2008

CSI Computer Crime & Security Survey

The latest results from the longest-running project of its kind

By Robert Richardson, CSI Director

For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations. Over 500 security professionals responded. Their answers are inside…

INTRODUCTION

For several years, this survey—perhaps the most widely quoted set of statistics in the industry—showed a steady drop in average estimated losses due to cybercrime. It seemed counterintuitive to some experts, accustomed to seeing the worst of the crime that's out there.

Last year the tide turned and respondents reported a significant upswing. Given the changes in the nature and severity of network-borne threats, this seemed only natural.

This year the average losses are back down again. And that's puzzling, honestly.

There seems little question that several sweeping changes in the overall state of IT practices—coupled with equally broad changes in the habits of the criminal world—are making significant, hard-hitting attacks easier and more lucrative for their perpetrators.

What these results suggest, though, is that on most days at most organizations, the attacks are less imaginative than what's currently theoretically possible. Which, for the moment, is good news.

Key Findings

This year's survey results are based on the responses of 522 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. This is the 13th year of the survey.

The most expensive computer security incidents were those involving financial fraud…

…with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with "bot" computers within the organization's network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.

Virus incidents occurred most frequently…

…occurring at almost half (49 percent) of the respondents' organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

Almost one in ten organizations reported they'd had a Domain Name System incident…

…up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

Twenty-seven percent of those responding to a question regarding "targeted attacks"…

…said they had detected at least one such attack, where "targeted attack" was defined as a malware attack aimed exclusively at the respondent's organization or at organizations within a small subset of the general business population.

The vast majority of respondents said their organizations either had (68 percent)…

…or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.

DETAILED SURVEY RESULTS

NOTE: The dates on the figures refer to the year of the report (i.e., 2008); the supporting data is based on the preceding year.

This is an informal survey. As one might expect, this report looks specifically at what the 522 respondents to this year's questionnaire had to say. In looking at this data, certain inherent constraints on interpretation should be born in mind.

First and foremost, this isn't a random sample of all the people in the country who are ostensibly responsible for the security of their networks. Rather, there is almost certainly a skew created by the fact that this is the CSI community—members of the organization and those who move in its orbit (attending paid conferences and the like) without necessarily being members. It's 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).

But an important question that we in the security field must have a ready answer for is this: Do current best practices produce results?

In a profession filled with (often quite justified) concerns about what will be different and more insidious about the next round of attacks, we must also take time to consider what the run-of-the-mill, present-day attacks look like and whether we've done anything worthwhile to keep the attackers at bay. While much of the news in the information security field isn't encouraging, there's arguably some fairly good news with regard to how practitioners who are making a concerted effort are faring against commonplace threats such as computer viruses.

And while we're not surveying the world at large, there's reason to believe that changes in survey results over time reflect changes in the CSI community. Five thousand surveys are sent out and 522 were received back, meaning there was a 10 percent response rate. That level of response is quite respectable, but the question requiring judgment is that of whether those who chose to reply were markedly different that those who did not.

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

We feel confident that similar groups complete the survey year over year. And, indeed, the vast majority of the questions yield virtually the same statistics year over year. The answers that have changed have been primarily the estimates of losses to cybercrime and we've seen them both rise and fall dramatically.

One could argue, as some have done, that security professionals simply don't have a clue how badly they are beaten down and robbed by their hacker adversaries. If that's the case, then their estimates of financial loss should simply be ignored. Our view is that this can only be the case if we take a needlessly dim view of the intellect of our peers. They almost certainly don't have an exact and accurate reckoning of losses due to, say, a denial-of-service attack (there's no standard way for arriving at such a number, so how could they?). But to say that they don't notice when their business is crippled due to such an attack is fear-mongering.

For our part, we think the rough reckoning of seasoned professionals is nevertheless worth attentive consideration. When the group says they lost less money this past year than they lost two or three years ago, we think it means they lost less money.

About the Respondents

The CSI survey has always been conducted anonymously as a way of enabling respondents to speak freely about potentially serious and costly events that have occurred within their networks over the past year. This anonymity introduces a difficulty in interpreting the data year over year, because of the possibility that entirely different people are responding to the questions each time they are posed. There is, despite that concern, real consistency in the demographics year over year.

As figure 1 shows, organizations covered by the survey include many areas from both the private and public sectors. The outer ring shows the current year's statistical breakdown, while the inner rings show the prior years. There is a fair degree of consistency in the breakdown over the past three years, though there have been some shifts due to the addition of new categories (military and law enforcement) last year.

The sectors with the largest number of responses came from the financial sector (22 percent), followed by consulting (15 percent), information technology (9 percent), and health services (7 percent). The portion coming from government agencies (combining federal, state, and local levels) was 13 percent (down 4 percent from last year) and educational institutions accounted for 7 percent of the responses. The diversity of organizations responding was also reflected in the 10 percent designated as "Other."

Figure 1: Respondent Organizations by Industry Sector

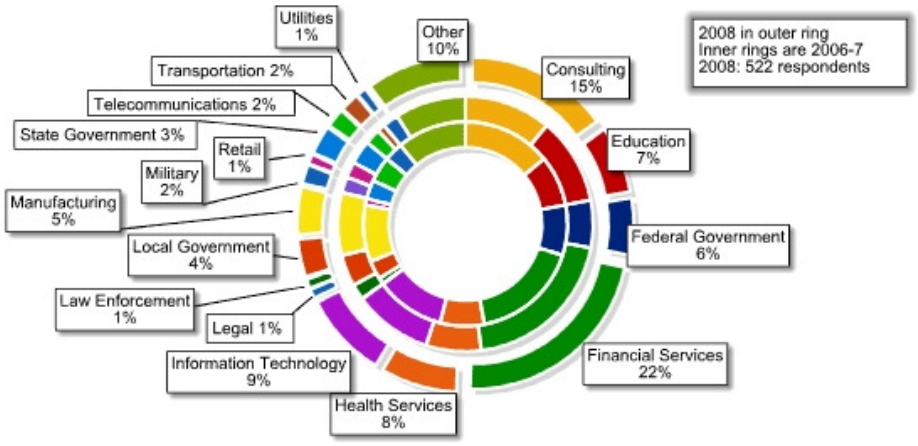


Figure 2 shows that the survey pool leans toward respondents from large enterprises. Organizations with 1,500 or more employees accounted for a little less than half of the responses. As the chart shows, the percentages of respondents from the various categories remained very close to this question's breakdown in 2006 and 2007. That breakdown clearly favors larger organizations, at least compared to the U.S. economy as a whole, where there is a preponderance of small businesses.

