6th Annual Survey:
Network and System Administrators

Commissioned study conducted by Amplitude Research, Inc.

May 6, 2009

About VanDyke Software

VanDyke Software® (www.vandyke.com) is a privately held software company located in Albuquerque, NM, with more than 1,000,000 registered users in over 100 countries.

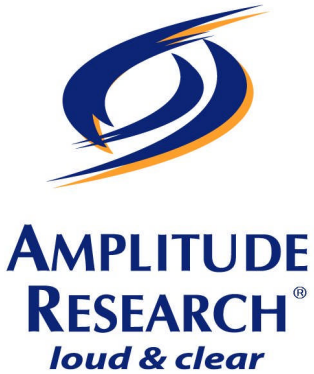
Busy IT professionals depend on VanDyke Software to deliver rock solid, highly-configurable software for data access, file transfer, terminal emulation, and remote administration. VanDyke's easy-to-use software, responsive customer support, and timely product enhancements have a daily impact on its customers' businesses. VanDyke Software creates exceptional value by blending innovative software development methods, close customer relationships, and expert customer service.

The company's product offerings include the SecureCRT® Secure Shell terminal emulator, the SecureFX® secure file transfer client, the VanDyke ClientPack, and the VShell® Secure Shell server.

- SecureCRT® is the tool of choice for solid security, fine-tuned session management, and reliable remote access, combining a feature-filled terminal emulator with the security of the Secure Shell (SSH) protocol.
- SecureFX is a versatile file transfer application that supports SFTP, FTP over SSL, as well as standard FTP.
- The VanDyke ClientPack combines a powerful set of command-line utilities for securely automating routine file transfer, shell, and public-key administration tasks on Windows, Linux, and UNIX.
- VanDyke Software's VShell® Secure Shell server replaces Telnet and FTP for secure network administration and end-user access on Windows and UNIX platforms.

VanDyke offers a fully-functional 30-day evaluation of its products prior to purchase. Evaluators have full access to VanDyke's expert technical support to assist with installation, configuration, and testing, providing both evaluators and customers with a higher level of service.

For more information about VanDyke Software, visit the company's website at http://www.vandyke.com.



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. Its leadership team has over 30 years of experience in quantitative survey research.

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 such as CEOs, CFOs, and other senior personnel at smaller size technology companies; 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 sixth consecutive year that VanDyke Software has commissioned an Amplitude Research® **survey of network and systems 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 2009 study was administered by Amplitude Research® during the third week of April among its nationwide IT web panel. In total, 320 surveys were completed by respondents who confirmed working as a "network or systems administrator" for their company / organization.

A "sample size" of 320 respondents has a "maximum sampling margin of error" of +/- 5.5 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 +/- 3.3 percentage points.

The number of surveys completed with network administrators nationwide was similar in each of the six 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
- 320 completed surveys in 2009

Organization Of Study Findings

Findings from the study are summarized on the following pages. A brief overview of some of the key highlights can be found starting on the next page. Then, given the economic climate in early 2009, the analysis begins with a discussion of how network administrators feel about current IT security budgets, followed by an examination of the impact of budget constraints as seen by network administrators. Then, plans related to the upcoming Microsoft Windows 7 release are discussed. After that we examine many key changes over time concerning various security issues, with six years of tracking results for many of the questions. Toward the end, new questions about virtualization of servers are covered. Although this is a "cutting edge" topic, it is covered toward the end because some of the related findings will be easier to follow after reviewing earlier parts of this summary.

Some Study Highlights

Although many important details are covered in this summary report, the following stood out as being of particular interest.

- ➔ Those seeing a decrease in their company / organization 2009 IT budget outnumbered those seeing an increase by roughly 2 to 1. Last year, the reverse was true.

- ➔ Almost half (46%) of network administrators in April 2009 feel that their company / organization has not budgeted sufficiently to support current information security needs. This is up significantly from 36% in 2008.

- ➔ Those feeling their company / organization has not budgeted sufficiently to support current information security needs were more likely than others (who feel better about their budgets) to face a number of concerns and worries. Highly portable devices used at their company like laptops and handheld devices were often of special concern for those responding that their company / organization has not budgeted sufficiently.

- ➔ Some good news is that more than half (57%) of the network administrators surveyed reported that their company / organization has formal policies regarding the offsite use of laptop computers, and roughly three-fourths (74%) of them in turn felt these policies have resulted in greater responsibility by laptop users.

- ➔ More good news is that the overall proportion dropped slightly in 2009 of those worried so much about a security breach to their network or website as to "keep them up at night."

- ➔ More than one-in-four (27%) were aware of their company / organization canceling 2009 IT security endeavors/projects as a result of a perceived poor economy.

- ➔ "Securing remote access" has been growing in importance relative to other major security management issues. Now, in 2009, there is also a renewed focus on "keeping virus definitions up to date" and "patching systems."

- ➔ However, the proportion ranking "secure file transfer" among their top 3 security management issues dropped in 2009.

- ➔ Using Telnet and HTTPS to configure network devices was significantly more common in 2009 than in the 2008 survey.

- ➔ At this point in time, approximately four-in-ten (39%) have plans to deploy Microsoft Windows 7.

- ➔ More than half (59%) reported that their organization uses virtualization of servers.

IT / Security Budgets

- Several different questions were asked in the 2009 survey about budget-related issues.

2009 SURVEY: *What change, if any, are you seeing in your overall IT budget for 2009 as compared to 2008?*

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	25.62%	82
2	Decrease by less than 10%	15.0%	48
3	No Change	28.75%	92
4	Increase by less than 10%	14.68%	47
5	Increase by more than 10%	7.81%	25
6	Don't know	8.12%	26
	Total (N)		**320**

- The above results indicate that 41% were seeing a decrease in their company / organization 2009 IT budget as compared to 2008 (i.e., 25.62% + 15.0%). At the same time, 22% were seeing an increase in their IT budget (i.e., 14.68% + 7.81%). Thus, roughly twice as many are seeing a decrease as are seeing an increase in their IT budget in 2009.

- Next, we compared the results above to the results below, which are based on a similarly worded question from the 2008 survey. In 2008, 18% were expecting a decrease in their company / organization IT budget as compared to 2007, while 44% were expecting an increase. This is the reverse of the 2009 results.

FROM THE SURVEY LAST YEAR: *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**

- Because this study is especially concerned with network *security* issues, a new question was added to the 2009 survey with wording that referred specifically to the "security" part of the IT budget, as shown below. Based on this question,

33% were seeing a decrease, and 15% were seeing an increase in their 2009 IT security budget. This confirms that budget cuts are impacting IT *security* as well as other parts of IT.

2009 SURVEY: *What change, if any, are you seeing in your **IT security budget** for 2009 as compared to 2008?*

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	21.25%	68
2	Decrease by less than 10%	12.18%	39
3	No Change	42.5%	136
4	Increase by less than 10%	10.0%	32
5	Increase by more than 10%	5.31%	17
6	Don't know	8.75%	28
	Total (N)		**320**

- While IT security budgets increase or decrease, a separate, but related issue is whether those budgets are adequate for current security needs. A budget decrease does not by itself mean that needs are not being met. This issue is addressed by a question (shown below) asking whether network administrators felt their budget was *sufficient*. Based on this question, slightly more than half (54%) in 2009 felt that their organization has budgeted sufficiently to support current information security needs.

