VanDyke
SOFTWARE

Amplitude Research®
loud & clear

5th Annual Survey:
Network and System Administrators

Commissioned study conducted by Amplitude Research, Inc.
April 30, 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 consists 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.
Amplitude Research® uses the moniker "loud and clear" to signify its commitment to high quality reporting with clear and concise presentation of the findings.
Amplitude's professional services include top-line reports, custom banner tabulations, significance testing, conjoint, cluster analysis, PowerPoint reports, verbatim coding, data entry, multivariate statistical analysis, complete survey administration, and comprehensive questionnaire design services.

Study History

This is the fifth year in a row that VanDyke Software has commissioned an Amplitude Research® survey of network and system 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 April 3rd to April 7th, 2008 among a nationwide web panel. In total, 300 surveys were completed by respondents who confirmed working as a "network or systems administrator" for their company / organization.

A "sample size" of 300 respondents has a "maximum sampling margin of error" of +/- 5.7 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%, while 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 +/- 3.4 percentage points.

The number of surveys completed with network administrators nationwide was similar in each of the five years this study was conducted:

- 340 completed surveys in 2004

- 280 completed surveys in 2005

- 255 completed surveys in 2006

- 300 completed surveys in 2007

- 300 completed surveys in 2008

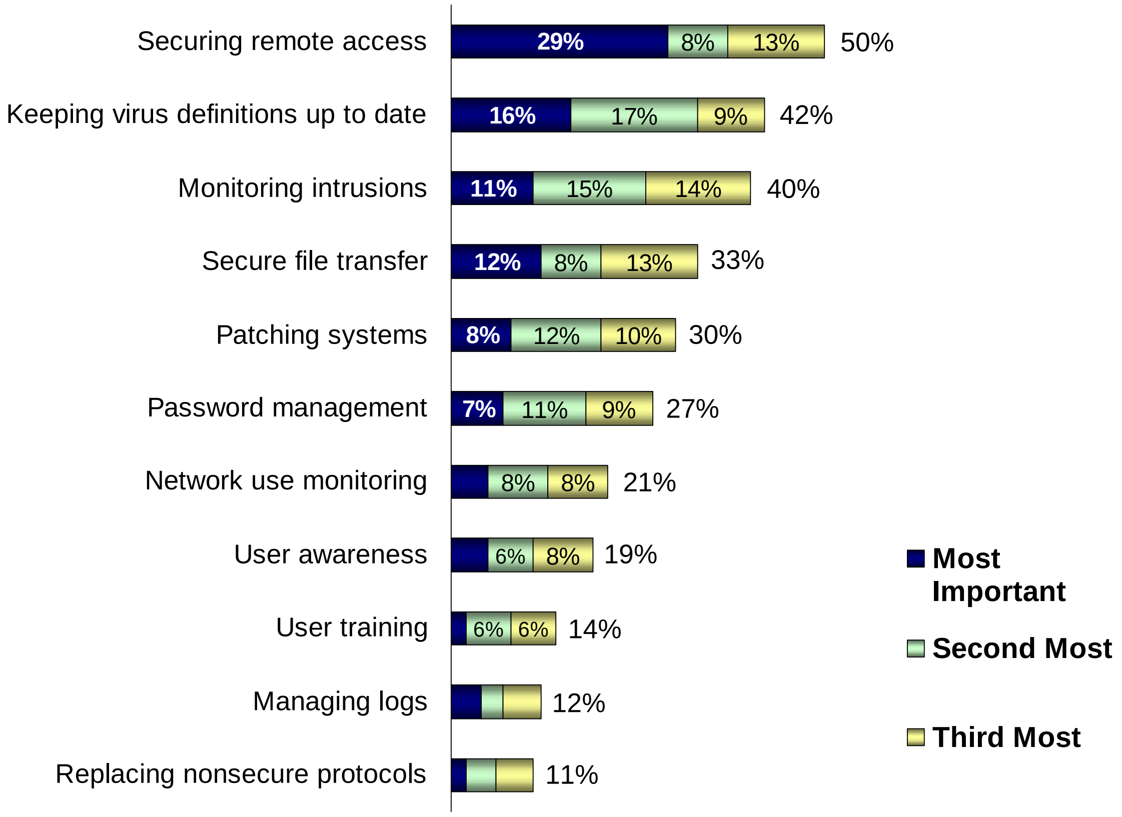
Study Findings

Key findings from the study are summarized on the following pages. The summary begins with a question about security management priorities. This helps to place the many different security issues in context. From there, the results for various specific topics are covered. Toward the end, with several new questions added to the 2008 survey, there is extensive discussion of network administrators' perceptions / expectations related to their 2008 IT budgets.

Security Management Priorities

- To help understand security management priorities, network administrators were asked to rank the top three issues facing their company / organization from a list of 11 items. The best way to begin examining the result is to first focus on the 2008 survey results, as shown in Figure 1 below. For example, 29% indicated that "securing remote access" is the #1 most important security management issue facing their company / organization. Another 8% gave "securing remote access" a rank of #2, and 13% gave it a rank of #3. In the end, 50% ranked "securing remote access" either 1, 2, or 3 in importance from the list of 11 items that are included in Figure 1.

Figure 1: Security Management Issues Ranked 1, 2, or 3 in Importance (2008 Results Only)



- After examining the 2008 results above, the next step is to make comparisons to previous years. One way to do this might be to create a chart like Figure 1 for each of the prior years, but making comparisons between these charts would be cumbersome for the reader. Fortunately, there are two alternative ways to examine the results over time. First, Figure 2 shows the proportion giving a #1 ranking for each issue each year. This helps to spot trends in how often each issue is considered the single most important priority. Second, Figure 3 shows the proportions ranking each item #1 or #2 or #3 (i.e., among their top three).