Figure 2: Respondent Organizations by Number of Employees

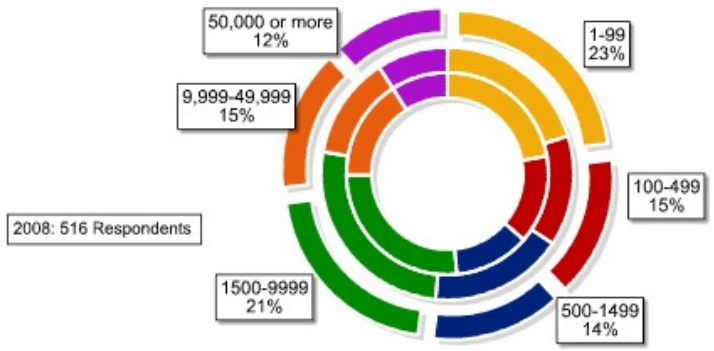


Figure 3: Organizations by Annual Revenue

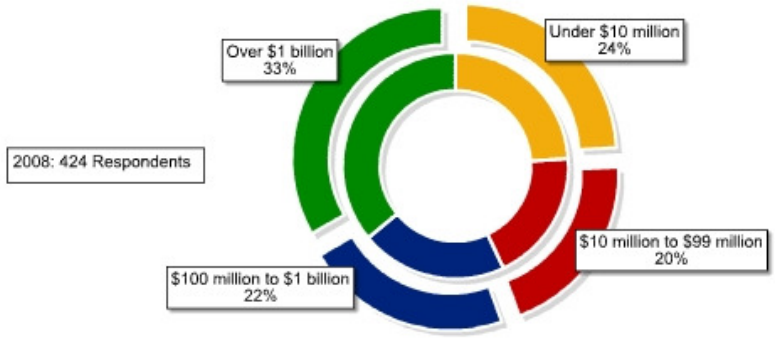
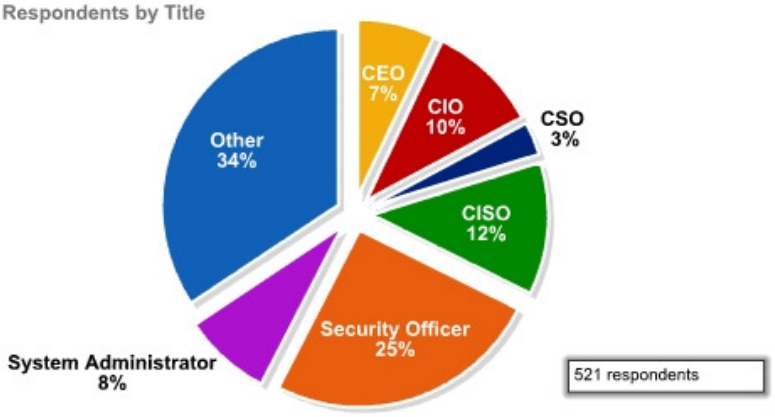


Figure 3 shows the composition of the responding commercial enterprises by the annual revenue they generated. Again the skew toward larger organizations is evident.

The survey also categorized respondents by job title. Figure 4 illustrates that 32 percent (slightly up from last year's 29 percent) of the respondents were senior executives with the titles of chief executive officer (CEO) (7 percent), chief information officer (CIO) (10 percent), chief security officer (CSO) (3 percent) or chief information security officer (CISO) (12 percent). The single largest category of specific respondents (25 percent) had the job title of security officer, while an additional 8 percent of respondents had the title of system administrator, while 34 percent had

various other titles. Last year's questionnaire turned up only one respondent who ticked the checkbox for chief privacy officer, but this year two turned up. While it's tempting to herald a doubling of the nation's CPOs, one suspects it means that positions with that specific title continue to find little traction in the enterprise world.

Figure 4: Respondents by Title



In short, the preponderance of respondents have full-time security responsibilities within their organizations. Additionally, as we've noted in this survey before, it's quite likely that the survey pool skews toward respondents who have an above-average interest in information security, this because all respondents are either members of the Computer Security Institute or have been paid attendees at CSI conferences and training events. It is reasonable to assume, thus, that they are more "security savvy" than would be a survey pool of randomly selected information technology professionals.

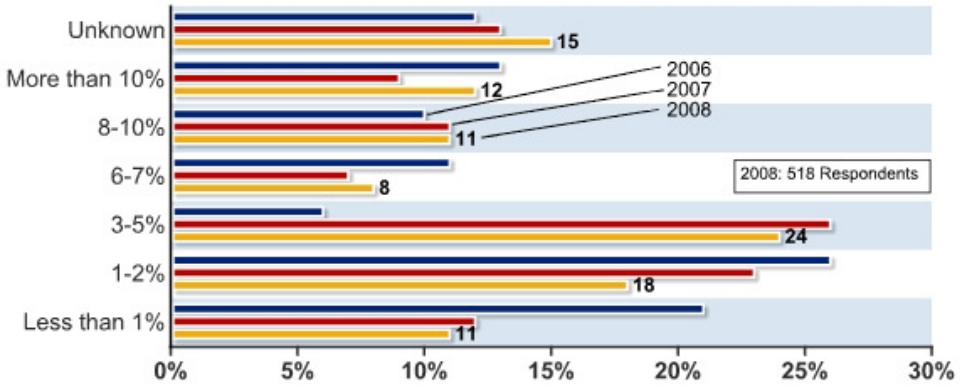
This is a point that is driven home with particular force by the recently released Verizon 2008 Data Breach Investigations Report, which concludes that, of more than 500 data breaches that were investigated, more than half required no or only a low degree of skill to perpetrate. Run-of-the-mill security tools and precautions would have prevented them. The skew in CSI respondent data is certainly toward the organizations that already have those basic steps behind them. How strong that bias is remains a matter for speculation and may not be as strong as one might assume. The Verizon report makes it clear that the failure to monitor systems and transaction logs was a huge factor in the success of attacks on the cases they looked at. We'll see in the CSI data that only half of respondents report using

some kind of security log management system. So, even the CSI respondents may well not be as diligent as one might hope.

Budgeting Issues

This survey has always contained a number of questions about the costs of computer crime, but for the past five years, it has also explored the budgeting and financial management of information security risk. In this year's survey, 53 percent said that their organizations allocated 5 percent or less of their overall IT budget to information security (figure 5). This is significantly lower than last year's 61 percent precisely on par with the 53 percent who indicated they fell into this range two years ago.

