollars, it is good news that more organizations are recognizing that security is essential, even in a slumping economy.

When organizations are cutting costs, as so many are these days, oftentimes staff numbers go down and outsourcing goes up. However, if our survey results are any indication, that rule does not apply to the security department. When we asked respondents what percentage of security functions were outsourced, we found that the amount of security outsourcing decreased significantly. (See the graph on page 24). Last year 41 percent of respondents told us that at least some security functions were outsourced; this year only 29 percent stated that they outsourced security. Further, those that do outsource are outsourcing less. Last year 15 percent of respondents outsourced over 20 percent of their security; this year only 8 percent outsourced that much.

Percentage of Security Functions Outsourced

By Percentage of Respondents
2009 Figures on Outside, 2008 Figures on Inside



2009 CSI Computer Crime and Security Survey 2009: 320 Respondents

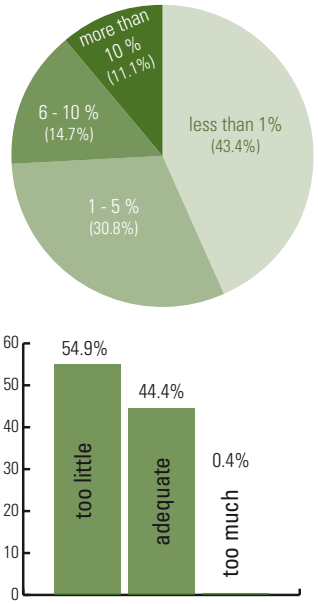
How are the security dollars being spent then? For the past couple of years we asked respondents how much of the security budget was devoted to end-user security awareness training. The numbers were always quite small. (Last year 42 percent of respondents said that less than 1 percent of their security budget was devoted 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. Thus, this year we decided to ask respondents not only how much was devoted to awareness, but also whether or not that investment was adequate.

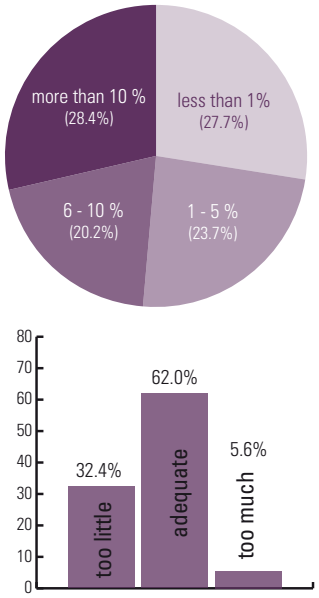
Plus, instead of just asking about awareness, we also asked about investments made in security technology, in security services, and in compliance efforts. The graphs on page 25 show their responses.

Percent of Security Budget Spent on Various Components
Is this investment adequate?

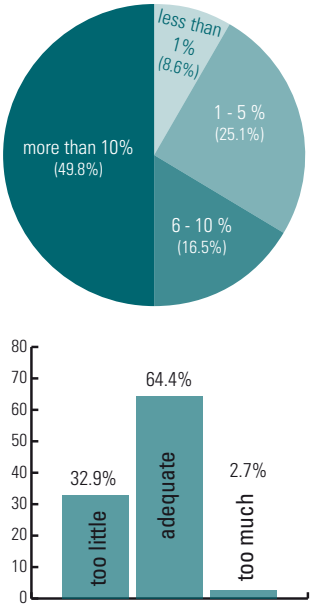
End-user Security Awareness Training



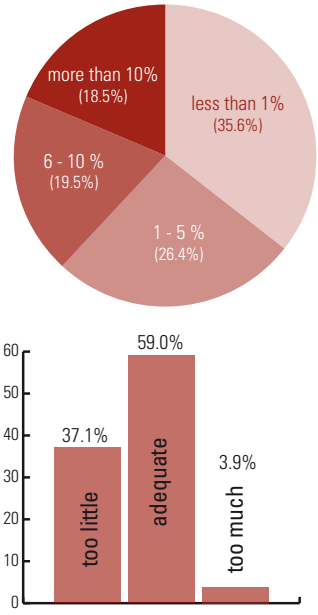
Regulatory Compliance Efforts



Security Technology



Security Services



2009 CSI Computer Crime and Security Survey

2009: 306 Respondents

Once again, back up and get a feel for the richness of the color in these graphs, to get the best sense of where the money is going. The first thing you'll notice is that the most richly colored pie is the one representing investment in security technology. Half of respondents spend greater than 10 percent of their budget on tech. (About 28 percent of respondents spend over 10 percent on compliance efforts and 18.5 percent of respondents spend over 10 percent on security services.) You'll also notice that end-user security awareness training has the palest pie. Once again over 40 percent (43.4 percent) of respondents spend less than 1 percent of their budget on awareness training. This brings us back to that earlier question. Maybe awareness is just intrinsically cheaper than other security elements, and maybe that small investment is fine.

