VanDyke®
SOFTWARE

Amplitude Research®
loud & clear

4th Annual Security Survey:
IT Executives and Network Administrators

Commissioned study conducted by Amplitude Research, Inc.

October 10, 2008

VANDYKE®
SOFTWARE

About VanDyke Software

VanDyke Software® (www.vandykesoftware.com) is a privately held software company located in Albuquerque, NM, with more than 1,000,000 registered users in over 100 countries worldwide. VanDyke sells its secure access and terminal emulation software using a try-before-you-buy model with online purchase, delivery, and licensing. IT professionals who are responsible for network administration and end-user access where security is critical rely on VanDyke Software's rock solid and easy to configure software.

The company's product offerings include the SecureCRT® Secure Shell terminal emulator, the SecureFX® secure file transfer client, and the VanDyke ClientPack. VanDyke's VShell® Secure Shell server is a secure alternative to Telnet and FTP on Windows and UNIX platforms.

VanDyke's easy-to-use software and accurate, responsive customer support have a daily impact on its customers' businesses. VanDyke's objectives are to make Secure Shell-based solutions easier to use and address its customers' evolving needs with timely product enhancements. In doing so, VanDyke solutions help lower the complexity and cost of integrating security into remote access, file transfer, and data communications.

AMPLITUDE
RESEARCH®
loud & clear

About Amplitude Research®

Amplitude Research® (www.amplituderesearch.com) is a privately owned survey research organization headquartered in Boca Raton, Florida, with blue chip clients located throughout the United States and Canada. Amplitude combines its powerful survey platform, experienced survey administration, top-quality sample, and high-quality reporting to deliver Loud and Clear™ results.

Amplitude's IT panel (www.panelspeak.com) was formed in early 2002, and now reaches over 75,000 IT professionals consisting of five distinct segments: (i) C level or higher IT professionals including CTOs, CIOs, and MIS managers; (ii) developers, software engineers, programmers, database administrators, and security experts; (iii) systems administrators, network administrators, and networking managers; (iv) business executives at smaller size technology companies such as CEOs, CFOs, and senior managers; and (v) other IT professionals such as project managers, technical support specialists, and intranet managers.

All surveys are programmed and hosted by Amplitude Research using its proprietary, multi-language platform supporting a myriad of question types and features including advanced skip logic, branching, piping, rotating ads, randomized response choices, image testing, conjoint, interactive maps, variable inserts, and 2,000 character text boxes.

Study History

This is the fourth year in a row that VanDyke Software has commissioned an Amplitude Research® survey of IT executives and network administrators on the subject of network security. Many of the same questions have been asked each year, although some questions have been added or deleted from time to time in order to cover special topics / industry developments.

Study Methodology

The 2008 study was administered by Amplitude Research® over the period September 17th to September 19th, 2008 among its nationwide web panel. In total, 350 surveys were completed by respondents who confirmed working as an IT executive or network administrator for their company / organization.

A “sample size” of 350 respondents has a “maximum” sampling margin of error of +/- 5.2 percentage points at the “95% confidence level.” Here, the word “maximum” refers to the sampling margin of error being highest for percentages from the survey near 50%. Given the same sample size, the sampling margin of error declines as percentages get further from 50%. For example, for percentages from the survey near 10% or 90%, the sampling margin of error at the 95% confidence level is +/- 3.1 percentage points.

The number of surveys completed nationwide was similar in each of the four years this study has been conducted:

- 360 completed surveys in 2005
- 350 completed surveys in 2006
- 350 completed surveys in 2007
- 350 completed surveys in 2008

Study Findings

- Key findings from the study are summarized on the following pages. The summary begins with a description of the types of respondents included in the survey and the types of companies / organizations they represent. In particular, the mix of company sizes represented is discussed, and this “sets the stage” for later sections, as much of the analysis is based on dividing companies / organizations into four categories based on number of employees. The next section addresses unauthorized intrusions, which have continued to be a challenge to many companies / organizations. Then, extensive information on company activity related to monitoring security is presented for servers specifically and also for user machines in office networks. A new section covers budget related questions first introduced in the 2008 survey. Lastly, a final section looks at sources used to learn about security best practices. A few of the study highlights follow, with much more detail in later sections:

- ➢ A sizable proportion of companies / organizations (almost half of the total sample in 2008) continue to report experiencing hacker / unauthorized intrusions of their user machines, networks, and/or servers.

- ➢ Among midsize companies (i.e., with between 1,000 and 4,999 employees in the U.S.) the incidence of hacker / unauthorized intrusions increased significantly in 2008.

- ➢ The incidence of hacker / unauthorized intrusions did not change significantly for other company size categories (i.e., micro, small, and large), but this implies that unauthorized intrusions are a relentless problem for many companies of all sizes.

- ➢ The majority of those experiencing unauthorized intrusions gave a rating of “high impact” or “medium impact” for the potential financial impact on their organization based on the information that might have been obtained.

- ➢ Similarly, the majority gave a rating of “highly sensitive” or “sensitive” for the information that might have been obtained as a result of unauthorized intrusions.

- ➢ After a slight decline between 2006 and 2007 in the proportion actively monitoring the security of 90% to 100% of their servers, there was a rebound in 2008. Similarly noteworthy patterns in other measures of security activity also surfaced in 2008.

- ➢ It was much more common to expect an IT security budget increase (47%) for 2008 over 2007 rather than a decrease (12%).

Respondent Characteristics

- The survey included opinions from managers and administrators concerned with computer and network security at their company / organization. For example, the most common job title reported by the survey respondents was “IT Manager” (41% in the 2008 survey). The next most common titles were “System or Network Administrator” (13%), followed by “CEO / President of a technology company” (13%), and CIO (12%).

- The types of organizations included privately held (55%), publicly traded corporations (29%), government (5%), non-profit (5%), and educational institutions (4%).

- A wide variety of industries were represented, such as manufacturing (14%), healthcare (10%), business services (8%), banking / finance (7%), consulting services (6%), retail (5%), and many others.

- Half (50%) of the respondents have worked in IT for more than 10 years, while more than one-fourth (27%) has worked in IT for 5 to 10 years.

- Organizations ranged in size from very small to large, where "size" was defined by the number of employees in the company or organization across all sites and locations within the U.S. For the purposes of analysis, four company size categories were defined as follows:

  - ➢ Micro: between 1 and 99 employees (20% of 2008 sample)
  - ➢ Small: 100 to 999 employees (33%)
  - ➢ Midsize: 1,000 to 4,999 employees (23%)
  - ➢ Large: 5,000 or more employees (25%)