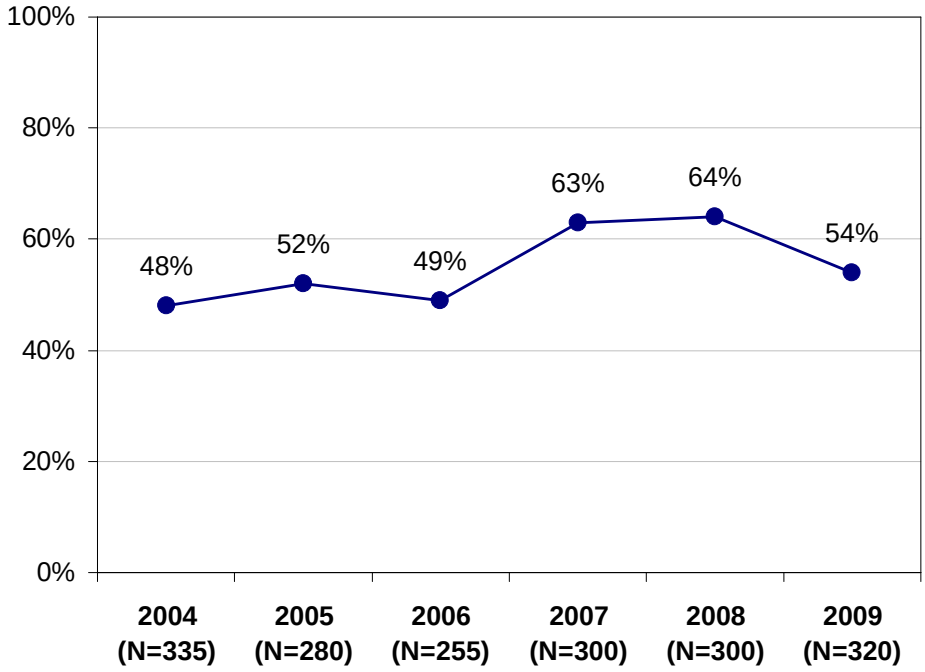
2009 SURVEY: *Do you feel your organization has budgeted sufficiently to support current information security needs?*

Legend	Response Choice	Frequencies	Count
1	No	46.25%	148
2	Yes	53.75%	172
	Total (N)		**320**

- The question above has been asked each year since 2004, and the results over time are shown in Figure 1 on the next page. This shows that the proportion of network administrators feeling their organization has budgeted sufficiently dropped significantly from 64% in 2008 to 54% in 2009. The 2009 result is also significantly lower than the result in 2007 (63%).

- Figure 1 also shows that before 2007 roughly half of the network administrators felt that their organization had budgeted sufficiently for their information security needs. Then there was a significant improvement between 2006 and 2007. The improvement in 2007 was maintained in 2008. Now, however, the 2009 result takes us back to near pre-2007 levels.

Figure 1: **Feel Organization Has Budgeted Sufficiently For Current Information Security Needs**



- If approximately half of the network administrators now feel their budget is sufficient to support current information security needs and the other half do not, it is relevant to examine how these two halves differ in their responses to other questions that might be impacted by size of budgets. To answer this question, we examined the 2009 survey results by dividing respondents into two separate subgroups. One subgroup consisted of those who said "Yes" to the question above, and the other subgroup consisted of those who said "No" to the question above. In other words, one subgroup indicated that their organization has budgeted sufficiently for current information security needs; the second group indicated the opposite -- i.e., that their company / organization has NOT budgeted sufficiently. Figure 2 below shows the results for these two subgroups in reference to the earlier question asking whether they were seeing a change in their IT security budget.

Figure 2: **What change, if any, are you seeing in your IT security budget for 2009 as compared to 2008?**	*Feel Budgeted Sufficiently For Security Needs:*	
	No	***Yes***
Decrease by more than 10%	37%	8%
Decrease by less than 10%	14%	10%
No change / don't know	41%	60%
Increase by less than 10%	5%	15%
Increase by more than 10%	3%	7%
(N = number of respondents)	(148)	(172)

- Figure 2 shows that among those feeling their budget was *not* sufficient (see the "No" column), 37% reported a decrease in their company / organization IT security budget of more than 10%. In contrast, among those who felt their company has budgeted sufficiently to support current information security needs (see the "Yes" column), only 8% reported seeing a decrease of more than 10% in their 2009 IT security budget. On the other hand, those with a sufficient budget were more likely than those with an insufficient budget to report an increase in their 2009 IT security budget. Overall, this shows a significant, although not perfect, correlation between feelings of budgeting sufficiently for IT security needs and actual increases or decreases in IT security budgets.

- Of particular interest, the two subgroups in Figure 2 had different response patterns to several other questions in the survey, which will be covered at different points later in this report.

The Economy

- In the question below, one-third selected "the economy" as the external event that had the greatest impact on their information security plans.

2009 SURVEY: *Which of the following external events has had the greatest impact on your information security plans?*

Legend	Response Choice	Frequencies	Count
1	Homeland security	5.0%	16
2	Legislative drivers (e.g., HIPAA, SOX, GLB)	26.25%	84
3	Customer/vendor/business partner requirements	23.12%	74
4	The economy	33.12%	106
5	None of the above	12.5%	40
	Total (N)		**320**

- Figure 3 below shows that among those feeling their budget was *not* sufficient (see the "No" column), 40% selected "the economy" as having the greatest impact when asked the question above. In contrast, among those who felt their company has budgeted sufficiently to support current information security needs (see the "Yes" column), 27% selected "the economy."

Figure 3: **Which of the following external events has had the greatest impact on your information security plans?**

	Feel Budgeted Sufficiently For Security Needs:	
	No	***Yes***
The economy	40%	27%
Legislative drivers (HIPAA, SOX, GLB)	30%	23%
Customer/vendor/partner requirements	17%	28%
Homeland security	3%	7%
None of the above	10%	15%

- In another question related to the economy (shown below), 27% were aware of their company canceling 2009 IT security endeavors/projects as a result of a perceived poor economy.

2009 SURVEY: *Are you aware of your company canceling any 2009 IT security endeavors/projects* ***as a result of a perceived poor economy****?*

Legend	Response Choice	Frequencies	Count
1	No	72.81%	233
2	Yes	27.18%	87
	Total (N)		**320**

- Further analysis reveals that among those feeling their company was not sufficiently budgeted for security needs, 39% were aware of their company canceling security projects. In contrast, 17% of those who felt their company was sufficiently budgeted were aware of their company canceling 2009 IT security endeavors/projects as a result of a perceived poor economy.