Or maybe not. Now take a look at the bar graphs on page 25, and you'll see that 55 percent of respondents stated that the investment made in awareness training was *in*adequate. 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 majority of respondents stated that they *were* adequate; some (not many) even said that too many resources were committed to those components. Although it was a spare few who thought they spent too much on anything, compliance efforts were considered the biggest money sink.

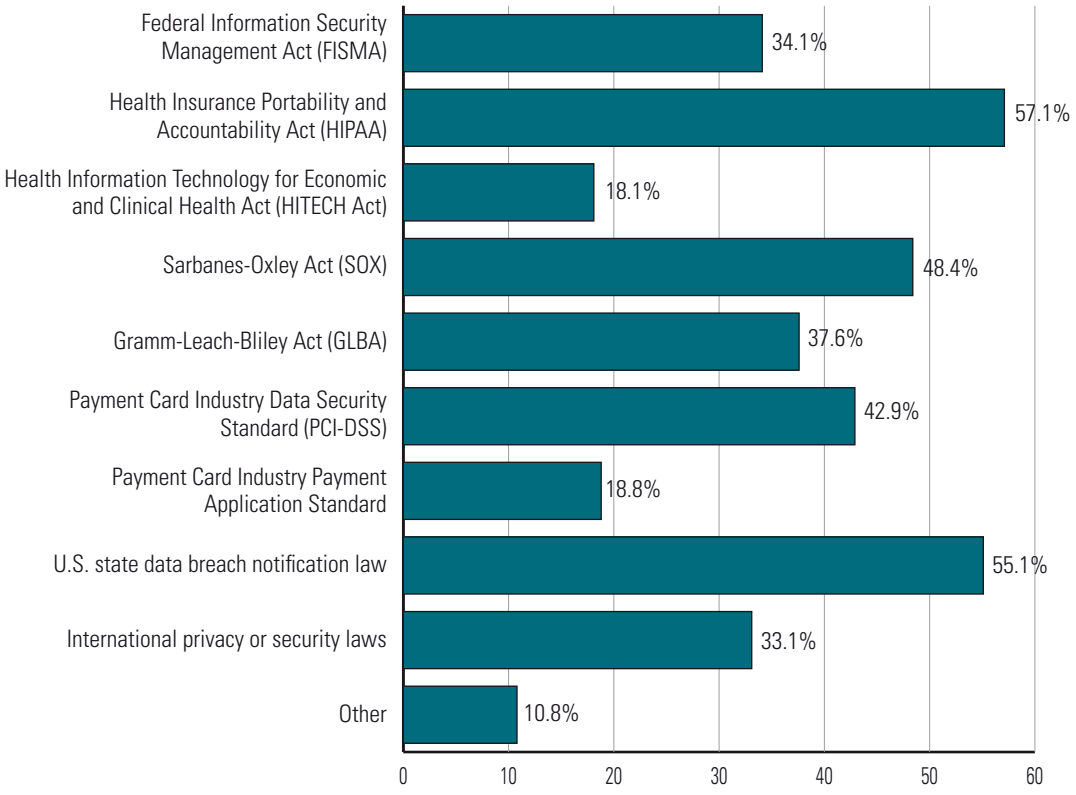
It's no secret that privacy and security regulations have had a big impact on organizations' security programs. We've asked some questions about regulatory compliance before, but this year for the first time we asked respondents what spectific regulations applied to their organization. As the graph on page 27 shows, CSI survey respondents have considerable compliance duties, which is not terribly surprising. What *is* surprising, however, is that, of all the regulations we asked about, more respondents had to comply with the Health Insurance Portabilitiy and Accountability Act (HIPAA) than any other regulation or category of regulations. This is somewhat perplexing, because HIPAA is intended to protect the privacy of personal health information. So why, if less than 8 percent of our respondents are from health services do fully 57 percent of respondents need to worry about protecting health information?

The picture becomes particularly peculiar when you hold these numbers up against the PCI-DSS numbers. Only 43 percent of respondents said they had to comply with the Payment Card Industry Data Security Standard, which is a regulation with which every single business that accepts credit cards as payment must comply. One would assume that more organizations would have cause to transmit and store credit card data than they would health data. So why do the numbers tell us a different story?

Privacy expert Rebecca Herold—a frequent contributor to CSI publications and speaker at CSI events—said that she is not surprised by the survey numbers regarding HIPAA. Her explanation is that the Health Information Technology for Economic and Clinical Health Act (HITECH Act)—part

Which Laws and Industry Regulations Apply to Your Organization?