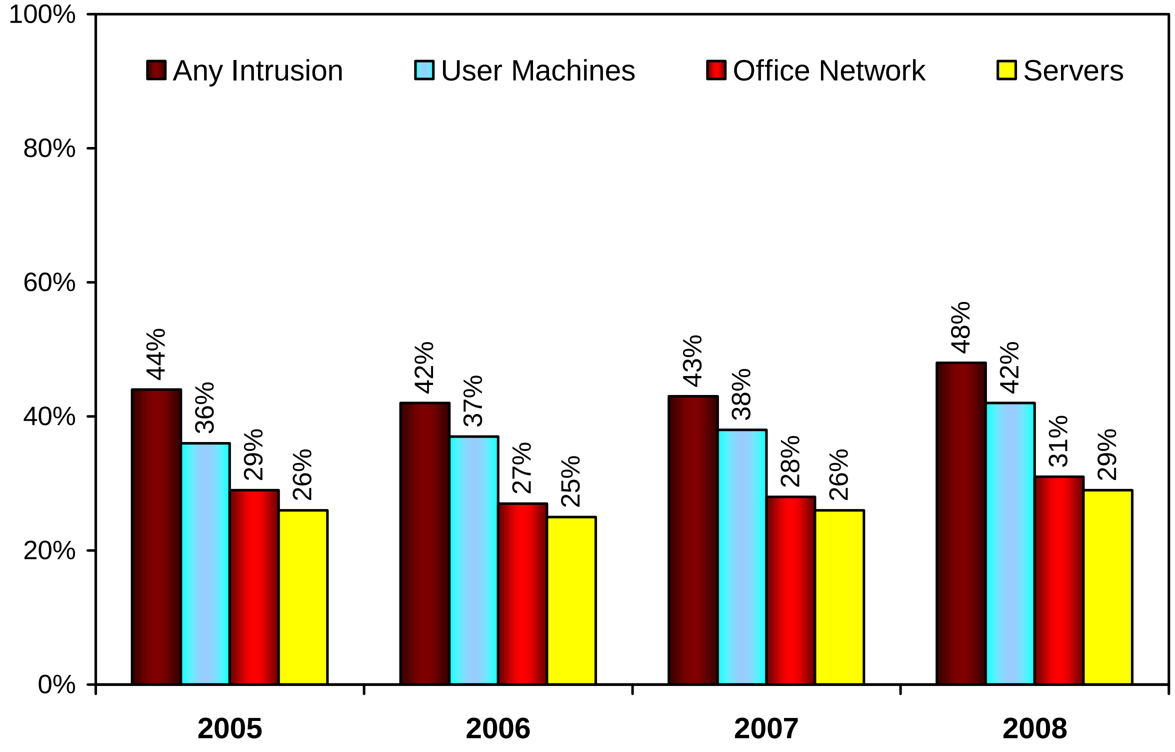
- The percentages shown for the various characteristics noted above were based on the 2008 survey, but the surveys conducted in earlier years were similar in terms of the distribution (or "mix") of these characteristics. In particular, the distribution of company sizes in the sample was very consistent year to year. To be more precise, the table below shows the number of survey respondents (i.e., "count") representing each company size category, and the proportion for each category is shown within each year.

			Year				
			2005	2006	2007	2008	Total
Co. Size (# Employees)	Micro (1-99)	Count	80	75	63	70	288
		% within Year	22.2%	21.4%	18.0%	20.0%	20.4%
	Small (100-999)	Count	107	113	109	114	443
		% within Year	29.7%	32.3%	31.1%	32.6%	31.4%
	Midsize (1,000-4,999)	Count	81	75	77	79	312
		% within Year	22.5%	21.4%	22.0%	22.6%	22.1%
	Large (5,000+)	Count	92	87	101	87	367
		% within Year	25.6%	24.9%	28.9%	24.9%	26.0%
Total		Count	360	350	350	350	1410
		% within Year	100.0%	100.0%	100.0%	100.0%	100.0%

Hacker / Unauthorized Intrusions

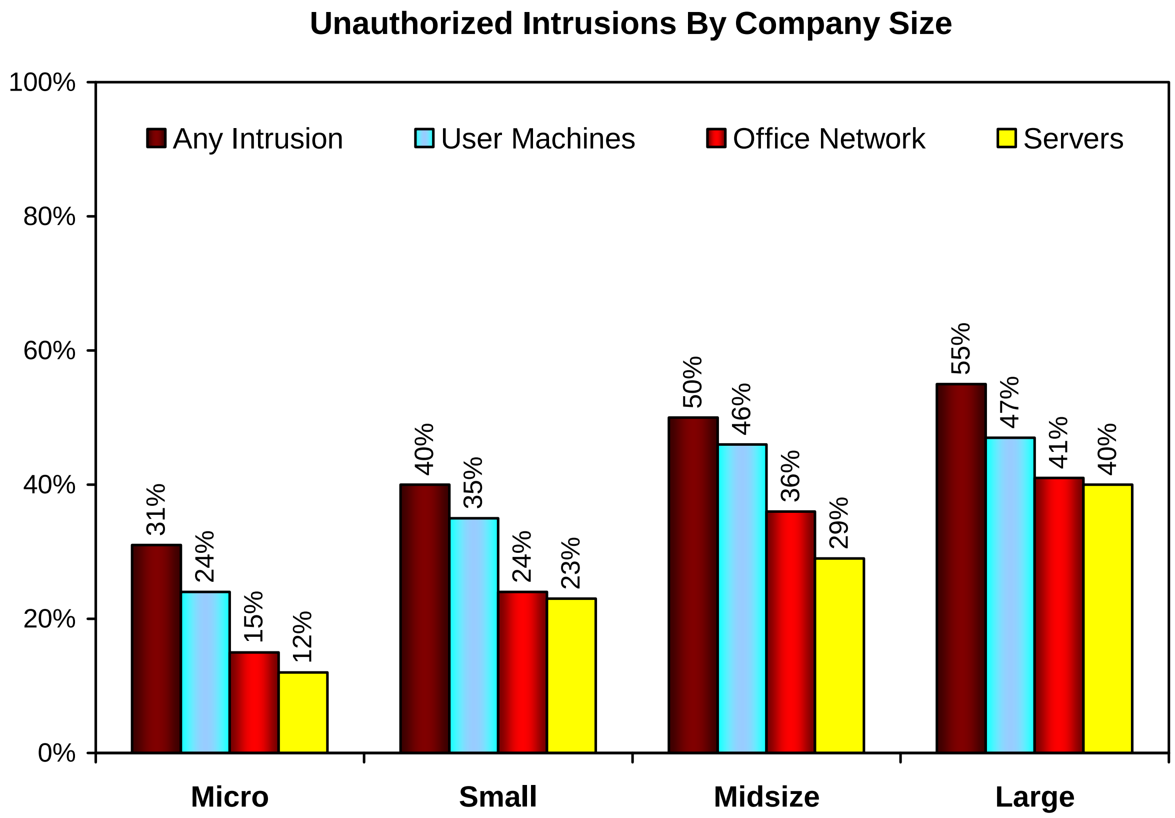
- Respondents were asked three questions about successful intrusions by a hacker or other unauthorized person in the past two years. In the first question, 42% in 2008 indicated that at least one user machine at their office experienced a successful intrusion. In the second question, 31% in 2008 indicated that their office network experienced a successful intrusion. In the third question, 29% reported that one or more of their servers experienced a successful intrusion. These results are shown in the chart below and compared to previous years.