Figure 2: Proportion Ranking Each Issue #1 in Importance

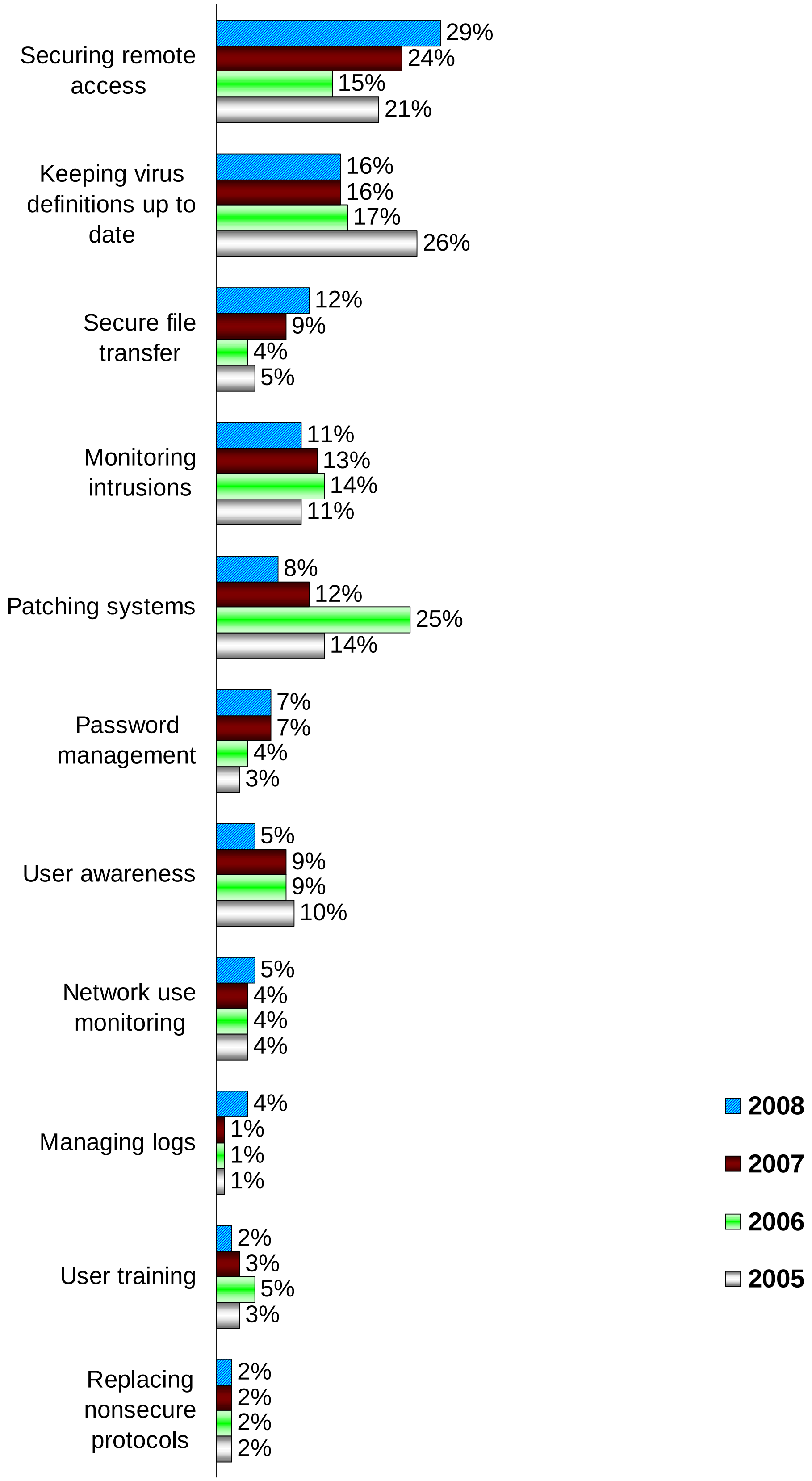
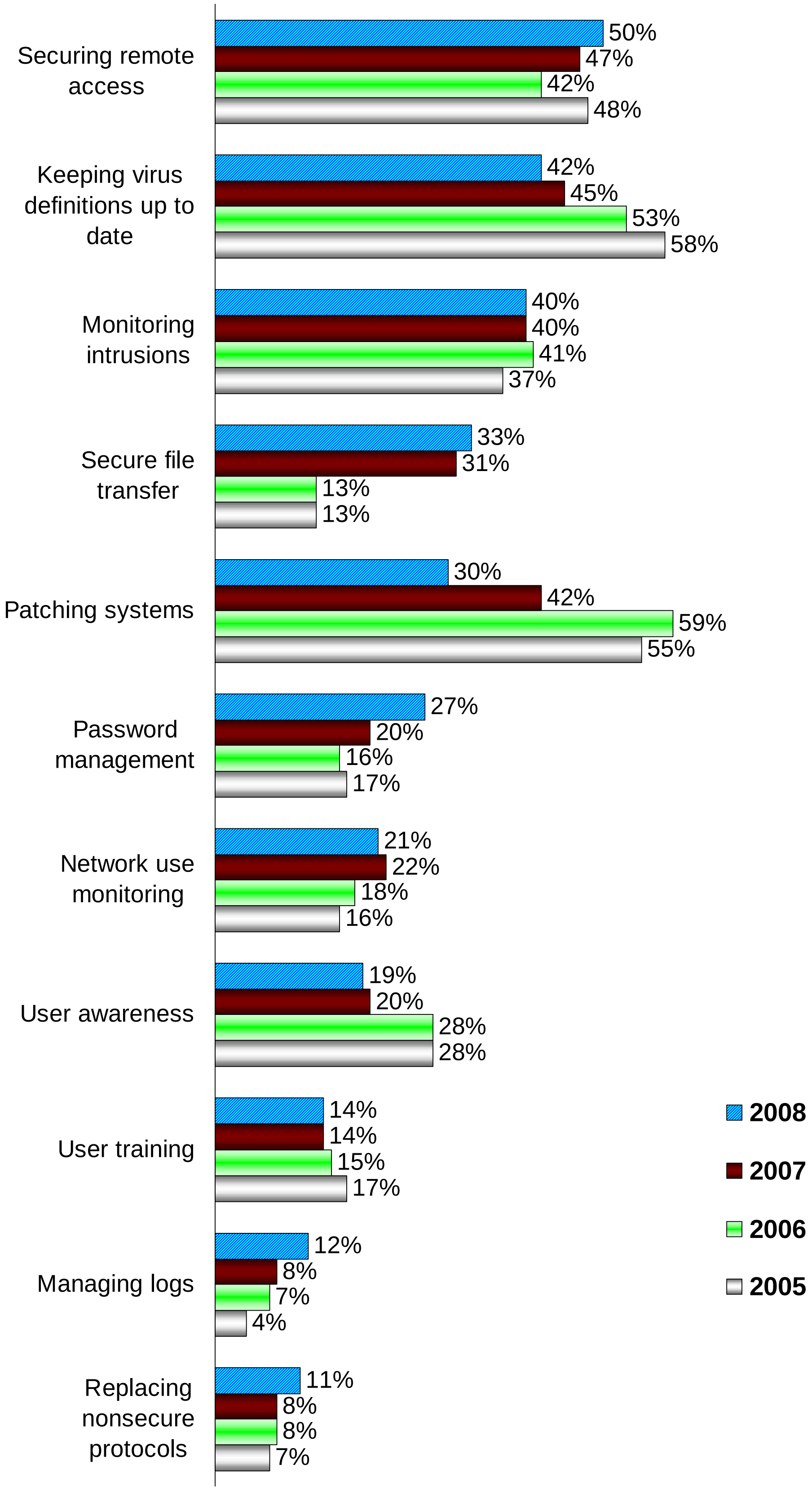