By Percent of Respondents



2009 CSI Computer Crime and Security Survey

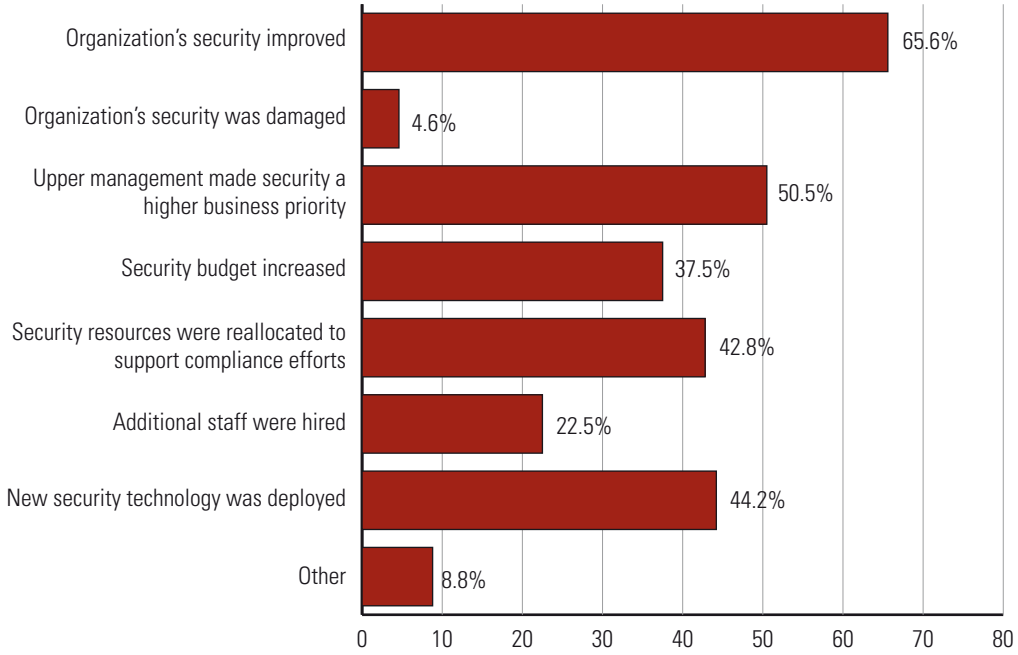
2009: 287 Respondents

of the American Recovery and Reinvestment Act of 2009—expanded the reach and strength of HIPAA so that far more organizations had to comply with HIPAA requirements.

As Herold says: "HITECH effectively expanded HIPAA compliance to exponentially more organizations that are business associates (BAs) not considered as covered entities (CEs), or even within the healthcare industry. Last year you would only have gotten a fraction of the numbers indicating that said they had to comply with HIPAA." On this we can only speculate, being that we only added this question this year.

How Have Regulatory Compliance Efforts Affected Your Overall Information Security Program?

