7th Annual Survey:
Network and System Administrators

Commissioned study conducted by Amplitude Research, Inc.

April 30, 2010

About VanDyke Software

VanDyke Software® (www.vandyke.com) is a privately held software company located in Albuquerque, NM, with more than 1,500,000 registered users in over 100 countries.

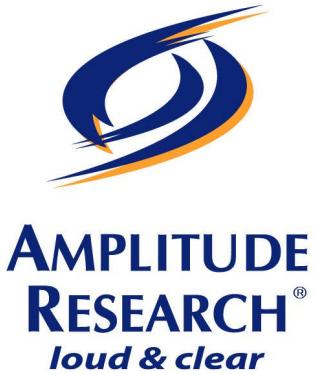
Busy IT professionals depend on VanDyke Software to deliver rock solid, highly-configurable software for secure file transfer, terminal emulation, and remote administration. VanDyke Software's easy-to-use software, responsive customer support, and timely product enhancements have a daily impact on its 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 (SSH) 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, flexible session management, and reliable remote access, combining a feature-filled terminal emulator with the security of the Secure Shell 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 Software offers a fully-functional 30-day evaluation of its products prior to purchase. Evaluators have full access to VanDyke Software'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 company headquartered in Boca Raton, Florida, with blue chip clients located throughout the United States, Canada, South America and Asia. Amplitude combines its powerful survey platform, experienced survey administration, top-quality sample, and expert reporting services to deliver Loud and Clear™ results. Its leadership team has over 70 years of combined experience in the survey and market research industries.

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® is known for its survey design, data analysis and survey reporting capabilities. Amplitude uses its proprietary software technologies and experienced team of statisticians and survey reporting professionals to deliver clear and concise reports ranging from top-line reporting to customized written reports based on in-depth analysis by professional statisticians.

For more information about Amplitude Research, visit the company's website at http://www.amplituderesearch.com.

Study History

This is the seventh 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, while some questions have been added or deleted from time to time in order to cover special topics / industry developments.

Study Methodology

Amplitude Research® administered the 2010 study during the second and third week of April among nationwide IT web panelists. In total, 353 surveys were completed by respondents who confirmed working as a "network or systems administrator" for their company / organization.

A "sample size" of 353 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%, 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 +/- 3.1 percentage points.

The number of surveys completed each year is shown below:

- 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
- 353 completed surveys in 2010

Organization Of Study Findings

Findings from the study are summarized on the following pages. A brief overview of many of the key highlights and research implications can be found starting on the next page. Then, given the economic climate, more detailed analysis begins with a discussion of how network administrators feel about current IT security budgets and changes they are seeing. Next, several new topics of special interest are covered, such as social media, cloud computing, and Mac OS X. After that, we examine many key changes over time concerning various security issues, with seven years of tracking results for many of the questions.

Some Study Highlights

Some of the study highlights are summarized below, while later sections of this report go into more detail.

- Nearly one-third (30%) of the network administrators surveyed reported that they are seeing an increase in their IT security budget for 2010 as compared to 2009. On the other hand, 20% were seeing a decrease. In 2009, only 15% were seeing an increase in their 2009 IT security budget as compared to 2008. One-third (33%) last year were seeing a decrease.

- More than half (57%) in the 2010 survey felt that their organization has budgeted sufficiently to support current information security needs. This result was similar to 2009 (54%).

- In terms of staffing, 17% were seeing an increase in the size of their IT security staff for 2010 as compared to 2009, while 12% were seeing a decrease. More than half (57%) felt that their organization is sufficiently staffed to support current information security needs.

- Often, but not always, those comfortable with their IT security budget are also comfortable with the size of their IT security staff. It turns out that 44% felt that their organization is *both* budgeted *and* staffed sufficiently to support current information security needs.

- Nearly four-in-ten (39%) were "kept up at night" worrying about a security breach to their network in 2010, which was significantly higher than in 2009 (27%). Similar proportions (each year) were "kept up at night" worrying about their users.

- Those who feel their organization has not budgeted sufficiently for information security needs were more likely than their counterparts (i.e., those who feel sufficiently budgeted) to be "kept up at night" worrying about their users and/or a security breach to their network.

- Four-in-ten (40%) were either "extremely concerned" (18%) or "moderately concerned" (22%) with employee use of social media as a security threat to their company. Only 12% were "not at all concerned," while others were either "slightly concerned" (22%) or "somewhat concerned" (26%).

- Those "moderately concerned" to "extremely concerned" with employee use of social media were also more likely than others to be "kept up at night" worrying about a security breach to their network, their users, the next virus, and/or a security breach to their website.

    - For example, among those "moderately" to "extremely" concerned with employee use of social media as a security threat to their organization, 50% were "kept awake at night" worrying about a security breach to their network. In contrast, among those "slightly" to "somewhat" concerned about employee use of social media, 35%

were "kept awake at night" by worrying about a security breach to their network. Among those "not at all concerned" about employee use of social media, only 16% lied awake at night worrying about a breach to their network.

- ✓ Of course, there are many possible reasons for worrying about a breach to their network, and we are not saying that social media is necessarily a primary cause. But, it is interesting that there is a statistically significant relationship between how concerned network administrators are about employee use of social media and how likely they are to worry about a security breach to their network. Although not absolute proof of "causation," the relationship is strong enough to recommend that organizations carefully consider the potential security risks related to employee use of social media.

- When asked in an open-ended manner, "What concerns you most about employee use of social media at your company?", network administrators mentioned viruses (22%), unproductive / time wasted (21%), security / intrusion risk (19%), data / information leaks (16%), privacy issues (7%), malware (5%), and bandwidth usage (4%).

- More than one-third (37%) reported that their organization allows employees unlimited access to social media when using the company network. Nearly half (48%) allow employees "limited" access. This leaves only 15% of the organizations represented by network administrators in this survey where employees have *no* access to social media via the company network.

- However, lack of access or limited access to social media via the company network did not reduce the proportion of network administrators at least "moderately concerned" about security threats related to employee use of social media.

- More than half (56%) indicated that their organization has a formal policy regarding employee use of social media. However, those with such a policy were not less likely than others to be "moderately" or "extremely" concerned about employee use of social media.

- 15% reported that their organization has adopted cloud computing for one or more applications. Another 47% were considering but have not yet adopted cloud computing.

- Among those who have adopted cloud computing, more than four-in-ten (43%) rated it "very secure," and another four-in-ten (43%) rated it "somewhat secure." (Caution is needed here, though, since these results are based on a small sample size of 53 cloud computing adopters.)

- Among those who have not adopted cloud computing but are considering it, 18% rated it "very secure," and 63% rated it "somewhat secure." Others "had no idea" (9%) how to rate the security of cloud computing or rated it less than "somewhat secure" (10%).

- More than one-third (37%) reported that their organization has adopted the Mac OS X platform for one or more of its computers. However, half the time, less than 10% of the organization's computers currently use the Mac OS X platform.

- Among users, more than one-in-five (21%) network administrators were "extremely satisfied" with the *security* of the Mac OS X platform, while another 30% were "very satisfied," and more than one-third (36%) were "moderately satisfied."

- In the 2009 report, there was concern about a significant drop between 2008 and 2009 in satisfaction with the security of handheld devices (e.g., Palm, PocketPC, Blackberry) at their company. In 2010, there was a significant improvement on this measure, although the results for handheld devices were still lower than for other types of equipment used by employees.

- There was also a slight increase between 2009 and 2010 in the proportion of network administrators satisfied with the security of remote access and with the security of virtual machines at their company.

- In a separate question (that was new in the 2010 survey), 9% gave an "extremely important" rating and 32% gave a "very important" rating for managing the security of employee smartphones, as compared to other security threats facing their company.

Some Implications Of The Research

- ➔ For 2010, more reported seeing an increase than reported seeing a decrease in their IT security budget. This is an encouraging sign, especially since the opposite was true in 2009.

- ➔ However, there are still many network administrators who feel their organization has not budgeted sufficiently to support current information security needs. On this measure, the 2010 result did not improve significantly vs. the 2009 survey.

- ➔ Network administrators facing what they feel is an insufficient budget also continue to be more likely than their counterparts (i.e., those who have a sufficient budget to work with) to worry about their users and/or a security breach to their network.

- ➔ Thus, there is plenty of room for further increases in IT security budgets in the future, if the economy continues to grow, as is hoped.

- ➔ The future path of the economy will likely be critical for IT security staffing. Currently, the proportion reporting gains in IT staff slightly exceeds the proportion seeing declines. If economic growth falters, it would not be surprising if the "tide turned" for IT security staffing. On the other hand, if economic growth continues, perhaps momentum could build for IT security staffing, given that many network administrators feel their organization is not sufficiently staffed to support current information security needs.