Figure 3: Total Proportion Ranking Each Issue 1, 2, or 3



- After examining Figures 2 and 3, the reader can identify a number of interesting changes over time. For example, back in 2005, the issue most often ranked #1 was "keeping virus definitions up to date" (26%), and this issue also had the highest proportion ranking it at least third in importance (58%). Since then, the proportion considering this issue to be among their top 3 priorities has fallen noticeably, but it still had a relatively high proportion ranking it 1, 2, or 3 in importance (42% in 2008).

- In 2006, the issue with the highest proportion ranking it #1 was "patching systems" (25%), while more than half (59%) ranked this issue at least third in importance. Since then, the proportion ranking "patching systems" #1 has declined significantly, as has the proportion ranking it 1-3.

- In 2007 and 2008, the issue with the highest proportion ranking it #1 was "securing remote access" (24% and 29%, respectively), while the proportion ranking it at least third in importance was close to half in 2007 (47%) and exactly half in 2008 (50%).

    - Figure 2 also shows a noticeable change between 2006 and 2008 in the proportion ranking "securing remote access" #1 in importance (from 15% to 29%). While results in Figure 2 are based on the total sample each year, it is also interesting to elaborate somewhat by noting similar changes within different company size categories. The change was from 12% in 2006 to 29% in 2008 among "small" companies (with fewer than 100 employees); from 15% to 28% among "midsize" companies (with 100 to 999 employees); and from 17% to 29% among "larger" companies (with 1,000 or more employees).

- Another interesting change worth emphasizing (as shown in Figure 3) is that the proportion giving a 1, 2, or 3 ranking for "secure file transfer" jumped significantly between 2006 and 2007 (from 13% to 31%), and then remained high in 2008 (33%).

    - To elaborate, changes from 2006 to 2008 in the proportion ranking "secure file transfer" 1-3 were evident for small companies (from 12% in 2006 to 32% in 2008), midsize companies (from 12% to 36%), and larger companies / organizations (from 13% to 31%).

- In general, these changes suggest that some network administrators have shifted their priorities more toward "securing remote access" and "secure file transfer" and away from "patching systems" and "keeping virus definitions up to date." This is not to say that the latter issues have become unimportant in *absolute* terms. While reflecting on the results, it is helpful to keep in mind that respondents were asked to *rank* the top three issues on the list. Even if they considered all of the issues important, they were still asked to identify the issues that they felt were the *most*, *second most*, and *third most* important from the list. For this reason, the results reflect *priorities*.