Incidence Of Hacker / Unauthorized Intrusions



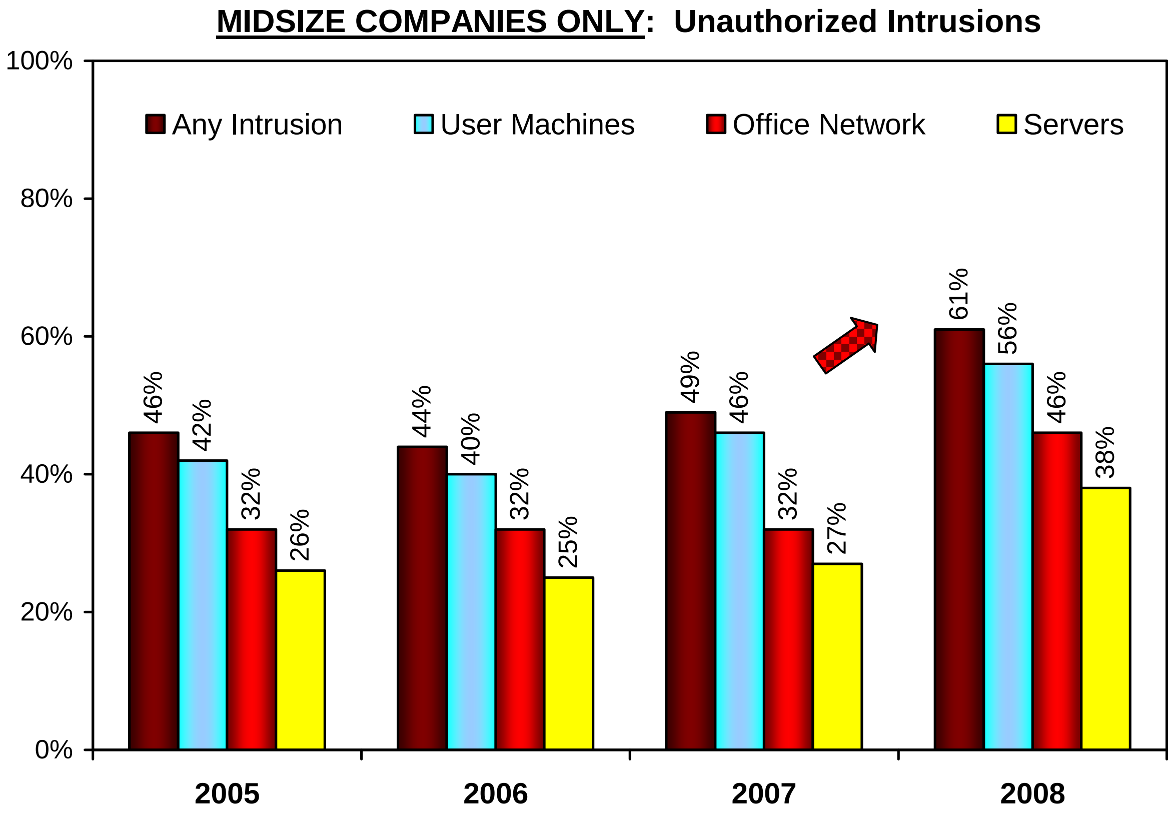
- The chart above shows that 48% in 2008 had experienced "any intrusion," which means a successful unauthorized intrusion of a user machine *or* office network *or* server. This 2008 result was higher than in previous years, although the increase was not quite large enough to be "statistically significant." However, one might have expected to find organizations reducing the incidence of hacker / unauthorized intrusions over time, whereas the study results suggest that there has been no overall progress.

- The incidence of experiencing a hacker / unauthorized intrusion increased with company size. As shown in the chart below, 55% of the respondents working for a large company reported an unauthorized intrusion, compared to 31% of "micro" companies (i.e., with less than 100 employees). (The results in the chart below are combined for all years to provide a robust sample size for each company / organization size category.)



- When looking at the results separately for each company / organization size category *by year*, the incidence of intrusions did not change significantly for micro, small, and large companies.

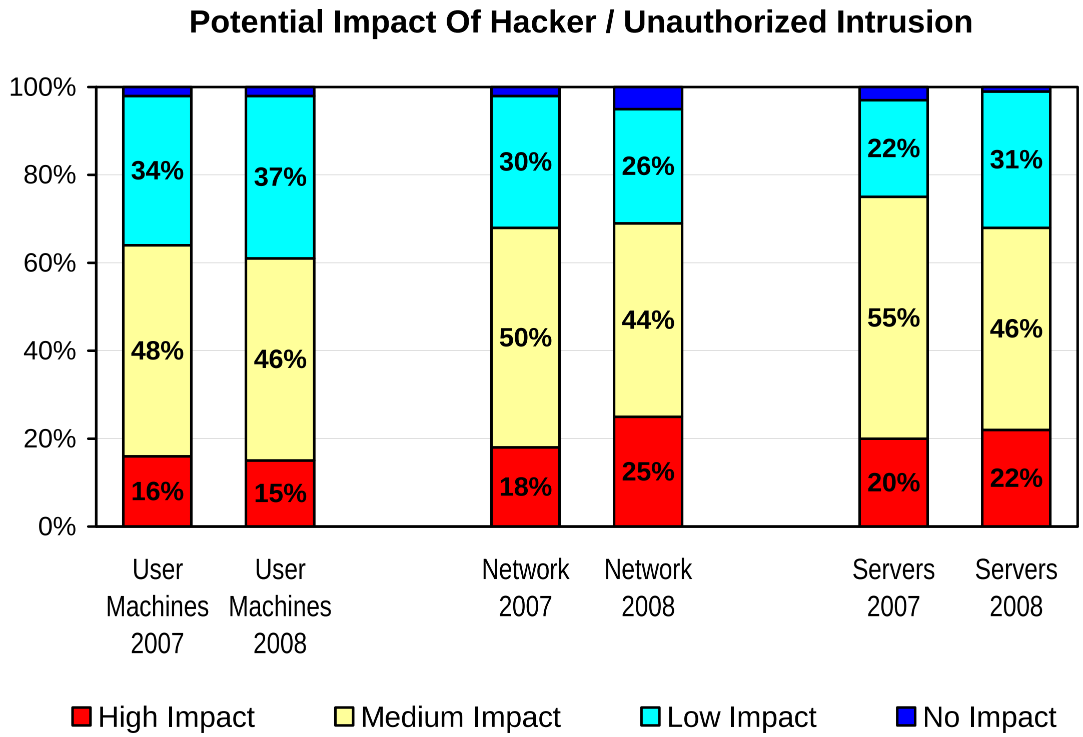
- However, results did in fact change significantly among midsize companies. As shown in the next chart, 61% of the respondents working for midsize organizations in 2008 reported a hacker / unauthorized intrusion. This was significantly higher than the average result over the previous three years (ranging from a low of 44% to a high of 49%).



- The chart above also shows noticeable increases in 2008 among midsize companies in unauthorized intrusions of user machines, the office network, and servers. These increases in 2008 (vs. the average results over the previous three years) were "statistically significant."

- It is one thing for a company to experience an unauthorized intrusion, but it is another thing if the intrusion has an impact, such as the possibility of a hacker obtaining sensitive information. The next chart shows how those who experienced an intrusion rated the potential financial impact on their organization based on the information that might have been obtained via unauthorized intrusions. For example, between 15% and 25%, depending on the type of equipment, gave a rating of "high impact." Between 44% and 55%, depending on the type of equipment and year, gave a rating of "medium impact."

    - The question about the impact of intrusions (and also another question to be covered shortly about sensitivity of the information) was first included in the 2007 survey, and this is why results are shown below only for 2007 and 2008.