- ➔ While social media might be a "dream come true" for many *users*, it can sometimes be a nightmare for network administrators. Even when employees do not have access to social media via the company network, network administrators are often still concerned. Apparently, home use of social media by employees can still create headaches in many ways for network administrators.

- ➔ Cloud computing appears to be in the early stages of adoption by network administrators. Since many more are considering it than have actually adopted it, this suggests potential for future growth in this area.

- ➔ However, there could appear to be a need to convince many more network administrators that cloud computing could be "very secure." Although many are willing to think of cloud computing as "somewhat secure," the technology might not fulfill its potential unless attitudes about its security are enhanced.

- ➔ On an encouraging note, only a minority of the respondents considers cloud computing to be "not very secure" or "not at all secure."

- ➔ The improvement between 2009 and 2010 in satisfaction with the security of handheld devices used by employees is encouraging, but there is still room for improvement. At the same time, managing the security of smartphones is often considered very important relative to other security risks.

- ➔ Looking forward, network administrators could benefit if effective technologies, software, methods, procedures, and/or policies can be shown and/or developed to help them address concerns they often have about the security of social media and smartphones used by employees.

Respondent & Company Characteristics

- As in previous years, the 2010 survey included experienced network administrators from a variety of company size categories, organization types, and industries.

2010: Please identify your primary job function or job title:

Legend	Response Choice	Frequencies	Count
1	Database administrator		0
2	Network or systems administrator	100.0%	353
3	Software engineer		0
4	Web developer		0
5	Other		0
	Total (N)		**353**

2010: How long have you worked in IT (Information Technology)?

Legend	Response Choice	Frequencies	Count
1	Less than 6 months	0.28%	1
2	6 months - 2 years	2.54%	9
3	2 - 5 years	10.19%	36
4	5 - 10 years	16.43%	58
5	More than 10 years	70.53%	249
	Total (N)		**353**

2010: 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	7.64%	27
2	10 to 24	5.38%	19
3	25 to 99	13.03%	46
4	100 to 249	9.63%	34
5	250 to 999	22.66%	80
6	1,000 to 4,999	15.01%	53
7	5,000 to 9,999	7.93%	28

8	10,000 to 19,999	5.09%	18
9	20,000 +	13.59%	48
	Total (N)		**353**

- Since company size is sometimes related to how network administrators answer some survey questions, it is worth noting that the "mix" of company sizes has been consistent. For example, the table below shows the mix for the 2009 and 2010 surveys when collapsing company size categories into three subgroups to facilitate comparisons.

	2009	**2010**
"Small" (1 to 99 employees)	25%	26%
"Midsize" (100 to 999 employees)	32%	32%
"Large" (1,000 or more employees)	43%	42%

2010: What kind of organization do you work for?

Legend	Response Choice	Frequencies	Count
1	Privately held	49.85%	176
2	Publicly traded corporation	24.92%	88
3	Non-profit	6.51%	23
4	Government	9.06%	32
5	Educational institution	8.21%	29
6	Other	1.41%	5
	Total (N)		**353**

2010: What industry is your company in?

Legend	Response Choice	Frequencies	Count
1	Aerospace/Defense Contracting	1.41%	5
2	Agriculture and Food/Beverage Products	0.56%	2
3	Automotive	0.84%	3
4	Banking/Finance	5.09%	18
5	Business Services	5.38%	19
6	Computer Hardware	1.69%	6
7	Computer Software	3.96%	14
8	Construction/Architecture	2.26%	8
9	Consulting Services	12.18%	43

9	Consulting Services	12.18%	43
10	Educational Institution	7.93%	28
11	Entertainment	1.41%	5
12	Government/Municipal	8.78%	31
13	Healthcare	7.64%	27
14	Insurance	2.54%	9
15	Internet E-commerce	2.54%	9
16	Legal	0.84%	3
17	Manufacturing	9.63%	34
18	Media	2.26%	8
19	Non-Profit	1.69%	6
20	Personal Use	0.56%	2
21	Pharmaceutical	0.56%	2
22	Retail	3.39%	12
23	Systems Integration	3.39%	12
24	Telecommunications	1.98%	7
25	Transportation	1.69%	6
26	Travel		0
27	Utilities	1.13%	4
28	VAR	1.41%	5
29	Web Hosting/ISP	1.41%	5
30	Other	5.66%	20
	Total (N)		**353**

IT / Security Budgets

- Several different questions were asked in the 2010 survey about budget-related issues. To begin, the table below shows that 15% of the respondents were seeing an increase in their *overall* IT budget by more than 10% for 2010, as compared to 2009. Another 23% (rounded up from 22.66% below) were seeing an increase of less than 10%. Combined, nearly four-in-ten (38% = 15% + 23%) were seeing an increase.

What change, if any, are you seeing in your **overall IT budget** for 2010 as compared to 2009?

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	12.18%	43
2	Decrease by less than 10%	9.91%	35
3	No change	34.27%	121
4	**Increase by less than 10%**	22.66%	80
5	**Increase by more than 10%**	15.29%	54
6	Don't know	5.66%	20
	Total (N)		**353**

- On the other hand, 12% of the respondents were seeing a decrease by more than 10% in their overall IT budget, and 10% (rounded up from 9.91%) were seeing a decrease of less than 10%. Combined, slightly less than one-fourth (22% = 12% + 10%) were seeing a decrease in 2010 relative to 2009.

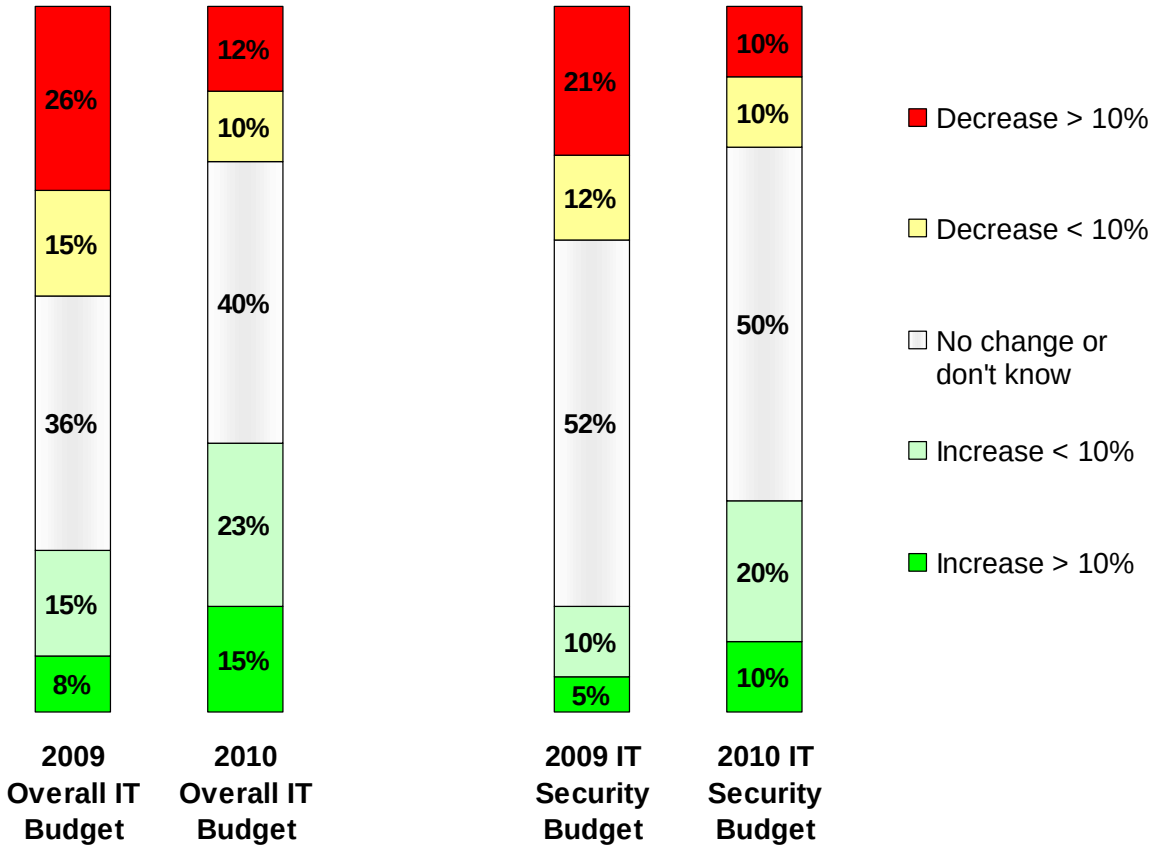
- While the above question covers the *overall* IT budget, the next question focuses on the IT *security* budget. One-in-ten (10%) were seeing an increase by more than 10%, while one-in-five (20%) were seeing an increase of less than 10% in their IT *security* budget for 2010, as compared to 2009. Combined, just under one-third (30% = 10% + 20%) were seeing an increase.