- The next question helps to quantify the impact of the cancelled projects:

2009 SURVEY: *What percentage does the cancelled IT security endeavors/projects represent of the total IT security budget planned for 2009?*

Legend	Response Choice	Frequencies	Count
1	Less than 10%	17.24%	15
2	10% to 20%	29.88%	26
3	21% to 30%	13.79%	12
4	31% to 40%	8.04%	7
5	41% to 50%	8.04%	7
6	51% to 60%	1.14%	1
7	61% to 70%	2.29%	2
8	71% to 80%	1.14%	1
9	81% to 90%	1.14%	1
10	More than 90%		0
11	Don't know	17.24%	15
	Total (N)		**87**

Security At Their Company / Organization

- In the following question, network administrators were asked to rate how satisfied or dissatisfied they are with the current security of different types of items.

2009 SURVEY: *How satisfied are you with the current security at your company for the following?*

	Very dissatisfied	Somewhat dissatisfied	Neutral	Somewhat satisfied	Very satisfied	Not applicable
Desktop PCs	8 2.5%	36 11.25%	35 10.94%	131 40.94%	110 34.38%	0
Laptops	17 5.31%	72 22.5%	40 12.5%	94 29.38%	92 28.75%	5 1.56%
Handheld devices (e.g., Palm, PocketPC, Blackberry)	30 9.38%	55 17.19%	99 30.94%	70 21.88%	40 12.5%	26 8.13%
Data Center / Server Farm	5 1.56%	11 3.44%	42 13.13%	85 26.56%	161 50.31%	16 5.0%
Wireless LAN	12 3.75%	32 10.0%	48 15.0%	109 34.06%	86 26.88%	33 10.31%
Remote access by employees, customers, and/or partners	9 2.81%	34 10.63%	58 18.13%	107 33.44%	101 31.56%	11 3.44%
Physical security (facility and workstation access)	9 2.81%	35 10.94%	45 14.06%	99 30.94%	128 40.0%	4 1.25%
Virtual Machines	6 1.88%	13 4.06%	77 24.06%	68 21.25%	92 28.75%	64 20.0%

- Since the table above shows the exact number and percentage for all response choices, the "not applicable" is included when calculating the percentages above. For further analysis, we recalculated the percentages separately for each item after excluding the respondents who gave a "not applicable" response for the item. Next, since this question has been asked each year since 2004, we have summarized how results have compared over time. To facilitate year-to-year comparisons, we focused on the percentage who were satisfied with the security of each item, and the end result was Figure 4 below.

Figure 4:
Satisfied (Very / Somewhat) With Security Of Equipment At Their Company

	2004	2005	2006	2007	2008	2009
Datacenter / server farm	82%	80%	86%	84%	74%	81%
Desktop PCs	76%	71%	74%	77%	74%	75%
Physical security	71%	61%	75%	71%	66%	72%
Wireless LAN	55%	49%	60%	63%	66%	68%
Remote access	64%	66%	68%	70%	66%	67%
Virtual machines	na	na	na	na	na	63%
Laptops	58%	50%	58%	62%	67%	59%
Handheld devices	45%	33%	44%	45%	52%	37%

- What is most interesting about the results in Figure 4 is that results declined significantly between 2008 and 2009 for laptops and handheld devices, while the results for other types of items did not decline in 2009, compared to 2008. Note that the percentage satisfied with the security of the laptops at their company went from 67% in 2008 to 59% in 2009. At the same time, the proportion satisfied with the security of the handheld devices at their company went from 52% in 2008 to 37% in 2009. This suggests that the most portable devices (i.e., laptops and handheld devices) appear to be of particular concern for many network administrators in 2009.

- Figure 4 also shows that results for laptops and handheld devices had been improving from 2005 through 2008. But then the 2009 results represent a significant reversal of what had been a positive trend.

- We next examine how network administrators with a sufficient budget compare to those who feel their organization has not budgeted sufficiently for current security needs. The results for laptops are broken out by these two subgroups in Figure 5 below. For example, of those who have a sufficient budget (the "Yes" column), 45% were very satisfied with the security of the laptops at their company. Of those who do not feel they have a sufficient budget (the "No" column), only 11% were very satisfied.

Figure 5: **How satisfied are you with the current security of <u>laptops</u> at your company?**

	Feel Budgeted Sufficiently For Security Needs:	
	No	***Yes***
Very dissatisfied	10%	2%
Somewhat dissatisfied	35%	12%
Neutral	16%	10%
Somewhat satisfied	28%	31%
Very satisfied	11%	45%
(N = excludes those rating "not applicable")	(145)	(170)

- Figure 5 also shows that, of those who have a sufficient budget (the "Yes" column), 12% were somewhat dissatisfied with the security of the laptops at their company. In contrast, of those who do <u>not</u> feel they have a sufficient budget (the "No" column), 35% were somewhat dissatisfied.

- These results suggest that insufficient budgeting for security needs often goes "hand in hand" with greater concern about (i.e., less satisfaction with) the security of laptops at the organization.

- Seeing how often network administrators are less than satisfied with the security of laptops at their company, the reader may wonder if companies are taking

steps to enhance security. For this purpose, the question below was added to the 2009 survey. Based on this question, more than half (57%) reported that their company has *formal* policies regarding the offsite use of laptop computers.

2009 SURVEY: *Does your company have FORMAL policies regarding the offsite use of laptop computers (such as password-protected screen savers, sign-out procedures, laptop audits, restrictions on software installation, marking or branding of laptop exteriors, etc.)?*

Legend	Response Choice	Frequencies	Count
1	No	37.5%	120
2	Yes	56.56%	181
3	Don't know	5.93%	19
	Total (N)		**320**

- While the results above are based on the total sample, we also looked at how results differed based on whether a network administrator felt their security budget was sufficient or not. Among those who are sufficiently budgeted, 63% reported that they have formal policies regarding the offsite use of laptop computers. In contrast, among those who do not feel their company has budgeted sufficiently for security needs, less than half (49%) reported that they have formal policies regarding the offsite use of laptop computers.

- All those who reported formal policies regarding the offsite use of laptop computers were next asked if they felt these policies have resulted in greater responsibility by laptop users. As shown below, 74% appeared to feel that these policies could make a positive difference.

2009 SURVEY: *Has your company's policies regarding the offsite use of laptop computers resulted in greater responsibility by laptop users?*

Legend	Response Choice	Frequencies	Count
1	No	25.96%	47
2	Yes	74.03%	134
	Total (N)		**181**

- Another new question from the 2009 survey is shown below that addresses laptop policies from a different perspective. This shows that three-fourths (75%) of the total sample says they have a designated person or department to contact in the event a laptop is stolen or missing. However, further analysis of the data revealed that, among those who felt their company has sufficiently budgeted for security needs, 82% had such a designated person / department. In contrast, among those not feeling their company was sufficiently budgeted for current security needs, 66% had such a designated person / department.