Figure 5: Percentage of IT Budget for Security

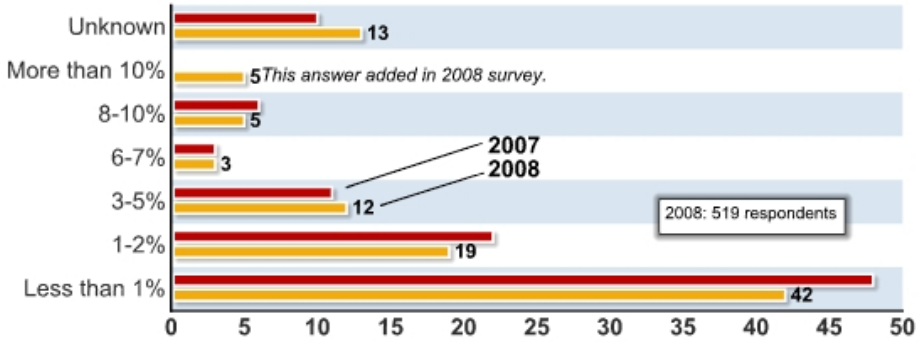


We should note that the question asked as of last year's survey clarified that the answer should be expressed as a percentage of the IT budget, even if not all the money in the security budget came from IT. Increasingly security is viewed as a problem that is far broader than technology alone—in some instance part of the security budget comes from audit and legal departments.

Training individuals with responsibility for sensitive enterprise databases is clearly part of the security agenda, and toward that end a new question was added in last year's survey, asking what percentage of the security budget was allocated for awareness training. As far as we're aware, this is the only survey that asks this question. Both years we've asked, we've been somewhat surprised to see that expenditures as a percentage are so low. Some 42 percent spend

less than 1 percent of their security dollars on awareness programs (figure 6). The overall graph shows some variation over last year, but by and large it paints a picture of there being relatively little money pushed into information security awareness efforts. It's difficult to say why these numbers are lower than some of the discussions around the importance of security awareness training might suggest. On the one hand, many forms of security awareness training can be delivered at a relatively low cost. Additionally, one of the principal costs of any sort of training—the time that employees spend away from productive work in order to take the training—is borne outside the security budget. But low training expenditures may also reflect a general cynicism about the necessity or effectiveness of awareness training.

Figure 6: Awareness Training as a Percentage of Security Budget

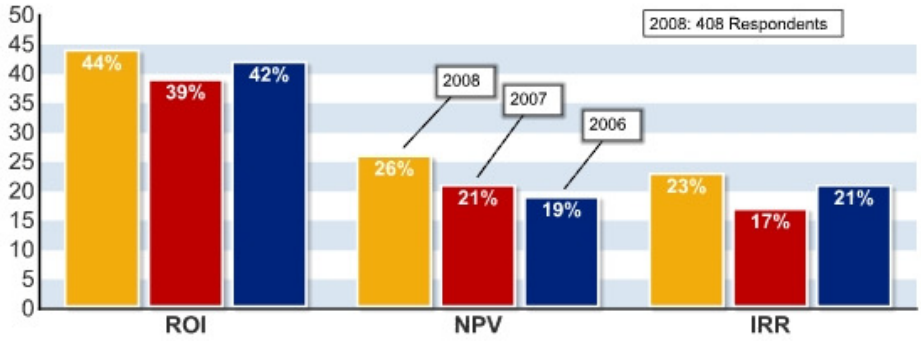


Business Justifications

For some time now, it has generally been believed that projects designed to increase an organization's information security will not automatically be approved by senior management (e.g., by the CFO), but instead need to be justified in economic terms. Hence, starting in 2004, a question was added to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the cost and benefits of computer security expenditures. In particular, survey participants were asked to indicate on a seven-point scale whether they agree or disagree that their organization uses ROI (NPV, IRR) to quantify the cost/benefit aspects of computer security expenditures. A response of 1, 2, or 3 was interpreted as disagreeing with the

statement, a response of 4 was interpreted as neither agreeing nor disagreeing, and a response of 5, 6 or 7 was interpreted as agreeing with the statement.

Figure 7: Percentage Using ROI, NPV, and IRR Metrics



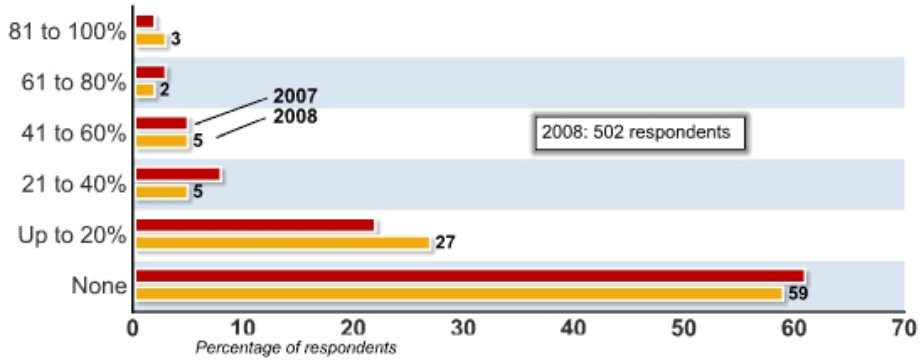
In last year's survey, 39 percent of respondents indicate their organizations used ROI as a metric, 21 percent use NPV, and 17 percent use IRR. This year, 44 percent said they use ROI, 26 percent use NPV, and 23 percent use IRR (figure 7). One might be tempted to decide that all three approaches were gaining ground, but it's worth noting that ROI and IRR remain lower than they were in 2004, the first year the question was included in the survey. At that time, the results were 55 percent, 25 percent, and 28 percent, respectively.

Over the past several years, a great deal of engaging work has been done to create an economic rationalization of security investments. While there is little question that the field of economics had had much to contribute to understanding certain aspects of cybercrime, it seems clear, from the relatively static nature of the results to this question, that economists haven't supplied the dominant mode of decision-making among information security professionals. Some practitioners clearly find it useful to think in terms of potential financial losses versus the cost of preventing them, but on the other hand these clearly aren't the predominant forces in current decision-making.

In another area pertaining to economics, the 2004 survey saw the introduction of questions that dealt with outsourcing cybersecurity and the use of insurance as a tool for managing cybersecurity risks. While outsourcing continues to receive media attention, the 2007

survey showed that outsourcing of computer security work remained at approximately the same levels found in the previous three surveys. This year's results (figure 8) show roughly the same picture, though some 2 percent of respondents shifted from saying they had done no outsourcing whatsoever. While there's certainly a market for outsourcing some kinds of security tasks (security testing of customer-facing Web applications being one such example) where the specialized nature of the work and the ability to segregate the task from access to key enterprise assets make outsourcing more appealing, most respondents say they are keeping most of their operations internally based.

Figure 8: Percentage of Security Outsourced



Like outsourcing, cyber insurance is a concept that has a great deal of intellectual appeal, has seen a degree of implementation, but that isn't taking the enterprise world by storm. Purchasing cyber insurance allows organizations to effectively outsource risks that remain after they have implemented direct, technical computer security measures such as one-time passwords, biometrics, anti-virus software, and the like. One problem, of course, is that it's difficult to say just how much residual risk remains. Indeed, at various times underwriters have approached CSI to discuss building in survey results as part of their actuarial tables. CSI doesn't share the underlying data of this survey outside the report team, but in any case one suspects that only a history of actual claim payments will provide the insurance industry with practical guidance for setting rates.

