CSI COMPUTER SECURITY INSTITUTE

15TH ANNUAL

# 2010/2011 COMPUTER CRIME AND SECURITY SURVEY

www.GoCSI.com

# Understanding the cyber threat is the first step in defending against it.

Cyber threats know no boundaries. In our heavily networked world, organizations across the globe are under attack 24/7/365.

General Dynamics has led cyber investigations on several of the largest network and data breaches in U.S. history. We understand that the interruption of operations, loss of data and customer confidence is only one cyber attack away.

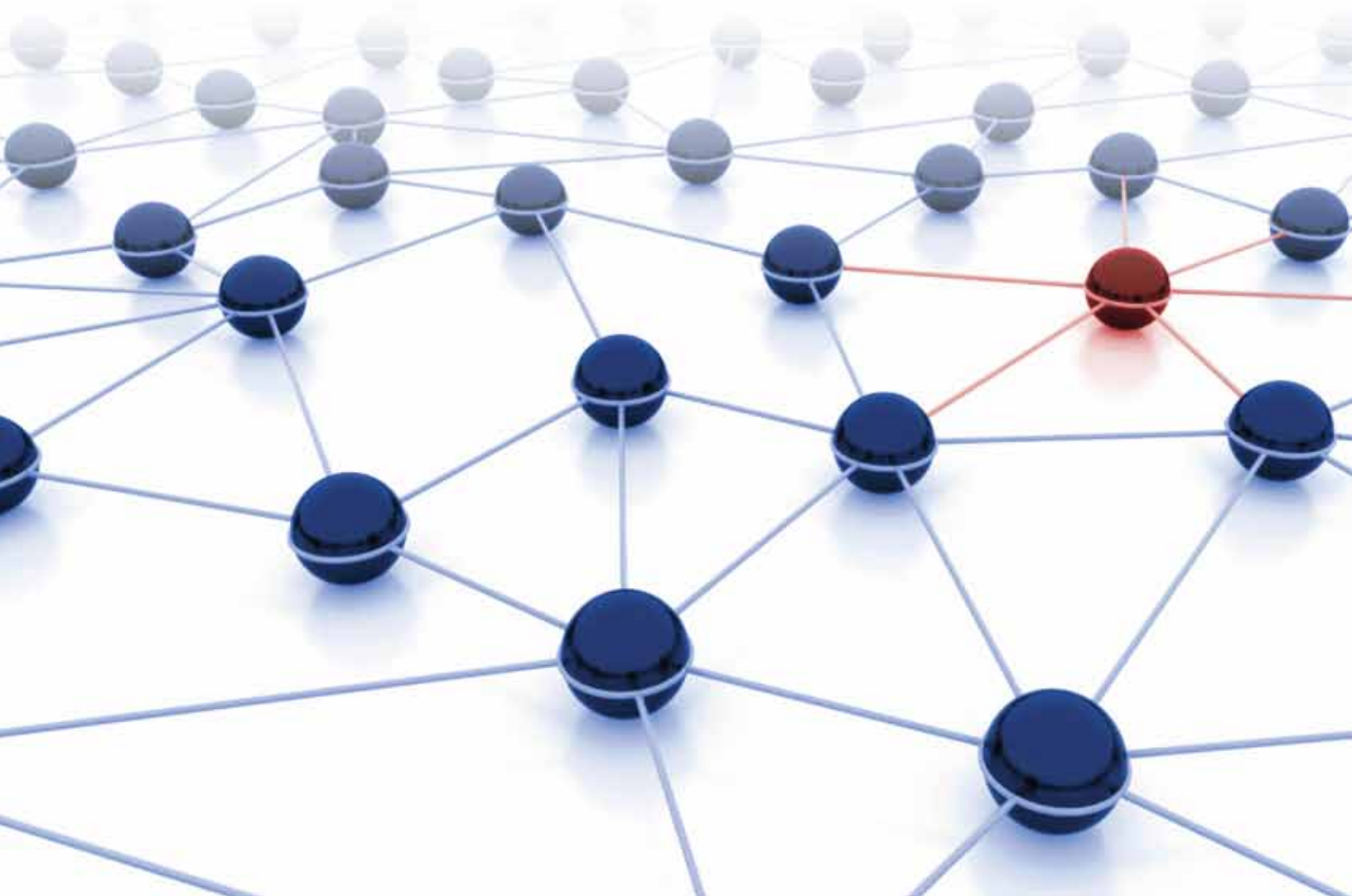
General Dynamics' corporate and Fortune 100 clients benefit from our incident response, digital forensics, and malware analysis experience gained by supporting US-CERT, the Department of Defense Cyber Crime Center, and the Intelligence Community.

We bring together experience and expertise to help you protect your enterprise.

---

**GENERAL DYNAMICS**
Advanced Information Systems

www.gd-ais.com



by Robert Richardson, CSI Director

# 2010 / 2011
# CSI Computer Crime and Security Survey

With this document, the CSI Survey achieves its fifteen-year mark. Both the aims and format of the survey continue to evolve. As you'll see in the findings that follow, many of the results reported by our respondents easily could have been predicted based on looking at results from the past several years. There has always been an almost surprising stability to answers about tools and methodology in this survey and this year is not an exception.

What is different, broadly speaking, is that there is considerably more context within which these results may be interpreted. There are a number of very good reports of various kinds now available on the Web. All of them that we're aware of, with the exception of this one, are either provided by vendors or are offered by analyst firms. That's not to say that there's anything wrong with these sources. A tremendous amount of useful information is offered in these various reports. But independent research seems fundamental and we believe the survey provides this.

Beginning last year, there were three important changes to this survey. The first was that a "Comprehensive" edition was offered, one of its key objectives being to attempt to take other report findings into account so that a proper context could be achieved. Additionally, the survey questionnaire added questions that attempted to determine not only what security technologies respondents used, but additionally how satisfied they are with those technologies. This year, we continue both with a more comprehensive report document but also with the questions regarding satisfaction with results.

As was the case last year, 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.

This lack of visibility into the severity of threats and the degree to which threats are effectively mitigated is a perennial problem in security and it presents problems for anyone trying to make sense of the state of information security. If respondents are unsure about what is happening on their networks, one could well argue, how can they possibly provide meaningful information on a survey questionnaire?

We would argue that, for typical security incidents, enterprise security departments have relatively reliable and accurate powers of observation. They generally know when one strain or another of a virus is making its way through their end-user population's computers. They know when money goes missing from key bank accounts. And even if their perceptions on some points aren't necessarily altogether accurate, having a gauge of the perceptions of security practitioners can be useful.

The respondents' concern about visibility into their networks has more to do with stealthier forms of data exfiltration and with newer, more complex attacks. Along with the respondents, we see plenty to worry about in this regard and will discuss it further at more than one point in this report.

Finally, 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.

## Key Findings

As was the case last year, this year's survey covered a midyear-to-midyear period, from July 2009 through June 2010.

- Malware infection continued to be the most commonly seen attack, with 67.1 percent of respondents reporting it.
- Respondents reported markedly fewer financial fraud incidents than in previous years, with only 8.7 percent saying they'd seen this type of incident during the covered period.
- Of the approximately half of respondents who experienced at least one security incident last year, fully 45.6 percent of them reported they'd been the subject of at least one targeted attack.
- Fewer respondents than ever are willing to share specific information about dollar losses they incurred. Given this result, the report this year does not share specific dollar figures concerning average losses per respondent. It would appear, however, that average losses are very likely down from prior years.
- Respondents said that regulatory compliance efforts have had a positive effect on their security programs.
- By and large, respondents did not believe that the activities of malicious insiders accounted for much of their losses due to cybercrime. 59.1 percent believe that no such losses were due to malicious insiders. Only 39.5 percent could say that none of their losses were due to non-malicious insider actions.
- Slightly over half (51.1 percent) of the group said that their organizations do not use cloud computing. Ten percent, however, say their organizations not only use cloud computing, but have deployed cloud-specific security tools.

## About the Respondents

As always, we note at the outset that this is an informal survey. All surveys of this sort have certain biases in their results. No exception here.

The survey was sent to 5412 security practitioners by post and by email, with a total of 351 surveys returned, yielding a 6.4 percent response rate. Assuming that the pool was properly representative of the larger pool of information security professionals and that those returning the form were in turn a random selection of the group, the number of returns would give us 95% confidence in our results with an approximately 5.25% margin of error. In other words, if we could magically find the right answer, then in 19 out of 20 cases it would be within 5.25 percent (either higher or lower) of the number you'll find here in the survey.

It's not quite that simple, of course. Remember that we began by assuming that the pool was representative and that the respondents were randomly chosen. Reality is seldom quite so well organized.

First and foremost, there is surely a skew among respondents 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. It's a sample of those with sufficient interest in security to be CSI members or to have attended a CSI paid event. 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, respondents fill out the questionnaire voluntarily, without any help from us. So one must reckon with the possibility that the respondents are self-selected based on some salient quality. 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?

All responses are submitted anonymously, which is done to encourage candor, but which also means that it is impossible to directly chase after those who have self-selected not to fill out the form. This anonymity furthermore 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.

All these caveats notwithstanding, it seems reasonable to assume that these results do represent a view of what engaged security professionals are seeing in the field. And while there are certainly limits to what should be assumed from longitudinal comparisons of the annual

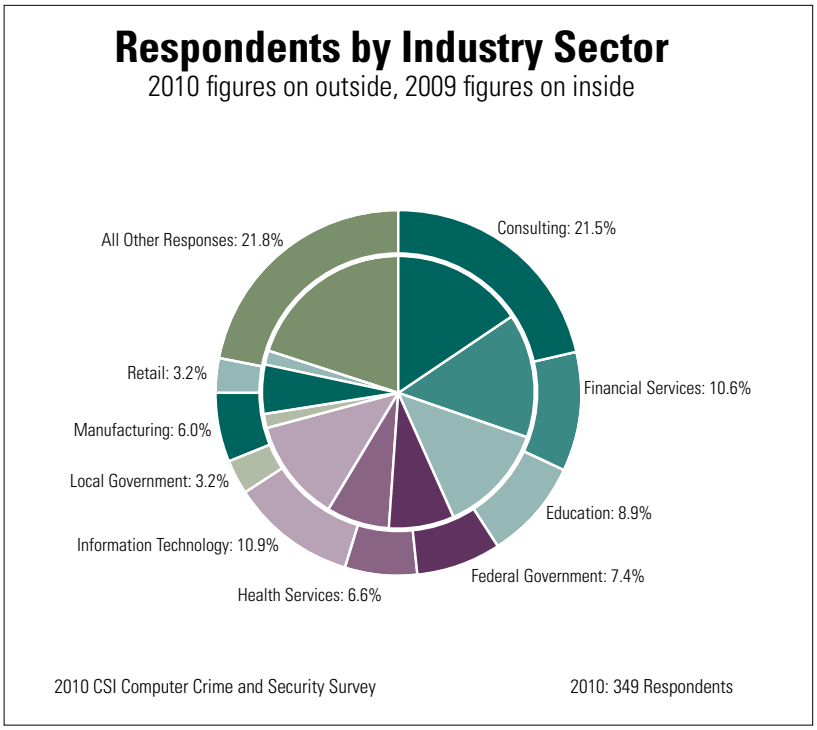



**Figure 1**

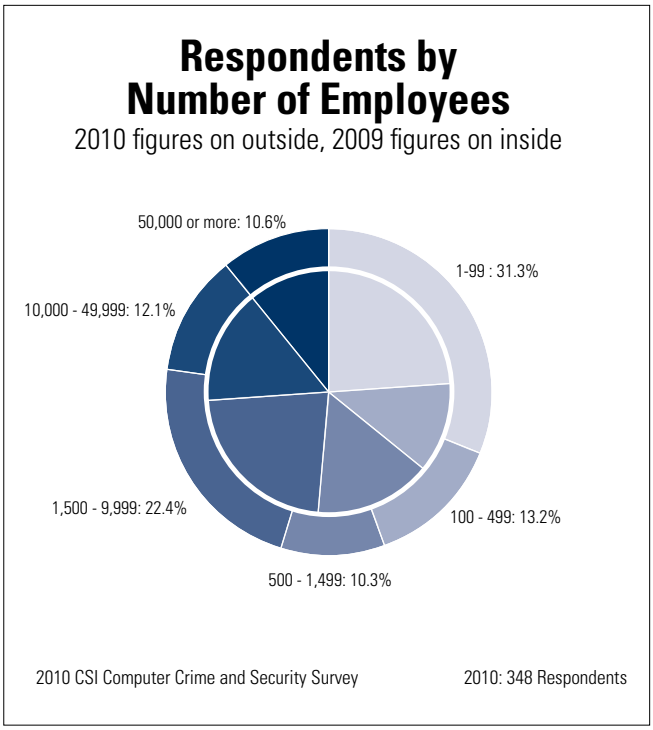



**Figure 2**

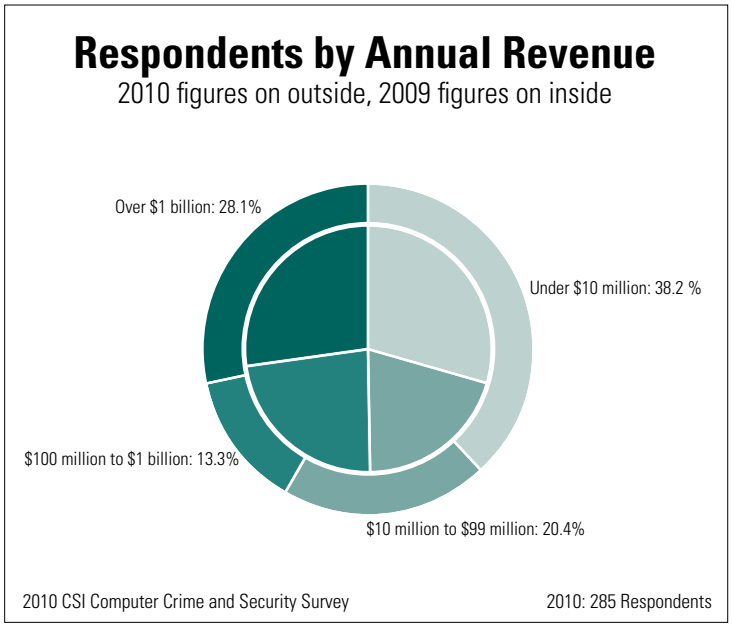



**Figure 3**

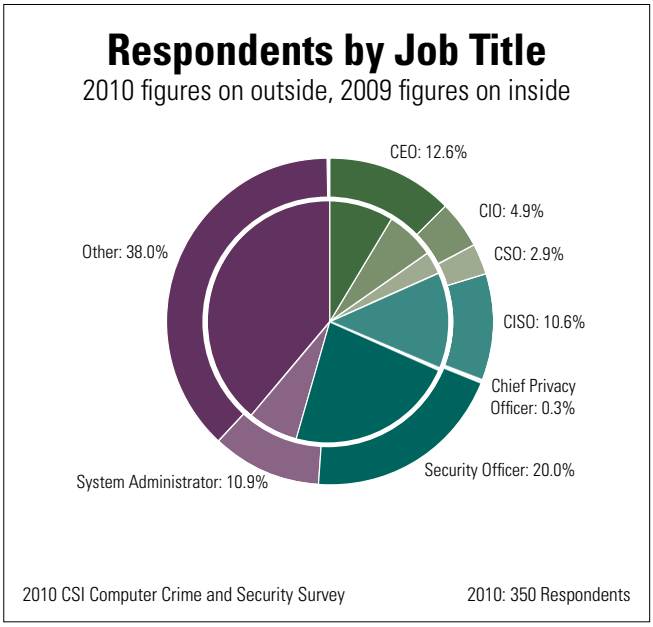



**Figure 4**

data sets, it's interesting to note that many of the baseline statistics from the survey remain remarkably consistent year over year, suggesting that the respondent group has a fair degree of consistency year over year.