What change, if any, are you seeing in your **IT security budget** for 2010 as compared to 2009?

Legend	Response Choice	Frequencies	Count
1	Decrease by more than 10%	9.63%	34
2	Decrease by less than 10%	9.63%	34
3	No change	45.32%	160
4	**Increase by less than 10%**	19.54%	69
5	**Increase by more than 10%**	10.19%	36
6	Don't know	5.66%	20
	Total (N)		**353**

- The above results are encouraging because more respondents were seeing an increase than a decrease in 2010 relative to 2009. More encouraging signs emerge when comparing results from the 2010 survey to the 2009 survey. Similar budget-related questions were asked last year, with the obvious change that the 2009 budget was being compared to 2008.

- The chart below facilitates comparisons between the 2010 and 2009 surveys on these questions. For 2010, the chart repeats information shown in the tables above. For example, the rightmost bar in the chart shows that one-in-ten (10%) were seeing an increase of more than 10% in their 2010 IT *security* budget, as compared to 2009. This is consistent with the previous table. However, the third bar from the left shows that 5% in 2009 reported seeing their IT *security* budget increase by more than 10%, as compared to 2008.



- Combining the results for a budget increase > 10% with a budget increase < 10% to get the total proportion seeing a budget increase, 30% from the 2010 survey were seeing an increase in their IT security budget, while only 15% from the 2009 survey were seeing an increase in their IT security budget.

- At the same time, 20% from the 2010 survey were seeing a decrease in their IT security budget, while 33% from the 2009 survey were seeing a decrease in their IT security budget.

- Also, although more were seeing an increase than were seeing a decrease in 2010, the opposite was true in 2009.

- In a different question, 57% in 2010 felt that their organization has budgeted sufficiently to support current information security needs.

2010: Do you feel your organization has budgeted sufficiently to support current information security needs?

Legend	Response Choice	Frequencies	Count
1	No	42.77%	151
2	Yes	57.22%	202
	Total (N)		**353**

- It is interesting to conduct further analysis by the two subgroups that can be defined based on the question above. That is, one subgroup indicated that their organization has budgeted sufficiently for current information security needs (answered "Yes" above). The other subgroup indicated the opposite (answered "No" above). The table below shows how these two subgroups compared on the earlier question about *changes* they are seeing in their 2010 IT security budget. For example, among those who feel their organization has budgeted sufficiently for security needs (i.e., the "Yes" column of the table below), 38% were also seeing an increase in their 2010 IT security budget. In contrast, among those who felt their organization has *not* budgeted sufficiently for security needs (i.e., the "No" column in the table below), 19% were also seeing an increase in their 2010 IT security budget.

What change, if any, are you seeing in your IT *security* budget for 2010 as compared to 2009?	*Feel Budgeted Sufficiently For Security Needs:*	
	No	***Yes***
Decrease by more than 10%	16%	5%
Decrease by less than 10%	12%	8%
No change / don't know	53%	49%
Increase by less than 10%	13%	25%
Increase by more than 10%	6%	13%

After combining categories above:

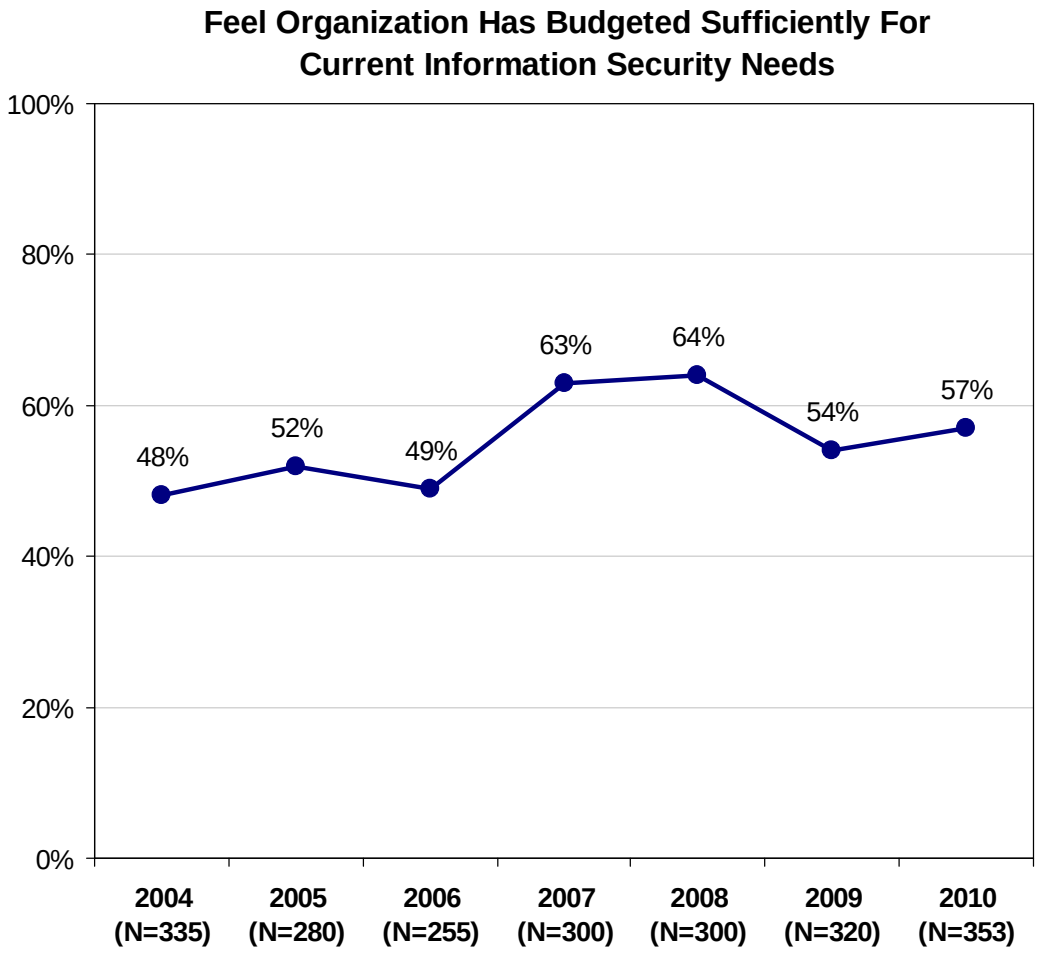
Decrease (by > 10% or < 10%)	28%	13%
Increase (by > 10% or < 10%)	19%	38%
(N = number of respondents)	(151)	(202)

- Those who felt that their organization has budgeted sufficiently were more likely to report an increase (38%) than a decrease (13%). The opposite was true

among those feeling their organization has not budgeted sufficiently (19% increase vs. 28% decrease).

- Later in this report, a table with a similar format to that above is used for several other questions to break out the results by those who do vs. those who do not feel their organization has budgeted sufficiently for current information security needs.

- However, before going to the next section, the chart below shows the proportion feeling sufficiently budgeted each year since 2004. The 2010 result falls below the highs in 2007 and 2008, and between the 2009 and 2008 results -- although not significantly different from either year. (By "not significantly different," we mean that the differences between 57% and 54% and between 57% and 64% were not large enough to be "statistically significant.") Although it is encouraging that many feel their organization has budgeted sufficiently, there has still been a sizable proportion each year feeling the opposite -- i.e., that their budget was not sufficient to support current information security needs.



IT Staffing

- When asked about *staffing* specifically (a new question group in 2010), one-in-six (17%) were seeing an increase in the size of their IT security *staff* in 2010, as compared to 2009. (This 17% combines the 1.13% below for "significant increase in size of IT security staff" with the 15.86% for "increase in size of IT security staff.")

What change, if any, are you seeing in the size of your IT security staff for 2010 as compared to 2009?

Legend	Response Choice	Frequencies	Count
1	Significant decrease in size of IT security staff	2.83%	10
2	Decrease in size of IT security staff	9.06%	32
3	No change	71.1%	251
4	**Increase in size of IT security staff**	15.86%	56
5	**Significant increase in size of IT security staff**	1.13%	4
	Total (N)		**353**

- On the other hand, 12% (after taking 2.83% + 9.06% from the table above) were seeing a *decrease* in the size of their IT security staff in 2010. Among just these respondents, the table below shows the reasons given for the reduction in IT security staff. For example, the most common reason was that a reduction in company sales or profit led to IT security staff cuts.