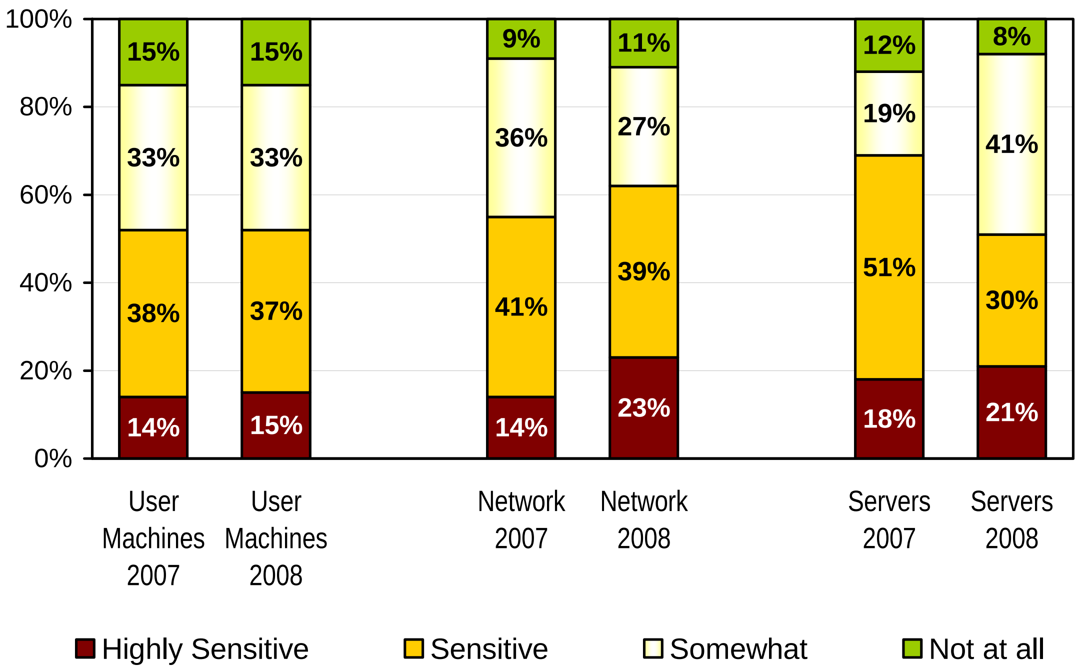


- The results shown above for 2008 were very similar to the 2007 results, and the small differences between years were not "statistically significant." However, the similarity in results between years confirms the findings that were first revealed in 2007. Last year, it was somewhat surprising to find that more than half of those experiencing intrusions felt there was a medium or high potential financial impact based on the information that might have been obtained. Now, the 2008 results confirm the 2007 findings and further suggest that unauthorized intrusions continued to be a serious concern for many companies / organizations.

- The next chart shows how respondents who experienced an intrusion rated the sensitivity of the information that might have been obtained as a result of unauthorized intrusions. Based on this measure, between 14% and 23% (depending on the type of equipment and year) rated "highly sensitive," while between 30% and 51% rated "sensitive."

- Results below for 2008 did not differ significantly compared to 2007 for user machines and office networks. However, there was a statistically significant change for servers, with fewer giving a "sensitive" rating (decline from 51% to 30%) and more giving a "somewhat sensitive" rating (from 19% to 41%).

Sensitivity Of Data That Might Have Been Obtained



Active Monitoring Of Server Security

- Most reported actively monitoring the security of their servers, although 10% in 2008 did not do so (as shown in the "none" row in the table below). Close to two-thirds (64%) in 2008 reported actively monitoring 90% to 100% of their servers. Interestingly, this result from the 2008 survey was similar to the 2005 and 2006 surveys, but there was a significant drop in 2007. That is, the proportion actively monitoring most (i.e., 90% to 100%) of their servers dropped significantly from 66% in 2006 to 55% in 2007 and then rebounded significantly in 2008 to 64%.

Percentage Of Servers Actively Monitored For Security

	2005	2006	2007	2008
None	13%	9%	10%	10%
Less than 50%	4%	5%	6%	3%
50% to 80%	15%	20%	29%	23%
90% to 100%	68%	66%	55%	64%

- The pattern of decline from 2006 to 2007 and then rebounding in 2008 occurred within the small, midsize, and large company size categories, as shown below. For example, 72% of small companies actively monitored most of their servers in 2006, but only 52% did so in 2007, and the proportion increased to 65% in 2008.

Proportion Actively Monitoring 90% to 100% Of Servers By Company Size

	2005	**2006**	**2007**	**2008**
Micro	59%	64%	71%	66%
Small	75%	72%	52%	65%
Midsize	68%	61%	55%	63%
Large	66%	67%	50%	63%

- As another example, the proportion of midsize companies actively monitoring most of their servers declined from 68% in 2005 to 61% in 2006 to 55% in 2007 and then rebounded to 63% in 2008.
  - Some caution is needed when examining the results specifically for midsize companies because the sample size each year ranged from 75 to 81 for this category. Because "statistical significance" is a function of sample size, as well as the magnitude of change, the trend noted above for midsize companies was not "officially" statistically significant. However, the significant drop in 2007 shown in the previous table for the total sample (i.e., all company sizes combined) was statistically significant. At the same time, the drop in 2007 and 2008 rebound occurred consistently across the small, midsize, and large categories. This consistency provides some additional support for the year-to-year pattern noted specifically for midsize companies.
- Given the earlier finding that midsize companies were more likely in 2008 vs. earlier years to report intrusions of their servers, one might hypothesize that actively monitoring less than 90% of their servers may have "caught up with them," and some may have reversed course in 2008 from insufficient security monitoring in 2007. After all, the question about intrusions was based on the timeframe of "in the past two years," so that insufficient monitoring of servers a year or two years ago may have had an impact on current results.
  - Given the nature of survey data, which is obviously not experimentally controlled to test theories of cause and effect, we

cannot prove that monitoring less than 90% of their servers led to a higher risk of intrusions. However, it is interesting to note that across all years and among all companies that reported actively monitoring the security of 90% to 100% of their servers, 22% also reported an unauthorized intrusion of their servers. In contrast, among those reporting actively monitoring the security of between 1% and 80% of their servers, 43% reported an unauthorized intrusion of their servers. In other words, actively monitoring the security of a higher percentage of servers was significantly associated with a lower incidence of unauthorized intrusions of servers.

  - It is also interesting that among those who monitor the security of 90% to 100% of their servers *and* experienced an intrusion of one or more of their servers, 38% reported that the intrusion(s) had a low impact or no impact. In contrast, among those monitoring the security of up to 80% of their servers *and* experiencing an intrusion, 19% reported a low or no financial impact from the intrusion. At the same time, those monitoring most of their servers but still experiencing an intrusion were less likely than those doing less monitoring and experiencing an intrusion to rate the information possibly obtained as “sensitive” or “highly sensitive” (52% vs. 68%).

- Among those who monitor the security of at least some of their servers, roughly four-in-ten in 2008 (41%, as shown in the table below) reported “daily” monitoring, while a similar proportion reported “weekly” monitoring (43%). The change in the proportion reporting daily monitoring declined significantly from 2006 to 2007. Daily monitoring rebounded in 2008, although the change between 2007 and 2008 was not quite large enough to be officially statistically significant.