As **Figure 1** shows, 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. What's less in line this year is the number of financial institutions reporting, a continued drop from last year. For several years, financial services made up the largest chunk of respondents, but last year finance (15 percent of respondents) was inched out by consulting (15.7 percent). This year financial services dropped to 10.6 percent of respondents, with consulting growing another five percent to 21.5 percent.

It's not clear why there would be such a precipitous drop in respondents from the financial sector. One might speculate that they are simply no longer willing to talk about their incidents. A Verizon study, to be discussed more thoroughly later in the report, cites the incredible statistic that 94 percent of the compromised data records tallied in their case library last year came from breaches in the financial services sector.

There is enough consistency to the key demographic breakdowns over time that it seems reasonable to make certain assumptions about trending, but it's important to bear in mind that any conclusions you draw based on the assumption that there's a longitudinal validity to the surveys over time is based on your judgment of similarity over time—there's nothing statistically provable about it.

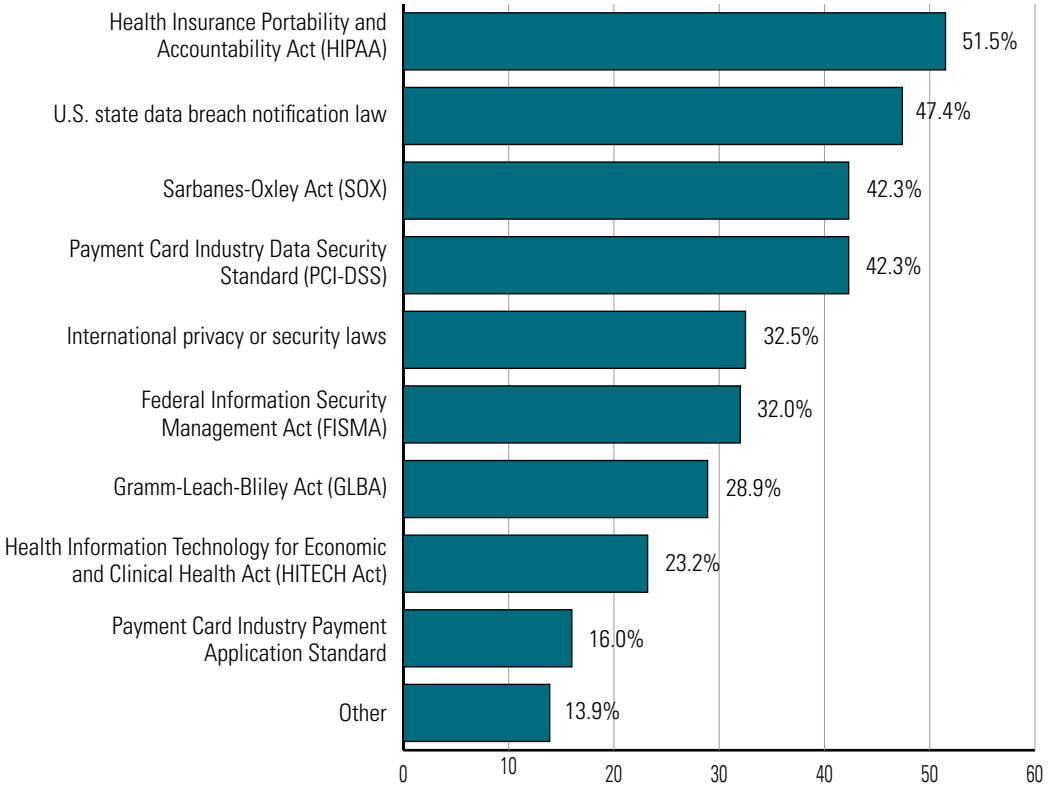
The CSI survey pool continues to lean toward respondents from large organizations (see **Figure 2**), but not quite so heavily as in past years. Still, the breakdown remains that, broadly speaking, organizations with 1,500 or more employees accounted for somewhat less than half of the respondents. Further, 42 percent of the respondents from commercial enterprises reported an annual revenue of $100 million or more (see **Figure 3**). This number has dropped over the past couple of years, perhaps as a result of the down economy. 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 (**Figure 4**). As the graph shows, 31 percent of the respondents are senior executives—chief executive officer (12.6 percent), chief information officer (4.9 percent), chief security officer (2.9 percent) and chief information security officer (10.6 percent). Last year these categories totalled 31.5 percent of respondents—again, the numbers 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 10.9 percent (up from 6.6 percent last year) of respondents, and 20 percent of respondents identified themselves as security officers. This left a sizable 38 percent of respondents (quite close to last year's 38.9) labeling themselves as "other." When examining the titles these "others" wrote in for themselves, one notes a wide diversity of titles, ranging from project leader to cyber security information analyst to GRC consultant. In past survey reports we

## Which Laws and Industry Regulations Apply to Your Organization?

By Percent of Respondents




2010 CSI Computer Crime and Security Survey

2010: 194 Respondents

**Figure 5**

have posited that the breadth of the titles, some clearly outside the realm of information technology entirely, might be evidence that the security function continues to expand into more business segments. And this may well be true. But it also seems plausible that this reflects the lack of consensus within the business world on the organizational locus of the security function.

"Others" aside, it is clear that at least 51 percent of respondents (C-level 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.

Beginning last year, we asked respondents to tell us which laws and industry regulations applied to their respective organizations (**Figure 5**). The numbers are fairly similar to last year's, which again suggests a certain year-over-year continuity in the respondent group. This is particularly interesting when you consider that some of these answers suggest that respondents may not realize (or perhaps simply don't acknowledge) that they are beholden to certain laws. Given that the survey applies exclusively to the United States and that there are (at time of writing) 46 states with breach notification requirements, it's hard to imagine that most businesses don't fall within the scope of these laws. Yet only 47.4 percent of respondents claim they are affected.

How can that be? Well, one thing to consider is that many of these laws are, arguably, a bit sloppy in what they define as a breach that requires notification. The original California law, on which many other state laws are based, referred to customer records. Thus, some non-profits, educational institutions, and health care facilities who may not feel that they have "customers" *per se*. Government organizations may also believe themselves outside the scope of these laws. Exactly why the number isn't higher is impossible to say with certainty, but it's fairly remarkable that less than half of respondents say that breach notification laws apply to them.

Equally remarkable—and it was striking last year as well—is the percentage of respondents who say that the Health Insurance Portability and Accountability Act (HIPAA) applies to their organization. This even though only 6.6 percent of respondents identified their organizations as being in the health care sector. As most readers will already know, HIPAA applies to any organization that interacts with data that has been previously identified as HIPAA-protected data. So an insurance company storing information about medical policy claims would fall under HIPAA, as would the accounting company to which they outsource customer billing data. The tendrils of HIPAA, alongside all the other legislative acts in the security world, spread farthest.

We leave for consideration later in the survey whether the pressure asserted by these various laws and regulations has had either a positive or a desultory effect on the actual security.

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. One study from the Ponemon Institute (sponsored by PGP Corporation) examined the costs incurred by 45 organizations that had experienced data breaches resulting in the loss of between 5000 and 101,000 records. As Dr. Larry Ponemon, chairman and founder of the Ponemon Institute explained to us in last year's CSI Survey report, the Institute 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 15 different industry sectors—the most heavily represented industry sectors were financial services and retail, with eight breaches each. Ponemon also told us that the Institute's report is best viewed as a synthesis of case studies of confirmed data breaches, as opposed to a more sweeping survey.

Verizon Business' Data Breach Investigations Report (DBIR), now in its third installment, looks at a growing library of cases ranging from 2004 to the present. This year, for the first time, the DBIR also incorporates a case database obtained from the U.S. Secret Service, which is listed as a co-sponsor of the report. Perhaps the most salient feature of the demographics here is that the entire sample comes from organizations that have suffered major data breaches. Given that banks are where the money is, it's not surprising to learn that the case load heavily tilts toward financial institutions, with 33 percent of cases, followed by 23 percent in the hospitality industry. That over half of the cases come from just two industries, though, may well seem problematic if one is trying to get a sense of the general level and nature of threat to enterprise network.

Also worth nothing in passing is that some of the cases in the DBIR database (specifically, from Verizon's case load) are from outside the U.S., and therefore outside the scope of the CSI Survey.

Other reports worth considering alongside the CSI report take a more machine-generated approach to the data, using sensors of various types to capture information about the data traversing networks and the configuration of all sorts of Internet-connected devices. One example of this sort of report is the MessageLabs Intelligence report, issued monthly by Symantec subsidiary MessageLabs. In this report, the primary data comes from mail traffic filtering that the company's services provide. Generally, this sort of report has the virtue of being highly accurate. When the report tells us that 87.5 percent of the mail traffic it handled in October was spam and that this was a 4.2 percent decrease from September, it is likely that these numbers may be taken at face value. The 4.2 percent decrease is not plus or minus some amount, rather there were some exact number of mail pieces fewer that amounted to an exactly 4.2 percent drop. This sort of exactitude isn't everything, though. Definitions such as what counts as spam can be highly significant—how does MessageLabs know that what it didn't count as spam really wasn't spam? And the interpretations of these numbers is what really counts in day-to-day provision of security. Perhaps it doesn't matter that so much spam gets sent because it is benign, for instance.

In any case, demographics don't drop entirely out of the picture in these "packet count" sorts of reports—it can matter whether a report is based disproportionately on monitoring a single industry segment—but they are less of a concern than is the case with survey response research projects.

In one way or another, nearly all of these surveys point to drops in the incidence of cybercrime. This may well not be consistent with your overall sense of what tech news sources are telling you, but it's also undeniably true that in recent years the "independent" news coverage found at technology media sites on the Web has gotten a narrower lens through which to view the world. Indeed, typical news sites are increasingly reliant on source information supplied by, on the one hand, vendors who stand to benefit from creating new concerns, and on the other, by vulnerability researchers who can best buff up their reputations by demonstrating particularly unexpected and potentially ferocious attacks. This doesn't mean that the news has become "untrue," but it does mean that the stories that fill the tech-media news well are predominantly reports that show huge percentage increases (because they are increases over small initial starting points) and news of vulnerabilities that must be cast as dangerous if they are to be taken seriously.

For an example of an "interpretive statistics" news story, consider *PandaLabs: 40 Percent Of All Total Fake Antivirus Strains Were Created In 2010*, which most readers would take to mean that nearly as many strains were written in 2010 than had been written over all time. As far as it goes, it's even true, it's just that fake antivirus strains only became a widely seen threat in 2008. So there are only two prior years, which one might distribute something like 25% in 2008, 35% in 2009, and 40% in 2010. Which of course shows some growth, but not as much as the significant drop, to take one example, shown in this CSI survey in denial of service attacks. Panda's results show that 5.4 percent of all PCs compromised in 2010 were compromised by fake anti-virus software. Even if it were 5.4 percent of all PCs (which it isn't), that would still track well below the 16.8 percent of enterprises that reported denial of service attacks. Particularly from an enterprise security perspective (given that fake anti-virus incidents usually victimize consumers), an increase in something on the order of 5 percent of a not particularly significant attack isn't really much more than a blip.

As for reporting on the findings of security researchers, consider the CNET story that led with news that "a startling percentage of the world's automated teller machines are vulnerable to physical and remote attacks that can steal administrative passwords and personal identification numbers to say nothing of huge amounts of cash." This is not to say that Barnaby Jack's demonstration at the 2010 Black Hat conference wasn't newsworthy—it was a dramatic demonstration of the truism that a determined and capable attacker will find his way through most defenses. It seems equally significant, though, that there are no reported instances of these types of attacks in the wild. Meanwhile, of course, ATMs in situ are attacked on a daily basis using considerably more bare-fisted approaches such as ripping them out of walls and blowing up their internal safes using improvised explosives (to mixed results, one hastens to add, ranging from a rainstorm of money to accidental death—see atmsecurity.com for more). Given that Jack reported elsewhere that he

spent a couple of years studying ATM machines he's purchased and that he's a top-rank security researcher, this approach can hardly be at the top of a typical ATM owner's threat model. Again, from the enterprise security point of view, this was very close to not really being relevant (not even to banks, as the kinds of ATM machines that Jack set his sights on are those used predominantly by independent operators).

The problem that faces the security community right now is not that the current news isn't fairly good—we would argue that in fact it is—but that the advanced attacks we don't see much of right now, should they become prevalent, will render many of our defenses moot.

## The Past Year: Moving to War Footing

The scope of this survey remains narrowly focused on what happens within enterprise networks, but the one-year period covered by the survey is one in which the broader context definitely matters. There isn't room for a detailed recounting of major cybersecurity events, but a few highlights bear mentioning.

- The **Aurora** attacks, which began in mid-2009 and continued through December 2009, made history in part because they were made public. The attacks were disclosed by Google in a blog post that appeared in mid-January 2010. The attacks, we learned, had successfully targeted dozens of organizations, including (we now know) Adobe Systems, Juniper Networks, and Rackspace. Media reports have claimed that Yahoo, Symantec, Northrop Grumman, and Dow Chemical were among other targets. This was viewed within the security community (and not wrongly) as something of the ultimate proof that so-called "Advanced Persistent Threat (APT)" attacks were real.