What are the reasons your company is seeing a reduction in IT security staff? (Select all that apply)

Response Choice	Frequencies	Count
Reduction in company sales or profit led to IT security staffing cuts	47.61%	20
Uncertainty about economy makes company reluctant to hire	30.95%	13
Change in business mix or strategy reduced need for number of IT security staff	26.19%	11
Increased automation or other technology advances reduced IT security staffing needs	9.52%	4
Other	11.9%	5
Total (N)		**42**

- It is one thing to see an increase or decrease in IT security staff. It is another thing to feel that staffing levels are *sufficient or insufficient*. As shown in the next table, network administrators were split 57% / 43% in 2010 on whether or

not they thought their organization was sufficiently *staffed* to support current information security needs.

2010: Do you feel your organization is sufficiently **staffed** to support current information security needs?

Legend	Response Choice	Frequencies	Count
1	No	43.05%	152
2	Yes	56.94%	201
	Total (N)		**353**

- The question above can be used to create two subgroups of respondents: one subgroup that feels their organization is sufficiently *staffed*, and another subgroup that does not. Then, the results to the question covered on the previous page can be broken out by these two subgroups, as in the table below. For example, among those who do not feel they are sufficiently staffed to support current information security needs (the "No" column), 16% were seeing an increase, and 21% were seeing a decrease in the size of their IT security staff for 2010.

What change, if any, are you seeing in the size of your IT security staff for 2010 as compared to 2009?	*Feel Staffed Sufficiently For Security Needs:*	
	No	***Yes***
Significant decrease in size of IT security staff	5%	2%
Decrease in size of IT security staff	16%	3%
No change	63%	78%
Increase in size of IT security staff	15%	16%
Significant increase in size of IT security staff	1%	1%

After combining categories above:

Total seeing decrease	21%	5%
Total seeing increase	16%	17%
(N = number of respondents)	(152)	(201)

- Among those who feel their organization is sufficiently staffed to support current information security needs, 17% were seeing an increase, and 5% were seeing a decrease in the size of their IT security staff.

- Next, it is interesting to "cross tabulate" the question about sufficient s*taff* with the question (covered in the previous section) about sufficient IT security *budgeting*. In the table below, the results to the question about sufficient *staff* were broken out by those who felt their IT security *budget* was sufficient vs. those who did not. For example, 78% of those who felt their organization has

budgeted sufficiently to support current information security needs also felt that their organization is sufficiently *staffed* for information security needs.

Do you feel your organization is sufficiently staffed to support current information security needs?	*Feel Budgeted Sufficiently For Security Needs:*	
	No	***Yes***
No	71%	22%
Yes	29%	78%
(N = number of respondents)	(151)	(202)

- With the information in the table above, it is possible to calculate how often network administrators find themselves in the ideal position of having *both* a sufficient budget *and* sufficient staff to support current information security needs. All of the 202 respondents in the rightmost column said "Yes," their organization has *budgeted* sufficiently to support current information security needs. At the same time, 78% of those 202 respondents also said "Yes," their organization is sufficiently *staffed* to support current information security needs. Taking 78% of 202 respondents yields 157 respondents, and they represent 44% of the total sample (i.e., 44% = 157 / 353).

    - Thus, 44% felt that their organization is both sufficiently staffed and sufficiently budgeted to support current information security needs. On the flip side, the other 56% feel they are either insufficiently staffed or insufficiently budgeted, or both.

- In a separate question, respondents were asked if they handle security issues with internal staff, employ a security consultant, or outsource. For example, 21% reported using a security consultant, as shown in the table below.

2010: How does your company address information security issues?

Legend	Response Choice	Frequencies	Count
1	We handle security using internal staff and resources.	76.48%	270
2	We employ a security consultant to advise and assist internal staff.	20.96%	74
3	We outsource to a Managed Service Provider or consulting firm (e.g., IBM, Accenture, etc.).	2.54%	9
	Total (N)		**353**

    - When the same question was asked in 2009, only 9% mentioned using a security consultant. In contrast, 32% in 2008 mentioned using a security consultant, while results were lower in 2007 (15%) and 2006 (10%). Thus, it appears as if a possible 2008 boom in

security consulting was "cut short" by 2009 (probably due to economic pressures), but it may be starting to rebound in 2010.

The Economy

- In the question below, nearly one-third (32%) selected the economy as the external event that had the greatest impact on their information security plans.

2010: Which of the following external events has had the greatest impact on your information security plans?

Response Choice	Frequencies	Count
The economy	32.29%	114
Customer/vendor/business partner requirements	27.19%	96
Legislative drivers (e.g., HIPAA, SOX, GLB)	21.52%	76
Homeland security	5.94%	21
None of the above	13.03%	46
Total (N)		**353**

  - When the same question was asked last year, a similar proportion selected the economy (33%), followed by legislative drivers (26%), and then customer/vendor/business partner requirements (23%).

- The table below shows that among those feeling their budget was *not* sufficient (see the "No" column), 42% selected the economy as having the greatest impact. In contrast, among those who felt their company has budgeted sufficiently to support current information security needs (see the "Yes" column), 25% selected the economy. As might be expected, this suggests that whether or not an organization has budgeted sufficiently for information security needs is significantly related to overall economic conditions.

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	42%	25%
Customer/vendor/partner requirements	20%	33%
Legislative drivers (HIPAA, SOX, GLB)	23%	20%
Homeland security	4%	7%
None of the above	11%	15%

- In another question related to the economy (shown below), 22% were aware of their company canceling 2010 IT security endeavors/projects as a result of a perceived poor economy.

- When the same question was asked last year, 27% had said they were aware of canceling 2009 IT security endeavors/projects.

2010: Are you aware of your company canceling any 2010 IT security endeavors/projects as a result of a perceived poor economy?

Legend	Response Choice	Frequencies	Count
1	No	77.9%	275
2	Yes	22.09%	78
	Total (N)		**353**

- The next two tables help to quantify the impact of cancelled projects.

2010: What percentage does the stopped/postponed/cancelled IT security endeavors/projects represent of the total IT security budget planned for 2010?

Legend	Response Choice	Frequencies	Count
1	Less than 10%	11.53%	9
2	10% to 20%	26.92%	21
3	21% to 30%	11.53%	9
4	31% to 40%	16.66%	13
5	41% to 50%	6.41%	5
6	51% to 60%	5.12%	4
7	61% to 70%	5.12%	4
8	71% to 80%	5.12%	4
9	81% to 90%	2.56%	2
10	More than 90%	1.28%	1
11	Don't know	7.69%	6
	Total (N)		**78**

2009: *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**

What Keeps You Up At Night?

- While slightly more than one-fourth (26%) were "sleeping like a baby," the remaining network administrators were "kept up at night" by worrying about various concerns, such as a security breach to their network, their users, their recovery plan (or lack thereof), the next virus, or a breach to their website:

2010: What keeps you up at night? (check all that apply)