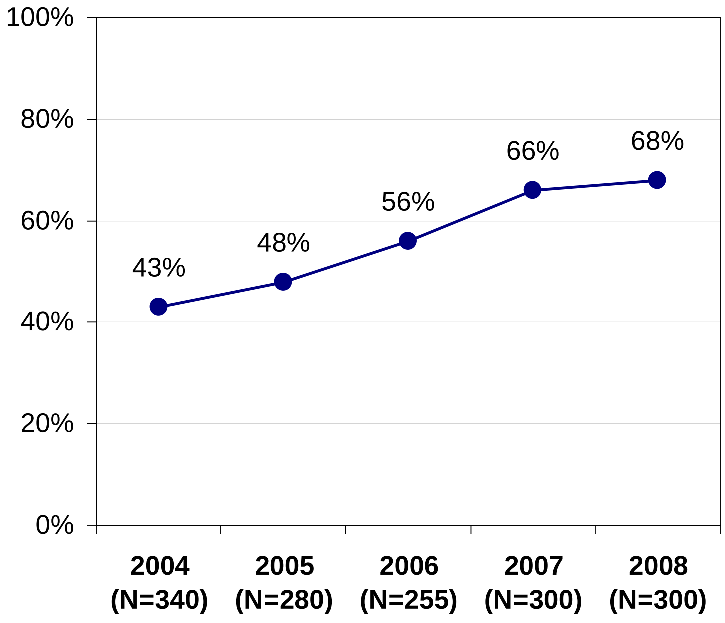
- While interpreting the study results, it is also helpful to keep in mind that as with any random *sample* (e.g., 300 respondents in 2008) from a much larger *target population* (i.e., many thousands of network administrators nationwide), the results are subject to sampling variability. As noted earlier, each percentage from the 2008 survey near 50% can be thought of as having a "margin of sampling error" of approximately 6 percentage points (at the "95% confidence level"), and results from earlier years have a similar margin of sampling variability. For results near 10% or 90%, the margin is approximately +/- 3 percentage points. Thus, changes from year to year must be more than a few percentage points in order to be confident that a trend evident in the survey results implies a trend in the target population. Also, the respondents were randomly selected from a web panel, which includes network administrators who are willing to participate in surveys.

- Results on other questions in the survey, as discussed next, can help to further understand trends related to many of these security management issues.

Securing Remote Access

- Approximately two-thirds in 2007 and 2008 reported that their company / organization uses Secure Shell (SSH). As shown in Figure 4 below, these recent results are significantly higher compared to prior years.

Figure 4: Use Secure Shell (SSH)



- When discussing security management priorities earlier, it was noted that in addition to changes in the total sample between 2006 and 2008 for "securing remote access" there were also consistent changes within different company size categories. This was true for usage of Secure Shell as well. Among small companies / organizations, usage of Secure Shell increased from 38% in 2006 to 49% in 2008. Among midsize companies, the increase was from 56% to 71%, and among large companies the increase was from 65% to 76%. Thus, the recent increase in the proportion of companies using Secure Shell was confirmed for small, midsize, and larger companies. Another interesting finding here, though, is that larger companies were significantly more likely than small companies to use Secure Shell (compare 76% vs. 49%).

- Since companies can use SSH1 or SSH2 or a mixture of both, users of Secure Shell were asked to indicate which type their company / organization is using, and the results are shown below. An important note about Figure 5 is that the results are based only on Secure Shell users each year (excluding a few respondents who did not answer), while the population of Secure Shell users has been growing, according to the results in Figure 4. An inflow of new users can potentially impact the mix of SSH1 and SSH2, while other technological trends can also have an impact.

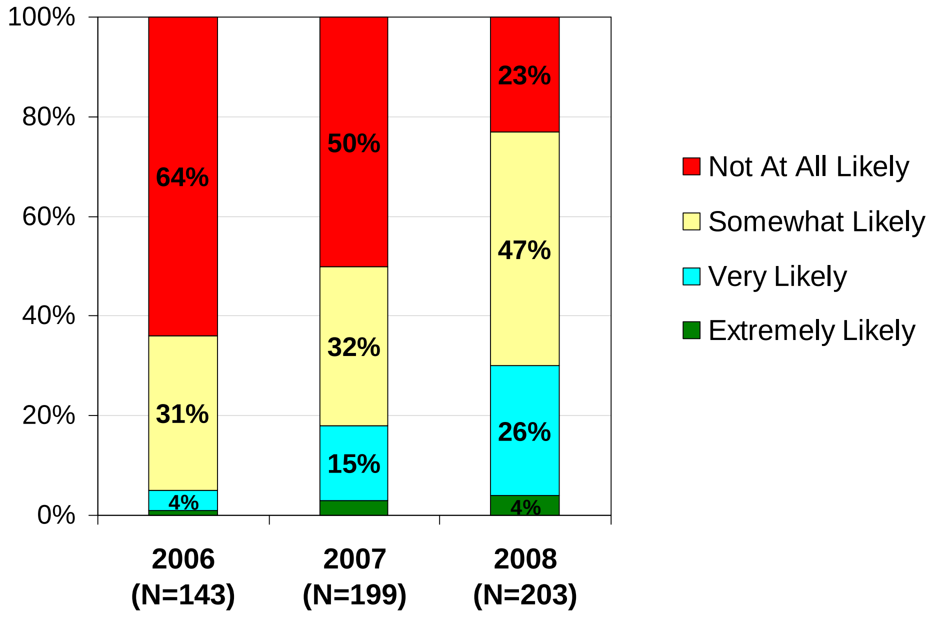
Figure 5: Are You Using SSH1 or SSH2?

	2004	2005	2006	2007	2008
All SSH1	21%	17%	7%	9%	8%
Mostly SSH1	26%	15%	25%	20%	29%
About 50/50	25%	27%	27%	29%	34%
Mostly SSH2	15%	27%	22%	25%	22%
All SSH2	13%	14%	19%	18%	8%
(N =)	(143)	(132)	(139)	(199)	(200)

- One might have expected to see a shift over time toward more usage of SSH2, but the opposite is actually evident in Figure 5. The proportion of Secure Shell users in 2008 reporting that they use "all SSH2" was actually significantly lower than in previous years. It is not clear why this is the case, but this decline in the proportion using "all SSH2" occurred among the small, midsize, and larger companies surveyed.