Over time one would expect that as insurance companies gain experience with this new product (there have been policies written for computer crime losses for several years now), the

additional risk premiums would shrink and prices for such policies would become more attractive. This, together with organizations becoming more familiar with this new insurance product, would lead one to expect that the use of cyber insurance should be growing each year. The last two years have shown flat results following a year in which the percentage actually dropped a bit. This year, however, saw a modest upward tick from 29 percent to 34 percent saying their organizations have external insurance policies.

Frequency, Nature and Cost of Cybersecurity Breaches

The CSI Survey has asked about what sorts of incidents were happening within enterprise organizations for longer than any other survey. In recent years, some other surveys that asked questions along similar lines have migrated their way toward less and less research about the frequency and type of occurrences on our nation's networks. The Symantec Internet Threat Report series, still an excellent resource, used to offer information regarding the number of attacks seen by its various worldwide traffic sensors. But of late the only useful metric it supplies with regard the amount of actual crimes (as opposed to the number of known vulnerabilities or instances of malware) relates to the prevalence of "bot" computers and the number of networks controlling those bots. The botnet information is highly useful, but it's unfortunate that reporting on "severe incidents," such as was offered in early reports, has been dropped.

Part of the reason other surveys may have moved away from questions regarding frequency and severity of attacks is that these are difficult measures to make. The approach taken in the CSI survey has been, and remains, unapologetically informal. The survey questionnaire simply asks whether respondents have seen certain kinds of incidents within their organizations, then asks what kinds of dollar losses were associated with the various categories of incident. Given that organizations don't explicitly incorporate the cost of the vast majority of computer security incidents into their accounting (as opposed to, say, accounting for the "shrinkage" of goods from retail stores), reporting of financial losses is invariably going to be approximate.

At the broadest level, the survey asks one question about whether or not there were any incidents that rose above the level of the nearly constant scanning that is the background noise of the Internet. As in prior years, roughly half of respondents say they have not encountered these sorts of problems (figure 10). This is a fairly interesting finding and it may well show the

bias of the sample group—their interest and involvement in security perhaps leads to a lower amount of attacks that succeed in drawing blood. Overall, this is down from a peak of 70 percent in 2000.

Figure 10: Experienced Security Incidents

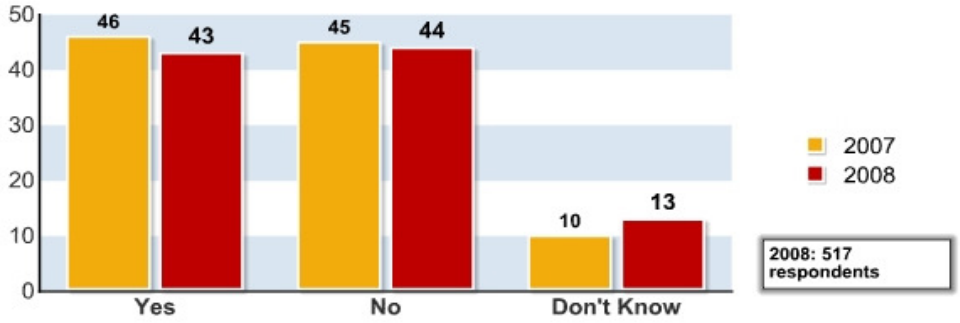
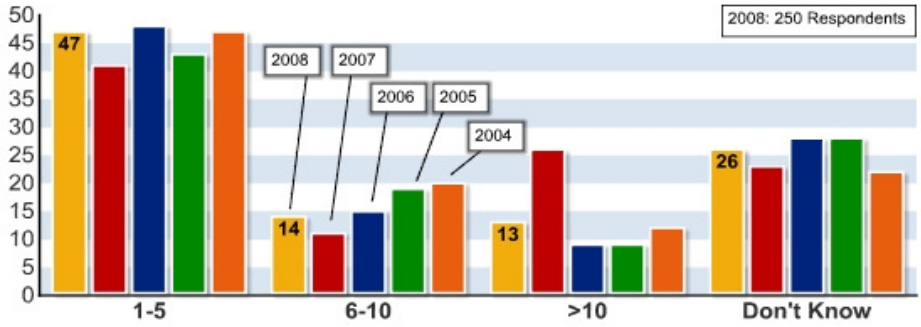


Figure 11: Number of Incidents by Percentage

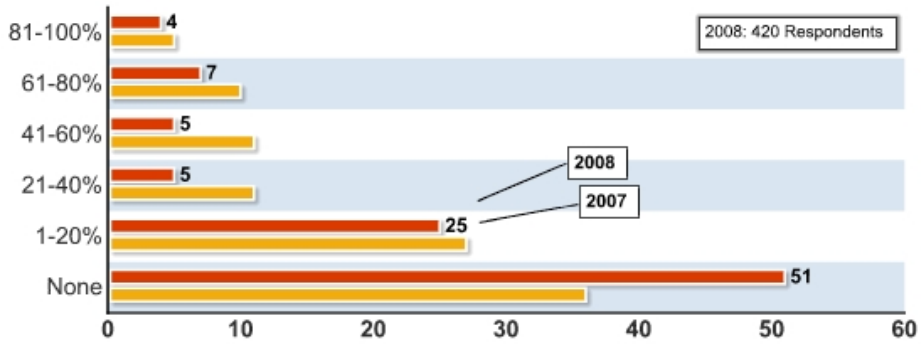


Before looking at the nature and cost of incidents, the survey asks respondents to estimate how many incidents they have had to deal with over the course of the year. As figure 11 indicates, almost half say that they have had between one and five incidents. Over the past four years (the length of time the question has been asked in its current framework), this estimate has remained fairly steady.

The survey also asks respondents to estimate the percentage of attacks coming from inside an organization versus those from outside, at least in terms of losses that result. Figure 12

shows the percentage of losses that respondents attributed to insiders, showing that considerably more respondents believed that their losses were due to attacks from outside the organization, jumping from 36 percent last year to just over half this year.

Figure 12: Percentage of Losses Due to Insiders



As noted in last year's report, a great deal is made of the insider threat, particularly by vendors selling solutions to stop insider security infractions. It's certainly true that some insiders are particularly well-placed to do enormous damage to an organization, but this survey's respondents seem to indicate that talk of the prevalence of insider criminals may be overblown. On the other hand, we're speaking here of financial losses to the organization, and in many cases significant insider crimes, such as leaking customer data, may not be detected by the victimized organization and no direct costs may be associated with the theft.

The survey asks about a number of different sorts of computer attacks and incidents. In figure 13, a subset of these are graphed, with data stretching back to 1999. In particular, this chart shows the four categories of highest incidence, namely viruses, insider abuse, laptop theft and unauthorized access to systems. Virus incidence fell below insider abuse last year, but reclaimed its position of most frequent occurrence this year. That said, both categories dropped compared to last year, and in fact all four of the most prevalent sorts of incidents fell. There appears to be a clear trend of lower and lower percentages of incidence being reported in these categories over the past several years. A glance at the full table of types of incident (table 1) shows that only four categories showed slightly increased percentages.