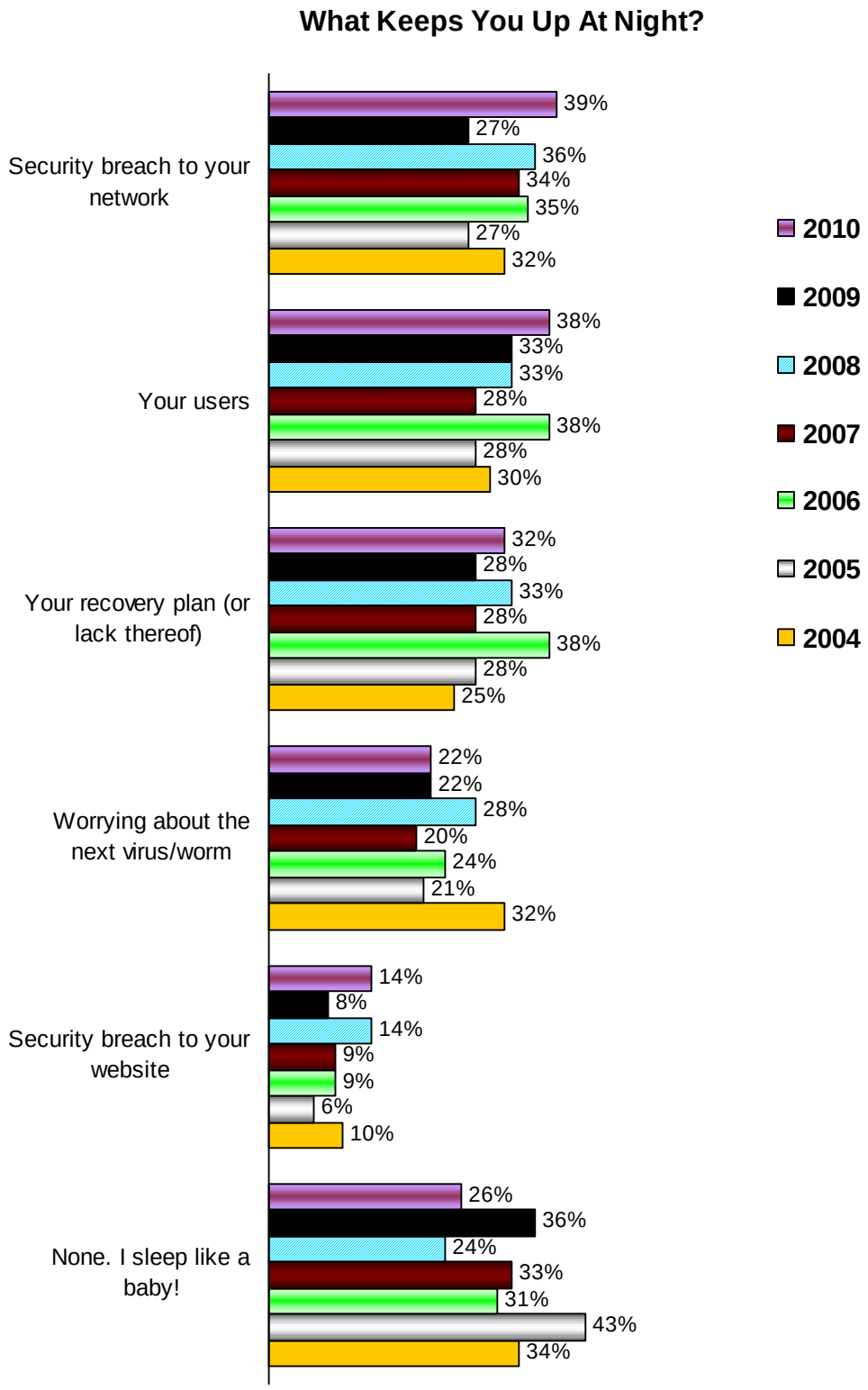
Response Choice	Frequencies	Count
A security breach to your network	38.81%	137
Your users	38.24%	135
Your recovery plan (or lack thereof)	32.29%	114
Worrying about the next virus/worm	22.37%	79
A security breach to your website	14.16%	50
None. I sleep like a baby!	26.06%	92
Total (N)		**353**

- The worries shown above were not divided equally among all types of network administrators. Those feeling they had an insufficient IT security budget were more likely to have a worry that "keeps them up at night," as shown in the following table. Note that among those who felt their organization has *not* budgeted sufficiently to support current security needs (see the "No" column), 18% were sleeping like a baby. In contrast, among those who felt their organization was sufficiently budgeted for information security needs (see the "Yes" column), 32% were sleeping like a baby.

What Keeps You Up At Night?	*Feel Budgeted Sufficiently For Security Needs:*	
	No	***Yes***
Your users	48%	31%
A security breach to your network	45%	34%
Your recovery plan (or lack thereof)	35%	30%
Worrying about the next virus / worm	25%	20%
A security breach to your website	15%	14%
None. I sleep like a baby	18%	32%

- At the same time, those who felt they did not have a sufficient budget were more likely than others to be kept awake at night by worries about their users and/or a security breach to their network.

- The question, "What keeps you up at night?" has been asked each year since 2004, and the year-to-year comparisons are shown below.



- Interestingly, between 2009 and 2010, there was a slight increase in the proportion worrying about each issue, except the next virus/worm (which was

steady). In particular, the proportion worrying about a security breach to their network increased significantly from 27% in 2009 to 39% in 2010.

Social Media

- Given the recent popularity of "social media," several new questions about this topic were added to the 2010 survey. As shown below, more than one-in-six (18%) were "extremely concerned" with employee use of social media as a security threat to their organization. More than one-in-five (22%) were "moderately concerned." Combined, four-in-ten (40% = 18% + 22%) were at least moderately concerned.

2010: How concerned are you with employee use of social media (social networks, blogs, online video, microsharing, widgets, etc.) as a security threat to your company?

Legend	Response Choice	Frequencies	Count
1	Not at all concerned	12.18%	43
2	Slightly concerned	22.09%	78
3	Somewhat concerned	26.06%	92
4	Moderately concerned	21.81%	77
5	Extremely concerned	17.84%	63
	Total (N)		**353**

- Another way to think about the results above is to note that only 12% were "not at all concerned." This suggests that most (88%) network administrators were at least slightly concerned about the potential security threat of employees using social media.

- Those at least slightly concerned were asked in an open-ended manner, **"What concerns you most about employee use of social media at your company?"** The original verbatim comments to this question were later evaluated and "coded" according to common themes, as listed below (with the percentage giving each type of response). For example, 22% mentioned viruses as their greatest concern about employee use of social media at their company. There were also many comments about reduced productivity, security / intrusion risks, potential for data leaks, and other issues.

    - Viruses (22%)
    - Unproductive / time wasted (21%)
    - Security / intrusion risk (19%)
    - Data / information leaks (16%)
    - Privacy (7%)
    - Malware (5%)
    - Uses bandwidth (4%)

- When hearing that employee usage of social media can heighten concerns about viruses, intrusions, data leaks, and malware, the reader might be reminded of the question covered earlier, "What keeps you up at night?" The table below shows results to this question broken out by the degree of concern about social media. For example, the rightmost column of the table focuses on those who were "moderately" to "extremely" concerned about the security threat of employee usage of social media. Among this group, 50% were kept up at night worrying about a security breach to their network.

	Concern About Employee Use Of Social Media As Company Security Threat:		
What Keeps You Up At Night?	***Not At All***	***Slightly/ Somewhat***	***Moderately/ Extremely***
A security breach to your network	16%	35%	50%
Your users	16%	35%	49%
Your recovery plan (or lack thereof)	35%	31%	34%
Worrying about the next virus / worm	5%	18%	33%
A security breach to your website	5%	9%	23%
None. I sleep like a baby	40%	27%	21%
(N = number of respondents)	(43)	(170)	(140)

- In contrast, among those "slightly" to "somewhat" concerned about the security threat of social media, 35% were kept up at night by worrying about a security breach to their network. Among those "not at all concerned" about social media, only 16% were kept up at night worrying about a breach to their network. Thus, the more concerned network administrators were about employee use of social media as a threat to company security, the more likely these network administrators were to stay awake at night worrying about a breach to their network.

  - Of course, there are many possible reasons for worrying about a breach to their network, and we are not saying that social media is necessarily a primary cause. But, it is interesting that there is a statistically significant relationship between how concerned network administrators are about employee use of social media and how likely they are to worry about a security breach to their network. Although not absolute proof of "causation," the relationship is strong enough to recommend that organizations carefully consider the potential risks related to employee use of social media.

- Similarly, those more concerned about social media were also more likely to be kept up by worries about their users, the next virus / worm, and/or a security breach to their website.

- From a separate analysis, what is perhaps encouraging news is that 41% of those "moderately" to "extremely" concerned about the security threat of social media were seeing an increase in their IT security budget for 2010, compared to 2009. Although we are *not* saying that the budget increases were because of

social media usage, it is still encouraging that some of those with concerns about social media are facing improving budget conditions.

- Not so encouraging is that, among those who felt their organization has not budgeted sufficiently, 46% were "moderately" to "extremely" concerned about the security threat of employee usage of social media. This is another reminder that worries often fall on those who do not feel they have a sufficient budget to support their current information security needs.

- The next table shows that more than one-third (37%) reported that their organization allows unlimited access to social media when using the company network, and close to half (48%) have limited access.

2010: What degree of access do employees have to social media when using your company network?

Legend	Response Choice	Frequencies	Count
1	No access	15.29%	54
2	Limited access	48.15%	170
3	Unlimited access	36.54%	129
	Total (N)		**353**

- However, employee usage of social media can still be a concern even when employees have limited or no access to social media via the company network. This is shown in the table below, which divides the respondents into three groups based on how much access their organization allows to social media via the company network. Interestingly, even when employees had no access to social media via the company network (i.e., see the "No Access" column of the table), 31% of the network administrators working in those organizations were still "extremely concerned" about the security threat of social media.