- Close on the heels of Aurora going public, a simulation exercise in which a working group of high-ranking former White House, Cabinet and national security officials came together to advise the President as the nation was (theoretically) undergoing a cyber attack. Called **Cyber Shockwave**, the exercise was aired nationally in mid-February by CNN. What was principally made clear through the event was that there was nothing much in the way of policy or law that the government would be able to draw on should an actual cyber attack occur.

- March saw the **sentencing of Albert Gonzalez**, who had previously pleaded guilty to the combined theft and subsequent reselling of more than 170 million credit and ATM cards and from 2005 through 2007, not only the biggest such fraud case in history but also including some of the most widely publicized data breaches, including Heartland Payment Systems and TJX. It seems clear that this successful prosecution (Gonzalez was sentenced to two concurrent twenty-year terms) had a chilling effect on the criminal community. We also note in passing that his initial entree into these companies was via SQL injection, one of the simplest sorts of application-layer attacks and one that continues to be a major source of problems.

- The **United States Cyber Command** (USCYBERCOM) was stood up in May as a direct subordinate to the U.S. Strategic Command. It's not the first military unit to have responsibilities related to information security, not a by good stretch, but it's perhaps the most significant expression and the one that has most openly admitted its development of offensive strategies.
- If the Aurora attacks gave some substance to "APT" as a term, June 2010 saw a full-throated example of what this sort of attack could look like in the form of **Stuxnet**, which used multiple zero-day vulnerabilities, targeted SCADA industrial control systems, and specifically targeted nuclear facilities in Iran. In almost every way, this was an advanced example of an attack that was very carefully targeted.

Generally, it was a year in which data breaches made fewer headlines (possibly as a result of the Gonzalez prosecution) and the tropes used in discussing computer security changed from the realm of law enforcement to that of the military theater of operations.

## A Layered Model

A key section of the CSI survey is that in which respondents are asked about attacks they've seen over the course of the year. In discussing attacks, the key components for managing a security program are the likelihood and the likely impact of an attack. One has to think about the relative importance of dealing with one sort of threat over another, and for that it is hugely helpful to have a sense of what other organizations are encountering.

On an average day, most respondents to this survey were ***not*** dealing with a significant security issue. In fact, half of them (49.6 percent—see **Figure 6**) didn't encounter an incident over the entire course of the one-year period covered by the survey. Anyone with hands-on experience knows that this is emphatically not because half of them weren't threatened. There were threats of many kinds and with a range of possible consequences, but generally these can be boiled down to

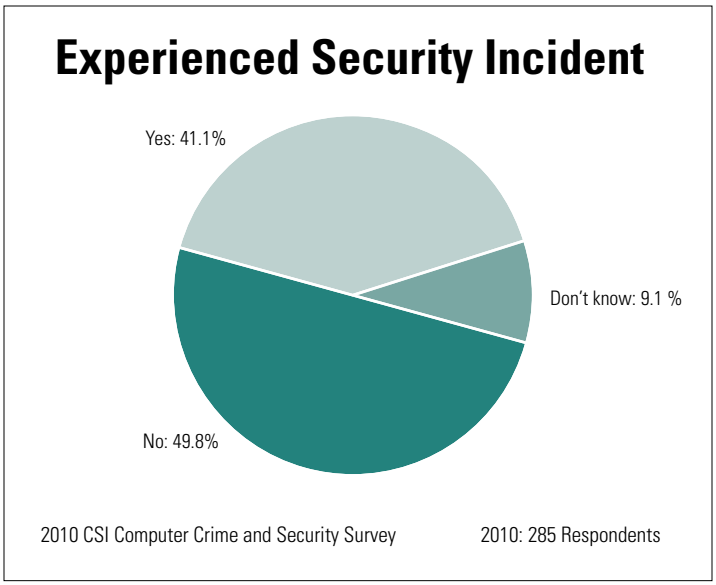



**Figure 6**

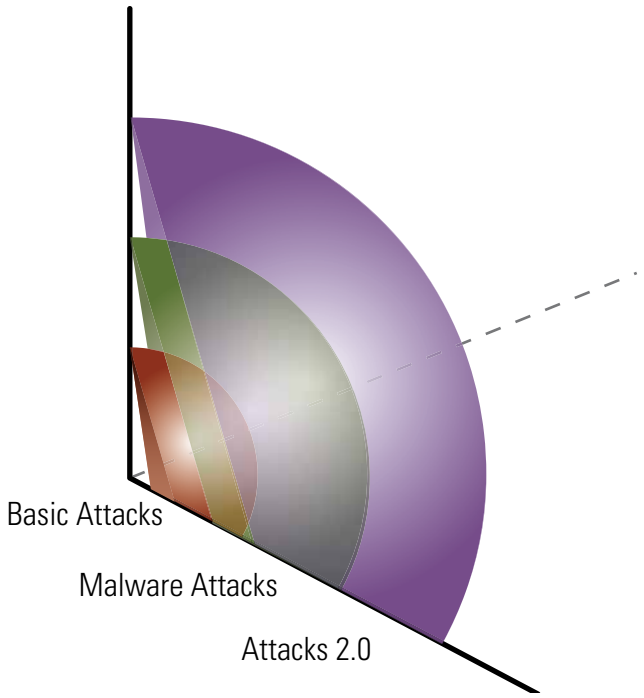



**Figure 7**

a few significant themes that have a great many variations. As we see it, these themes form what might be called three axes of a continuum of attacks, with one axis being whether the attack is purely opportunistic or is aimed at a single target, and another being an axis running from no-skill-required cookie-cutter attacks (such as carpet-bombing Nigerian scam emails) to sophisticated attacks using multiple zero-day vulnerabilities and the like. A third axis considers the spectrum between trying to do harm to an organization as opposed to attacks aimed at stealing something of value (whether money or missile launch codes).

A three-axis model is overly simple, to be sure, but it has at least two virtues. First is that it provides convenient groupings along the axes when considering the most salient features of various attack methods. Opportunistic versus targeted is a useful way to think about phishing versus spearphishing, for example. But beyond that, one notices that dividing the conceptual space into three "shells" that correspond to points that lay in the same region on each axis creates a layered model of attack that fits well with the insights emanating from this report as well as the other reports we've looked at (**Figure 7**).

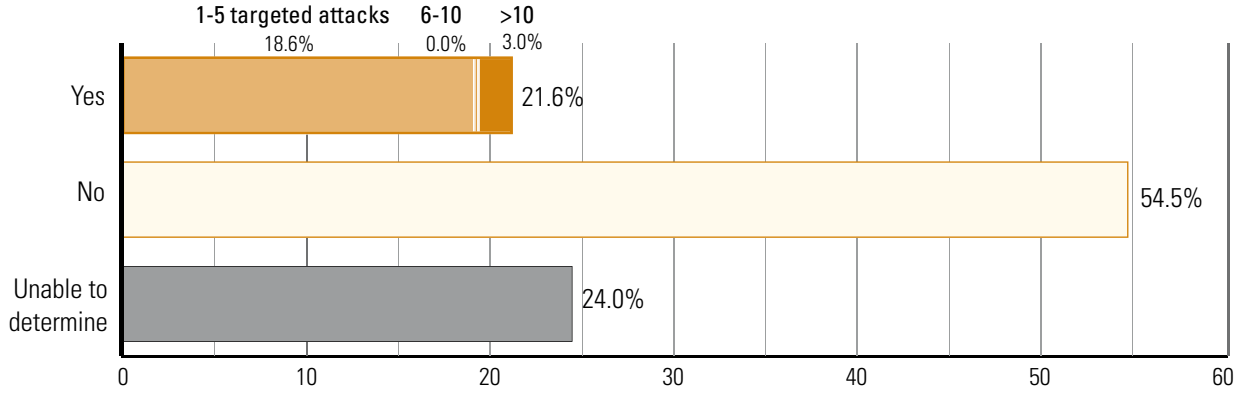
The inner shell, which one can think of as a basic core of unelaborated attack vectors, comprises basic attacks—phishing, rudimentary port scans, brute force attacks on password-protected accounts, and old-school viruses. That they are simple in no way implies that they don't do plenty of damage. In fact, in many cases they are as much about causing harm as anything else. They are akin to smash-and-grab attacks on retail storefronts. Every organization is exposed to this shell's attacks on a day-in, day-out basis. Broadly speaking, a properly protected organization will not view these as more than a nuisance. They may very well, in fact, be able to repel them altogether.

The middle shell, a layer of extended versions of prior attacks, is the realm of malware created from generation and customization toolkits, of phishing attacks that use real names known to a class of intended victims in order to improve the credibility of the scam, and of tools that scan for unpatched systems with known vulnerabilities. In our view, most intentional insider crimes fall into this category as well (one might argue that we're stretching things a bit here, given that insider attacks are of course targeted on a single organization, but case studies suggest that many insiders are attacking their employers simply because that's where they have access). Here one could generalize by saying that an effort to deal with these middle shell attacks by adding increasing sophistication to the inner shell tools has met with only middling success. Heuristic approaches added to virus scanning products, for instance, failed when NSS Labs conducted a test several weeks after the Aurora attacks were announced (the overall Aurora attacks showed unusual sophistication, but purely where malware detection is concerned, it was a matter of existing tools not keeping up with the threat).

The outermost sphere, what might be called an Attack 2.0 layer, is roughly that of the Advanced Persistent Threats, as many are now calling them. There's continued 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.

How significant is this Attack 2.0 shell? We'll have more to say on the subject, but consider for a moment just the matter of attacks being increasingly targeted. Twenty-two percent of CSI survey respondents told us (**Figure 8**) that at least some of their security incidents involved targeted attacks—3 percent told us they experienced more than 10 targeted attacks. Targeted isn't the

## Did Any of These Security Incidents Involve Targeted Attacks?




2010 CSI Computer Crime and Security Survey

2010: 167 Respondents

**Figure 8**

whole story when it comes to sophisticated attacks, but it's a defining one. And 22 percent isn't any kind of majority, but it's a strong indication that this kind of attack has become more than a theoretical discussion point.

Our larger point here is that the news about security is different depending on which shell or layer you're examining. At the core layer, the news is good. Attacks persist, but they are largely rebuked. At the extended layer, we are in an arms race where we're holding our own, but struggling against the inventiveness of the criminal element. Each extension in, say, the ability of rootkits to avoid detection, has to be met with equal inventiveness. The boundary between the extended level and the outer, Attack 2.0 level, is blurry. Part of what makes an attack rise to the outer boundaries of being targeted, of being sophisticated, and so on, is that multiple elements are combined in unexpected and highly effective ways. The buzzword for this Advanced Persistent Threat. It's as loosely defined a category as you could hope for, but what gives it a certain validity is precisely this—that it combines vectors and tactics in ways that feel qualitatively different. This kind of attack is by no means uniquely associated with Web applications, but Web applications do seem to be a particularly fruitful target for attacks that migrate from the extended middle layer out to the outermost shell. If we ask what the news looks like when considering this level and when considering the current state of Web development and vulnerability, the news is discouraging.

## Attacks and Losses

The CSI Survey has always asked respondents about the 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.

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

Two years ago we added four new categories to cover various aspects of data breach: 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. Last year we made a clarification: instead of "customer data" we specified "personally identifiable information (PII) or personal health information (PHI)." This change was made, as one would expect, because what we were truly interested in were the breaches of data that would be covered by privacy regulations.

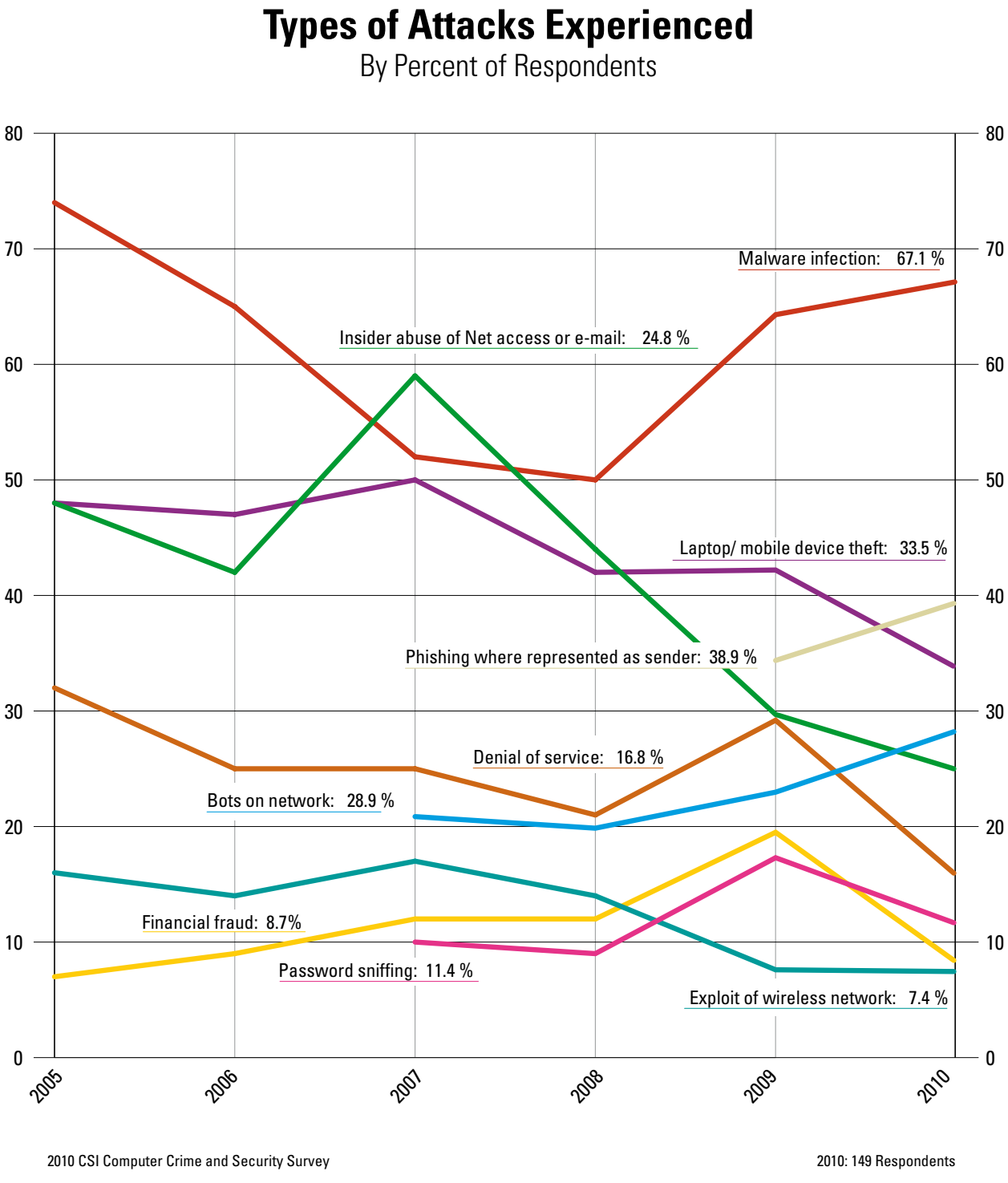

Types of Attacks Experienced
By Percent of Respondents
80
70
60
50
40
30
20
10
0
2005
2006
2007
2008
2009
2010
Malware infection: 67.1 %
Insider abuse of Net access or e-mail: 24.8 %
Laptop/ mobile device theft: 33.5 %
Phishing where represented as sender: 38.9 %
Denial of service: 16.8 %
Bots on network: 28.9 %
Financial fraud: 8.7%
Password sniffing: 11.4 %
Exploit of wireless network: 7.4 %
2010 CSI Computer Crime and Security Survey
2010: 149 Respondents

**Figure 9**

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."