2009 SURVEY: *Does your company have a designated person or department to contact in the event a laptop is stolen or missing?*

Legend	Response Choice	Frequencies	Count
1	No	17.5%	56
2	Yes	74.68%	239
3	Don't know	6.25%	20
4	Not applicable – our company does not allow offsite use of laptop computers	1.56%	5
	Total (N)		**320**

- As noted earlier, in addition to laptops, handheld devices were often of particular concern. As shown in Figure 6 below, this was especially true for network administrators facing a budget that is not sufficient for their security needs (see the "No" column). Figure 6 is similar to Figure 5 shown earlier, except that Figure 6 shows the results for handheld devices. Again, these results suggest that insufficient budgeting for security needs often goes "hand in hand" with greater concern about the security of handheld devices at the organization.

Figure 6: **How satisfied are you with the current security of handheld devices (e.g., Blackberry, Palm, Pocket PC) at your company?**

	Feel Budgeted Sufficiently For Security Needs:	
	No	***Yes***
Very dissatisfied	17%	4%
Somewhat dissatisfied	28%	10%
Neutral	35%	32%
Somewhat satisfied	13%	34%
Very satisfied	7%	20%
(N = excludes those rating "not applicable")	(139)	(155)

What Keeps You Up At Night?

- While slightly more than one-third (36%) were "sleeping like a baby," the remaining network administrators were "kept up at night" by worrying about various concerns, such as their users, their recovery plan (or lack thereof), the next virus, or a breach to their network or website:

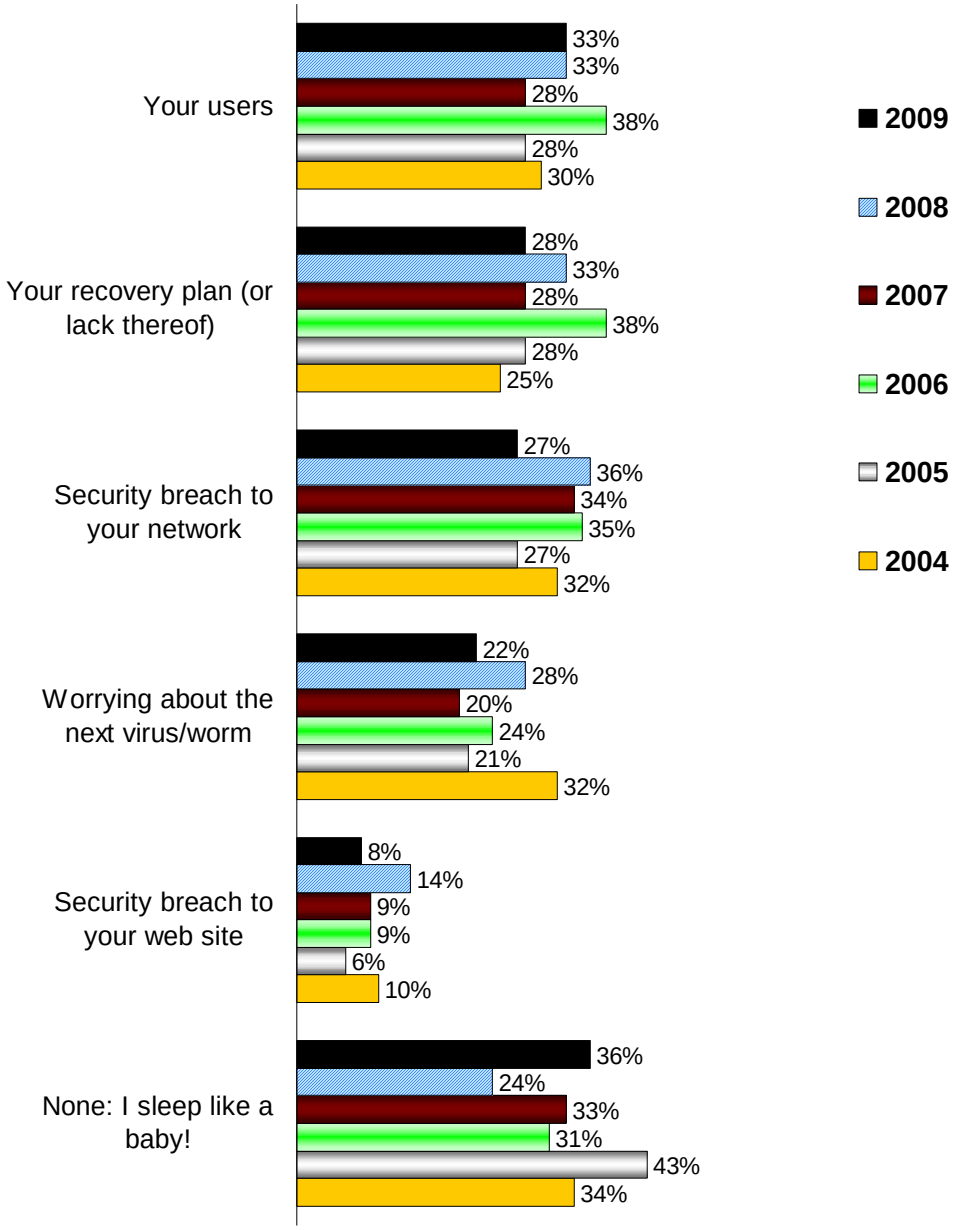
2009 SURVEY: *What keeps you up at night? (check all that apply)*

Legend	Response Choice	Frequencies	Count
1	Worrying about the next virus/worm	21.87%	70
2	Your users	32.5%	104
3	Your recovery plan (or lack thereof)	27.5%	88
4	A security breach to your network	27.18%	87
5	A security breach to your website	8.12%	26
6	None. I sleep like a baby!	35.62%	114
	Total (N)		**320**

- The question above has been asked in each year since 2004, and the year-to year-comparisons are shown in Figure 7 below. Interestingly, between 2008 and 2009 there has been a slight decline in the proportion worrying about each issue, with the exception of "your users." In particular, the proportion worrying about a security breach to their network dropped significantly from 36% in 2008 to 27% in 2009.

- There had been a drop in 2008 in the proportion who felt that they "sleep like a baby," but that was reversed in 2009. In this case, a reversal is good news, as this means more network administrators were sleeping like a baby in 2009.

Figure 7: **What Keeps You Up At Night?**



- It is worth noting that the worries shown above were not divided equally among all types of network administrators. Those with an insufficient budget are more likely to have a worry that "keeps them up at night," as shown in Figure 8 next. Note that among those who felt their organization has budgeted sufficiently to support their current security needs, 48% were sleeping like a baby (see the "Yes" column). In contrast, among those facing an insufficient budget (see the "No" column), only 22% were sleeping like a baby.

Figure 8: **What keeps you up at night?**

	Feel Budgeted Sufficiently For Security Needs:	
	No	***Yes***
Your users	41%	25%
Your recovery plan (or lack thereof)	39%	18%
A security breach to your network	34%	22%
Worrying about the next virus / worm	28%	16%
A security breach to your website	7%	9%
None: I sleep like a baby	22%	48%

- This shows that an insufficient IT security budget often goes "hand in hand" with greater worries and less sleep for network administrators.