Figure 13: Percentages of Key Types of Incident

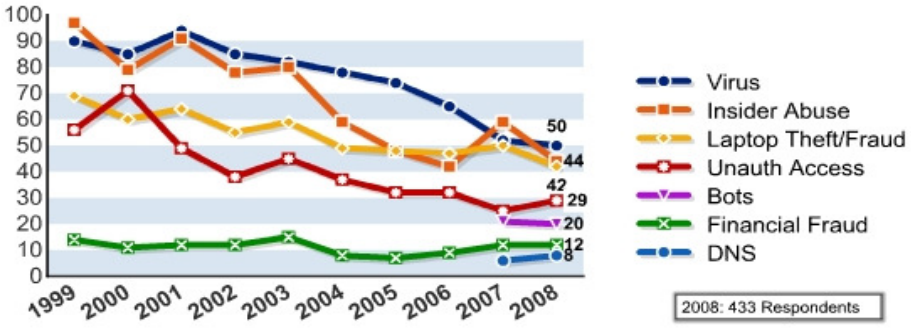
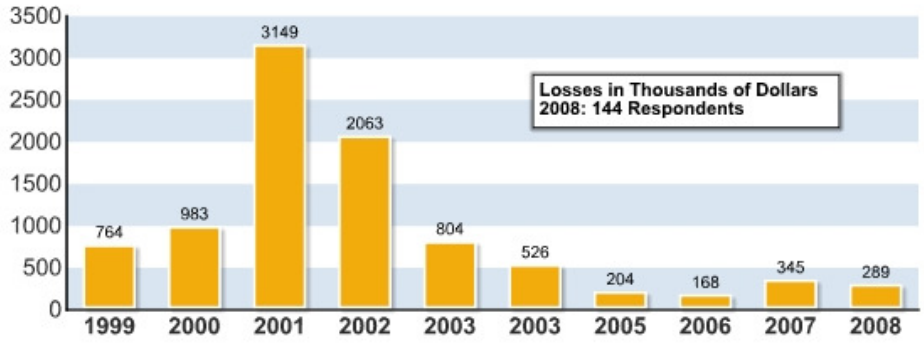


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Respondents' estimates of the losses caused by various types of computer security incident dropped significantly for five consecutive years, but more than doubled last year, when taken as an average per respondent (figure 14). This year, the average loss per respondent was $288,618, down from $345,005 last year, but up from the low of $167,713 two years ago.

Figure 14: Average Losses Per Respondent



This year, even fewer respondents were willing to share details of their financial losses than last year—144 respondents answered questions about dollar losses. Last year, while there were more respondents (198) who answered this question, we also saw a drop from previous years, in which roughly half of respondents shared financial loss information.

The number of respondents to this question should definitely be taken into consideration when considering this part of the survey's findings. Because the base of responses is small, the losses in most specific categories come from few enough reporters that it seems unwise to focus too much attention on most categories by themselves. It seems worth mentioning, though, that the most expensive kind of incident on average was financial fraud, with an average reported cost of $463,100, followed by dealing with "bot" computers within the organization's network, reported to cost an average of $345,600 per respondent. As a point of interest, dealing with loss of either proprietary information or loss of customer and employee confidential data averaged at approximately $241,000 and $268,000, respectively.

Previous survey reports have spent time considering why the loss numbers might legitimately be falling (as opposed to falling simply because of the self selection of those choosing to respond). Rather than reiterate those lines of thought, it's perhaps worth drawing a distinction between current losses and future threats. What the survey responses clearly show is that most of the attacks respondents see are relatively standard attacks like viruses and the theft of mobile devices like laptop computers. Although the loss of a laptop computer may well be quite expensive if it contains unencrypted confidential data, many laptops are lost that don't cost more than replacement and associated administrative costs. Virus incidents cost organizations that reported financial loss data an average of only $40,141; hardly a threat to the viability of most organizations.

That the most frequently noted incidents are also relatively low-cost would be encouraging if one could say with confidence that they would continue to be the most prevalent sorts of attacks—but that's hardly the case.

As was noted in last year's survey report, security professionals observing the state of the "hacker" underworld have long been very concerned about several significant factors likely to change the face of cybercrime within organizations.

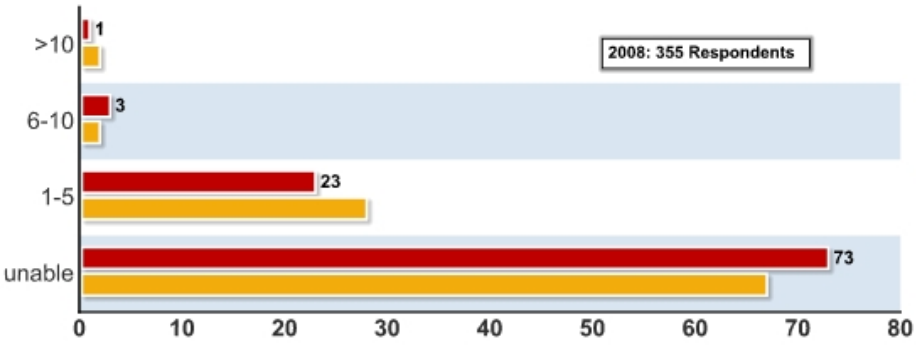
The first of these is the shift toward a "professionalization" of computer crime. This has been well documented elsewhere and is outside the scope of this report. Suffice it to say, though, that more of the perpetrators of current computer crime are motivated by money, not bragging rights.

Additionally, the security measures that organizations have taken against their attackers, such as the anti-virus and firewall components discussed above, are fundamentally imperfect. This is because much of the defensive posture of a typical organization relies on technologies that attempt to identify known, broadly distributed attacks that have easily recognizable "patterns" in them.

This approach of looking for the "signatures" of known threats can often be highly practical, but over time developers of malware (viruses and their ilk) have been gradually increasing the sophistication of their methods and are arriving at points where it is possible to bypass an anti-virus package more or less at will, at least within a limited time frame.

Malware authors have moved toward stealthier attacks that are more effective because they are targeting specific organizations or industry segments. In this year's survey we asked about targeted attacks, using a fairly broad definition where a "targeted attack" was understood to mean a malware attack aimed exclusively at your organization or at organizations within a small subset of the general business population (such as organizations within a specific area or industry). This was the second year we'd asked, so there was some basis for comparison year over year (figure 15).

Figure 15: Number of Targeted Attacks



Last year, 32 percent of those who answered the question about targeted attacks said that at least some of those incidents involved targeted attacks under this definition. This year, that number is slightly lower, at 27 percent. Nevertheless, it is clear that targeted attacks—hypothetical just a handful of years ago—are a significant reality today.