By Percent of Respondents



2009 CSI Computer and Security Survey

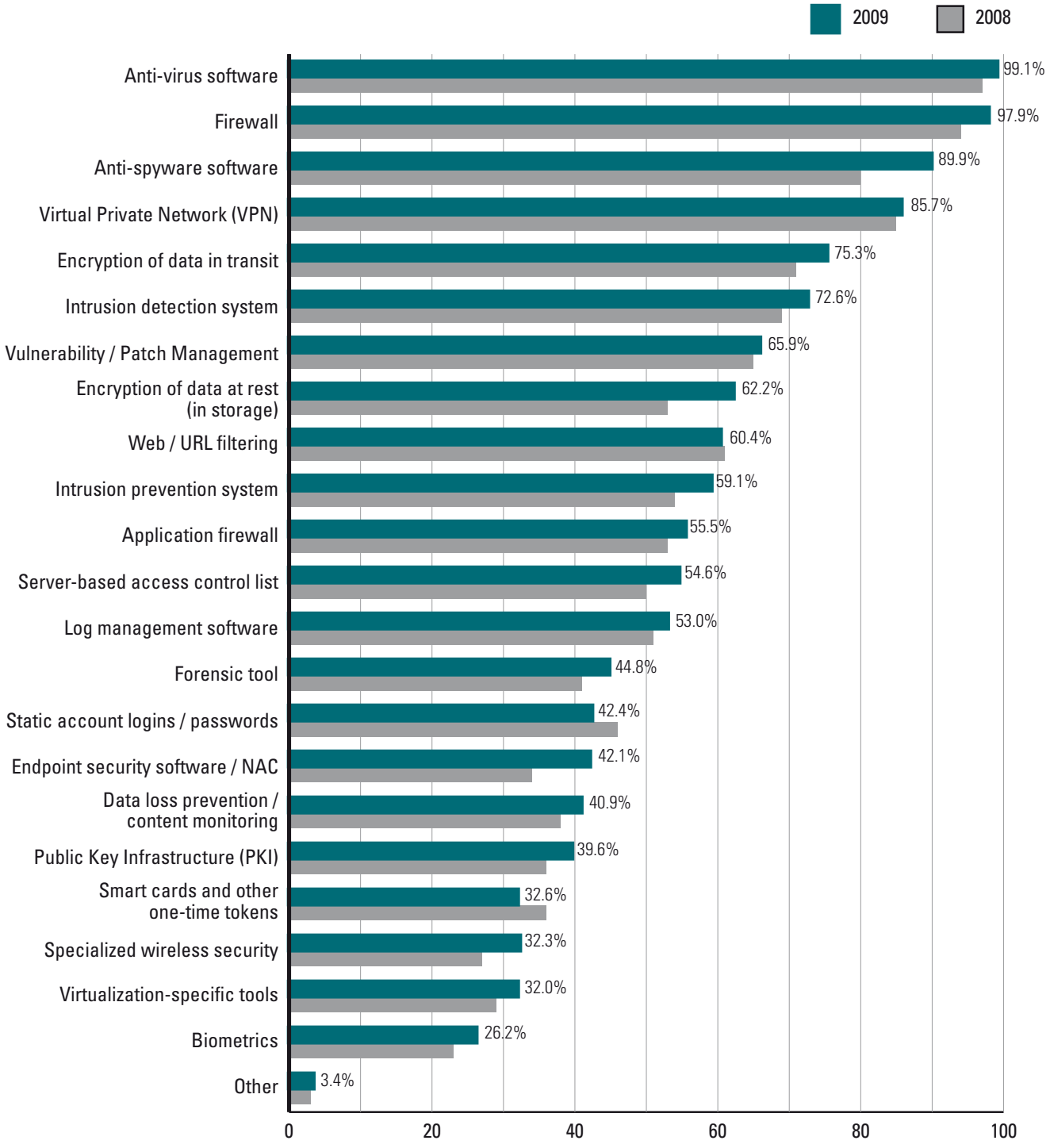
2009: 285 Respondents

It's also worth noting that one-third of respondents had to maintain compliance with international data privacy and security regulations.

Although compliance efforts create a lot of headaches for security professionals, most respondents told us that compliance requirements have had a positive effect on their organizations' security and security program. As the graph on page 28 shows, 65.6 percent of respondents said that their organization's security improved, 50.5 percent stated that regulatory compliance necessities pushed upper management to make security a higher business priority, 37.5 percent said that the security budget increased, 22.5 percent said that additional staff were hired and 44.2 percent said that new security technology was deployed. There were, however, 4.6 percent of respondents who stated that compliance efforts have damaged their organization's security.

Types of Security Technology Used

By Percent of Respondents



2009 CSI Computer Crime and Security Survey

2009 Respondents: 328

The fact that some respondents felt that compliance has had a negative effect on security is not surprising—in fact it's a bit surprising that there weren't a few more respondents who made this claim. In recent years many security professionals in the CSI community have begun moving from a traditional security program—the idea being to simply lock everything down—to a risk-based security program, in which the business may decide that while some risks to the business merit information security measures, other risks to the business may be deemed acceptable and thus not worth the investment in stricter security. Moving to a more risk-based approach, however, is a challenge in organizations that are heavily regulated, because security teams must try to balance the fluidity of risk management against the rigidity of compliance requirements. Further, "compliant" also does not necessarily mean "secure." Security professionals in the CSI community continue to tell us that upper management will agree to invest in whatever security measures are necessary to achieve compliance, but will not consent to invest in security past that.

The effects of increasing compliance requirements may be hinted at in the graph on page 29, which shows what types of security technology respondents used. Respondents reported notable increases in the use of 19 of the 22 technologies listed. One of the most significant increases was in the use of encryption of data in storage—whether it be in the form of individual file encryption or of whole-disk encryption of a hardware device. Encryption of data in storage is often perceived as a safe harbor or a "Get Out of Jail Free card" for organizations that experience data breaches, because in some cases these organizations will neither need to report the breach to the public nor incur penalties, as long as the breached data was encrypted. We first added the option of "encryption of data-at-rest" to this question in the 2006 Computer Crime and Security Survey. At that time, 48 percent of respondents said they used data-at-rest encryption. This number dropped marginally to 47 percent in 2007, inched up to 53 percent in the 2008 survey and jumped up this year to 62.2 percent.