- Among Secure Shell users, close to half (47%) in 2008 indicated that they were "somewhat likely" to purchase a new or replacement Secure Shell solution within the next 12 months. Another 26% were "very likely," and 4% were "extremely likely." Close to one-fourth (23%) were "not at all likely." However, as shown in Figure 6, the proportion "not at all likely" has declined significantly over the past three years. More positively, the proportion saying they are at least "somewhat likely" to purchase a new / replacement Secure Shell solution increased significantly in 2008 (among Secure Shell users).

Figure 6: Likelihood Purchase New or Replacement Secure Shell Solution in Next 12 Months



- When asked how they configure their network devices, sizable proportions mentioned each of the options listed in Figure 7. However, usage of Telnet declined between 2006 and 2008.

Figure 7: How Do You Configure Your Network Devices?

	2004	2005	2006	2007	2008
Telnet	55%	48%	54%	38%	28%
SSH1	21%	23%	22%	29%	36%
SSH2	19%	25%	28%	38%	34%
HTTP	48%	43%	48%	48%	39%
HTTPS	43%	58%	65%	57%	41%
(N =)	(340)	(280)	(255)	(300)	(300)

- Usage of SSH2 increased between 2004 and 2007 but then dropped slightly in 2008 (although the change between 2007 and 2008 was not "statistically significant"). Usage of SSH1 increased slightly between 2006 and 2007 and between 2007 and 2008.

- Usage of HTTPS increased until 2006 but then fell in 2007 and 2008.

Secure File Transfer

- Eight-in-ten (80%) network administrators surveyed in 2008 indicated that transferring files containing sensitive, confidential, or proprietary information is an integral part of their business. This proportion increased from 68% in 2005 to 71% in 2006 to 81% in 2007, and the result was steady in 2008 (80%).

  - When examining results by company size, changes from 2006 to 2008 in the proportion considering transferring sensitive files integral to their business increased among small companies (from 55% in 2006 to 68% in 2008), among midsize companies (from 72% to 82%), and among larger companies / organizations (from 77% to 86%).

- Approximately three-fourths in 2008 (76%) and 2007 (76%) reported using a secure method of file transfer (at least sometimes) when exchanging sensitive data with customers, vendors, suppliers, or other third parties. The result was significantly lower in 2006 (62%) and 2005 (58%). Figure 8 below shows more detail on secure file transfer usage.

Figure 8: To What Extent Does Your Company Use a Secure Method of File Transfer When Exchanging Sensitive Data With Customers, Vendors, Suppliers, or Other Third Parties?

	2005	2006	2007	2008
Always* use secure file transfer	24%	32%	41%	42%
Mostly* use secure file transfer	18%	14%	20%	23%
Sometimes** use secure file transfer	16%	16%	15%	11%
Do not use secure methods / do not exchange sensitive data with 3rd parties	10%	9%	5%	4%
File transfer not integral to business	32%	29%	19%	20%
* Total “always” / “mostly”	42%	46%	61%	65%
** Total “always” / “mostly” / “sometimes”	58%	62%	76%	76%
(N =)	(280)	(255)	(300)	(300)

- Figure 9 on the next page is similar to Figure 8 above except that Figure 9 addresses *internal* transfers. More than two-thirds reported using a secure method of file transfer at least sometimes when exchanging sensitive data *internally* between remote offices in 2008 (73%) and 2007 (68%). Again, the result was significantly lower in 2006 (52%) and 2005 (52%).

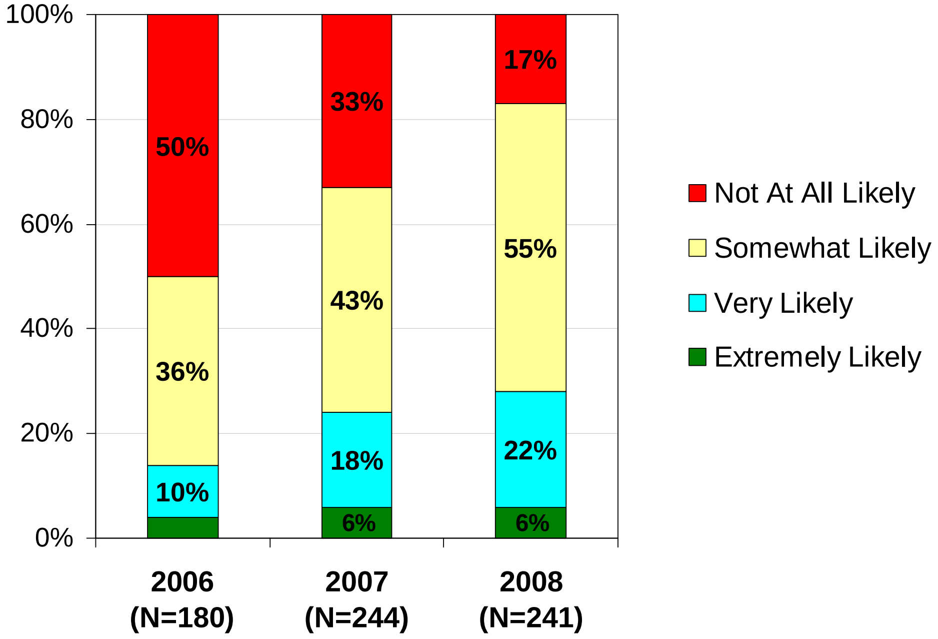
- In addition to the proportion using a secure method of file transfer at least “sometimes,” Figure 9 also shows that the proportion saying they “mostly” or “always” use a secure method for internal file transfers of sensitive data increased noticeably from 42% in 2006 to 54% in 2007 to 63% in 2008.