Microsoft Windows 7

- When asked if their organization has plans to test Windows 7, just under one-fourth (23%) indicated that they are currently beta testing. More than one-fourth (27%) are waiting for the official release before they begin testing, while slightly less than half do not have plans to test Windows 7.

2009 SURVEY: *Does your organization have plans to test Windows 7?*

Legend	Response Choice	Frequencies	Count
1	Currently beta testing	23.43%	75
2	Waiting for official release to begin testing	26.87%	86
3	Not at this time	48.43%	155
4	Other*	1.25%	4
	Total (N)		**320**

- However, the results to the question above varied significantly by whether network administrators were seeing an increase or decrease in their overall IT budget. As shown in Figure 9 below, among those experiencing an increase in their IT budget in 2009, 38% were currently beta testing Windows 7 (see the "Increase" column). In contrast, among those experiencing a decrease in their IT budget, only 18% were beta testing Windows 7 (see the "Decrease" column).

Figure 9: **Does your organization have plans to test Windows 7?**

	Change in 2009 Overall IT Budget	
	Decrease	***Increase***
Currently beta testing	18%	38%
Waiting for official release to begin testing	30%	26%
Not at this time	51%	36%
Other	1%	0%
(N =)	(130)	(72)

- While the above results addressed plans to *test* Windows 7, the question below was added to the 2009 survey to cover plans for *deploying* Windows 7.

2009 SURVEY: *Does your organization have plans to deploy Windows 7?*

Legend	Response Choice	Frequencies	Count
1	Yes...after successful completion of beta testing.	5.0%	16
2	Yes…after successful completion of testing of the official release.	14.37%	46
3	Yes...after Service Pack 1 for Windows 7 is released.	10.31%	33
4	Yes...but only on new PCs with Windows 7 pre-installed.	9.06%	29
5	Not at this time.	59.06%	189
6	Other*	2.18%	7
	Total (N)		**320**

- Results for the question above also varied by whether network administrators were experiencing an increase or decrease in their company / organization IT budget. As shown in Figure 10, among those experiencing a decrease in their budget, 61% did not have plans at this time to deploy Windows 7. In contrast, among those experiencing an increase in their IT budget, only 42% did not have plans to deploy Windows 7.

Figure 10: **Does your organization have plans to deploy Windows 7?**

	Change in 2009 Overall IT Budget	
	Decrease	***Increase***
Yes...after successful completion of beta testing	4%	8%
Yes…after successful completion of testing of the official release	11%	25%
Yes...after Service Pack 1 for Windows 7 is released	10%	14%
Yes...but only on new PCs with Windows 7 pre-installed	12%	11%
Not at this time	61%	42%
Other	2%	0%
(N =)	(130)	(72)

- To help understand motivations for using or not using Windows 7, the following two questions were asked.

2009 SURVEY: *What is the primary reason that you have no current plans to deploy Windows 7?*

Legend	Response Choice	Frequencies	Count
1	No features in Windows 7 worth upgrading to.	7.93%	15
2	Too many features have been dropped (e.g., WINFS).	0.52%	1
3	Can't justify the return on investment.	33.33%	63
4	Feel more comfortable sticking with current versions of Windows.	44.97%	85
5	Do not use a Windows operating system.	1.58%	3
6	Other*	11.64%	22
	Total (N)		**189**

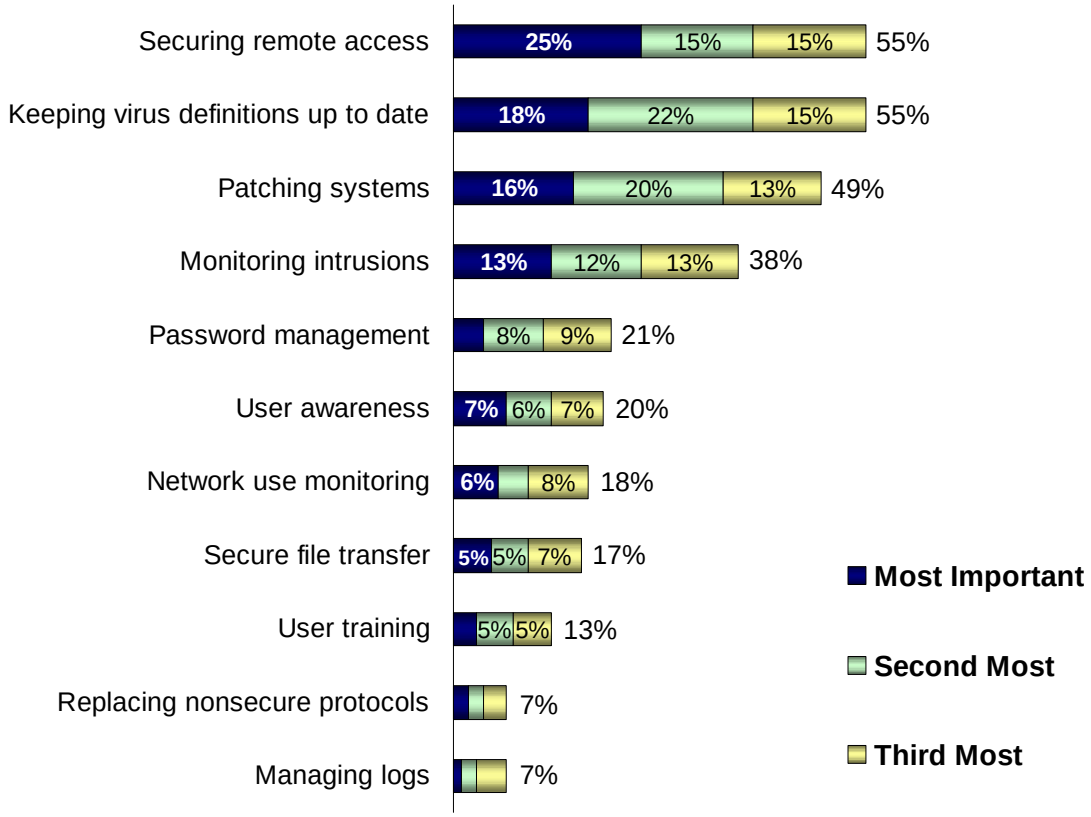
2009 SURVEY: *What is the primary reason for your interest in Windows 7?*

Legend	Response Choice	Frequencies	Count
1	Security enhancements (e.g., improved firewall, anti-spyware)	36.31%	65
2	Limited user accounts	9.49%	17
3	Improved usability	44.69%	80
4	Other*	9.49%	17
	Total (N)		**179**

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 results is to first focus on the 2009 survey results, as shown in Figure 11 below. For example, 25% indicated that "securing remote access" is the #1 most important security management issue facing their company / organization. Another 15% gave "securing remote access" a rank of #2, and 15% gave it a rank of #3. In the end, 55% ranked "securing remote access" either 1, 2, or 3 in importance from the list of 11 items that are included in Figure 11.