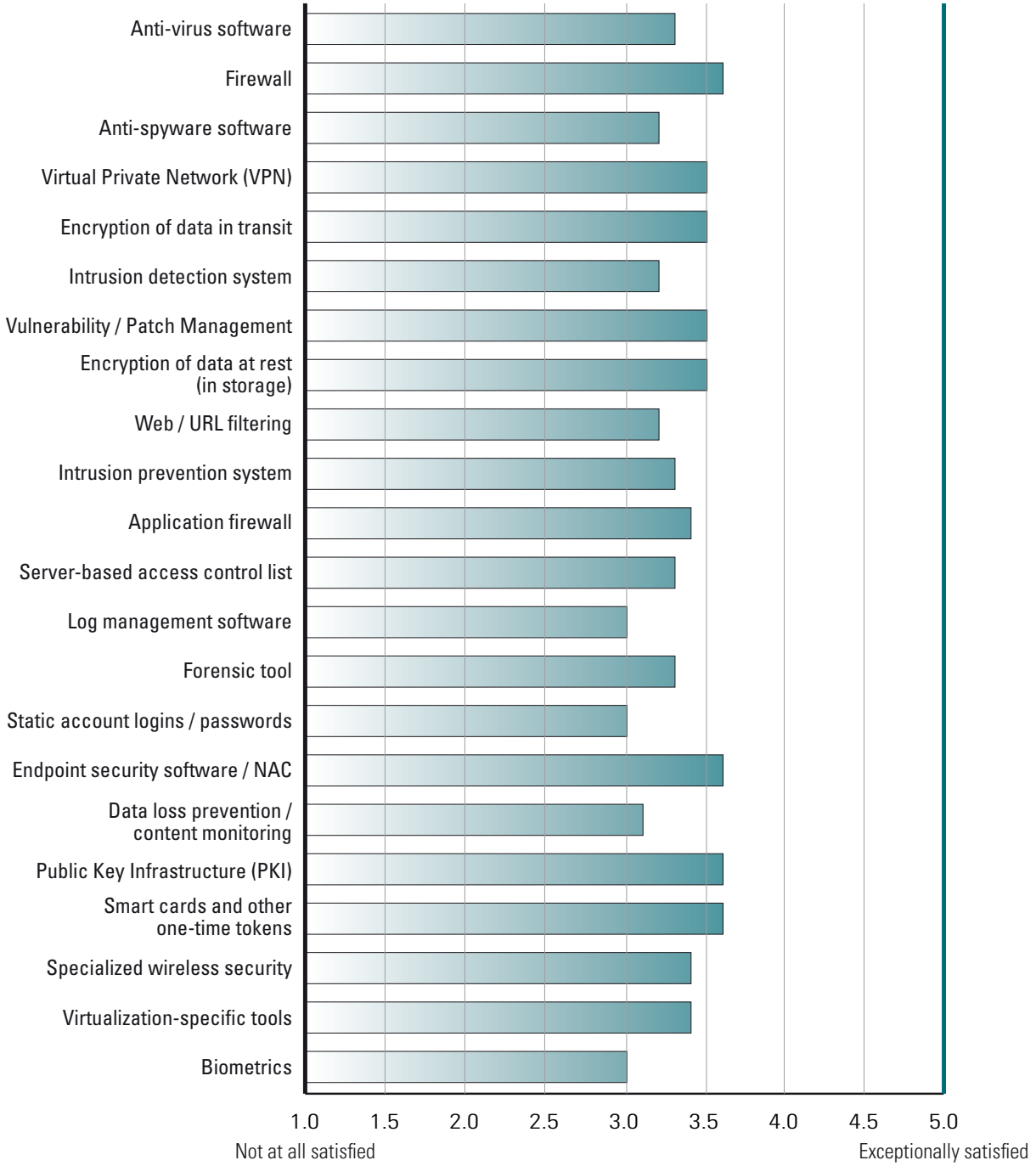
The use of anti-spyware software also made a big jump this year, from 80 percent of respondents to just about 90 percent (89.9 percent). The most-used technologies, however, continue to be anti-virus software (99.1 percent) and firewalls (97.9 percent).

One of the three technologies that dropped in usage was Web/URL filtering, but it is a change hardly worth mentioning—merely a shallow dip from 61 percent to 60.4 percent.

More interesting are the drops in static account logins / passwords (from 46 percent to 42.4 percent) and smartcards and other one-time tokens (from 36 percent from 32.6 percent). Although neither of these are drastic changes, it's worth noting that both are authentication technologies. Use of biometrics, another authentication technology, increased this year (from 23 percent to 26.2 percent), but it was still used less than any other technology (as it has since we added it to the survey). None of the identity and access management technologies listed (which also include server-based access control lists) made it anywhere near the top 10 most-used security technologies.

Satisfaction With Security Technology

On a scale of 1 to 5



2009 CSI Computer Crime and Security Survey

2009 Respondents: 243

For the first time, we asked respondents this year to rate their satisfaction with all of these security technologies—a rating of 1 meant "not at all satisfied," a rating of a 3 meant "satisfied" and a 5 meant "exceptionally satisfied." The figure on page 31 shows the average ratings earned by all the security technologies used. It also shows that, on average, respondents were satisfied with (though not exactly overwhelmed with admiration for) every single security technology listed; all scores ranged from 3.0 to 3.6. It should be noted too, that these middle-of-the-road averages aren't a result of polarization (lots of respondents giving a 5, lots of respondents giving a 1, thus averaging a 3). Rather, a strong majority of respondents rated each one of these technologies a 3.