Generally, we've held the same field of attack types over a long period of time. Historically, virus (more lately subsumed under the rubric of malware) attacks have topped the list, in recent years closely seconded or event beaten out by theft of laptop or mobile device. These two categories remain "winners" this year, but only malware is on the rise, respondents say. Indeed, while malware edged up a few points, laptop/mobile theft dropped a impressive 9 percent.

Indeed, the overall impression of **Figure 9** is that of threats being less often seen than in prior years. Yes, there are bounces up in some categories, but those that saw a bump last year have largely dropped to levels lower than the year before. **Figure 10** shows all of the categories we currently track.

It's difficult to attribute direct causes to these sorts of drops. But it seems undeniable that, with the exception of malware attacks, our respondents are seeing fewer incidents. It's important to realize, furthermore, that this is not limited to CSI's results. Symantec's reports are, in our opinion, never altogether forthright in their discussion when the numbers are headed down, but their reports nevertheless confirm at least one important downward trend. Their measurement of the median number of active bot-infected computers worldwide has dropped from a peak of more than 100,000 per day in early 2008 to approximately 50,000 per day at the close of 2009.

Symantec points out a few non-benign reasons that might account for the decrease, primarily hinging on the idea that the bot software is becoming more sophisticated and that therefore fewer bots are required. There's no question that bots are more complex now than a couple of years ago, so there's probably something to this, but we think it's not entirely unreasonable to think that organizations—in part by using the protections offered by companies such as Symantec—have met with some measure of success in detecting and eliminating this rogue software within their networks.

Where data breaches are concerned, the Verizon report strongly supports the notion that such events are down. For starters, Verizon had a lower caseload of confirmed breach cases last year. Additionally, as the report notes, when looking at available measures of cybercrime:

> One of them, public breach disclosures, fell noticeably in 2009. Organizations that track disclosed breaches like DataLossDB and the Identity Theft Resource Center reported figures that were well off 2008 totals. Private presentations and hallway conversation with many in the know suggested similar findings. (Verizon, p. 6)

We can't help but comment that the Symantec contains a full discussion of breach statistics drawn directly from these same public sources and somehow never quite manages to mention that the overall numbers have dropped.

# Types of Attacks Experienced

By Percent of Respondents

| Type of Attack | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Malware infection | 74% | 65% | 52% | 50% | 64% | 67% |
| Bots / zombies within the organization | added in 2007 | | 21% | 20% | 23% | 29% |
| Being fraudulently represented as sender of phishing messages | added in 2007 | | 26% | 31% | 34% | 39% |
| Password sniffing | added in 2007 | | 10% | 9% | 17% | 12% |
| Financial fraud | 7% | 9% | 12% | 12% | 20% | 9% |
| Denial of service | 32% | 25% | 25% | 21% | 29% | 17% |
| Extortion or blackmail associated with threat of attack or release of stolen data | option added in 2009 | | | | 3% | 1% |
| Web site defacement | 5% | 6% | 10% | 6% | 14% | 7% |
| Other exploit of public-facing Web site | option altered in 2009 | | | | 6% | 7% |
| Exploit of wireless network | 16% | 14% | 17% | 14% | 8% | 7% |
| Exploit of DNS server | added in 2007 | | 6% | 8% | 7% | 2% |
| Exploit of client Web browser | option added in 2009 | | | | 11% | 10% |
| Exploit of user's social network profile | option added in 2009 | | | | 7% | 5% |
| Instant messaging abuse | added in 2007 | | 25% | 21% | 8% | 5% |
| Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.) | 48% | 42% | 59% | 44% | 30% | 25% |
| Unauthorized access or privilege escalation by insider | option altered in 2009 | | | | 15% | 13% |
| System penetration by outsider | option altered in 2009 | | | | 14% | 11% |
| Laptop or mobile hardware theft or loss | 48% | 47% | 50% | 42% | 42% | 34% |
| Theft of or unauthorized access to PII or PHI due to mobile device theft/loss | option added in 2008 | | | 8% | 6% | 5% |
| Theft of or unauthorized access to intellectual property due to mobile device theft/loss | option added in 2008 | | | 4% | 6% | 5% |
| Theft of or unauthorized access to PII or PHI due to all other causes | option added in 2008 | | | 8% | 10% | 11% |
| Theft of or unauthorized access to intellectual property due to all other causes | option added in 2008 | | | 5% | 8% | 5% |
| 2010 CSI Computer Crime and Security Survey | | | | | | 2010: 149 Respondents |

**Figure 10**

The Ponemon report that looks at the U.S. cost of a data breach only looks at a certain range of companies that definitely had a data breach, so it's not well suited to determining whether overall data breaches are up or down. One very interesting finding from that report, however, is that malicious (as opposed to accidental) data losses increased markedly (from 12 percent of the sample group to 24 percent), which does suggest a greater criminal effort to steal data records. Note that it *doesn't* suggest that criminal activity rose (or fell, for that matter), because it's a sample only of breached companies that opted to participate in the survey. It seems likely from other data sources that Ponemon had fewer breached companies to choose from overall.

Whereas last year saw a jump in financial fraud from 12 percent to 19.5 percent, this year saw the number drop again, a drop all the way down to 8.7 percent. Even though not all participants choose to answer this question on the survey and the sample size for that specific question therefore drops, this drop is large enough that it's reasonable to believe that the drop is a statistically significant one.

One other general area we think it's important to keep a close eye on is that of "Web 2.0." There are lots of definitions of the term and we're not trying to work with a precise definition. We're simply referring to the wave of movement toward placing increasingly sophisticated browser-based applications into service within U.S. enterprises. Thus the IT world has seen a lot of focus on creating customer-facing Web applications, a trend that seems certain to continue. And with this shift comes a shift toward exploits specifically targeted at Web applications.

Within our own statistics, we didn't see much movement this year. Web site defacement actually dropped from 14 percent last year to 6.7 percent this year. Our option for all other exploits of public-facing Web sites ticked up a point from 6 to 7.4 percent. Exploit of client Web browsers ticked down, by contrast, from 11 percent to 10.1 percent.

None of these numbers are large when set alongside malware, but the degree to which vulnerabilities are being found and exploits being created within the Web space is reflected in at least some of the other studies in the field. Although it's prior to the timeframe of this CSI study, a report issued by Breach Security analyzed global security incidents that occurred from January 1 through July 31, 2009 and found a 30 percent increase in overall web attacks compared to 1H 2008. Generally speaking, it's hard to find statistics like these that directly measure Web attack frequency. However, there's a strong hint of the extent that the Web is used as an attack vector in the Verizon report. Consider that 70 percent of Verizon's breaches resulted from external sources, that 40 percent resulted from hacking, and that 98 percent of data records lost were lost from servers. Given that the most available attack surface for an external attacker is a Web application running on a Web server, we'll bet that a large percentage of those outside attacks liberated the stolen data from Web servers. Verizon also says that 94 percent of the data breaches involved malware in some way—20 percent of that malware was installed via a Web vector. It's an area where we'd like to know more. And where we suspect the worst.

## Financial Losses

As to the financial losses visited upon the respondents and their various industry segments, we've arrived at a point of significant change from prior CSI Survey reports. This year, the lowest number of respondents in the survey's history (77) were willing to share numerical estimates of their financial losses. That number, of course, isn't nothing. Indeed, it is a higher number of respondents than either Ponemon or Verizon is drawing on for the 2009 period. But because of the way those other reports are designed, they are drilling down in more detail into specific breach incidents. Furthermore, they are dealing only with organizations where a significant breach occurred. In our case, we've already observed that half of the respondents didn't report a significant incident for the period.

So, whereas we've shared the average loss per respondent as part of the survey, this year we are concerned that doing so will encourage too much weight to be put on the number. Instead, we'd like to share some general observations about what we did see in those responses.

First, there were only two cases out of the 77 where genuinely large losses were shared. One amounted to $20 million in overall losses, another to $25 million. In terms of producing meaningful survey results, outliers like this muddy the waters considerably. In the case of the $25 million, the amount was reported in the single category of loss of mobile hardware (laptops, mobile phones, and so on). Bearing in mind that the value of data lost when mobile hardware went missing was explicitly considered in a different category, this is a rather stunning loss of notebooks. Indeed, if it were actually notebooks, it would likely amount to several thousand of them. Of course it could have been something else, some smaller number of far more valuable mobile equipment items. In this sort of survey, one doesn't know.

What is certainly true is that no other reported losses across the remaining 75 respondents are anywhere near these sorts of numbers. The overwhelming majority of respondents reported small losses.

One is tempted to suppose that this might be because only those who had lost very little would be willing to share their losses. But in prior years, this has not at all been the case. Much larger figures were routinely reported and the total loss amount was vastly higher. Indeed, in the first several years of the survey's history, there were critics who argued that respondents overstated their losses in order to produce frighteningly large loss numbers that would scare their managers into supporting security budget increases. The point is, we don't know, but it's certainly the case that most of the group that reported, say, attacks on DNS servers they maintained reported only very small financial losses as a result.

For what it's worth, if the two large figures reported above are discarded as outliers, the average loss across the group that shared financial data would fall below $100,000 per respondent, the

lowest it's ever been. We don't think there's enough data to state an exact number or to claim that this sort of number is gospel, but we do think it's suggestive.

One other thing: we do believe that not being able to offer an overall average loss figure leaves a bit a hole in our industry's understanding of what happens to average enterprises who suffer moderate sorts of incidents. Some better accounting (and we really do mean accounting) needs to occur.

The CSI survey historically has also asked respondents to estimate what percentage of monetary losses were attributable to actions or errors by individuals within the organization (**Figure 11**). As we've noted in prior reports, much is made of "the insider threat," but this threat really rolls up two separate threat vectors, on the one hand those posed by malicious employees, and on the other those who have made some kind of unintentional blunder. Beginning last year, we asked survey respondents to specify between malicious insiders and non-malicious insiders.

Last year, 43.2 percent of respondents stated that at least some of their losses were attributable to malicious insiders, but non-malicious insiders were clearly the bigger problem, with 16.1 percent of respondents estimating that nearly all their losses were due to non-malicious actors. More broadly, non-malicious insiders were clearly responsible for more loss than malicious ones, but even more to the point, there was clearly a great deal of loss that was not due to insiders at all.

**FIGURE 11**

| | None | Up to 20% | 21 to 40% | 41 to 60% | 61 to 80% | 81 to 100% |
|---|---|---|---|---|---|---|
| Malicious insider actions | 59.1% | 28.0% | 5.3% | 0.8% | 3.8% | 3.0% |
| Non-malicious insider actions | 39.5% | 26.6% | 6.5% | 8.9% | 4.0% | 14.5% |

This year's data is consistent with last year's. In keeping with the notion that more than half of losses are not due to malicious insiders, the percentage of respondents reporting no losses due to malicious insiders edged up to 59.1 percent.

87.1 percent of respondents said that 20 percent or less of their losses should be attributed to malicious insiders. 66.1 percent of respondents said that 20 percent or less of their losses were attributed to non-malicious insiders.

For a long time it was something of an old chestnut among security professionals that most breaches were perpetrated by insiders. The CSI survey never showed results that supported this view, but particularly in the past couple of years, following some rewording of the survey instrument to clarify the responses, we've taken the view that external attackers accounted for at least half of the damage done. This year we are quite confident that internal actors are responsible for

no more than approximately half of significant cyber security breaches.

This is in part because the Verizon study provides strong correlation of this position, with 62 percent of threat agents being external to the breached organization and 48 percent involving internal actors.

It should also be noted that Verizon's results last year were vastly different and attributed only 20 percent of breaches to some sort of insider involvement. The primary cause for the shift to a more even division in their report this year is the inclusion of the USSS data set. This is interesting because the USSS cases are far more numerous and more varied, whereas Verizon tends to deal only with the larger and more dramatic sort of breach. If you're a large organization with a lot to lose, the Verizon-only cases are likely more representative of your situation and you are far more likely to lose data due to attacks from external sources. In particular, Verizon found that across it's case load from 2004 to 2009, data records lost to internal-only threat agents amounted to approximately 29 million. In contrast, there were over 800 million records lost to external-only threat agents across the same period.

What's not clear from the two reports is the degree to which the percentage breakdown of financial loss in the CSI survey correlates to the breakdown of records lost in the Verizon study. But if there's any correlation at all, it would indicate that data records lost to insider attacks cost a good deal more than those lost to outsiders. And this might well make sense, insofar as outsiders grab what they can get hold of, whereas insiders have a better view into which stolen records will yield the most spoils and which can be left untouched.

## Direct Expenses

As in recent prior years, we asked about the percentages of losses that are direct, versus those that are indirect. Direct losses would include costs of things like responding to an incident, hiring a forensic investigator, sending out data breach notification letters and so on. Roughly, anything attributable to the breach that the company has to write a check for. Indirect losses, on the other hand, include relatively hard to measure items such as loss of customers, loss of future business, and loss of capital due to a drop in the stock price of a publicly traded company.

Both last year and, in an even somewhat more pronounced way, this year (**Figure 12**), respondents fell pretty cleanly into two camps, with either all of the money lost indirectly (42% this year, 48% last year) or all the money lost directly (21.9 percent last year, 25.9 percent this year).