Figure 9: To What Extent Does Your Company Use a Secure Method of File Transfer For Exchanging Sensitive Data INTERNALLY Between Remote Offices?

	2005	2006	2007	2008
Always* use secure file transfer	24%	28%	34%	40%
Mostly* use secure file transfer	15%	14%	20%	23%
Sometimes** use secure file transfer	13%	10%	14%	10%
Do not use secure methods / do not exchange sensitive data with remote offices	16%	19%	13%	7%
File transfer not integral to business	32%	29%	19%	20%
* Total “always” / “mostly”	39%	42%	54%	63%
** Total “always” / “mostly” / “sometimes”	52%	52%	68%	73%
(N =)	(280)	(255)	(300)	(300)

- Among all those who consider transferring sensitive/confidential files integral to their business, more than half in 2008 said their organization was “somewhat likely” (55%) to purchase a new or replacement secure file transfer solution within the next 12 months. Another 22% were “very likely” and 6% were “extremely likely.”

Figure 10: Likelihood Purchase New or Replacement Secure File Transfer Solution Next 12 Months



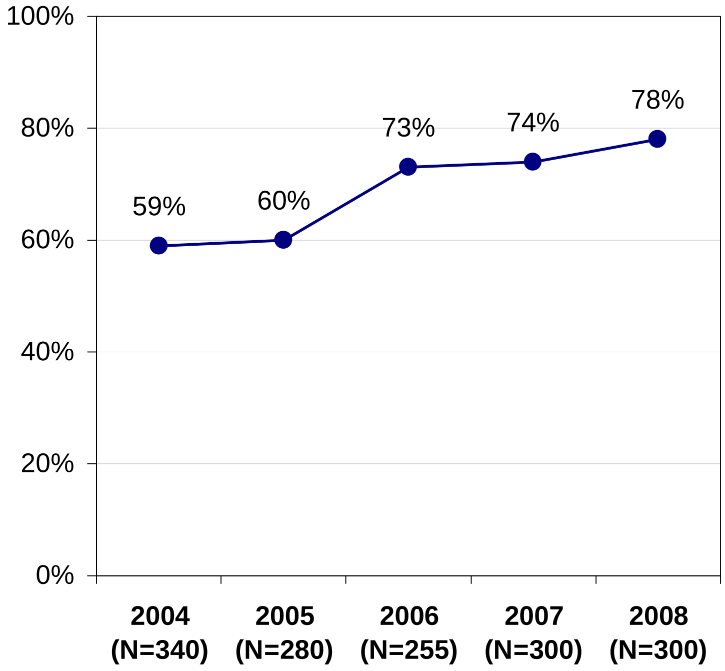
- More than eight-in-ten in 2008 (83%) were at least "somewhat likely" to purchase a new / replacement secure file transfer solution within the next 12 months, and this was significantly higher than the proportion in 2007 (67%) and 2006 (50%).

- In another question, among those using secure file transfer (externally or internally), the proportion indicating that their organization's security policy identifies what "sensitive data" should be exchanged using a secure method of file transfer has been trending upward – from 60% in 2006 to 73% in 2007 to 80% in 2008.

Patching Systems

- More than three-fourths (78%) in 2008 reported using an automated patch management tool to distribute and install critical updates to operating systems and/or applications, and this was up noticeably from a few years ago:

Figure 11: Use Automated Patch Management Tool

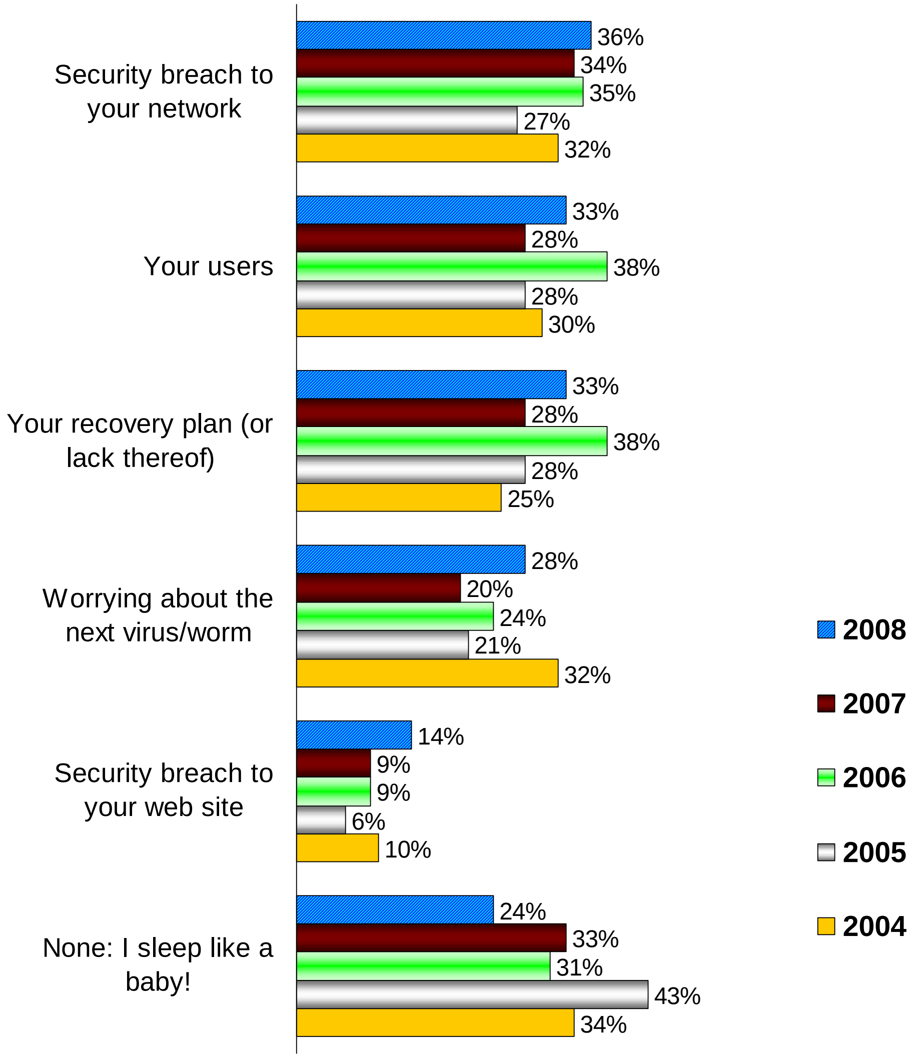


- Interestingly, Figure 3 earlier showed that in 2006 "patching systems" was ranked 1-3 in importance more often than any of the other listed security management issues. In Figure 11 above, 2006 is also the year when there was the largest jump in usage of automated patch management systems.

What Keeps You Up At Night

- As shown earlier in Figure 3, "Keeping virus definitions up to date" and "monitoring intrusions" were each ranked 1-3 in importance by around four-in-ten. The proportion ranking the former 1-3 was not as high in 2008 as in previous years, but this issue is still keeping some network administrators "up at night" as shown in Figure 12 below. Also, slightly more than one-third in each of the last three years worried about a security breach to their network enough to "keep them up at night."

Figure 12: What Keeps You Up At Night?

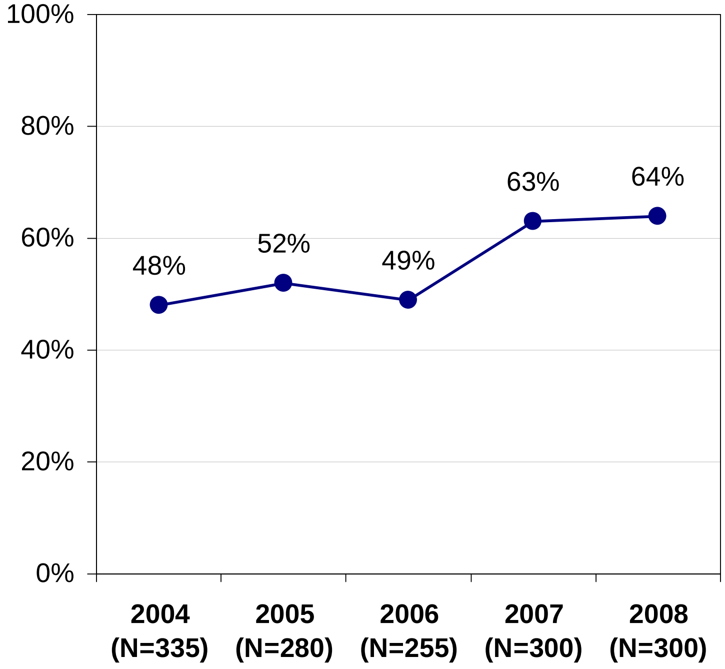


- In the end, when considering the various issues that can worry network administrators, the proportion saying they "sleep like a baby" was at a five year low in 2008.

IT / Security Budgets

- A solid majority in 2008 (64%) and 2007 (63%) felt that their organization has budgeted sufficiently to support current information security needs. As shown in Figure 13, however, results had been significantly lower in prior years.

Figure 13: Feel Budgeted Sufficiently For Current Security Needs



- Earlier (see Figure 12) it was noted that the proportion who "sleep like a baby" fell between 2007 and 2008. Yet, the proportion who felt their company has budgeted sufficiently for security needs was steady between 2007 and 2008 (see Figure 13). One might wonder if and how budgeting for security needs might impact network administrators' sleep. It turns out that the proportion "sleeping like a baby" dropped between 2007 and 2008 among both those who felt they had a sufficient budget to address security needs and among those who did not. More specifically, among just those with a sufficient budget, the proportion who reported that they "sleep like a baby" declined from 37% in 2007 to 30% in 2008. Among just those who did *not* feel their company has budgeted sufficiently to address security needs, the proportion who could "sleep like a baby" dropped from 23% in 2007 to 13% in 2008.

- Additional observations can be made based on these results: The proportion who "sleep like a baby" was lower among those who did not feel they had a sufficient budget compared to those who felt they did have a sufficient budget. At the same time, though, it is also interesting that even among those with a sufficient budget, a minority (30% in 2008) felt that they could "sleep like a baby."

- In the 2008 survey, several new questions were added to gain further insight into IT budgeting. Although one might expect reduced IT spending in light of the current economic climate, the table below shows that more expected budget *increases* (44%) than expected budget decreases (18%).

Figure 14: What change, if any, do you expect to see in your IT budget for 2008 as compared to 2007?