***Frequency* Of Actively Monitoring Servers For Security**

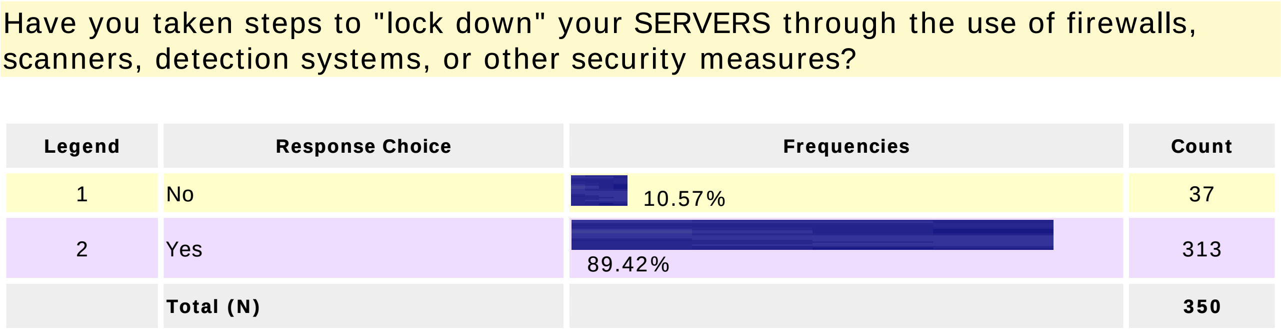
	2005	**2006**	**2007**	**2008**
Daily	45%	43%	36%	41%
Weekly	38%	43%	43%	43%
Monthly	8%	8%	15%	12%
Quarterly	1%	3%	1%	1%
As time permits	8%	3%	5%	3%

- The table below shows the proportion by company / organization size who perform daily monitoring of their servers (among those monitoring the security of at least some of their servers). For micro, small, and large companies, there was a slight decline between 2006 and 2007, followed by a slight rebound in 2008. Among midsize companies, there was a decline between 2007 and 2008, although the change was not large enough to be statistically significant.

Proportion Monitoring Server Security
***Daily* By Company Size**

	2005	**2006**	**2007**	**2008**
Micro	37%	48%	35%	40%
Small	43%	36%	22%	42%
Midsize	37%	43%	44%	35%
Large	58%	51%	44%	48%

- Related to monitoring server security, a question was asked about taking steps to "lock down" servers, and a follow-up question was asked about the specific steps taken. As shown below, most respondents reported locking down their servers, and the most common step was to install a firewall appliance.



Have you taken steps to "lock down" your SERVERS through the use of firewalls, scanners, detection systems, or other security measures?

Legend	Response Choice	Frequencies	Count
1	No	10.57%	37
2	Yes	89.42%	313
	Total (N)		**350**

What steps have you taken to lock down your SERVERS:

Legend	Response Choice	Frequencies	Count
1	Installed a firewall appliance (e.g., Cisco, Juniper, etc.)	70.92%	222
2	Installed a software firewall (e.g., Windows Firewall, Zone Alarm, etc.)	56.86%	178
3	Turned off non-secure protocols like Telnet or FTP	47.92%	150
4	Set up a DMZ	37.38%	117
5	Installed an Intrusion Detection System (IDS)	46.96%	147
6	Use of a port scanner to locate out-of-policy services on the server(s)	43.13%	135
7	Use of a network analyzer (e.g., Microsoft Baseline Security Analyzer)	50.15%	157
8	Implemented WiFi security (e.g., WEP, WAP, brand-specific like 3Com)	39.29%	123
	Total (N)		**313**

- The above results are based on 2008, but the results did not change very much year to year for most of the different types of "lock down" steps taken. One exception was that setting up a DMZ was significantly less common in 2008 (37%), compared to 2007 (46%). Another exception was that implementing WiFi security was up significantly in 2008 (39%) vs. 2007 (31%). However, in both cases the 2008 results were not significantly different from the 2005 and 2006 results, and we would suggest tracking future results to verify if a true trend began with the change between 2007 and 2008.

- The finding shown above that 89% have taken steps to "lock down" servers applies to all company sizes combined for 2008. The table below shows the proportions for each company size category by year. Even among the smallest companies, more than eight-in-ten have locked down their servers, while more than nine-in-ten midsize and large companies have done so.

Have Taken Steps To "Lock Down" Servers By Company Size

	2005	2006	2007	2008
Micro	81%	84%	87%	83%
Small	88%	89%	88%	85%
Midsize	94%	95%	91%	96%
Large	92%	90%	97%	94%

Active Monitoring Of User Machine / Office Network Security

- Most reported actively monitoring the security of their user machines and/or office network, although 11% in 2008 did not do so (as shown in the "none" row in the table below). Just over half (51%) in 2008 reported actively monitoring the security of 90% to 100% of their user machines / office network, and this did not differ significantly from previous years.

Percentage Of User Machines / Network Actively Monitored For Security

	2005	2006	2007	2008
None	17%	14%	10%	11%
Less than 50%	6%	8%	8%	5%
50% to 80%	24%	27%	37%	33%
90% to 100%	53%	51%	45%	51%

- Although the slight dip in 2007 in the proportion monitoring 90% to 100% of their user machines / network was not statistically significant, there was a slight dip that year among small, midsize, and large companies, as shown below.

Proportion Actively Monitoring 90% to 100% Of User Machines / Network By Co. Size

	2005	2006	2007	2008
Micro	54%	56%	56%	56%
Small	58%	46%	43%	46%
Midsize	49%	51%	44%	46%
Large	51%	54%	42%	58%

- Across all years and company sizes, those actively monitoring 90% to 100% of their user machines / office network were less likely than those monitoring up to 80% to report an unauthorized intrusion (39% vs. 54%). This is similar to the finding noted earlier for servers. Thus, in general, monitoring 90% to 100% of a company's user machines, office network, and/or servers was associated with a lower incidence of unauthorized intrusions, compared to those monitoring up to 80% of their machines / networks / servers.

- Among those who monitor the security of at least some of their user machines / network, the proportion performing "daily" monitoring declined significantly between 2006 and 2007 and then rebounded significantly between 2007 and 2008. A similar pattern for servers was noted earlier, but the pattern in the table below was slightly more pronounced compared to results for servers.

Frequency Of Actively Monitoring User Machines / Network For Security

	2005	**2006**	**2007**	**2008**
Daily	39%	37%	28%	39%
Weekly	37%	44%	48%	44%
Monthly	12%	11%	14%	9%
Quarterly	2%	2%	1%	4%
As time permits	10%	6%	9%	4%

- The pattern of a drop in the proportion reporting daily monitoring between 2006 and 2007, followed by a rebound in 2008, was evident among small, midsize, and large companies, as shown below.

Proportion Monitoring User Machine / Network Security _Daily_ By Company Size

	2005	**2006**	**2007**	**2008**
Micro	27%	35%	32%	30%
Small	43%	34%	17%	42%
Midsize	29%	35%	26%	31%
Large	52%	44%	38%	51%

- Most respondents reported locking down their user machine / office network and the most common step was to install a network firewall.