Figure 11: **Security Management Issues Ranked 1, 2, or 3 in Importance (2009 Results Only)**



- After examining the 2009 results above, the next step is to make comparisons to previous years. Figure 12 shows the proportion giving a #1 ranking for each issue each year. Figure 13 shows the proportions ranking each item #1 *or* #2 *or* #3 (i.e., among their top three). (In Figures 12 and 13, the 3 lowest percentage items were excluded to enhance readability.)

Figure 12: **Proportion Ranking Each Issue #1 in Importance**

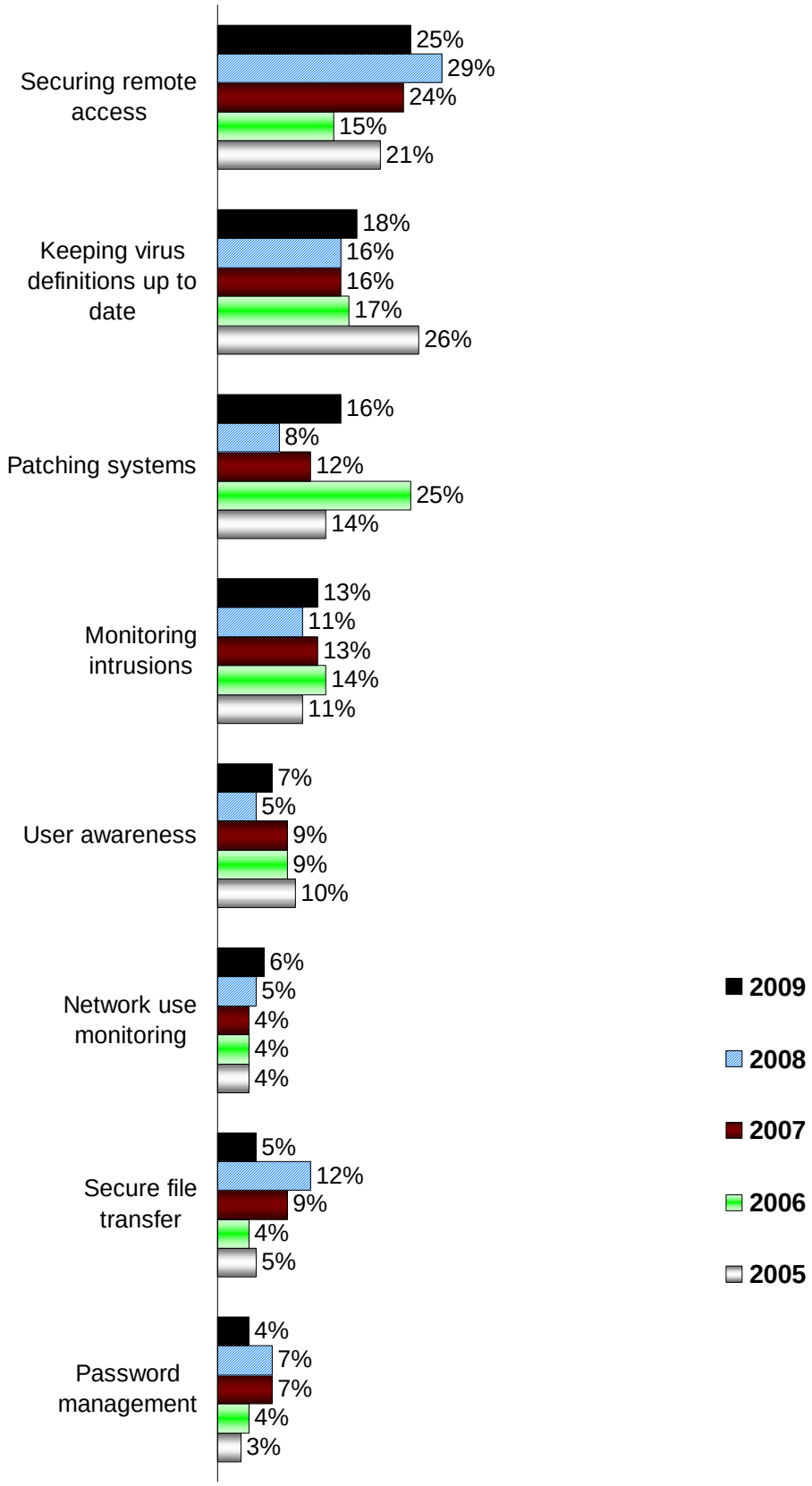
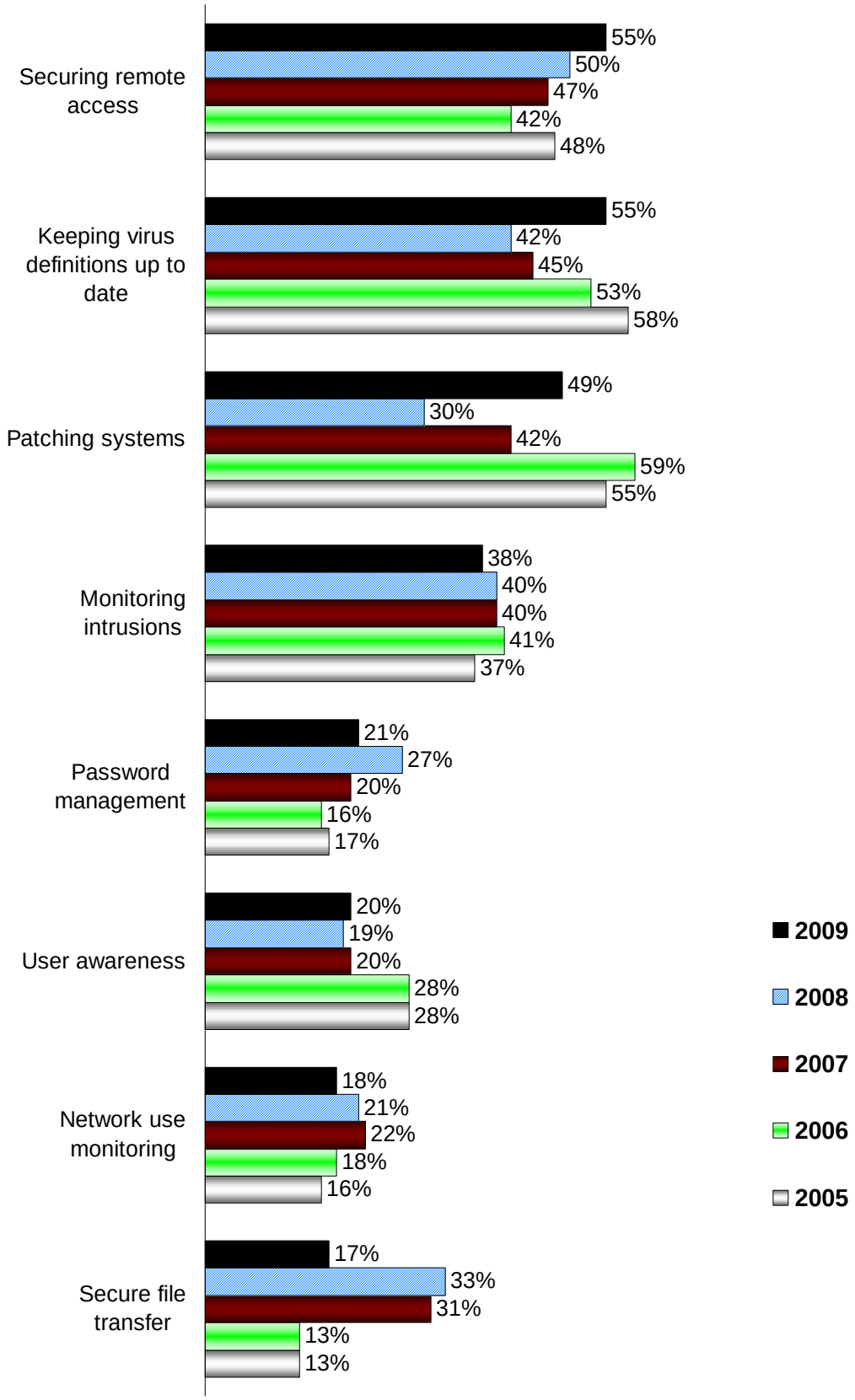