How concerned are you with employee use of social media as a security threat to your company?	*Employee Social Media Access When Using Company Network:*		
	No Access	***Limited Access***	***Unlimited Access***
Not at all concerned	19%	10%	12%
Slightly concerned	15%	19%	30%
Somewhat concerned	20%	29%	24%
Moderately concerned	15%	25%	21%
Extremely concerned	31%	17%	13%
(N = number of respondents)	(54)	(170)	(129)

- At the same time, when employees have limited access, 17% of the network administrators at these organizations were extremely concerned, and 25% were moderately concerned about employee use of social media.

- Employee use of social media can be governed by a formal company policy, but this is frequently not the case. As shown below, slightly more than half indicated that their organization has such a policy.

2010: Does your company have a formal policy regarding employee use of social media?

Legend	Response Choice	Frequencies	Count
1	No	44.47%	157
2	Yes	55.52%	196
	Total (N)		**353**

- Next, it is interesting to compare those who have vs. those who do not have a formal policy. For example, as shown in the table below, when there is no formal policy (see the "No" column), 59% of these organizations allow employees unlimited access to social media when using the company network. When there is a formal policy in place (see the "Yes" column), only 18% of those organizations allow unlimited employee access.

What degree of access do employees have to social media when using your company network?	*Have Formal Policy Regarding Employee Use Of Social Media:*	
	No	***Yes***
No access	6%	23%
Limited access	35%	59%
Unlimited access	59%	18%
(N = number of respondents)	(157)	(196)

- We do not know all of the aspects of the formal policies related to employee usage of social media. Some of these policies might provide guidelines about appropriate and inappropriate sharing of company information when using social media. Some policies might restrict or prohibit using social media while at work and/or with company equipment. This is a topic that could be investigated further in future research. At this stage, in light of the results above, it appears that formal policies about employee usage of social media may often (but certainly not always) involve restrictions on access using the company network.

- However, the majority of the time there is not a complete prohibition of employees using social media on the company network. In fact, even at

organizations with formal policies in place (see the "Yes" column above), 59% still allow employees *limited* access to social media via the company network.

- Moreover, it does not appear that a prohibition on social media usage at work would solve security problems. As noted previously, even at organizations that do not allow social media access via the company network, many network administrators are still concerned about the risk posed by employee use of social media.

  - For example, one can imagine an employee using social media only at home but also sometimes working from home and sharing files between home and work. In this case, home use of social media could still ultimately lead to a virus being inadvertently transferred to the company network.

  - As another example, even if social media is used only at home, an employee could reveal information (perhaps unwittingly) on a social media site that could later turn out to be useful to a hacker interested in gaining unauthorized access to the network where the employee works. During purely personal social media usage, an employee may reveal where they work and many other details about their company and/or work practices.

- To further investigate, the table below shows how those with and without a formal policy compare on concern about social media as a security threat to their organization. For example, of those with a formal policy (see the "Yes" column), 22% were still extremely concerned. In fact, this was even higher than among those who do not have a formal policy (see the "No" column).

How concerned are you with employee use of social media as a security threat to your company?	*Have Formal Policy Regarding Employee Use Of Social Media:*	
	No	***Yes***
Not at all concerned	14%	11%
Slightly concerned	26%	19%
Somewhat concerned	29%	24%
Moderately concerned	19%	24%
Extremely concerned	12%	22%
(N = number of respondents)	(157)	(196)

- Only 11% of those with a formal policy were "not at all concerned," and this suggests that the formal policies currently in place are far from a perceived "cure" for the potential risks associated with employee usage of social media.

  - As a side note, there are some nuances that may impact the results shown above. For example, greater concern about social media could sometimes make an organization more likely to adopt formal policies about employee usage of social media. Although it is possible that these policies may be helpful to some extent, they may not have

enough impact to sufficiently alleviate the risks involved. This could leave network administrators still extremely concerned, even with formal policies in place. This may be one reason that the proportion "extremely concerned" above is higher among those with vs. those without formal policies.

- As a final note about the concern network administrators have about social media, some may wonder if results differ by company size, but it turns out that network administrators from small, midsize, and large companies were about as likely to be concerned. For example, among "small companies" (i.e., with between 1 and 99 employees), 35% were moderately to extremely concerned about social media usage by employees. Among "midsize companies" (with 100 - 999 employees), 41% were moderately to extremely concerned about social media. Among "large companies" (with 1,000 or more employees), 41% were moderately to extremely concerned about employee use of social media as a security threat to the company.

- In addition to the question referring to "concern" about the potential security threat of employee use of social media, a separate question covered below was similar in some respects but differed by referring to the "importance" of managing the security of social media "as compared to other security threats facing your company." For this question, 9% gave a rating of "extremely important," and 35% gave a rating of "very important." Combined, more than four-in-ten (44% = 9% + 35%) felt that managing the security of social media was "very" or "extremely" important relative to various other security threats. This confirms that social media is often considered a relatively important company security issue.

2010: As compared to other security threats facing your company, how important is managing the security of social media being used by company employees?

Legend	Response Choice	Frequencies	Count
1	Not at all important	9.34%	33
2	Slightly important	15.86%	56
3	Somewhat important	30.87%	109
4	Very important	34.56%	122
5	Extremely important	9.34%	33
	Total (N)		**353**

Smartphones

- The question below utilized the same rating scale as above (i.e., ranging from "not at all important" to "extremely important") but this question was about "Smartphones."

2010: As compared to other security threats facing your company, how important is managing the security of employee smartphones (Blackberry, iPhone, Palm Pre, Palm Treo, Motorola Q, comparable models by Nokia or Sony Ericsson, or other similar type of phone with a data plan or PC-like functionality)?

Legend	Response Choice	Frequencies	Count
1	Not at all important	12.74%	45
2	Slightly important	17.84%	63
3	Somewhat important	28.32%	100
4	Very important	32.01%	113
5	Extremely important	9.06%	32
	Total (N)		**353**

- When comparing the results for smartphones above to the results for the importance of managing social media on the previous page, the reader might notice that the results look fairly similar. One reason is that the two questions were significantly correlated. That is, network administrators who gave a high importance rating in one question often gave a high importance rating for the other question. At the same time, those who gave a low rating for one question often gave a low rating for the other question. In the end, this is not surprising, since employees who use smartphones may often use social media; and, among various other tasks, they may use their smartphones *for* social media.

    - The following finding may help to "quantify" the relationship discussed above. Among those who rated managing the security of social media very or extremely important, 66% also rated managing the security of smartphones very or extremely important.

Cloud Computing

- Another topic covered for the first time in the 2010 survey involved "Cloud Computing." As shown below, a minority (15%) has already adopted it, and close to half (47%) are giving it consideration.

2010: To what extent has your company adopted cloud computing for one or more applications?

Legend	Response Choice	Frequencies	Count
1	Have not adopted and not currently considering	38.24%	135
2	Currently considering but not adopted	46.74%	165
3	Adopted	15.01%	53
	Total (N)		**353**

- Network administrators were next asked to rate the security of cloud computing. As shown in the first table below, among those who have already adopted cloud computing, more than four-in-ten (43%) rated it "very secure." In the table after that, 14% of those who have *not* yet adopted cloud computing rated it "very secure."

2010: **[IF ADOPTED]** How would you rate the security of cloud computing?

Legend	Response Choice	Frequencies	Count
1	Not at all secure	1.88%	1
2	Not very secure	7.54%	4
3	Somewhat secure	43.39%	23
4	Very secure	43.39%	23
5	Have no idea	3.77%	2
	Total (N)		**53**

2010: **[IF NOT ADOPTED]** Based on your current understanding, how would you rate the security of cloud computing?

Legend	Response Choice	Frequencies	Count
1	Not at all secure	3.33%	10
2	Not very secure	11.33%	34
3	Somewhat secure	56.0%	168
4	Very secure	13.66%	41

5	Have no idea	15.66%	47
	Total (N)		**300**

- However, more than two-thirds (70%) of those who have not adopted cloud computing rated it at least "somewhat secure" (i.e., 13.66% "very secure" plus 56.00% "somewhat secure").

    - Among just those who are currently considering cloud computing but have not adopted it yet, 18% gave a "very secure" rating, and 63% gave a "somewhat secure" rating.

- Small percentages of non-users rated cloud computing "not at all secure" (3%) or "not very secure" (11%). In a follow-up question, as shown below, security was often their reason for not adopting, but this question was asked only of those who rated cloud computing less than somewhat secure. (Pay careful attention to the "Total N" shown in each table of this section. For example, only 44 respondents were asked the question below.)