The four highest-rated technologies (all earning a 3.6) are firewalls, endpoint security software (including NAC systems), Public Key Infrastructures (PKI) and smartcards and other one-time tokens. With the exception of firewalls, nowhere near half of respondents told us that they use these top-rated technologies.

The three lowest-rated technologies (all earning a 3.0) are static account logins and passwords, biometrics and log management software.

These results confirm some of CSI's suspicions that identity and access management continues to be a major weak spot in security programs, as does what we'll refer to as "visibility." By visibility we mean any systems that provide some indication of how secure an organization is at any moment, and foremost among those technologies is log management. These suspicions were further confirmed by the responses we received to an open-ended question we added to the survey this year: If you could wish for one security solution, product or service—either existing or imagined—what would it be?

The overwhelming response was that these "visibility" technologies—log management, security information and event management (SIEM) and security dashboards—were at the very top of respondents' wishlists. Further, respondents demanded that these tools show what is happening across an organization's entire environment, not just a few devices. Some of the specific answers included "a discovery tool that would gather data and report the overall security health of the organization," "decent, easy-to-use, centralized log management," "a reporting dashboard that builds a comprehensive profile of online activity used by various business units," "consolidated security incident management," "a logging standard so that all logs would be easily parsed and understood," and many instances of simply "SIEM" and "log management."

A strong second-place went to identity and access management technologies. Specific responses included "role-based access control," "cheap but effective strong authentication for Web sites that is not subject to man-in-the-middle attacks," "identity management regulated across all platforms and applications," "a single sign-on product that works," "mandatory biometric use," "something

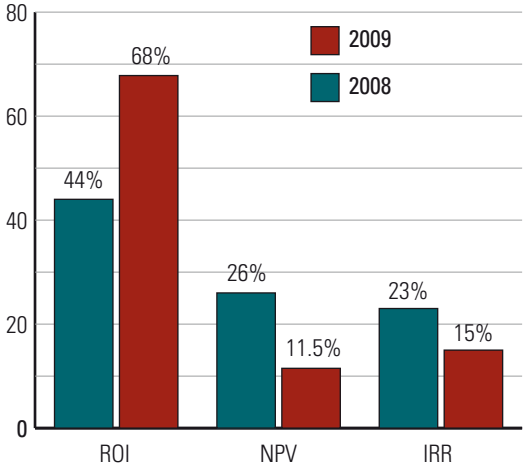
to completely replace the common password," "better multi-factor authentication solutions," "integrated ID management products that provide workflow, provisioning, RBAC and auditing/reporting."

A number of respondents also wished for better awareness training, better endpoint security, and better anti-malware tools.

Something that didn't make the list was an external insurance policy to help manage security risks. However, as the graph on page 32 shows, 32 percent of respondents already do have these policies.

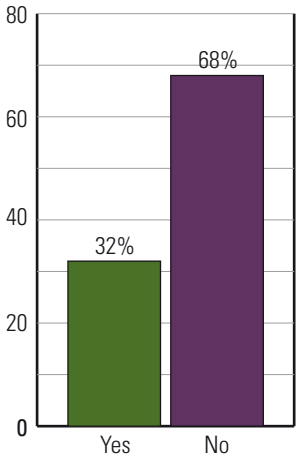
In fact security is often compared to insurance—something that everyone needs and hopes never to use. Security is seen as merely an expense, rather than something that supports the business, and for this reason security professionals have struggled to find a way to express security's value in business terms and financial terms. It has been generally believed that projects designed to increase an organization's information security will not automatically be approved by senior management without adequate economic justification. Hence, starting in 2004 a question was added to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the costs and benefits of computer

Percentage of Respondents Using ROI, NPV and IRR Metrics



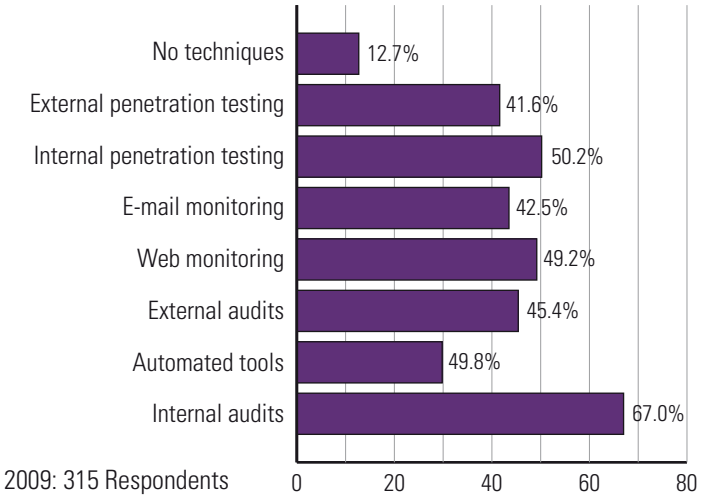
2009 Respondents: 227

Do You Have Any External Insurance Policies To Manage Cybersecurity Risks?