Security Technologies Used

As in previous years, respondents were asked to identify the types of security technology used by their organizations. As in almost all other years, organizations use the sorts of technologies one would expect them to use, with nearly all reporting the use of firewalls and anti-virus software, and 80 percent reporting that they use anti-spyware tools (the same level as last year). We asked whether or not organizations are using VPNs for the second year, with 85 percent reporting that they are. Some key categories are shown in figure 16, with reference back two years. The full list of technologies asked about in the survey questionnaire is shown in table 2.

Figure 16: Security Technologies Used

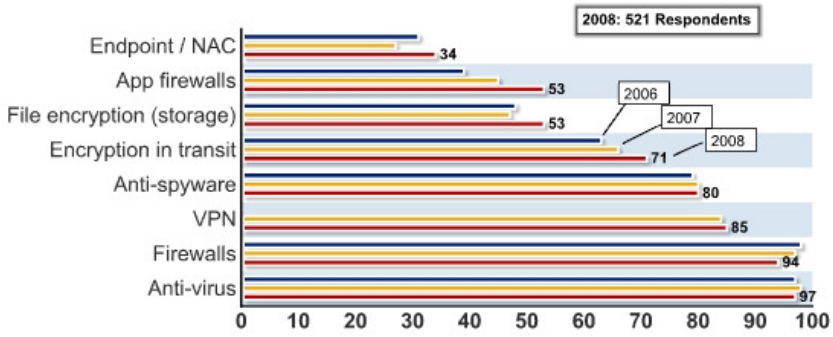


Table 2: Technologies Used	2008
Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
Firewalls	94 %
Forensics tools	41 %
Intrusion detection systems	69 %
Intrusion prevention systems	54 %
Log management software	51 %
Public Key Infrastructure systems	36 %
Server-based access control lists	50 %
Smart cards and other one-time tokens	36 %
Specialized wireless security systems	27 %
Static account / login passwords	46 %
Virtualization-specific tools	29 %
Virtual Private Network (VPN)	85 %
Vulnerability / patch management tools	65 %
Web / URL filtering	61 %
Other	3 %

Security Audits and Security Awareness Training

Implementing security measures is one thing; verifying that they are properly in place and effective on an ongoing basis is another. We asked: "Which techniques does your organization use to assist in the evaluation of the effectiveness of its information security?" Figure 17 illustrates that internal security audits are (not too surprisingly) the predominant approach, but also that automated tools now play a significant role, with 55 percent of respondents reporting their use. As the chart shows, e-mail and Web monitoring are in place at half of respondent organizations, as is the use of external audits.

For the first time this year the survey also asked about measures organizations had adopted to gauge the effectiveness of their security awareness training programs. Figure 18 shows, among other things, that 18 percent of respondents don't use awareness training (a percentage equal to last year's results), implying that 4 out of 5 respondent organizations do in fact engage in training their employees about security risks and appropriate handling of sensitive data. Although a strong majority performs this kind of training, many of the respondent organizations (32 percent) make no effort to measure the effect of this training on the organization.

Figure 17: Techniques Used To Evaluate Security Techology

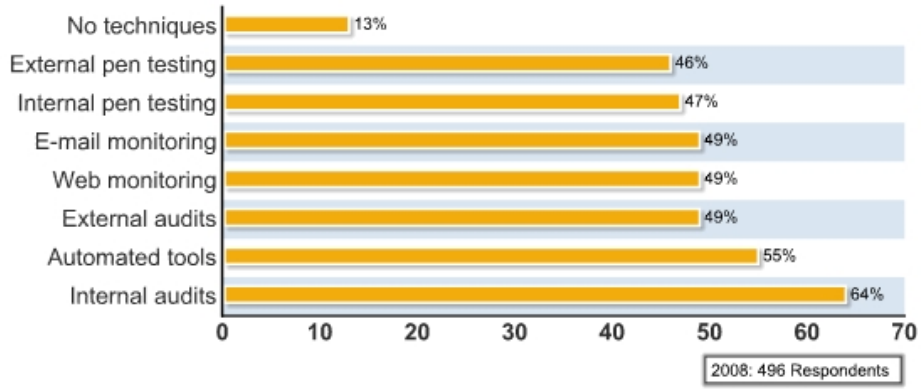
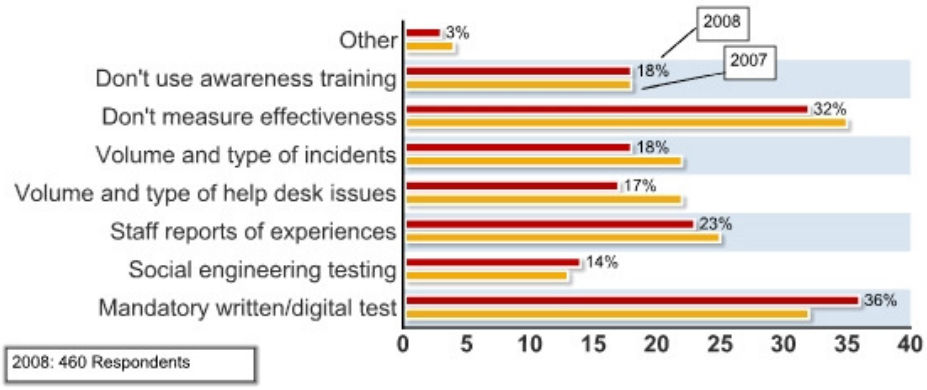


Figure 18: Awareness Training Metrics



Information Sharing

Over the last several years there have been many calls for increased sharing of information as a way of combating cyber attacks. Since 2004, CSI has tracked membership in a few key information-sharing organizations and, on the whole, it would appear that organizations are becoming somewhat less actively involved in sharing (or else are finding informal approaches more appealing).

As shown in figure 19 (next page), the percentage of respondents who say their organization doesn't belong to any information sharing organization has grown over the past two years. Reported membership in INFRAGARD dropped by 6 percent (we suspect that actual membership in INFRAGARD has grown over that period), though reported membership in an ISAC did tick up by 2 percent.

As has been noted in previous reports, there's "no clear surge in growth of membership in such groups." Indeed, membership appears to be falling off, at least within this survey group.

Beyond inquiring about membership in information sharing organizations, respondents were asked whether they shared information on computer intrusions with law enforcement and legal counsel, and more generally what their actions were following a computer intrusion.

Figure 20 shows a picture that is relatively static compared to last year (and previous years as well, except that the range of possible responses was broadened last year). Organizations tend to use the resources they have on hand to find the perpetrator where they can. As in previous years, only about one-quarter of respondents say they've contacted a law enforcement agency. The highest percentage of respondents giving this answer in the survey's history was in 2001, when 36 percent said they'd reported incidents to law enforcement. Since then, it has dropped into the twenties, where it sits this year as well, at 27 percent.