2010: **[IF NOT ADOPTED *AND* RATED LESS THAN SOMEWHAT SECURE]** Are security concerns the primary reason you have not yet adopted cloud computing?

Legend	Response Choice	Frequencies	Count
1	No	38.63%	17
2	Yes	61.36%	27
	Total (N)		**44**

- To help clarify, the 27 respondents who said "Yes" to the question above represent 8% of the total sample (i.e., 8% = 27 / 353). This shows that only a small percentage of the network administrators surveyed both gave a "low rating" (i.e., "not at all secure" or "not very secure") for the security of cloud computing *and* indicated that their security concerns were the primary reason for not adopting cloud computing.

Mac OS X

- More than one-third, as shown below, has adopted the Mac OS X platform.

2010: Has your company adopted the Mac OS X platform for one or more of its computers?

Legend	Response Choice	Frequencies	Count
1	No	63.45%	224
2	Yes	36.54%	129
	Total (N)		**353**

  - Interestingly, adoption of Mac OS X was very similar among small (35%), midsize (36%), and large (38%) organizations.

- About half of the time when adopting Mac OS X, less than 10% of the company computers were using the platform.

2010: What percentage of your company computers currently uses the Mac OS X platform?

Legend	Response Choice	Frequencies	Count
1	Less than 10%	50.38%	65
2	10% to 25%	25.58%	33
3	26% to 50%	13.17%	17
4	51% to 75%	8.52%	11
5	More than 75%	2.32%	3
	Total (N)		**129**

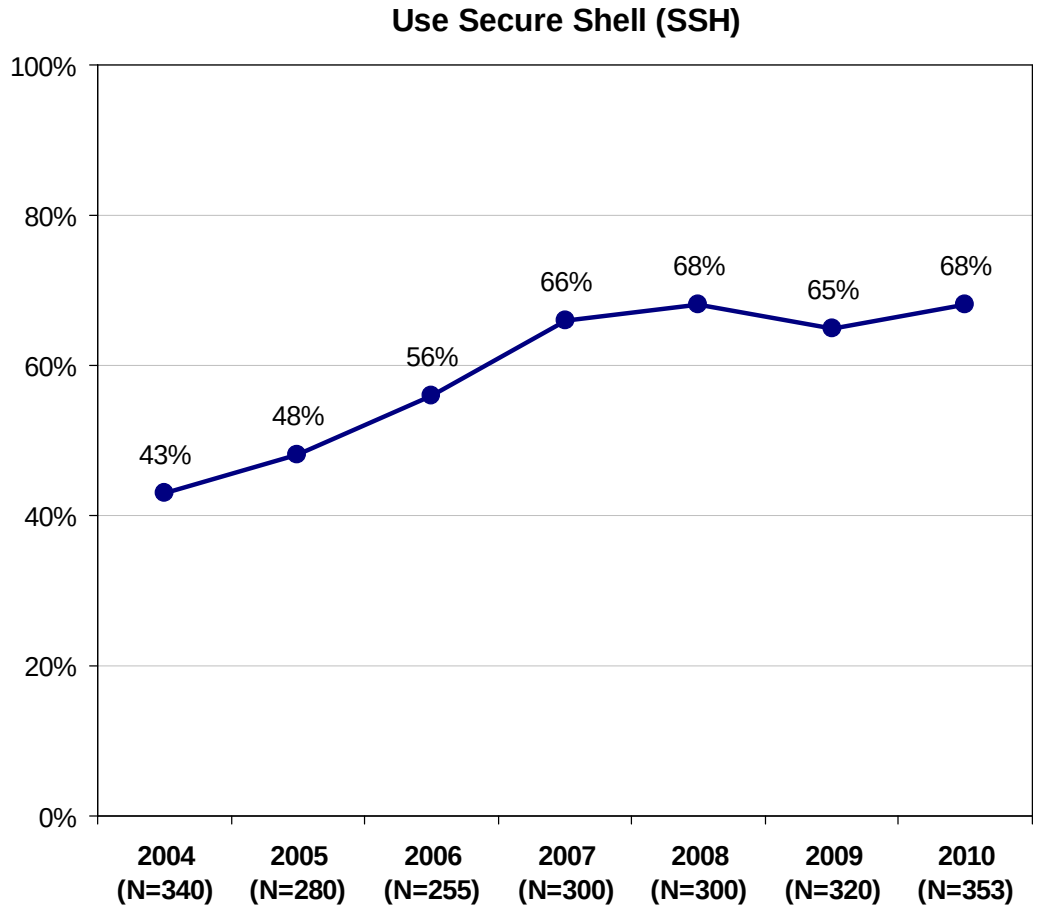
- Among organizations adopting Mac OS X, 21% of the network administrators surveyed were "extremely satisfied" and 30% were "very satisfied" with the *security* of the platform. However, this also means that 49% were less than "very satisfied".

2010: How satisfied are you with the security of the Mac OS X platform in comparison with the system you last used?

Legend	Response Choice	Frequencies	Count
1	Not at all satisfied	3.87%	5
2	Slightly satisfied	9.3%	12
3	Moderately satisfied	35.65%	46
4	Very satisfied	30.23%	39
5	Extremely satisfied	20.93%	27
	Total (N)		**129**

Securing Remote Access

- Approximately two-thirds in 2010 (68%) reported that their organization uses Secure Shell (SSH). As shown below, there was an upward trend between 2004 and 2007, followed by a fairly steady trend afterward.



- Since companies can use SSH1 or SSH2 or a mixture of both, users of Secure Shell were asked to indicate which type their organization is using. In 2010, 19% reported using "all" SSH2, and 25% reported "mostly" SSH2.

Are You Using SSH1 or SSH2?

	2004	2005	2006	2007	2008	2009	2010
All SSH1	21%	17%	7%	9%	8%	12%	8%
Mostly SSH1	26%	15%	25%	20%	29%	18%	17%
About 50/50	25%	27%	27%	29%	34%	30%	31%
Mostly SSH2	15%	27%	22%	25%	22%	26%	25%
All SSH2	13%	14%	19%	18%	8%	14%	19%
(N =)	(143)	(132)	(139)	(199)	(200)	(207)	(239)

- Next, when all respondents were asked how they configure their network devices, the most common response was HTTPS, as nearly two-thirds (65%) reported configuring their devices with HTTPS in 2010.

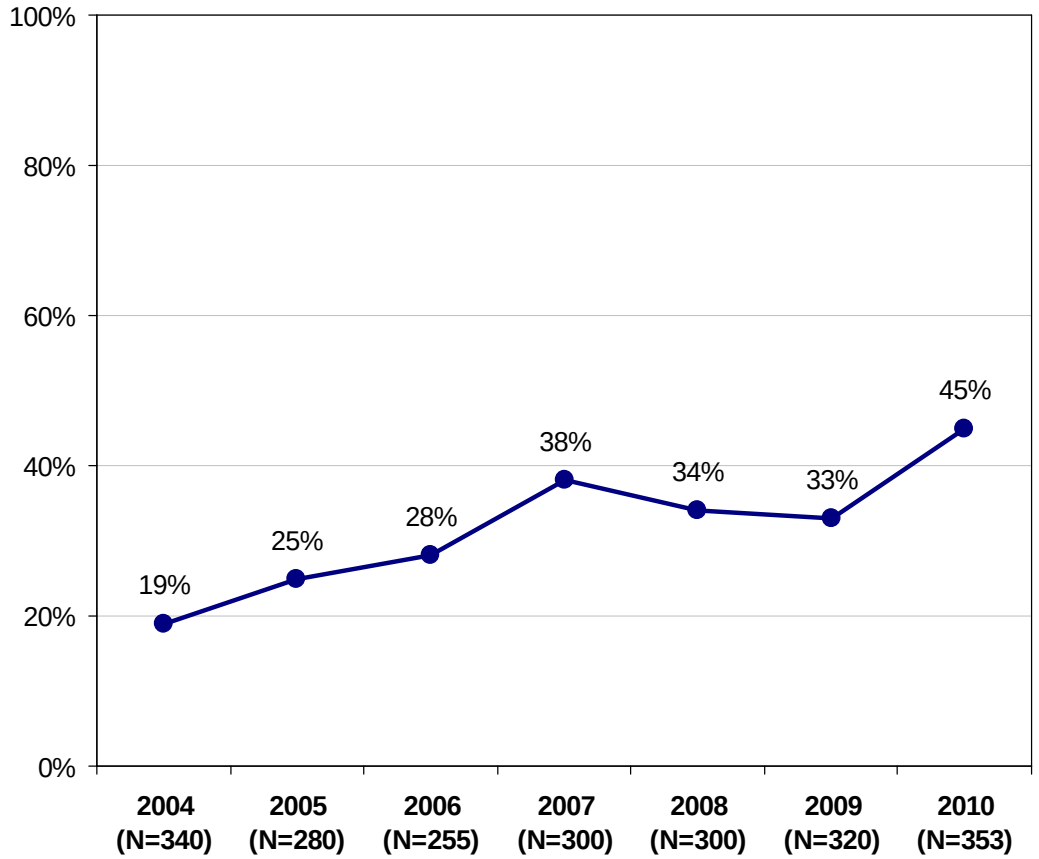
How Do You Configure Your Network Devices?