Have you taken steps to "lock down" your USER MACHINES and/or OFFICE NETWORK through the use of firewalls, scanners, detection systems, or other security measures?

Legend	Response Choice	Frequencies	Count
1	No	8.85%	31
2	Yes	91.14%	319
	Total (N)		**350**

What steps have you taken to lock down your USER MACHINES and/or OFFICE NETWORK:

Legend	Response Choice	Frequencies	Count
1	Installed a network firewall	89.65%	286
2	Installed a user-based firewall (e.g., Windows Firewall, Zone Alarm, etc.)	53.91%	172
3	Turned off non-secure protocols like Telnet or FTP	46.08%	147
4	Set up a DMZ	38.87%	124
5	Installed an Intrusion Detection System (IDS)	52.35%	167
6	Use of a port scanner to locate out-of-policy services on the network	42.31%	135
7	Use of a network analyzer (e.g., Microsoft Baseline Security Analyzer)	49.52%	158
8	Implemented WiFi security (e.g., WEP, WAP, brand-specific like 3Com)	53.29%	170
	Total (N)		**319**

- The above results are based on 2008, but the results did not change significantly year to year for most of the different types of "lock down" steps taken. One exception was that implementing WiFi security was up significantly in 2008 (53%) vs. 2007 (42%). However, 50% reported implementing WiFi security in 2006, which was not significantly different from 2008.

- The finding shown above that 91% have taken steps to "lock down" user machines and/or their network applies to all company sizes combined for 2008. The table below shows the proportions for each company size category by year. Even among the smallest companies, more than eight-in-ten have locked down their user machines and/or network, while more than nine-in-ten midsize and large companies have done so.

Have Taken Steps To "Lock Down" User Machines / Network By Company Size				
	2005	**2006**	**2007**	**2008**
Micro	81%	83%	84%	89%
Small	94%	86%	89%	86%
Midsize	91%	95%	90%	99%
Large	91%	91%	97%	93%

Company Resources Monitoring / Maintaining IT Equipment

- The proportion of companies / organizations assigning 10 or more IT professionals to be actively involved in monitoring, maintaining, and/or updating user machines, office networks, or servers was similar in 2007 and 2008, while results in these two years were slightly higher than in 2005 and 2006.

Number Of IT Professionals Monitoring / Maintaining Computers / Network / Servers				
	2005	**2006**	**2007**	**2008**
1	16%	12%	9%	11%
2 to 5	33%	31%	23%	27%
6 to 10	19%	20%	24%	21%
11 to 25	13%	17%	20%	23%
More than 25	19%	20%	24%	18%
More than 10	32%	37%	44%	41%

- Of course, one would expect the number of IT employees to be highly correlated with company size, and the results by size category by year are shown in the next table. However, the above table is still worth examining because the distribution of company sizes in the total sample each year was not significantly different. When the distribution of company sizes is similar but there are changes in the number of IT employees actively monitoring / maintaining and/or updating IT equipment, then this can be noteworthy. To be sure, the changes in the table above are slight. It may have been more interesting if the increase between 2006 and 2007 was matched by a similar or larger increase between 2007 and 2008. But, in fact, the 2008 proportion for more than 10 IT professionals fell between the 2006 and 2007 proportions.

More Than 10 IT Professionals Monitoring / Maintaining IT Equipment By Co. Size

	2005	**2006**	**2007**	**2008**
Micro	1%	4%	3%	1%
Small	10%	18%	22%	26%
Midsize	43%	51%	69%	60%
Large	75%	80%	75%	74%

- Not surprisingly, nearly all micro-sized companies did not have 10 or more IT professionals actively involved in monitoring, maintaining, and/or updating user machines / networks / servers, while approximately three-fourths of large companies did. What is more interesting, though, is that the results in 2007 and 2008 were higher than in 2005 and 2006 for small and midsize companies.

- When it comes to the share of the respondent's average work week spent on monitoring, maintaining or updating user machines, networks, or servers, more than half gave a response of at least 25%.

Share Of Work Week Monitoring / Maintaining Computers / Network

	2005	**2006**	**2007**	**2008**
Less than 10%	17%	18%	15%	16%
10% to 25%	41%	34%	28%	26%
25% to 50%	23%	26%	27%	28%
50% to 75%	12%	15%	22%	21%
75% to 100%	7%	7%	8%	9%
At least 25%	42%	48%	57%	58%

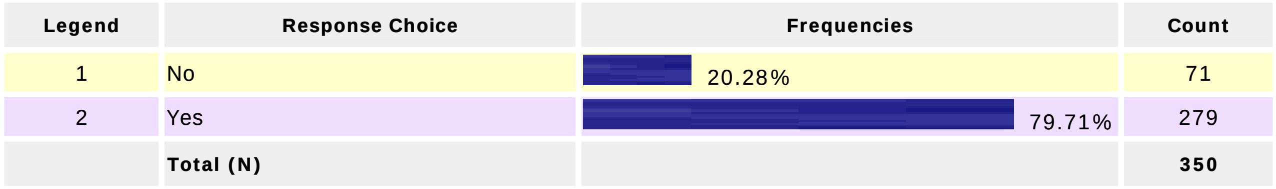
- When examining the results by company size, the 2007 and 2008 results were higher than the 2005 and 2006 results among small, midsize, and large companies.

At Least 25% Of Work Week Monitoring / Maintaining Computers / Network By Co. Size				
	2005	**2006**	**2007**	**2008**
Micro	28%	33%	29%	30%
Small	42%	46%	66%	66%
Midsize	46%	52%	56%	61%
Large	50%	59%	65%	69%

IT Budgeting

- A number of new questions related to IT budgeting were added to the 2008 survey. Although we do not have comparisons to previous years on these questions, the 2008 results alone are revealing. To start with, eight-in-ten (80%) respondents felt that their organization has budgeted sufficiently for information security needs.

Do you feel your organization has budgeted sufficiently to support current **information security** needs?



Legend	Response Choice	Frequencies	Count
1	No	20.28%	71
2	Yes	79.71%	279
	Total (N)		**350**

- When examining the results by company size, 76% of micro-sized companies, 79% of small companies, and 82% of midsize and large companies felt their organization has budgeted sufficiently. The next two figures show expected budget changes for 2008, first for their overall IT budget, and then more specifically for their IT security budget.

What changes, if any, are you seeing in your **overall** IT budget for 2008 as compared to 2007?

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	4.85%	17
2	Decrease by less than 10%	8.85%	31
3	No change	32.0%	112
4	Increase by less than 10%	32.0%	112
5	Increase by more than 10%	20.28%	71
6	Don't know	2.0%	7
	Total (N)		**350**

What changes, if any, are you seeing in your **IT security budget** for 2008 as compared to 2007?

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	4.57%	16
2	Decrease by less than 10%	7.14%	25
3	No change	38.28%	134
4	Increase by less than 10%	29.42%	103
5	Increase by more than 10%	17.42%	61
6	Don't know	3.14%	11
	Total (N)		**350**

- This shows that the results for the IT budget overall were similar to results for the IT security budget specifically. Given this similarity, and since the survey was primarily concerned with IT security issues, we will focus more on the latter while making several points. First, it is interesting that a significantly higher proportion expected an increase (47%) than expected a decrease (12%) in their IT security budget.