It's reasonably easy to understand the idea of a breach that caused nothing but direct costs. If one imagines a breach that is not publicly disclosed, for example, the cost of the incident might be confined to the cost of investigating the breach, and the cost of any internal remediation and patching. Of course, there may be plenty of costs outside the organization. Stolen credit card data may cause fraud that must eventually be paid for by banks and/or account holders.

The scenario where there is nothing but indirect costs is a bit harder to sort out. Still, generally speaking direct costs are those that are directly tied to a product or project, so in some instances respondents are very likely viewing the staff costs of investigating a breach as a sunk, indirect overhead cost. If the remedy required to prevent the same attack from occurring again boils down to reconfiguring or using internal resources to harden an application, then one can imagine a loss with no direct costs. It may also be that, in some cases, any direct costs are simply dwarfed by estimated indirect costs—in particular against loss of future business.

In most instances it's devilishly hard, we should note, to get a handle on how much future business one has lost as a clear result of a security incident. Any time losses include estimates of loss of future business, as is the case in the Ponemon Institute report, losses jump drastically upward. The Ponemon report pegged 2009 indirect costs (per record lost) at $144, as opposed to $60 per record for direct costs. It's an interesting finding insofar as it assumes that businesses are able to accurately calculate lost business. And to some degree, the Ponemon report shows, they can. One of the elements the survey tracks is the loss of customers directly associated with the breach event. This year, the average loss was 3.7 percent, affecting some industries (pharmaceuticals, communications, health care) at the far higher rate of 6 percent.

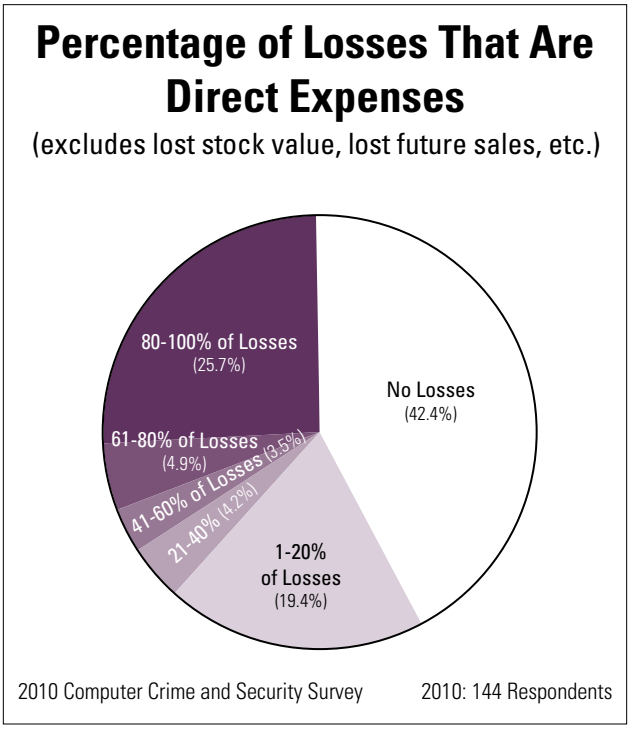



**Figure 12**

Still, a good estimate is hard to come by when looking into the future. How far into the future is the lost customer's revenue still relevant? Presumably over the average time that customers are associated with the company. But if that's multiple years, has the time value of the lost custom been taken into account? The churn percentages are a valuable contribution made by the Ponemon survey, but estimating lost future business is a tricky thing to do with any accuracy.

# Actions Taken After an Incident

By Percent of Respondents


2010 CSI Computer Crime and Security Survey

2010: 138 Respondents

**Figure 13**

## Reactions to Events

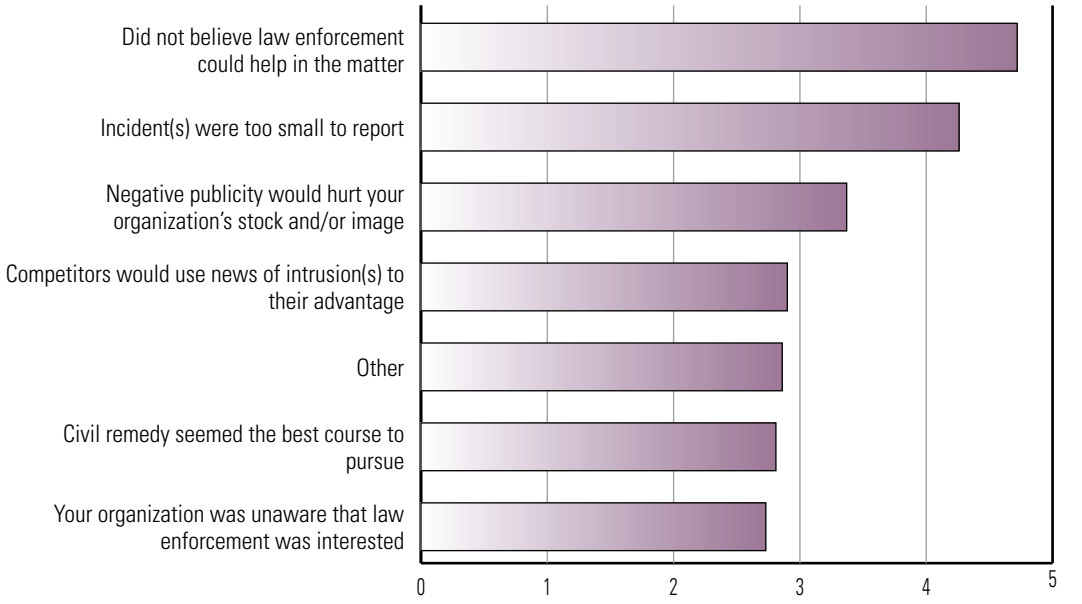
As was the case last year, respondents appear to be more proactive when dealing with incidents than they have been in past years (**Figure 13**). This year, 62.3 percent of respondents had patched vulnerable software following an incident. This was admittedly down from last year's 68.3 percent, but up markedly from prior years when the number was below 50 percent. Generally speaking, many of the categories in this question dropped slightly, but within the likely margin of error, such that it's difficult to say whether there was really any particular dropoff.

There were some changes that are of interest. There was a significant jump in those reporting that they installed additional security software, rising from 37.8 percent last year to 48.6 percent. For the first time, we asked whether an internal forensics investigation was conducted and nearly half—44.2 percent—reported that they had. The attempt to identify the perpetrator continues to drop—from 60 percent two years ago, to 37.2 percent last year, and now this year down to 23.9 percent. It would seem that mitigation and recovery are much higher priorities than attempting to find the wrongdoer and mete out justice.

After a high point of 35 percent of respondents saying that they'd reported incidents to law enforcement last year, the percentage dropped back into its historically more customary range at 27.5 percent. There was a slight (and possibly not significant) dip in the extent to which incidents were reported to the media, falling from 5.6 percent to 3.6 percent. We provided this answer as an option beginning only last year. At the time, we didn't make much of the figure, but now

## Reasons for Not Reporting to Law Enforcement

On Scale of 1-5 in level of importance




2010 CSI Computer Crime and Security Survey

2010: 88 Respondents

**Figure 14**

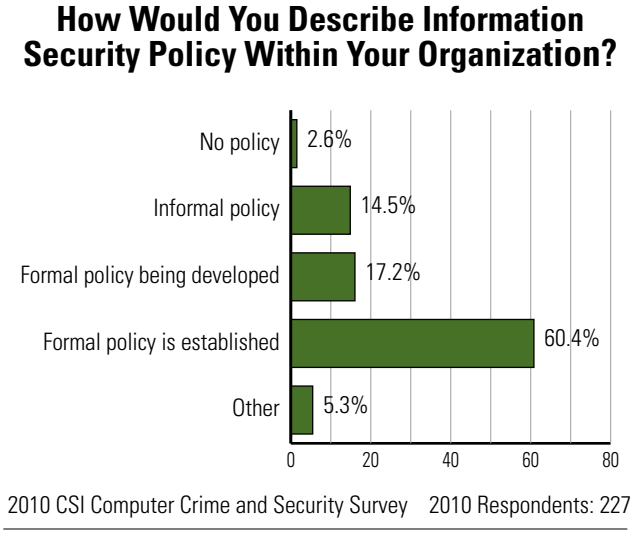



**Figure 15**

that it has come in very low for a second year, it seems time to underline that the prevalent belief that most of the cybercrimes out there aren't things we hear about. Of course, many of these incidents wouldn't constitute news even if they were reported to the media, but nevertheless one can say with some certainty that having only four or five percent of incidents appearing in the news means that we read only about the tip of the proverbial iceberg.

Corresponding to low incidence of reports to the media, there was a jump in not going public to anyone at all outside of the organization, with that percentage rising from 15.6 percent last year to 25.4 percent this year. Organizations appear to becoming more secretive than ever about the security incidents they encounter.

There's clear support for this in the Verizon report, where it's admitted that approximately two-thirds of the breaches in their (not the USSS) caseload had not been publicly disclosed.

For a number of years, we've asked those who said that they did not report incidents to law enforcement why it was that they didn't. We ask this in the form of a series of possible reasons that are weighted from 1 to 7 in terms of relative importance, with 1 being "of no importance" and 7 being "of great importance." Looking at the average weights for importance from this year to last, there are no significant changes (**Figure 14**). What's clear from looking at this question over time (and of course including this year) is that the two reasons that are more important than the others by more than a point on the one-to-seven scale are the incidents were too small to report or that they did not believe law enforcement could help in the matter. The assessment that the incidents are too small to fiddle with is surely accurate in many instances, but the perceived threshold for where an incident should be reported may also be a function of whether it is believed that law enforcement can be brought to engage themselves in the matter. Organizations may well have been "trained" by past interactions with the police that there's no point in calling.

## Security Program

Historically, this survey finds its roots in asking about cybercrime. For several years now, however, the survey has also branched out into asking about how respondents are dealing with their defensive postures. By way of broad generalization, we've found that survey respondents are proactive about defense.

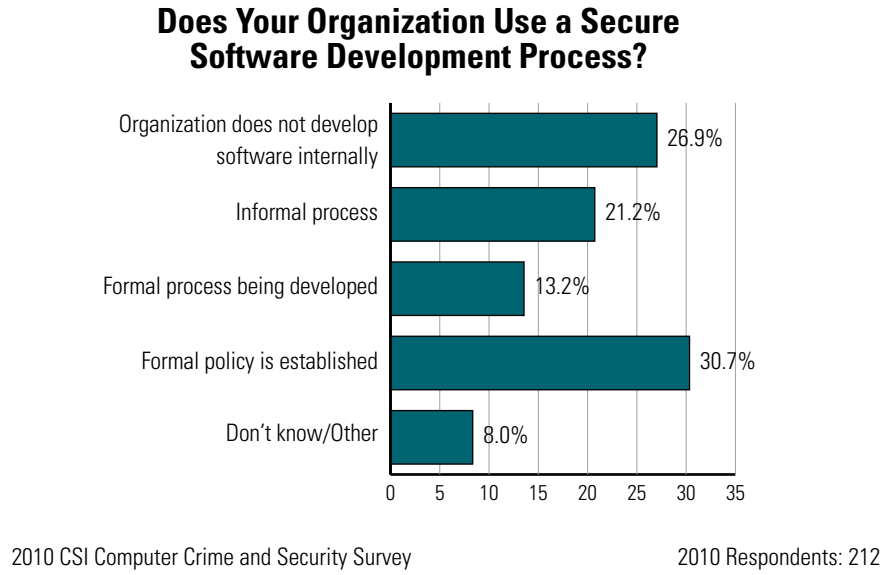


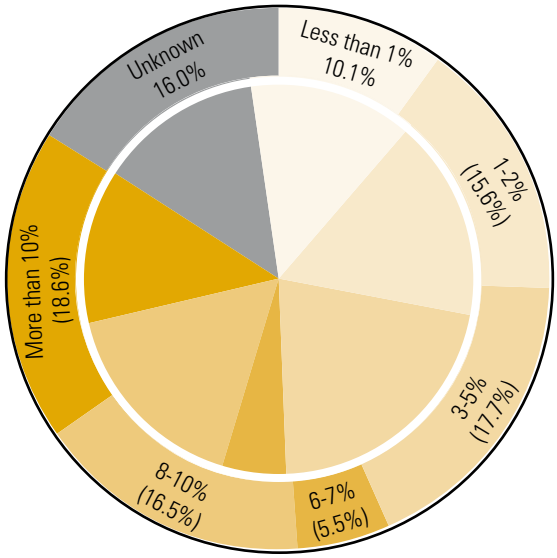

**Figure 16**

One area we've examined is the status of security policies within organization (**Figure 15**). We've been interested in whether organizations have formal policies to describe what should be happening (and not happening) in terms of security. Curiously, the number of respondents saying their organizations had a formal security policy in place dropped to 60.4 percent from last year's 68.8. The difference was made up in "no policy" and in "other," which makes it possible that there is perhaps some slight shift in the makeup of the respondent pool. It may also be that the bar for what counts as "formal" may have shifted slightly upward. What is meant by "other" is something that may be worth examining in subsequent editions of the survey. In any case, the primary takeaway is that the vast majority of organizations have something in the way of a security policy in place.

An important school of thought within security argues that software development is the primary culprit in breaches, insofar as the development process seems almost helpless to prevent the creation and deployment of software that has significant vulnerabilities. One important element in reducing the number of software vulnerabilities may well be the use of disciplined software development processes within organization. Accordingly, the survey asks whether respondent organizations use such a process. In large measure, they do, but have not changed significantly in the extent to which they do over last year. To put it another way, if you're banking on broader adoption of such processes to improve the security situation, you're still waiting. As **figure 16** shows, roughly 31 percent of respondents reported having a formal development process in place, approximately the same as last year's 31.7 percent.

## Percentage of IT Budget Spent on Security

2010 Figures on Outside, 2009 Figures on Inside




2010 CSI Computer Crime and Security Survey

2010 Respondents: 237

**Figure 17**

One could furthermore argue that these numbers, viewed in broad strokes, aren't really very good news. While roughly a quarter of respondents don't work at organizations that develop their own software, three-quarters of them do. Since only two-thirds of them have a formal policy, approximately half of organizations responding to the survey have formalized their secure development process. And while an informal policy is likely to be better than a complete disregard for security, it would seem reasonable to assert that it's precisely the formality of the process that yields applications that don't leave loose ends trailing where vulnerabilities are concerned.