Figure 13: **Total Proportion Ranking Each Issue 1, 2, or 3**



- After examining Figures 12 and 13, a number of interesting highlights can be identified. First, the four items with the highest proportion of respondents considering them a priority were securing remote access, keeping virus definitions up to date, patching systems, and monitoring intrusions.

  — One-fourth considers securing remote access to be their #1 priority. More than half now consider this to be among their top 3 priorities. When looking at the proportion ranking "securing remote access" 1-3, there has been a slow but steadily increasing trend from 2006 through 2009.

  — The proportion ranking "keeping virus definitions up to date" 1-3 increased significantly between 2008 and 2009. There was a downward trend for this issue between 2005 and 2008, but the 2009 result shows a noticeable rebound.

  — Recent renewed importance was also evident for patching systems.

- However, the proportion making "secure file transfer" a top priority declined significantly in 2009.

- When examining the issues with significant changes in 2009, one might wonder if these changes were consistent for different company sizes (where we can define "company size" by the number of employees). To do this, it is necessary to track year-to-year changes within different company size categories. Figure 14 shows this information for the three issues that had significant increases and the one issue that had a significant decline in 2009. These results generally show that the changes are not dependent on a single company size category and therefore can be thought of as fairly broad based.

  — The proportion ranking securing remote access #1 or #2 or #3 increased in 2009 within both small and large company categories.

    o To be sure, the sample sizes are not large after dividing the results by year and company size. The purpose of Figure 14 is not to promote detailed trending by company size category, but rather to give a general feeling for how well trends apparent for the total sample hold up after breaking out the results by different company size categories.

  — The proportion ranking keeping virus definitions up to date 1/2/3 increased in 2009 among small, midsize, and large company categories.

  — Results were up among midsize and large companies for patching systems.

  — Results were down for secure file transfer among all three company size categories. Although the decline for secure file transfer came as somewhat of a surprise, the consistency in this trend within each company size category shows that this change is well entrenched.

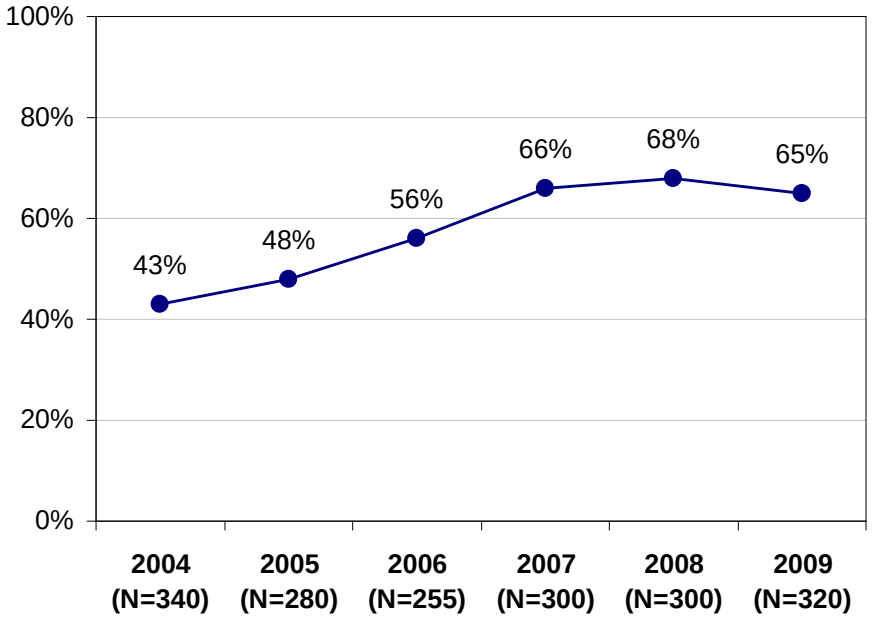
Figure 14: **Proportion Ranking 1/2/3 By Company Size & Year**

Results By # Of Employees	And By Year	Securing remote access	Keeping virus defns. up to date	Patching systems	Secure file transfer
1 to 99 employees	2006	47%	59%	52%	12%
(Small)	2007	45%	59%	33%	29%
	2008	43%	51%	37%	32%
	2009	55%	55%	33%	19%
100 to 999	2006	37%	49%	63%	12%
(Midsize)	2007	52%	36%	41%	36%
	2008	55%	34%	25%	36%
	2009	49%	61%	52%	16%
1,000 +	2006	42%	52%	60%	13%
(Large)	2007	45%	47%	47%	29%
	2008	50%	45%	32%	31%
	2009	60%	50%	55%	16%

Securing Remote Access

- Close to two-thirds in 2009 reported that their company / organization uses Secure Shell (SSH). As shown in Figure 15 below, Secure Shell usage has been fairly steady over the past three years, after growing noticeably between 2004 and 2007.

Figure 15: **Use Secure Shell (SSH)**



- 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 16 is that the results are based only on Secure Shell users each year.

Figure 16: **Are You Using SSH1 or SSH2?**

	2004	2005	2006	2007	2008	2009
All SSH1	21%	17%	7%	9%	8%	12%
Mostly SSH1	26%	15%	25%	20%	29%	18%
About 50/50	25%	27%	27%	29%	34%	30%
Mostly SSH2	15%	27%	22%	25%	22%	26%
All SSH2	13%	14%	19%	18%	8%	14%
(N =)	(143)	(132)	(139)	(199)	(200)	(207)

- When asked how they configure their network devices, sizable proportions mentioned each of the options listed in Figure 17. Interestingly, usage of Telnet, as well as HTTPS, increased significantly in 2009.