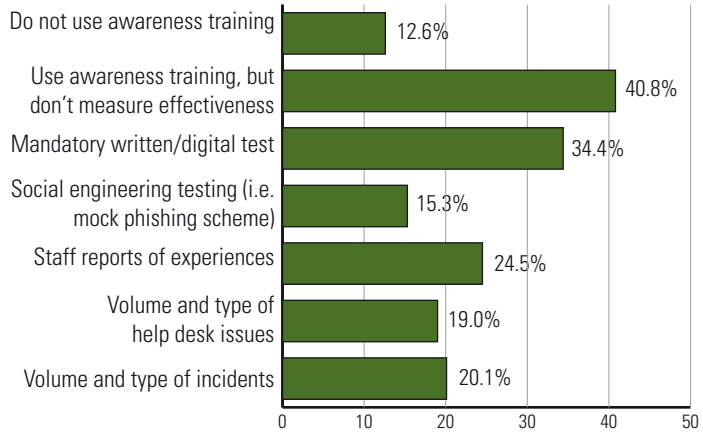
2009 Respondents: 316

Techniques Used to Evaluate Effectiveness of Information Security



2009: 315 Respondents

Techniques Used to Evaluate Effectiveness of Awareness Training



2009: 294 Respondents

security expenditures. For several years the percentages of respondents using these technologies were staying relatively stable: ROI hovered around 40 percent, NPV and IRR around 20 percent. This year, these numbers changed significantly all around. As the graph on page 33 shows, the use of ROI leapt from 44 percent of respondents in the 2008 survey to 68 percent this year. Meanwhile NPV fell well out of favor, dropping from 26 percent of respondents to 11.5 percent. IRR also took a dive, from 23 percent of respondents to only 15 percent.

Clearly ROI is most popular for communicating to upper management; but once outside of the board room, security professionals continue to question whether any of these metrics really work for security. Earlier this year security professionals Andy Willingham and Jack Daniel sparked an energetic discussion about metrics when they pondered whether "Failure on Investment" might be a better metric for security

than Return on Investment. What began as a tongue-in-cheek exchange grew into a lively, serious discussion, which unfortunately did not ultimately generate any brilliant new measurement tools.

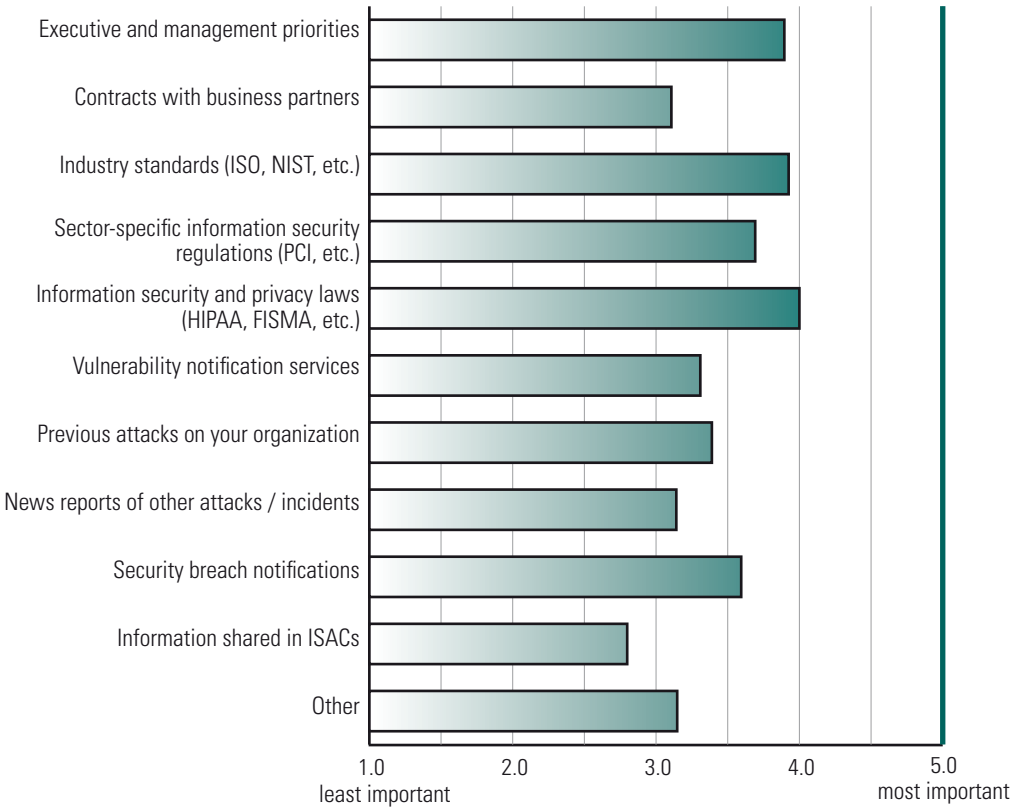
Not only are metrics troublesome when trying to communicate the success and value of security department to upper management, they're often difficult to communicate even to ourselves. The graphs on page 34 show what techniques respondents are using to measure the effectiveness of their information security and what techniques they're using to measure the effectiveness of their security awareness training, specifically. Even now, almost 13 percent of respondents don't use *any* techniques to evaluate the effectiveness of information security. However, since over 40 percent of respondents claimed to use each of the other seven techniques, it's clear that most respondents are using multiple methods to evaluate their information security. The most common method is internal auditing, which 67 percent of respondents said they used.