## Budget and Strategy

A critical element of having a security program is being able to pay for it, so we have for many years asked about much budget they have available. We ask survey respondents how much of the overall IT budget is allocated to security (**Figure 17**). Since budget for security operations can come from sources outside of the IT department (coming, for example, from legal or physical security departments), we tried to clarify the question this year by asking that respondents consider their budget as a percentage of the IT budget, even if that's not actually where the money comes from.

As the figure shows, there is a continued shift toward more funding of security, relative to IT overall. Respondents saying that their security programs receive more than ten percent of the budget

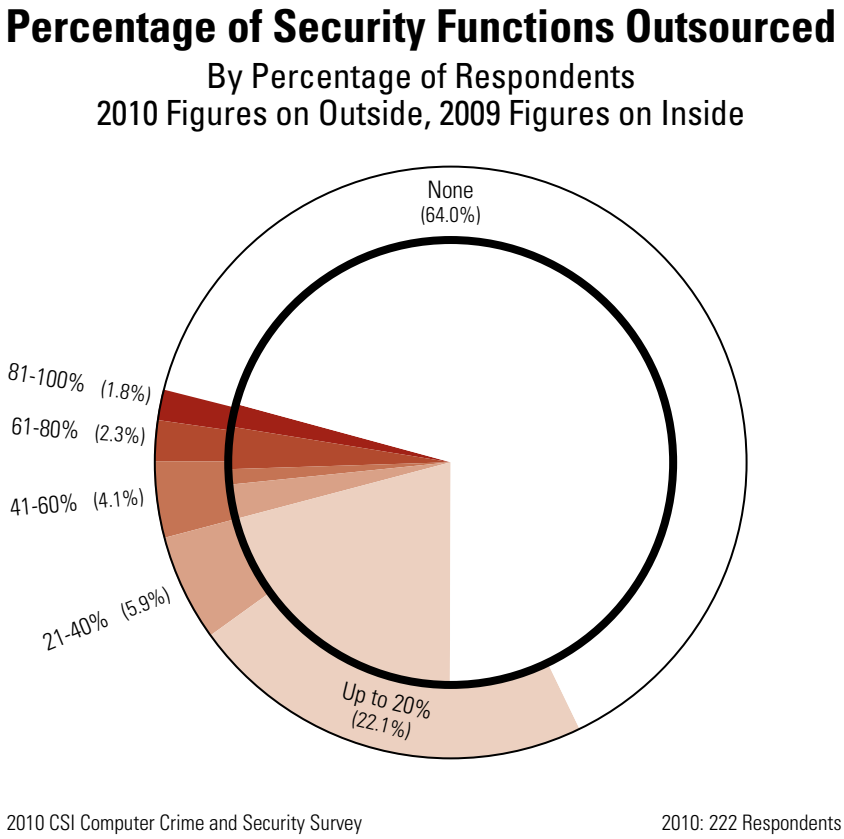



**Figure 18**

grew from 12.8 percent last year to 18.6 percent this year, with the increased percentage offset by drops in the categories below 5 percent of the IT budget. This continues a similar jump noted last year.

This doesn't mean, necessarily, that security departments were given more money to spend this time around. One perfectly rational explanation would be that IT budgets were trimmed overall, but security expenditures were deemed to be an investment that simply had to be made. That said, however, estimates from other organizations showed IT expenditures overall either holding steady or only declining slightly during 2009 (U.S. economic woes not withstanding), thus it is our belief that security spending actually rose to some degree.

The survey additionally asks about outsourcing of security. Last year there was a noticeable decrease in outsourcing over the prior year. This year, **figure 18** shows that numbers fell far closer to the previous year. It's too early to be sure, but we're inclined to see last year's percentages as something of a blip. Two years ago, for instance, the percentage of respondents who said they'd outsourced more than 20 percent of their security functions was 15 percent. While it dropped to only 8 percent last year, this year's results return to 14.1 percent. All that said, it remains the case

# Cloud Computing

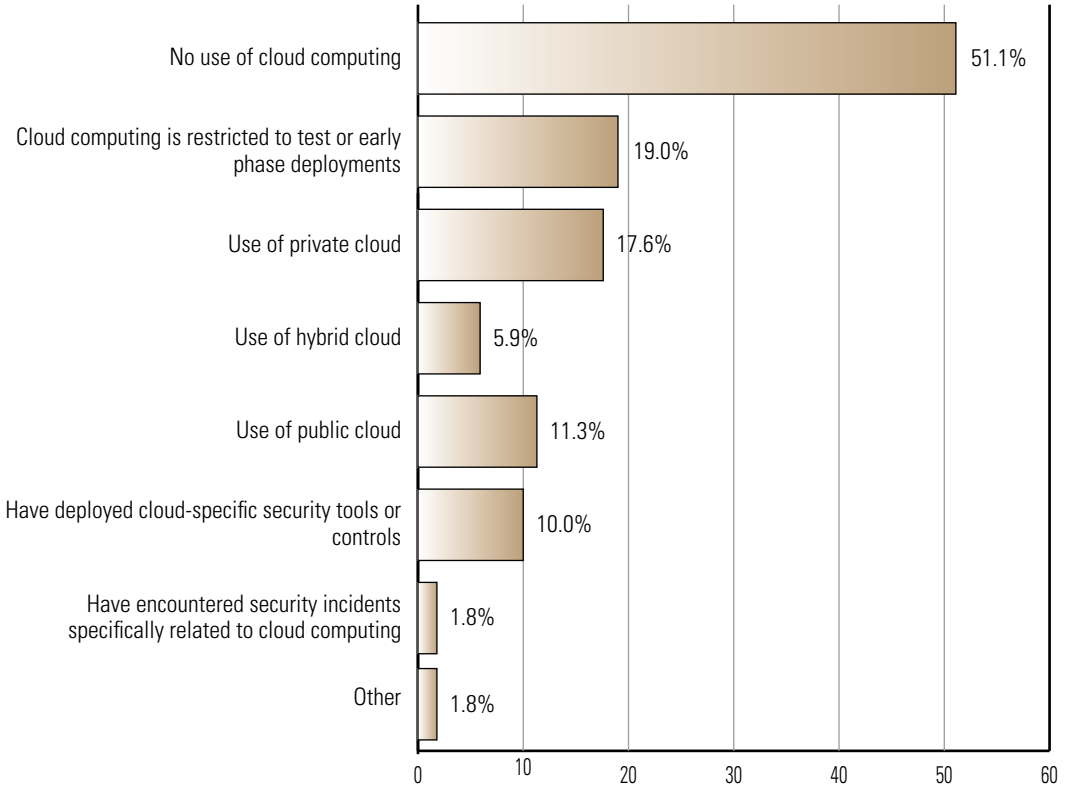



**Figure 19**

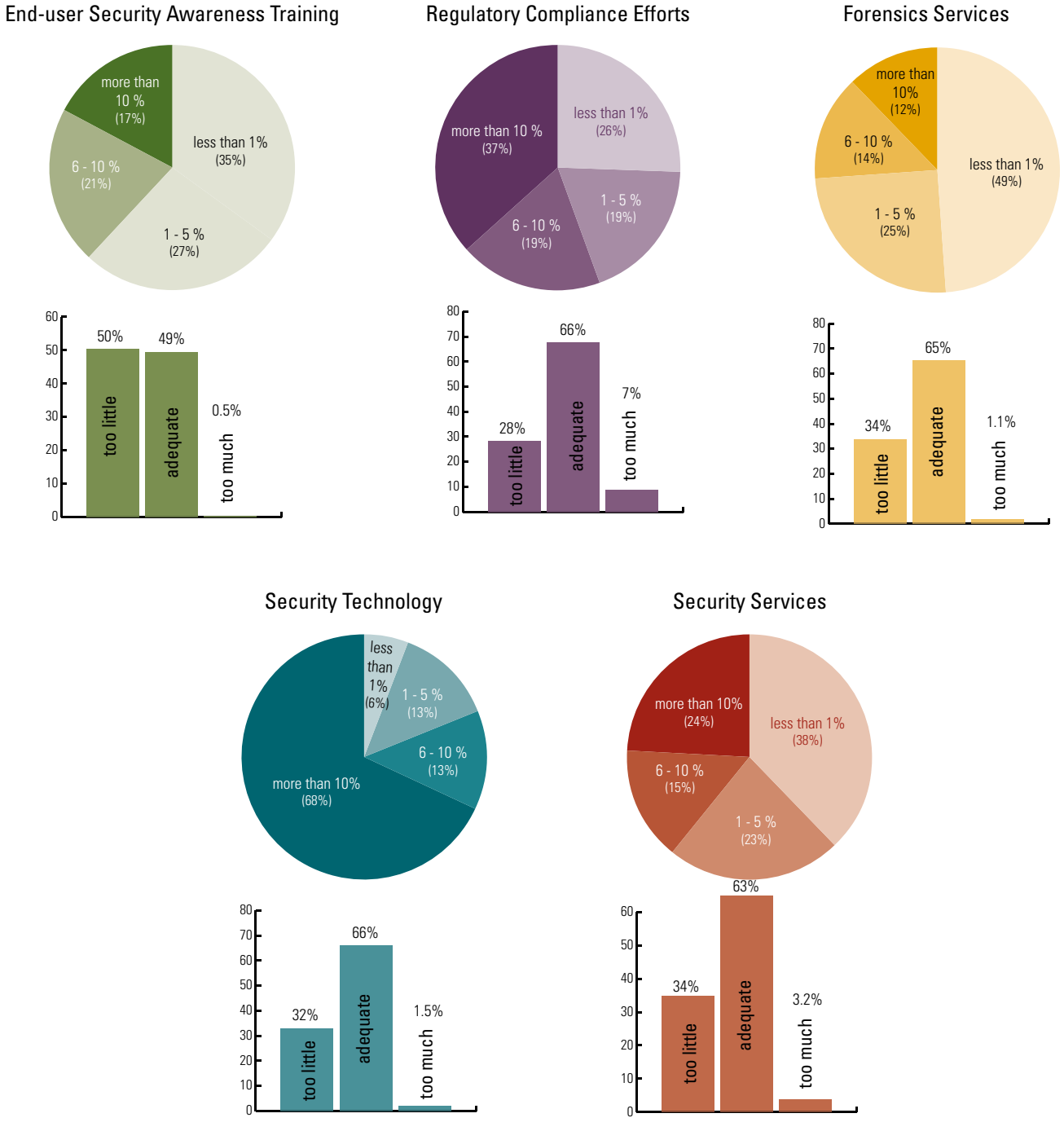
that most organizations report that they don't outsource any security functions—64 percent of respondents said they fell into that category.

One area of intense interest within IT is cloud computing. While there's a school of thought that takes the position that cloud computing is nothing new, we see it a bit differently. Yes, it may be true that viewing certain computing resources as being in a "cloud" has been around conceptually for what would seem eternities in Internet time, what is currently called cloud is a disruptive technology. How businesses go about fulfilling their basic computing needs is changing in ways that, for instance, radically change the balance of capital expenditure versus operating costs.

That said, the move to cloud computing may not be quite the rush it's cracked up to be, at least not yet. **Figure 19** shows that 51.5 percent of respondents said their organizations made no use

# Percent of Security Budget Spent on Various Components

## Is this investment adequate?




2010 CSI Computer Crime and Security Survey

2010: 196 Respondents

**Figure 20**

of cloud computing, with an additional 19 percent saying that cloud adoption is limited to test or early phase projects. 17.6 percent—not an insignificant number by any means—reported that their organizations use private cloud deployments. And it may be a surprise to some readers to see that 11.3 percent report that their organization uses a public cloud solution.

Cloud deployments face most of the same threats that conventional IT faces, but also presents some new security challenges of its own, particularly where monitoring and logging are concerned. To see how this was being dealt with, we asked respondents whether they used cloud specific security tools or controls. An even 10 percent reported that they do. A small number—1.8 percent—reported cloud-specific security incidents. This is a percentage that seems destined to rise and it will likely make sense to ask more detailed questions about cloud security in future surveys.

For the past few years, we've asked respondents how much of their security budget was devoted to end-user security awareness training. The numbers were always quite small, leaving open the question of what part of the budget *other* areas enjoyed. Beginning last year, therefore, we expanded our question to cover several areas of security investment (**Figure 19**). We further added a follow-on question that asked respondents to tell us whether, in each category, the level of investment seemed too little, too much, or about right.

It was interesting to see, last year, what large percentages said the amount was about right (**Figure 20**). Consider, for instance, that although 83 percent of respondents said their organizations spent 10 percent or less on security awareness training, half of them (49.2 percent considered this level of investment adequate.

Not only that, but security awareness was the only category in which the percentage of respondents saying the level of investment was too little was larger than the percentage saying the investment was adequate. It's probably no surprise whatsoever to see that very few respondents thought too much was being invested in any given category, though it's interesting to note that 6.5 percent did feel that too much was being spent on regulatory compliance.

## Effect of Compliance

Speaking of compliance, earlier in this report we mentioned that there were some laws that ought to affect a greater percentage of respondents than respondents actually indicated. That said, there's no question that most organizations recognize that they may be required to comply with several rather different laws. Indeed, for the 32.5 percent who reported that their organizations fall under the guidance of international privacy and security laws, some of the requirements are contradictory and the problem of being compliant with all the requirements at once becomes highly complicated, if not impossible. The question arises, therefore, whether all the regulation causes more problems than it solves.