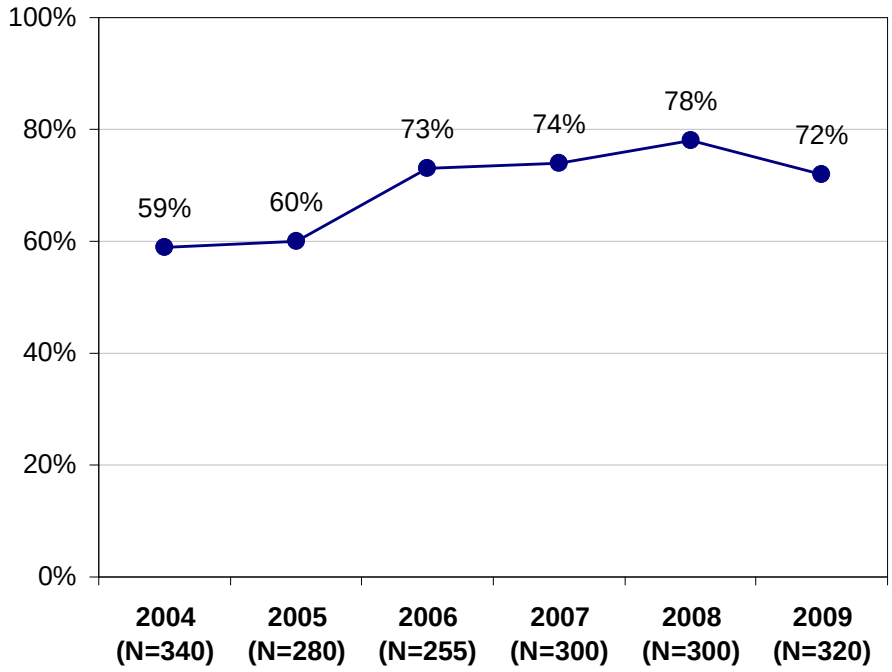
Figure 17: **How Do You Configure Your Network Devices?**

	2004	**2005**	**2006**	**2007**	**2008**	**2009**
Telnet	55%	48%	54%	38%	28%	52%
SSH1	21%	23%	22%	29%	36%	30%
SSH2	19%	25%	28%	38%	34%	33%
HTTP	48%	43%	48%	48%	39%	41%
HTTPS	43%	58%	65%	57%	41%	67%
(N =)	(340)	(280)	(255)	(300)	(300)	(320)

Automated Patch Management

- More than two-thirds of the respondents in each of the past four years reported using an automated patch management tool to distribute and install critical updates to operating systems and/or applications. Although the 2009 result shown in Figure 18 is lower, the change between 2008 and 2009 was not statistically significant.

Figure 18: **Use Automated Patch Management Tool**



- Earlier it was noted that an increased proportion in 2009 included "patching systems" among their top security management priorities, but this has not yet translated into a significant increase in the proportion using an *automated* patch management tool.

Virtualization Of Servers

- Based on a new question added to the 2009 survey (shown below), 59% of network administrators say their company uses virtualization of at least some of its servers.

2009 SURVEY: *Does your company use virtualization with any of its servers?*

Legend	Response Choice	Frequencies	Count
1	No	32.81%	105
2	Yes	59.06%	189
3	Not applicable/Don't know	8.12%	26
	Total (N)		**320**

- Larger companies were significantly more likely than smaller companies to use virtualization of servers. For example, among network administrators working for large companies (i.e., with 1,000 or more employees), 73% reported that their company uses virtualization of servers. For midsize companies (100 to 999 employees), 62% reported using virtualization of servers. For small companies (1 to 99 employees), 31% reported using virtualization of servers.

- At the same time, organizations that use virtualization of servers were more likely than those not using virtualization to report using an automated patch management tool (80% vs. 53%). That is, among those who use virtualization of servers, 80% also use an automated patch management tool. Among those who do not use virtualization, 53% also use a patch management tool.

- In addition, organizations that use virtualization of servers were more likely than others to use Secure Shell (74% vs. 49%).

- Responses to the question below suggest that the bulk of network administrators feel that the overall security of virtual servers is comparable to or better than servers that do not use virtualization.

2009 SURVEY: *How does the security of your virtual servers(s) compare with the overall security of servers that do not use virtualization?*

Legend	Response Choice	Frequencies	Count
1	Far less secure	2.11%	4
2	Somewhat less secure	6.87%	13
3	About the same	70.37%	133
4	More secure	17.46%	33
5	Far more secure	3.17%	6
	Total (N)		**189**

Firmographics

- As in prior years, the 2009 survey included experienced network administrators from a variety of company size categories, organization types, and industries.

2009 SURVEY: *How long have you worked in IT (Information Technology)?*

Legend	Response Choice	Frequencies	Count
1	Less than 6 months	0.31%	1
2	6 months - 2 years	3.43%	11
3	2 - 5 years	8.12%	26
4	5 - 10 years	22.5%	72
5	More than 10 years	65.62%	210
	Total (N)		**320**

2009 SURVEY: *Please tell us about the number of employees in your company or organization overall including all sites and locations within the U.S.*

Legend	Response Choice	Frequencies	Count
1	1 to 9	9.68%	31
2	10 to 24	4.68%	15
3	25 to 99	10.62%	34
4	100 to 249	11.25%	36
5	250 to 999	20.93%	67
6	1,000 to 4,999	17.81%	57
7	5,000 to 9,999	6.87%	22
8	10,000 to 19,999	4.06%	13
9	20,000 +	14.06%	45
	Total (N)		**320**

2009 SURVEY: *What kind of organization do you work for?*

Legend	Response Choice	Frequencies	Count
1	Privately held	44.37%	142
2	Publicly traded corporation	21.87%	70
3	Non-profit	7.81%	25
4	Government	12.5%	40
5	Educational institution	11.25%	36
6	Other	2.18%	7
	Total (N)		**320**

2009 SURVEY: *What industry is your company in?*

Legend	Response Choice	Frequencies	Count
1	Aerospace/Defense Contracting	1.87%	6
2	Agriculture and Food/Beverage Products	0.31%	1
3	Automotive	0.93%	3
4	Banking/Finance	4.06%	13
5	Business Services	4.06%	13
6	Computer Hardware	2.18%	7
7	Computer Software	5.31%	17
8	Construction/Architecture	2.18%	7
9	Consulting Services	9.68%	31
10	Educational institution	10.93%	35
11	Entertainment	0.93%	3
12	Government/Municipal	10.31%	33
13	Healthcare	8.43%	27
14	Insurance	2.81%	9
15	Internet E-commerce	1.25%	4
16	Legal	1.25%	4
17	Manufacturing	8.43%	27
18	Media	2.18%	7
19	Non-Profit	3.12%	10
20	Personal Use	0.31%	1
21	Pharmaceutical	0.93%	3

22	Retail	2.5%	8
23	Systems Integration	2.18%	7
24	Telecommunications	3.12%	10
25	Transportation	2.81%	9
26	Travel		0
27	Utilities	1.25%	4
28	VAR	1.87%	6
29	Web Hosting/ISP	0.62%	2
30	Other	4.06%	13
	Total (N)		**320**