Figure 19: Information Sharing

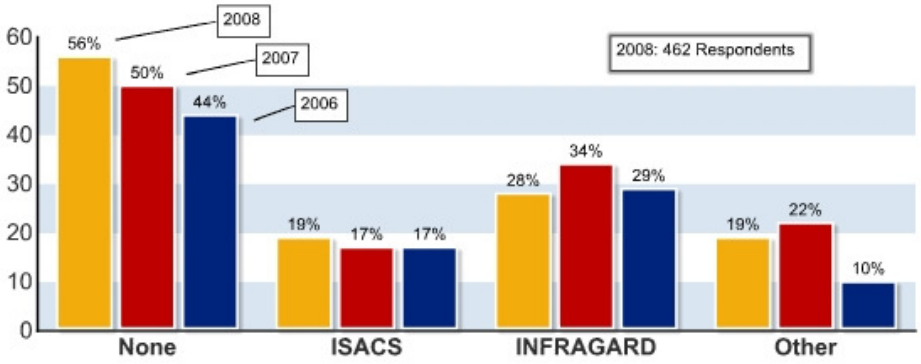
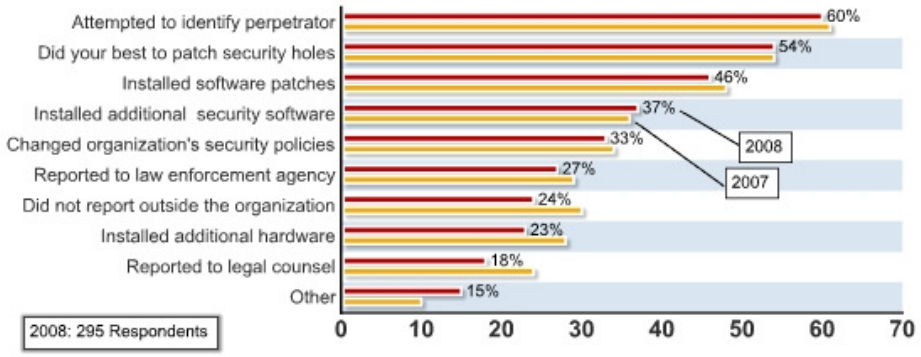


Figure 20: Actions Taken After an Incident



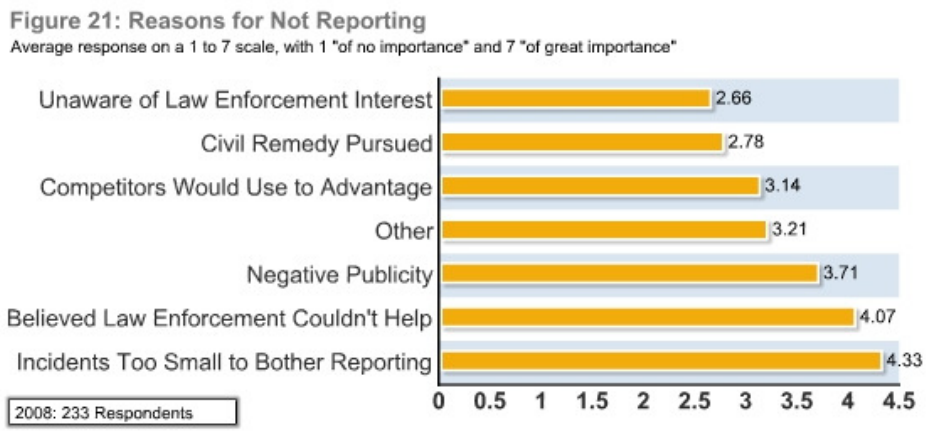


Figure 21 summarizes the reasons why organizations did not report intrusions to law enforcement. The question asked respondents to rate each possible reason on a scale from 1 to 7, where 1 meant the reason was “of no importance” and 7 held that it was “of great importance.” Shown in the figure is the average response for each answer.

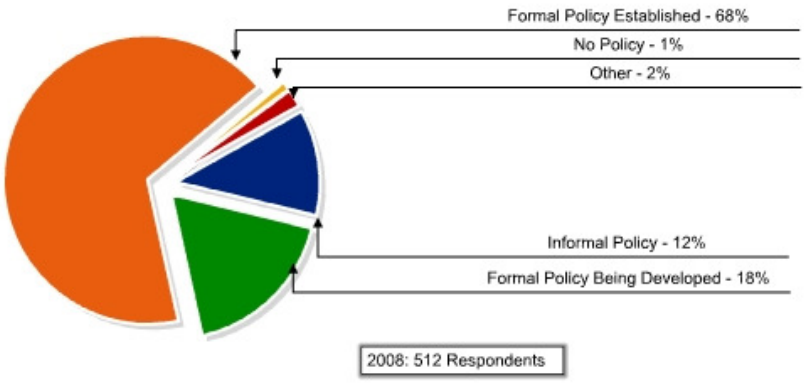
In previous years, the most important reason given for not reporting security incidents (by those indicating that their organizations would not report an intrusion to law enforcement) was the perception that resulting negative publicity would hurt their organization’s stock and/or image. This year added the option of saying that the incident was too small to bother reporting and this category is, somewhat surprisingly, the answer with the highest average indication of importance.

The most interesting finding from the question last year was the strong response to a newly added option: "Did not believe that law enforcement could help in the matter," which garnered 22 percent overall agreement. This year, perhaps even more surprisingly, 47 percent of respondents agreed with this proposition. One suspects this doesn’t say good things about general perceptions of the capability of law enforcement agencies to deal with cybercrime.

New Questions

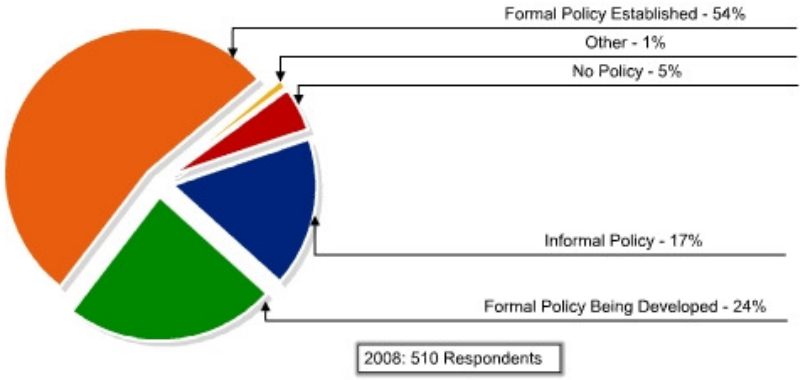
Three new questions made their debut in the 2008 questionnaire. The first aimed simply at getting a feel for the degree to which formal security policies were in place within respondent organizations. It may be possible, with further research, to suggest some relationship between the degree to which organizations have implemented formal policies and the degree to which they do or don't suffer significant cybercrime losses. At this point, there is insufficient data to draw meaningful conclusions. Nevertheless, it's worth noting that almost all respondents either have policies (whether formal or informal) or are developing them.