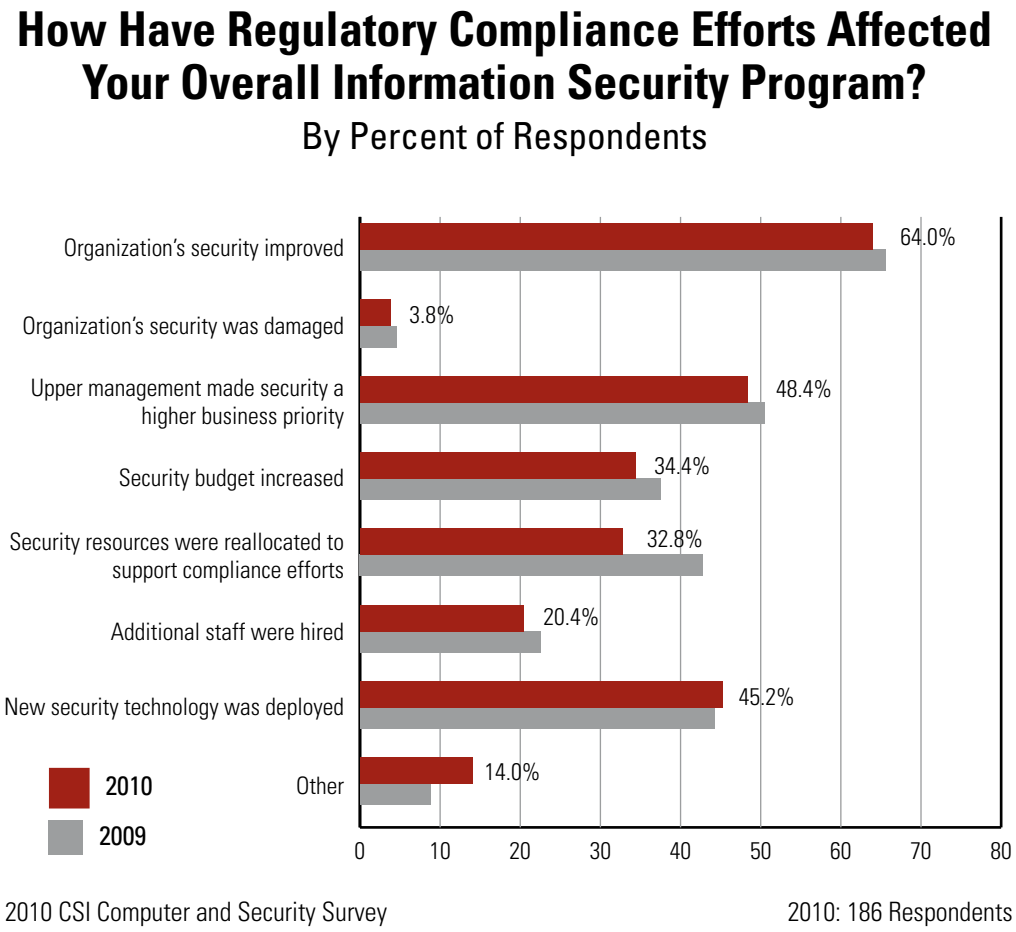



**Figure 21**

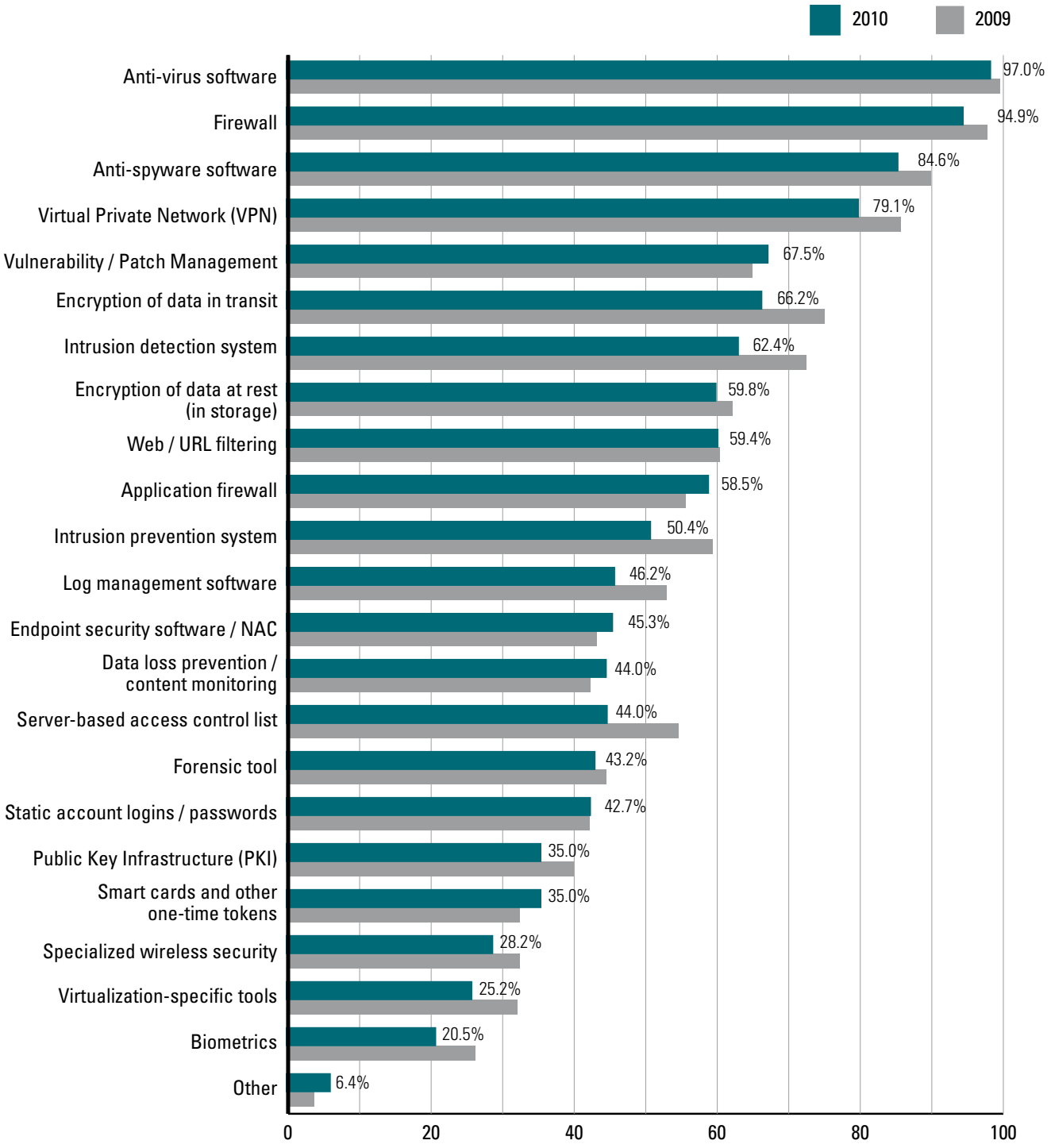
The answer seems to be no. More than half of respondents say regulatory compliance improved security at their organization and half of them report that upper management made security a higher business priority (**Figure 21**). In 45.2 percent of cases, respondents report that new technology was deployed (which might or might not be a good thing for security, but one at least hopes that it helps. At CSI events we are often told anecdotally that regulatory compliance is what has turned the tide in receiving budgetary support for security investments that had been requested for years without success.

## Technologies Deployed

Throughout the life of the survey, we've asked what security technologies our respondents have deployed to protect their organizations. Invariably and not surprisingly, anti-virus systems and firewalls have topped the list with respondents reporting their deployment into the high ninetieth percentiles. As **figure 22** shows, this year is no exception and, furthermore, values for the numerous technologies we inquire about have by and large remained close enough to their values last year that we don't think they particularly merit comment.

# Types of Security Technology Used

## By Percent of Respondents




2010 CSI Computer Crime and Security Survey

2010 Respondents: 234

**Figure 22**

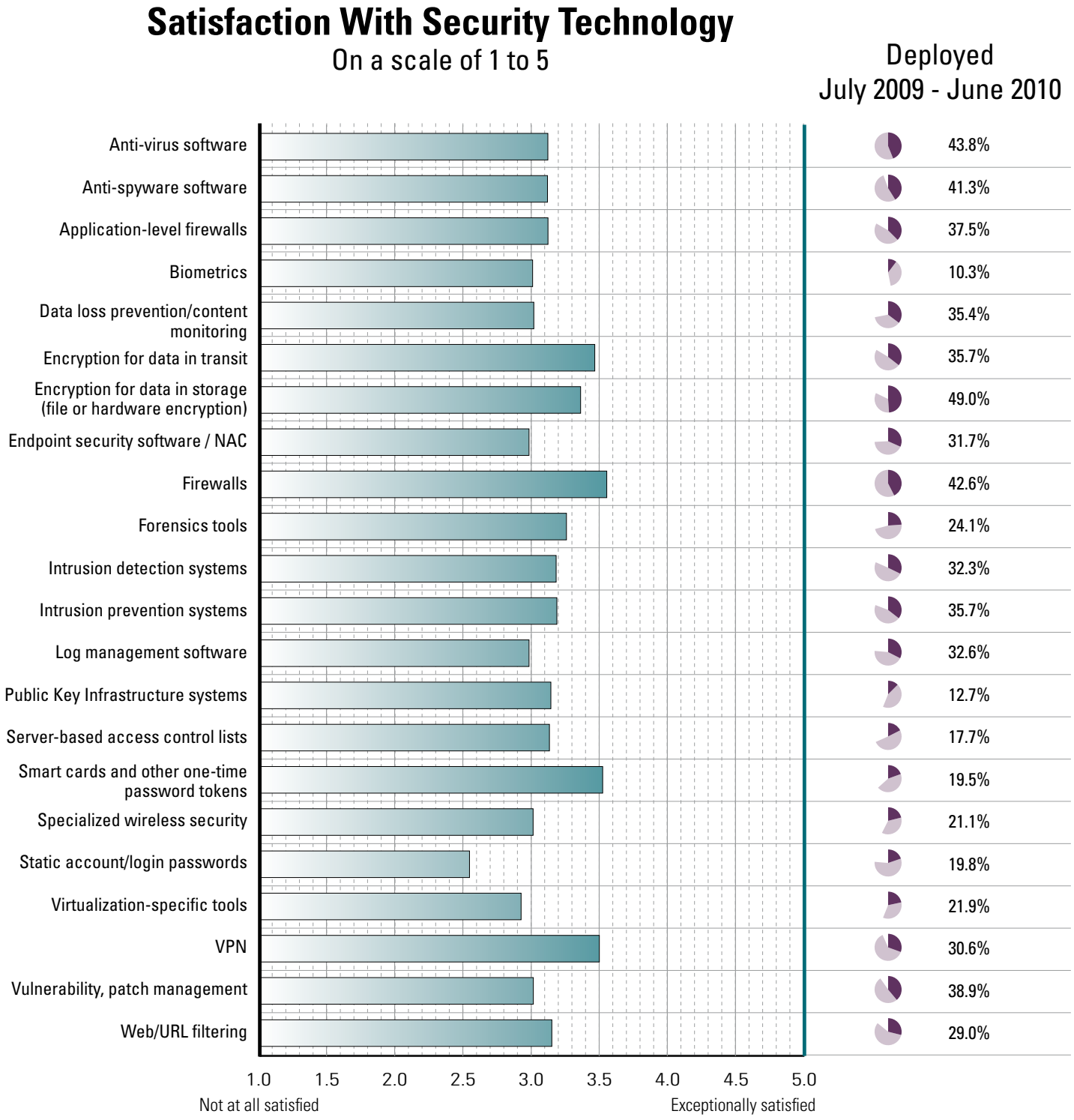

Satisfaction With Security Technology
On a scale of 1 to 5
Deployed
July 2009 - June 2010
Anti-virus software
Anti-spyware software
Application-level firewalls
Biometrics
Data loss prevention/content monitoring
Encryption for data in transit
Encryption for data in storage (file or hardware encryption)
Endpoint security software / NAC
Firewalls
Forensics tools
Intrusion detection systems
Intrusion prevention systems
Log management software
Public Key Infrastructure systems
Server-based access control lists
Smart cards and other one-time password tokens
Specialized wireless security
Static account/login passwords
Virtualization-specific tools
VPN
Vulnerability, patch management
Web/URL filtering
43.8%
41.3%
37.5%
10.3%
35.4%
35.7%
49.0%
31.7%
42.6%
24.1%
32.3%
35.7%
32.6%
12.7%
17.7%
19.5%
21.1%
19.8%
21.9%
30.6%
38.9%
29.0%
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
Not at all satisfied
Exceptionally satisfied
2010 CSI Computer Crime and Security Survey
2010 Respondents: 166

**Figure 23**

There were four instances that did seem worth calling out, however. For one, the reported use of intrusion detection systems fell from 72.6 percent in last year's survey to 62.4 percent this year. This is interesting, insofar as the category wasn't one that respondents showed any particular dislike for, either this year or last, when asked how satisfied they were with their deployment.

Less surprising is that use of server-based access control lists (ACLs) dropped from 54.6 percent last year to 44 percent this year. While there are still situations where the use of an ACL is warranted, by and large this is an approach who's relevance is on the wane. Declining numbers are therefore no surprise.

Log management's drop from 53 percent to 46.2 percent, though, is puzzling, given the degree to which other studies show compelling the value of log monitoring. The Verizon study found that 86% of victims had evidence of the breach in their log files. On the other hand, that same study made it clear that organizations were overwhelmingly unable to keep on top of monitoring the logs, almost invariably failed to see the warning signs in their logs, and it may be the case that organizations are simply giving up on log management in recognition of the reality that, at least given the tools presently available to them, they aren't able to do an adequate job of sorting through the ever-growing log volume.

In one other noticeable change, it seems a bit strange that respondents reported using virtualization-specific tools in fewer instances, with last year's 32 percent dropping to this year's 25.2 percent.

We note in passing that last year's 26.2 percent of respondents saying they used biometrics has dropped back to 20.5 percent, a figure in line with several previous years. It's a technology that remains the unloved stepchild of the field.

Beyond the fact of deploying a given security technology, there is the question of whether it produces satisfactory results. Even though your average security professional, when stopped in a hall outside a conference session, will tell you that security is a terrible as ever, or words to that effect, you'd never know that things were so dire by looking about the level of satisfaction reported for all of the security technologies we ask about. Collectively the meal is scarcely edible; each individual dish, however, is fairly tasty.

In terms of shift from the results of last year, which was the first year we asked about satisfaction, there's really nothing much to report. We asked respondents to rate their satisfaction with all of these security technologies—a rating of 1 meaning "not at all satisfied," a rating of 3 meaning "satisfied" and a rating of 5 meaning "exceptionally satisfied." **Figure 23** shows the average ratings earned by all the security technologies used. It shows that, on average, respondents were satisfied with every single technology listed. It should be noted, too, that these middle-of-the-road averages aren't a result of polarization. Generally, respondents were satisfied. Only very seldom was one "exceptionally satisfied."