When it comes to end-user awareness training the results are less heartening. Not only did 40.8 percent of respondents state that they do not measure the effectiveness of their awareness training, but an additional 12.6 percent said they do not use any awareness training at all.

Finally, one last question was added to the survey this year to ascertain what sources of information make the biggest impact on organizations' security priorities and practices. This question was added as the result of a suggestion made by researchers Deirdre Mulligan, David Thaw and Aaron Burstein at the University of California at Berkeley's School of Information, the Berkeley Center for Law and Technology and Berkeley's Samuelson Law, Technology and Policy Clinic. Respondents were asked to rate how important various sources of information are, on a scale of 1 to 5, 1 being least important and 5 being most essential. As the graph on page 36 shows, security professionals are most heavily guided by information security and privacy laws like HIPAA and the Federal Information Security Management Act (FISMA)—these laws received an importance score of 4 out of 5. (Once again, compliance flexes its muscles.) Other information sources of high importance to respondents were industry standards—like those created by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO)—and the priorities of respondents' organization's executives. Information Sharing and Analysis Centers (ISACs) on the other hand were of lowest (but not exactly little) priority to respondents, scoring a 2.8 out of 5.

When Prioritizing Security Needs and Developing a Security Strategy, How Useful Are the Following Sources of Information?

On a scale of 1 to 5



2009 CSI Computer Crime and Security Survey

2009 Respondents: 298

Concluding Comments

The most important question for security professionals probably isn't "how much money are we losing," but rather "are our security measures working."

Based on the results of this survey and, for that matter, CSI surveys over the years, we think the answer is a cautious and conditional "yes." No matter how we look at our numbers, our security-savvy respondents seem to be suffering less than other organizations, and as respondents' use of security tools and techniques go up, their losses go down.

That said, security professionals are still in need of better tools to manage identities and get a clearer picture of what is happening on their networks, on their Web sites and at their endpoints at any given moment. For without that crucial information, how are they to know quite what security incidents they experienced? Sure, if organizations received a grievous wound they'd know, even if they didn't know right away; but will organizations know if a breach of their data caused thousands or millions of individuals grievous wounds? The slicker attackers become, the harder it may be to link one person's financial fraud to one organization's data breach.

Just as threats to businesses are threats to individual consumers, threats to consumers are threats to businesses. When asked to predict what security issues will be most critical to their organizations in 2010, several respondents expressed concerns about user-owned consumer devices—particularly smartphones—infiltrating business environments, without the proper enterprise security controls in place.

Respondents also expressed concerns about more business functions moving into the cloud, because cloud users will have to rely upon the cloud service providers to properly secure the data centers storing the users' data. Cloud users won't have control over—nor even knowledge of—how those resources are secured and they won't have access to the logs that are so crucial to proving compliance with data privacy regulations.

Perhaps "control" is something security professionals need to learn to live without, or at least learn to live with with less of. Businesses require agility, smartphones are one of the technologies that provide such agility, and if employees are willing to foot the bill, so much the better. Virtualization, cloud computing and mobile devices also provide businesses with agility and have the potential of saving them money. If data assets, the users who access them and the companies that own the devices on which they reside are going to become ever more widely distributed, then security professionals will need to adapt, and become, themselves, more agile.

How will the security industry fare against these new challenges? That's a question to be answered in the 2010 survey.

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. Many thanks as well to Dr. Larry Ponemon and Dean Turner for generously providing their expert perspectives. Thanks as well to Deirdre Mulligan, David Thaw and Aaron Burstein of the University of California at Berkeley School of Information, who consulted on the survey questionnaire and contributed the question on page 36 about sources of informarion.

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, e-mail csi@ubm.com, visit GoCSI.com, join our LinkedIn group, follow us on Twitter, or become a fan of CSI on Facebook.