Legend	Response Choice	Frequencies (2008)	Count
1	Decrease by more than 10%	7.66%	23
2	Decrease by less than 10%	10.66%	32
3	No Change	38.0%	114
4	Increase by less than 10%	29.0%	87
5	Increase by more than 10%	14.66%	44
	Total (N)		**300**

- Yet, there were still some specific projects impacted by concerns about the economy:

Figure 15: Are you aware of your company stopping/postponing/canceling any IT security endeavors/projects as a result of a perceived poor economy?

Legend	Response Choice	Frequencies (2008)	Count
1	No	66.33%	199
2	Yes	33.66%	101
	Total (N)		**300**

- At first glance, the results in Figure 15 might appear to contradict the results in Figure 14. However, when comparing Figure 14 to Figure 15, it is important to note the exact wording used in each question. The question covered by Figure 15 refers to "any IT security endeavors/projects," whereas the question covered by Figure 14 refers to "your IT budget for 2008." In other words, Figure 15 addresses specific projects, while Figure 14 addresses the total IT budget. Thus, it is possible for a company to stop, postpone, or cancel some specific security projects but still increase spending on other priorities so that there is a net increase in the overall IT budget. On the other hand, it is also possible to have the delayed / canceled projects lead to a net reduction in the IT budget. In the end, whether or not the *total* IT budget increases or decreases depends on the potential cost of the specific projects that were delayed / canceled.

- Figure 16 below shows how the size (potential cost) of the delayed / canceled security projects compared to the total IT *security* budget. In many cases, the specific security projects in question represented less than one-third of the total IT security budget planned for 2008.

Figure 16: What percentage does the stopped/postponed/cancelled IT security endeavors/projects represent of the total IT security budget planned for 2008?

Legend	Response Choice	Frequencies (2008)	Count
1	Less than 10%	4.95%	5
2	10% to 20%	20.79%	21
3	21% to 30%	19.8%	20
4	31% to 40%	11.88%	12
5	41% to 50%	10.89%	11
6	51% to 60%	7.92%	8
7	61% to 70%	8.91%	9
8	71% to 80%	7.92%	8
9	81% to 90%	2.97%	3
10	More than 90%	2.97%	3
11	Don't know	0.99%	1
	Total (N)		**101**

- Another way to examine the results is to compare the total IT budget expectations of those aware of delayed / cancelled projects vs. those not reporting any delays or cancellations. As shown in Figure 17 below, even among those who were aware of delayed / cancelled projects, about four-in-ten (42%) expected an overall increase in their 2008 IT budget, compared to their 2007 IT budget.

Figure 17:

	Any IT Security Projects Delayed / Canceled?	
	Yes	**No**
Change Expected for 2008 IT Budget:		
Decrease by more than 10%	13%	5%
Decrease by less than 10%	19%	6%
No Change	26%	44%
Increase by less than 10%	24%	32%
Increase by more than 10%	18%	13%
(N =)	(101)	(199)

- As an aside, it is possible that some of the projects delayed may be restarted later in the year. In this case, delaying a project due to very near-term economic uncertainties would not necessarily change the 2008 IT budget, assuming resumption before the end of 2008.

- Yet another way to help gauge trends in spending is to examine and compare Figure 18 and Figure 19 below. These tables show authorized spending without additional signatures this year vs. last year. Interestingly, the results for "this year" did not change significantly compared to "last year."

Figure 18: **This year**, what dollar amount are you authorized to spend without additional signature(s)?

Legend	Response Choice	Frequencies (2008)	Count
1	$0, an authorizing signature is required for all purchases	11.66%	35
2	$1-500	8.66%	26
3	$501-1,000	19.0%	57
4	$1,001-4,999	28.66%	86
5	$5,000 or above	25.33%	76
6	Don't know	6.66%	20
	Total (N)		**300**

Figure 19: **<u>Last year</u>**, what dollar amount were you authorized to spend without additional signature(s)?

Legend	Response Choice	Frequencies (2008)	Count
1	$0, an authorizing signature was required for all purchases	11.66%	35
2	$1-500	11.33%	34
3	$501-1,000	18.0%	54
4	$1,001-4,999	29.0%	87
5	$5,000 or above	23.33%	70
6	Don't know	6.66%	20
	Total (N)		**300**

Other Topics

- Figure 20 below shows the proportions saying they "already did" or have plans to move to IPv6. The proportion saying they "already did" was significantly higher in 2008, compared to previous years. At the same time, the proportion saying they plan to move to IPv6 "sometime in the next 12 months" increased significantly from 2006 to 2007 to 2008.

Figure 20: When Do You Plan To Move To IPv6?

	2005	2006	2007	2008
Already did* more than 12 months ago	1%	1%	3%	5%
Already did* in past 12 months	2%	3%	7%	16%
Sometime** in next 12 months	12%	15%	26%	36%
Sometime** in next 12 to 24 months	13%	16%	15%	14%
No plans	48%	43%	28%	20%
Don't know	24%	22%	21%	9%
* Total "already did"	3%	4%	10%	21%
** Total "sometime"	25%	31%	41%	50%
(N =)	(280)	(255)	(300)	(300)

- Given the upcoming election, a new question was added in 2008 about the expected impact of different election outcomes. Close to half (47%) do not believe that the individual elected to the White House will impact their job security.

Figure 21: Which statement do you agree with the most?

Legend	Response Choice	Frequencies (2008)	Count
1	A Democratic President of the United States would bolster my job security.	25.33%	76
2	A Republican President of the United States would bolster my job security.	16.0%	48
3	An Independent Party President of the United States would bolster my job security.	8.0%	24
4	A Green Party President of the United States would bolster my job security.	4.0%	12
5	I don't believe that who is President of the United States impacts my job security.	46.66%	140
	Total (N)		**300**