**Percentage of Respondents Using ROI, NPV and IRR Metrics**

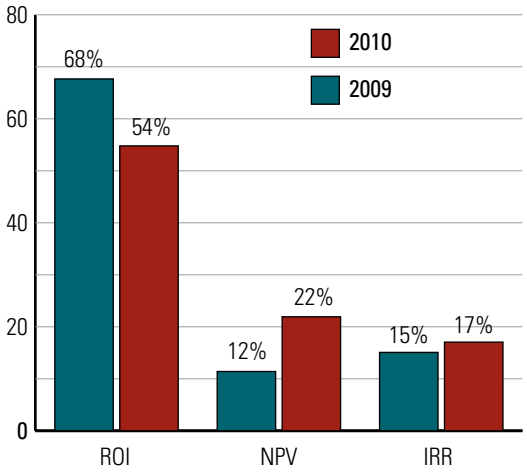



**Figure 24**

And this is strange. 50.6 percent of respondents answered with a 3 for anti-virus software, this in a climate where speaker after speaker at recent conferences has assured us that attackers can bypass conventional anti-virus defenses at will. This in a climate where we have seen spectacular proof of malware bypassing these defenses in the case of the Aurora/Google attacks and in the case, more recently, of Stuxnet.

Partly what this says is that respondents have a realistic view of what any given piece of an enterprise's defenses can be expected to deliver. They are happy if an anti-virus solution can be updated with new signatures rapidly and if it reliably stops traditional malware without the scanning process being too onerous. The fact that any determined attacker can, without too much difficulty, create custom malware that will bypass this solution appears to be a separate consideration.

It's hard to say, furthermore, that satisfaction is out of order, given that half of the respondents said they'd encountered no security incidents during the year. Regardless of what the headlines say, there are plenty of organizations out there that aren't being torn apart by hackers.

On the other hand, we really don't have reliable solutions for the latest generation of threats. New investments will need to be made—and security managers have always had difficulty in convincing organizations to invest adequately in totally new security technology initiates (things such as federated identity management and trusted computer systems spring to mind).

When it comes to asking for support from business managers for deployment of security technologies, it has been generally believed that such projects won't be approved by senior management without adequate economic justification. Thus, in 2004 we introduced a question to determine the popularity of various approaches to reckoning the value to the organization of a proposed investment. **Figure 24** shows that approximately half of them (54.4 percent) use Return on Investment (ROI).

Discussions that we have had with a wide range of security professionals, though, make us suspect that not everyone is using the term in what economists would consider the correct way. Most seem actually to be considering the time required to break even, which is not quite the same thing. A textbook ROI calculation would yield an answer that was the return achieved as a percentage of

the investment. Furthermore, it seems very often to be the case that security managers find additional, non-security benefits that come as a byproduct of the investment and rely more on the value of those benefits when calculating return. There's nothing wrong with this, insofar as these are real benefits accruing as a result of the investment, but they do muddy the water as far as justifying security investments is concerned.

## Techniques Used to Evaluate Effectiveness of Information Security

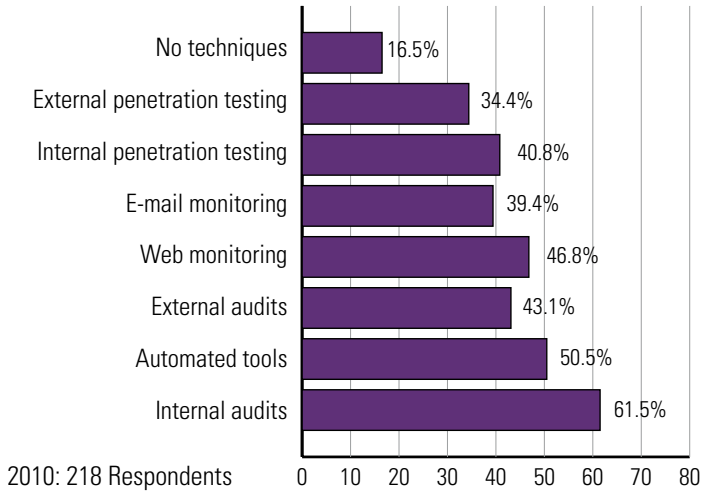



**Figure 25**

The 54.4 percent figure, we should note, is down considerably from last year's 68 percent, but that figure was quite an outlier. Previous years had seen the percentage hovering around 40. Clearly, there's been an increase from prior years, but it's perhaps not as much as last year's figures might suggest.

The same conclusion (up, but not as much as last year's numbers) applies to the other two metrics we asked about. The use of Net Present Value (NPV) was reported by 21.5 percent of respondents. 16.5 percent reported that they use Internal Rate of Return (IRR) as a way of evaluating potential investments. Both NPV and IRR take the time value of money into consideration, which is of course a sensible thing to do when considering capital investments. The inherent difficulties of ROI—namely, that it is very difficult to quantify the value of losses that have been prevented—are only compounded once a longer time window is adopted, however.

The survey questionnaire also asked about non-financial metrics that respondents use in order to measure the effectiveness of their security programs. The figures on pages 37 and 38 show what techniques respondents are using to measure the effectiveness of their security programs in general and, more specifically, what techniques they're using to measure the effectiveness of their security awareness training.

Compared to last year, which was the first year this question was posed in its current format, it would appear that, while many of the responses are more or less the same this year, evaluation in general appears to have slipped down a notch (**Figure 25**). Internally conducted security audits dropped from 67 percent to 40.8 percent—a breathtaking drop in a survey where most answers only move a few points at a time. The drop was not due to a shift to outside help; external audits also dropped slightly this year. Internally conducted penetration tests dropped ten points, from 50.2 to 40.8. And again, this was not due to a shift to outside specialists; external penetration

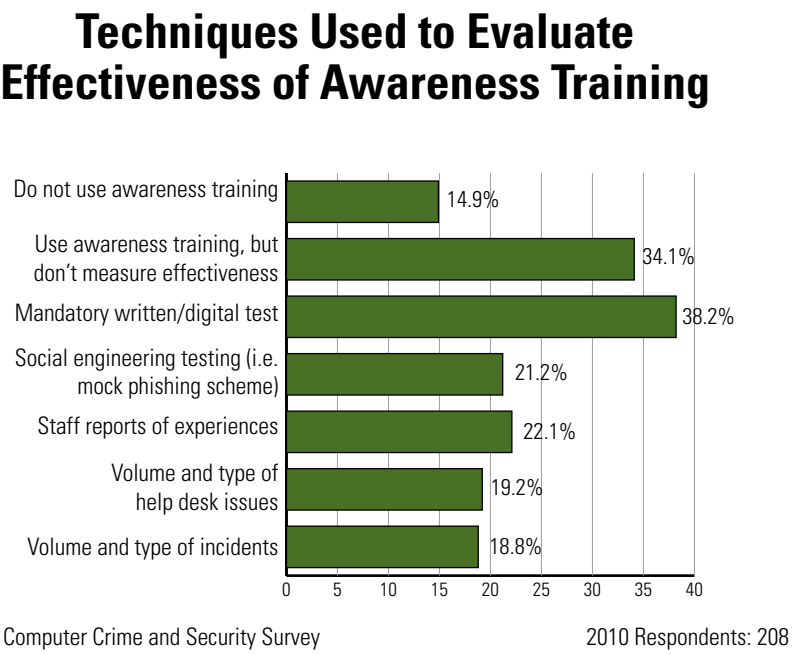



**Figure 26**

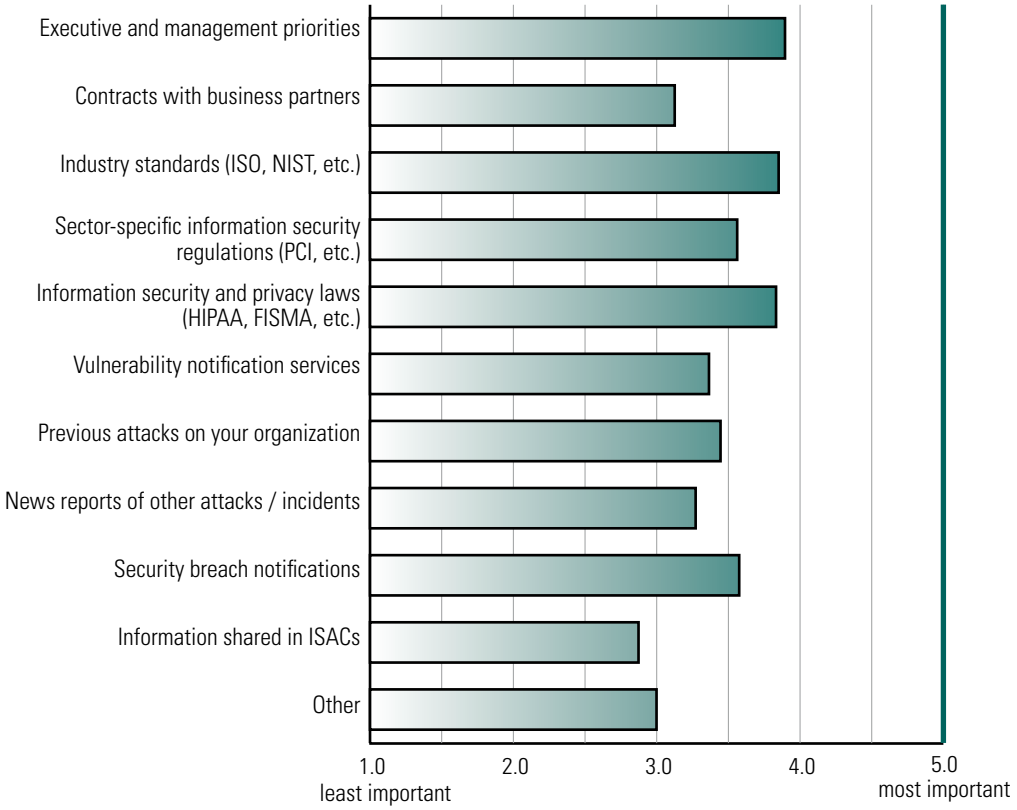
testing dropped from 41.6 percent to 34.4 percent. Clearly, there's no single, prevalent method of determining whether a given security program is effective.

CSI has always taken a particular interest in security awareness training as a non-technical way to address some of the most common vulnerabilities, namely the mistakes that employees make that can sometimes give away the entire store. On the one hand, it seems only logical that educating end users would prevent problems such as poor password hygiene. But while training programs abound, it is devilishly hard to prove that they actually accomplish anything and harder even than that to describe what the effect might be in quantitative terms. **Figure 26** shows that this year, 14.9 percent of respondents reported that their organizations had no awareness training, up a couple of points over last year. But whereas 40.8 percent last year said that they have a program but don't measure its effective, this year saw a drop to 34.1 percent. Primarily, the measurements take the form of end-user testing after the training or social engineering testing (such as seeing whether employees will take the bait when sent fake phishing emails). Whether any of these measurements yields anything really convincing about the effectiveness of training in general remains to be seen.

Finally, we added a question last year that asked what sources of information make the biggest impact on organizations' security priorities and practices (**Figure 27**). Respondents were asked to rate the importance of the various sources on a scale of 1 to 5, 1 being the least important and 5 being most essential. There was not a wide range among the average importance of the options,

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

On a scale of 1 to 5




2010 CSI Computer Crime and Security Survey

2010 Respondents: 211

**Figure 27**

truth be told, which implies that professionals use a broad mix of inputs. Clearly, though, both this year and last year the top sources were information security and privacy laws, industry standards, and the obvious influence of executive and management priorities. Least important, interestingly, was information shared in ISACs. We suspect that ISACs, like many instances where voluntary sharing is encouraged, suffer from what economists call the "free rider" problem. This is not to say that ISACs have little value, only that they have inherent challenges that prevent them from becoming highly influential.

## Concluding Remarks

Information security is both gradually improving—a trend we've seen for several years—and may be challenged by wholesale changes to the Internet that will threaten to send it rapidly spiraling out of control.

CSI survey results from the past several years show plenty of good news. The percentages of respondents who have seen various kinds of attacks has generally dropped over time. Half of respondents this year said they'd suffered no security incidents. And notwithstanding all the discussion and news regarding targeted attacks, most respondents have seen no evidence of "advanced persistent threat" attacks.

This year and last, however, responses to open-ended questions we asked about what respondents either saw as growing concerns or desired as improved tools made it clear that what is needed is better visibility into networks, Web applications, and endpoints (particularly as those endpoints become increasingly mobile).

Among current attacks, there are a growing number of highly sophisticated attacks (sophisticated at least in comparison with the attacks of, say, five years ago—one is still sometimes amused by the mistakes one sees in malware, whether that software can change polymorphically or not). The attacks are also more malign. More money is lost when an attack is successful. More records are breached.

And the field is changing to the attacker's advantage. The move to more sophisticated Web applications that expose more of an organization's internal processes to the Internet continues, but many of the organizations building these applications have neither an organized secure development approach nor perform penetration tests that might uncover flaws before they are exploited.

The infrastructure of the Internet, meanwhile, is undergoing three radical shifts as we speak. Virtualization blurs the boundaries between servers and redraws network topologies, often without clear boundaries where firewalls traditionally might have kept watch. Cloud computing blurs the locality of data and running processes. There are more questions about how this will ultimately play out than clear indications, but it's an enormous wave of change that has really only just begun to arrive in full force. Finally, we are in the throes of a massive expansion of the number of things in the world that have IP addresses. If one the top desires of security professionals is to have better visibility into the security status of their networks, the explosion of endpoints is one of the primary reason why the are unlikely to get it anytime soon.

Whatever may be coming, though, the primary takeaway of the survey (and, we would argue, of the other surveys and reports we've touched on here) is that the state of enterprise information security is, for the moment, stronger than people like to think. It may not last, and it won't seem that way if your organization is unlucky enough to suffer a major data breach catastrophe. But, on the whole, attacks are down, the effects of the attacks for average organizations are less pronounced, and our survey respondents are reasonably satisfied with the tools they have at their disposal. Certainly ten years ago most of us would have been absolutely delighted to achieve these results.

## Other Surveys and Research Referenced in This Report

**Messagelabs Intelligence October 2010**
http://www.messagelabs.com/intelligence.aspx

**Ponemon Institute 2009 Annual Study: Cost of a Data Breach**
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

**Symantec Global Internet Security Threat Report**
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

**Verizon 2010 Data Breach Investigations Report**
http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

## Use of Survey Statistics

CSI encourages most citations of the survey. For purely academic, non-profit classroom use, you may cite 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 400 words or reproducing more than one figure, you need special permission.

Second, you must of course give appropriate credit—state that the material you are excerpting is from the 2010/11 CSI Computer Crime and Security Survey, used with the permission of the Computer Security Institute, GoCSI.com.

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. For marketing and advertising uses, you must have purchased a copy.

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:

Robert Richardson, Director
Robert.Richardson@ubm.com
Computer Security Institute
350 Hudson Street, Suite 300
New York, NY 10014

## 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 the CSI Annual Conference each 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**.