Figure 22: Information Security Policy w/n Your Organization



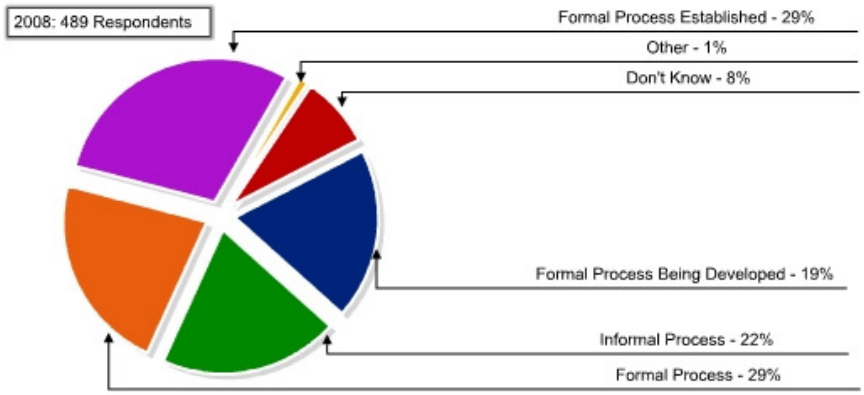
One aspect of policy that has received steadily increasing attention in this era of notorious data breach incidents is the entire question of when and whether an organization should store sensitive data. A new survey question, the results of which are summarized in figure 23, shows that about half of organizations have a formal data retention/destruction policy. Another quarter of those responding are working on a formal policy.

Figure 23: Data Retention Policy w/n Your Organization



One other area where there's been increasing focus is on the degree to which security can be improved if internally created software applications used for business processes within enterprises were designed and programmed with fewer vulnerabilities to begin with. Some organizations have focused on educating their development teams on practices that help prevent the inadvertent introduction of vulnerabilities as applications are created or maintained. As shown in figure 24, the movement toward the establishment of formal processes has not progressed as far as the movements toward general security policies and data retention policies. Nevertheless, more than one quarter of respondents reported that their organizations have a formal secure development process in place.

Figure 24: Software Development Process w/n Your Organization



General Concerns

As has been done in the prior two years, this year's survey also included the following open-ended question, “What do you think will be the most critical computer security issue(s) your organization will face over the next two years?” Some 353 respondents provided their input.

To get a better view of the key topics across the breadth of these responses, they were categorized into basic topic areas, such as "data protection" and "phishing." There are, of course, some answers that might be interpreted in different categories than were decided upon here, but generally speaking, the top areas of concern were protecting customer data, the threat of mobile and wireless devices and the general area of management concerns (how to make the case for security to upper management, how to retain good staff, how to retain current levels of security if budget levels decrease).

Last year saw more mention of legal issues and compliance, but these were well-represented among this year’s answers as well. Concerns around the security of Web applications (and the secure design of applications in general) also appeared with more-than-average frequency.

As you’d expect, a number of other topics were mentioned, such as implementing security policy, rootkits and malware, insider threats, botnet denial-of-service attacks, the effect of virtualization on security and next-generation identity management. Unlike last year, when there were several mentions of concerns about migration to the Microsoft Vista operating

system, the OS seems to have fallen so completely from corporate radar that security professionals aren't worried about it anymore.

CONCLUDING COMMENTS

In this survey's recent years, the graph of average financial losses due to cybercrime has looked like nothing so much as a parabolic line nearing a horizontal asymptote. There were several years in which reported losses dropped significantly, followed by a jump last year, dropping again this year.

The notion of relatively low losses isn't an idea that plays well in certain segments of the computer security community. This is particularly true among experts who are actively engaged in dealing with the more spectacular crimes that inevitably happen each year. It is important to recognize that while there are a handful of spectacular crimes in a year, there are *millions* of enterprise networks that do not make headlines.

We must furthermore draw a distinction between *developing* threats and *actual* successful attacks. There is, this author believes, cause for great concern regarding the sorts of attacks that become possible as we move to a more service-oriented Web, but these are not threats that have seen widespread use—not yet, at least not among those responding to this survey.

What we see in this survey are the results of many years of improving and fine-tuning tools that, by and large, promote security by *surrounding* and *scanning*. Tools like the venerable firewall create a gate between an enterprise's network assets and the untrusted outside Internet. Traffic that traverses such gateways is conceptualized as crossing a perimeter, and such traffic is inspected and compared to a list of known attacks. It is an approach that works, but only to a point.

By now, it's old hat to declare that "the perimeter is dead," but the truth is that a great many key security tools still function as variants of surrounding and scanning. The survey suggests that applying these tools in a conscientious way has yielded lower losses.

That's all well and good, but while it is satisfying to see security professionals estimating that their losses were down last year, it also seems clear that such a trend won't continue

indefinitely, especially not given that several factors observable within the online world point toward troubled times ahead. Current technologies won't bring these losses lower and, by all appearances, the current status quo isn't secure enough to suit either security professionals or the end users they protect.

There are technologies and security architectures—some developed to the point that they are being rolled out in full (though early) implementations—that may well provide better mechanisms for dealing with developing threats. So while a surround-and-scan approach may be at the outside edge of its effectiveness, that needn't mean that network security is soon to careen out of control. Rather, the usual back and forth between the security and criminal communities will continue.

Where will the balance between vulnerabilities and safeguards lie in a year's time? The more information we can gather on the causes and consequences of computer crime, the better we will be able to make judgments of our progress and, one hopes, the better CSI's view is that this survey, while an informal tool, is an important part of gathering information for a better understanding of the state of information security.

A NOTE FROM ROBERT RICHARDSON, DIRECTOR, CSI:

CSI offers the survey results as a public service. The report is free at the CSI Web site (GoCSI.com). CSI funds the project and is solely responsible for the results.

Regarding Methodology

The survey was distributed to 5000 information security practitioners in the United States in early January 2008, both in a hardcopy, first-class mailing and in a Web e-mail distribution. Two subsequent mailings and e-mailings followed at approximately two-week intervals. Print surveys were returned by business-reply mail; both print and Web surveys were administered anonymously.

Regarding Use of Survey Statistics

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

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

Second, you must of course give appropriate credit—you must say that the material you are excerpting came from the CSI Computer Crime and Security Survey and mention the year of the survey.

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

Finally, when the published or broadly distributed work in which you are using the quotation appears, you must agree to send a copy of the work, link to the work online, or clear indication of how the material was used to CSI at the contact addresses below. You are *not* granted permission to use any part of the survey if you do not agree to this provision—an important part of the service we try to provide with the annual survey involves knowing how the survey is used.

If you can meet these four requirements, you are hereby given permission to use the survey. If not, you should seek additional special permission.

Robert Richardson is Director of the Computer Security Institute (rrichardson@techweb.com).