- Second, those who felt their company has budgeted sufficiently to support current information security needs were less likely than those who did not feel this way to say that they expected a decrease in their IT budget (8% vs. 28%). At the same time, among those feeling their company has budgeted sufficiently, 51% expected an increase in their IT security budget for 2008. Among those feeling their company has not budgeted sufficiently, 32% expected an increase for 2008 in their IT security budget.

- Third, the proportion expecting an increase or decrease in their IT security budget varied somewhat by company size, as shown below:

Changes Expected In IT Security Budget For 2008 Compared To 2007

	Micro	Small	Midsize	Large
Decrease more than 10%	7%	4%	4%	3%
Decrease less than 10%	3%	8%	9%	8%
Total decrease	10%	12%	13%	11%
No change / don't know	61%	38%	27%	43%
Increase less than 10%	16%	33%	41%	25%
Increase more than 10%	13%	17%	19%	21%
Total increase	29%	50%	60%	46%

- Of particular interest, 60% of midsize companies expected an increase in their IT security budget. This may not be too surprising after examining the findings presented earlier related to unauthorized intrusions. As the incidence of hacker / unauthorized intrusions increased significantly among midsize companies, it makes sense that many would expect an increase in their IT security budget to help battle intrusions.
    - Ideally, we would like to be able to verify the connection among midsize companies between likelihood of increasing the IT security budget and experiencing intrusions. However, the question about budgeting was first introduced in the 2008 survey, and the total number of respondents representing midsize organizations in 2008 was 79. Breaking out the results on intrusions for midsize companies with different IT budget expectations would result in sample sizes that are too small to justify conclusions for this company size category. We recommend continuing to ask budget related questions in future years to accumulate more data to allow further analysis. However, when examining all companies that expect an increase in their IT security budget, 56% reported an unauthorized intrusion during the past two years; whereas, among those expecting no change in their IT budget, 39% reported an

unauthorized intrusion. For those who expected a decrease in their IT security budget, we only have 41 respondents (a sample size too small to draw solid conclusions), but 51% of them reported an unauthorized intrusion.

- Another way to assess changes in IT spending is to compare results in the following two figures. The first figure shows amounts authorized without additional signatures in 2008, while the second figure shows results for the same question but referring to 2007. In the end, the results were very similar, suggesting there has not been a noteworthy change between 2007 and 2008.

This year (**2008**), what dollar amount are you authorized to spend without additional signature(s)?

Legend	Response Choice	Frequencies	Count
1	$0, an authorizing signature is required for all purchases	9.42%	33
2	$1-500	5.71%	20
3	$501-1,000	10.28%	36
4	$1,000-$4,999	26.0%	91
5	$5,000 or above	43.71%	153
6	Don't know	4.85%	17
	Total (N)		**350**

Last year (**2007**), what dollar amount were you authorized to spend without additional signature(s)?

Legend	Response Choice	Frequencies	Count
1	$0, an authorizing signature was required for all purchases	9.71%	34
2	$1-500	6.0%	21
3	$501-1,000	11.71%	41
4	$1,000-$4,999	24.85%	87
5	$5,000 or above	42.85%	150
6	Don't know	4.85%	17
	Total (N)		**350**

- Less that one-third (29%, as shown below) were aware of their company postponing (but not canceling) any IT security projects during 2008 as a result of a perceived poor economy. By company size, 21% of micro-sized, 25% of small, 35% of midsize, and 36% of large organizations reported postponing IT security projects during 2008 for economic reasons.

Are you aware of your company **postponing** (but not canceling) any IT security endeavors/projects during 2008 as a result of a perceived poor economy?

Legend	Response Choice	Frequencies	Count
1	No	70.85%	248
2	Yes	29.14%	102
	Total (N)		**350**

- Among those who felt their company has budgeted sufficiently to support current information security needs, 27% were aware of a postponed IT security project, and this compares to 39% of those not feeling their company has budgeted sufficiently. However, although there was a difference based on the perceived sufficiency of IT security budgeting, it is noteworthy that many companies that have postponed an IT security project were still thought to have a sufficient budget for information security needs. In a way, this is not too surprising, since 80% felt their company has budgeted sufficiently, and this is most of the sample. Yet, it is worth keeping in mind that a postponed project does not always mean that the overall IT security budget becomes insufficient for information security needs.

- Also, among those aware of their company postponing an IT security project, 61% still expected an increase in their IT security budget for 2008 as compared to 2007. This shows that postponing IT security projects does not necessarily mean a decrease in the overall annual budget.

- Despite the above observations, though, every company is different, and there were some expecting that postponed IT projects would account for a large percentage of their total IT security budget. For example, the next figure shows that 26% reported that postponed projects represented more than 70% of their total IT security budget.

    - As a caveat, we do not know how long IT projects have been postponed and whether or not spending on some of these projects could be resumed before year-end.

    - We also don't know if some IT projects were postponed while spending was increased on other activities, such as monitoring for intrusions, for example. It is still interesting that many are postponing IT projects for economic reasons, but this does not necessarily point to reductions in overall IT security spending. (Similar caveats apply to a later question about *canceling* IT projects.)

What percentage does the postponed endeavors/projects represent of the total IT security budget planned for 2008?

Legend	Response Choice	Frequencies	Count
1	Less than 10%	6.86%	7
2	10% to 20%	10.78%	11
3	21% to 30%	17.64%	18
4	31% to 40%	8.82%	9
5	41% to 50%	5.88%	6
6	51% to 60%	11.76%	12
7	61% to 70%	10.78%	11
8	71% to 80%	17.64%	18
9	81% to 90%	5.88%	6
10	More than 90%	2.94%	3
11	Don't know	0.98%	1
	Total (N)		**102**

- Less that one-fourth (23%, as shown below) were aware of their company *canceling* any IT security projects during 2008 as a result of a perceived poor economy. By company size, 14% of micro-sized, 16% of small, 32% of midsize, and 32% of large organizations reported canceling IT security projects during 2008 for economic reasons.

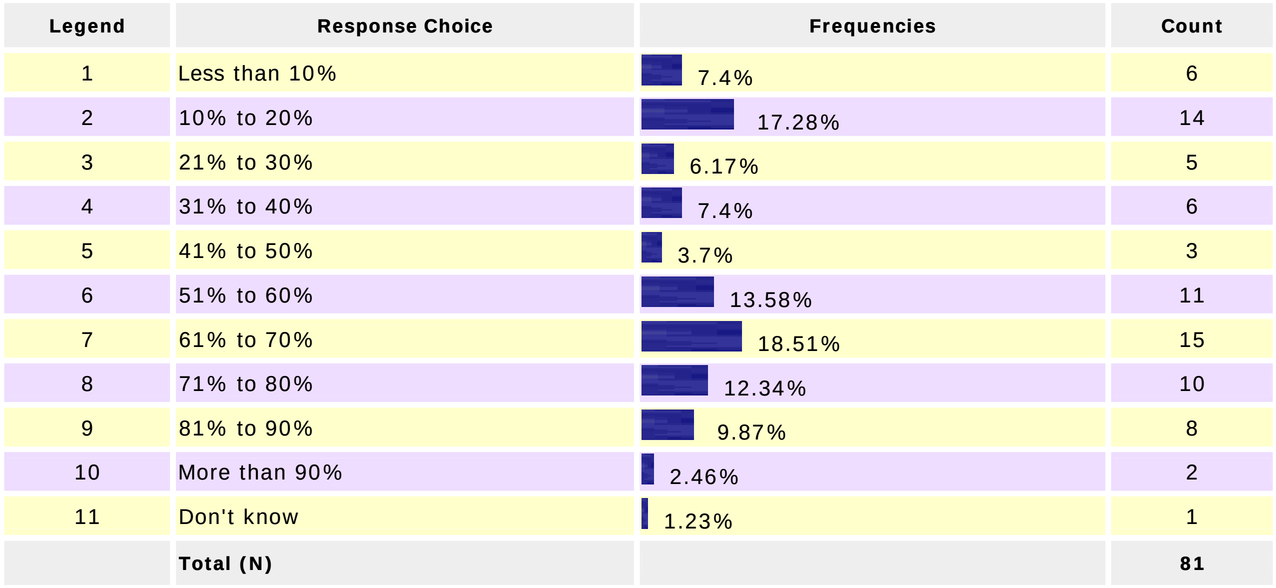
Are you aware of your company **canceling** any IT security endeavors/projects during 2008 as a result of a perceived poor economy?

Legend	Response Choice	Frequencies	Count
1	No	76.85%	269
2	Yes	23.14%	81
	Total (N)		**350**

- Among those who felt their company has budgeted sufficiently to support current information security needs, 22% were aware of a canceled IT security project, and this compares to 28% of those not feeling their company has budgeted sufficiently. In this case, the difference between 22% and 28% was not statistically significant, and this suggests that canceling some IT security projects is not necessarily associated with insufficient budgeting for information security needs.

- Also, among those aware of their company canceling an IT security project, 65% still expected an increase in their IT security budget for 2008 as compared to 2007. This shows that even canceling IT projects does not necessarily mean a decrease in the overall annual budget. Yet, there were still some who reported canceled projects as a fairly high percentage of the total IT security budget, as shown below.

What percentage does the canceled endeavors/projects represent of the total IT security budget planned for 2008?



Legend	Response Choice	Frequencies	Count
1	Less than 10%	7.4%	6
2	10% to 20%	17.28%	14
3	21% to 30%	6.17%	5
4	31% to 40%	7.4%	6
5	41% to 50%	3.7%	3
6	51% to 60%	13.58%	11
7	61% to 70%	18.51%	15
8	71% to 80%	12.34%	10
9	81% to 90%	9.87%	8
10	More than 90%	2.46%	2
11	Don't know	1.23%	1
	Total (N)		**81**

- As mentioned for the question about postponing IT security projects, we do not know why IT projects were cancelled. There are probably many different reasons, and each company may face a different set of circumstances. In some cases, new projects may have been cancelled to make room to devote more resources to more mundane efforts to fend off security threats. This is a hypothesis at this point, but an interesting finding inspires it. Among those aware of their company canceling any IT security projects during 2008 as a result of a perceived poor economy, 84% also reported that their company had a successful hacker / unauthorized intrusion. This can be compared to 38% experiencing a successful intrusion among those not aware of any IT security projects being cancelled.

    - We do not know why there is such a strong association between canceling IT projects and experiencing intrusions. One might expect company size to be a related factor, but the relationship holds *within* each company size category. (To be sure, sample sizes get very small when cutting by company size *and* awareness of canceled IT security projects, but the results were still consistent within each company size category.) One might also wonder if the canceling of IT security projects was a cause of more intrusions. But, we cannot conclude this based on the currently available data. The incidence of intrusions is based on experiences over the past two years, whereas the question about canceling projects refers to economic conditions in 2008. To say something even mildly suggestive about "cause and effect" we would want to see the cancellation of IT security projects occur *first* and then see this *followed* at a later time by increased intrusions. Yet, even though we cannot draw major cause and effect conclusions, it is still very interesting that a very high proportion of those canceling IT security projects reported experiencing successful hacker / unauthorized intrusions over the past two years.

- The next table shows results for a new question added to the 2008 survey that is not as directly related to budgeting as the previous questions, but it is still somewhat related because a formal security audit may require money allocated from the IT security budget. The results ranged from 12% reporting an outside security audit as frequently as twice a year or more often to 20% having never undergone a formal security audit by an outside organization.

How often does your organization undergo a formal security audit by an **OUTSIDE** organization?

Legend	Response Choice	Frequencies	Count
1	Never	20.28%	71
2	Every three years or less often	13.71%	48
3	Every two years	26.28%	92
4	Once a year	27.42%	96
5	Twice a year or more often	12.28%	43
	Total (N)		**350**

- One of the first questions the reader may ask is, how does the frequency of conducting an outside security audit relate to experiencing unauthorized intrusions? Based on the data we have at this point, the picture is not entirely clear. Part of the reason is that 2008 is the first year this question about security audits was asked. Asking the same question in future years can provide more data to allow further analysis. At this point, we can say that 44% of those undergoing an audit twice a year or more often reported a successful intrusion. However, this is based on only

43 respondents who reported having an outside audit twice a year or more often. Among those who have had an outside security audit once a year or every two years, 59% reported an intrusion. This would almost suggest that frequent outside security audits help reduce intrusions. But, among those having a security audit every three years or less often, 44% experienced an unauthorized intrusion in the past two years. Among those never having an outside security audit, 27% experienced an unauthorized intrusion. This last point is related to the fact half of those never having an outside security audit were micro-sized, and this category was also less likely to experience unauthorized intrusions. However, there were other factors involved as well, and we do not yet have enough data to clarify the findings – we do not yet have multiple years of data to “mine” for insights on this issue.

- The next figure shows results for a similar new question, but this one referred to *internal* security audits. (Similar issues as noted above surfaced for internal audits as for outside audits, and this question would be needed in future survey waves to accumulate more data for further analysis.)

How often does your organization undergo an **INTERNAL** security audit?

Legend	Response Choice	Frequencies	Count
1	Never	7.14%	25
2	Every three years or less often	8.0%	28
3	Every two years	16.28%	57
4	Once a year	38.0%	133
5	Twice a year or more often	30.57%	107
	Total (N)		**350**

Sources of Information About Security Best Practices

- A wide variety of sources are used to learn about security best practices, as shown in the table below. For many sources, the results were very consistent year to year. However, there has been a slight decline in usage of books and newsletters. The 2008 proportions selecting these sources were significantly lower vs. 2005, while results trended very slightly downward between 2005 and 2008.

Where Do You Get Information About Security Best Practices?				
	2005	**2006**	**2007**	**2008**
Security-related websites	69%	67%	68%	65%
Trade magazines (e.g., eWEEK, Network Computing, Secure Enterprise)	68%	68%	64%	62%
Training courses from professional organizations (e.g., SANS)	53%	54%	61%	58%
Conferences (e.g., NetSec, USENIX)	50%	55%	54%	59%
Online discussion forums	49%	51%	47%	50%
Books (e.g., O'Reilly, Wiley, Addison-Wesley, Microsoft Press)	49%	43%	42%	37%
Newsletters	49%	43%	41%	36%
Local training courses (e.g., college or university, user groups)	37%	34%	36%	37%
Security-related blogs	33%	35%	38%	33%
USENET groups	33%	33%	34%	32%