	2004	2005	2006	2007	2008	2009	2010
HTTPS	43%	58%	65%	57%	41%	67%	65%
HTTP	48%	43%	48%	48%	39%	41%	42%
SSH2	19%	25%	28%	38%	34%	33%	45%
SSH1	21%	23%	22%	29%	36%	30%	31%
Telnet	55%	48%	54%	38%	28%	52%	36%
(N =)	(340)	(280)	(255)	(300)	(300)	(320)	(353)

- Curiously, the proportion configuring network devices with Telnet trended downward between 2006 and 2008 (going from 54% to 28%), then rebounded sharply in 2009 (52%), only to decline significantly in 2010 (36%).

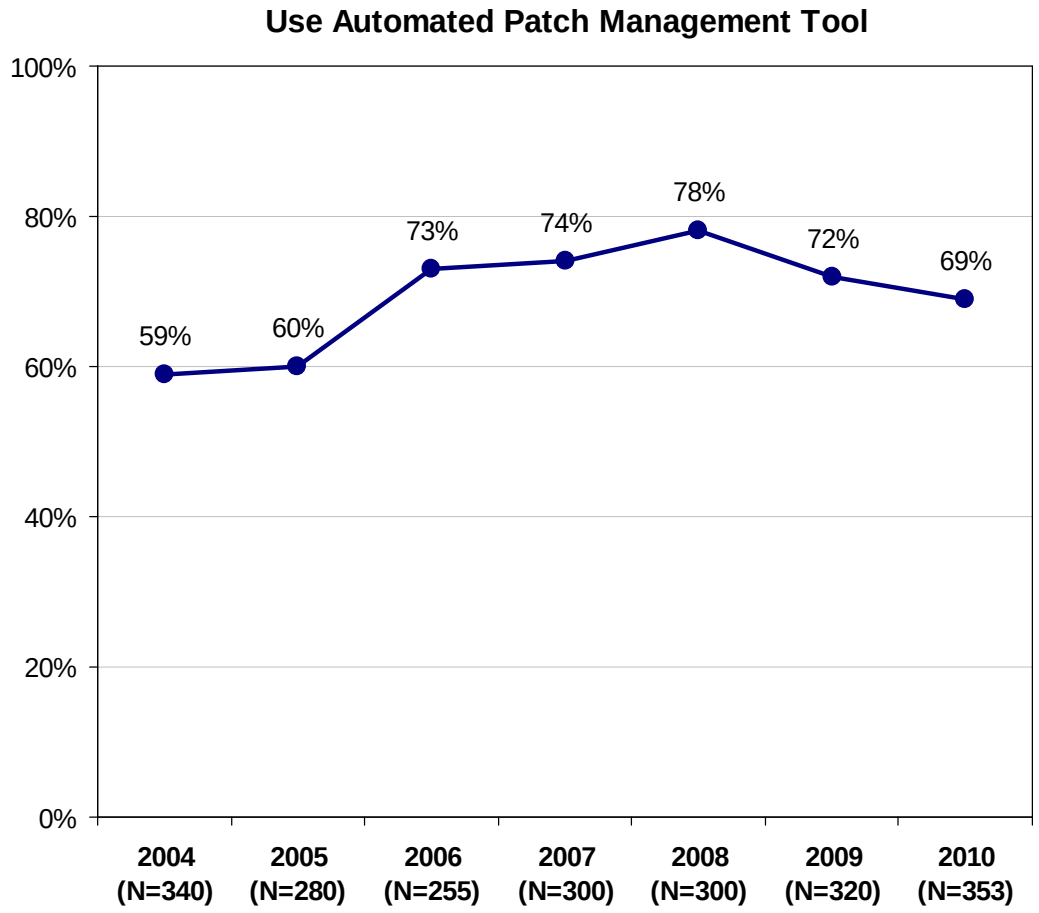
- The proportion selecting SSH2 increased in 2010 to 45%, up significantly from 33% in 2009. The chart below shows results for SSH2 from 2004 through 2010.

Configure Network Devices With SSH2



Automated Patch Management

- More than two-thirds of the respondents in each of the past five years reported using an automated patch management tool to distribute and install critical updates to operating systems and/or applications. However, the result in 2010 (69%) was significantly lower than the peak result in 2008 (78%).



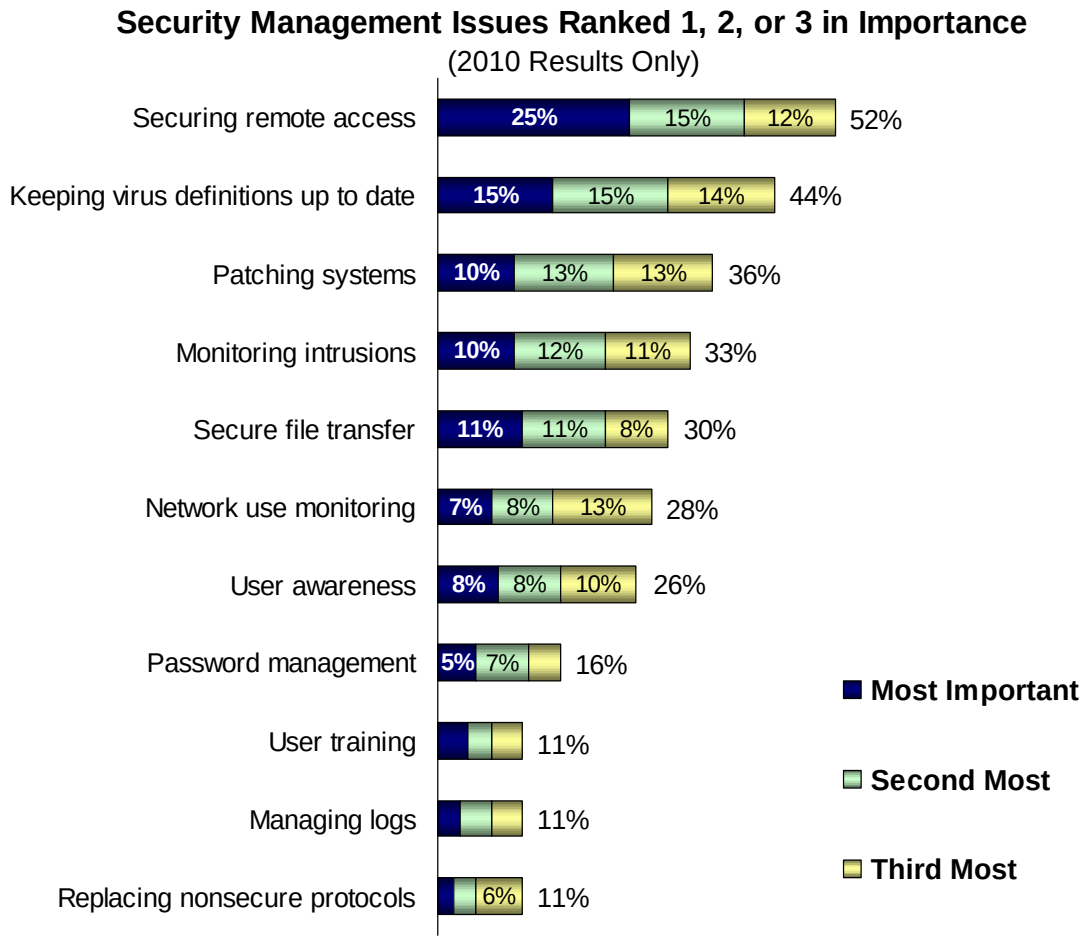
- When those who don't use an automated patch management tool were asked why not, the top reason was "it is not a priority" (35%), followed by "cost" (29%).

2010: What is the primary reason that you do NOT use automated patch management tools?

Response Choice	Frequencies	Count
Not a priority	34.86%	38
Cost	29.36%	32
Security Issues	21.11%	23
Other	14.67%	16
Total (N)		**109**

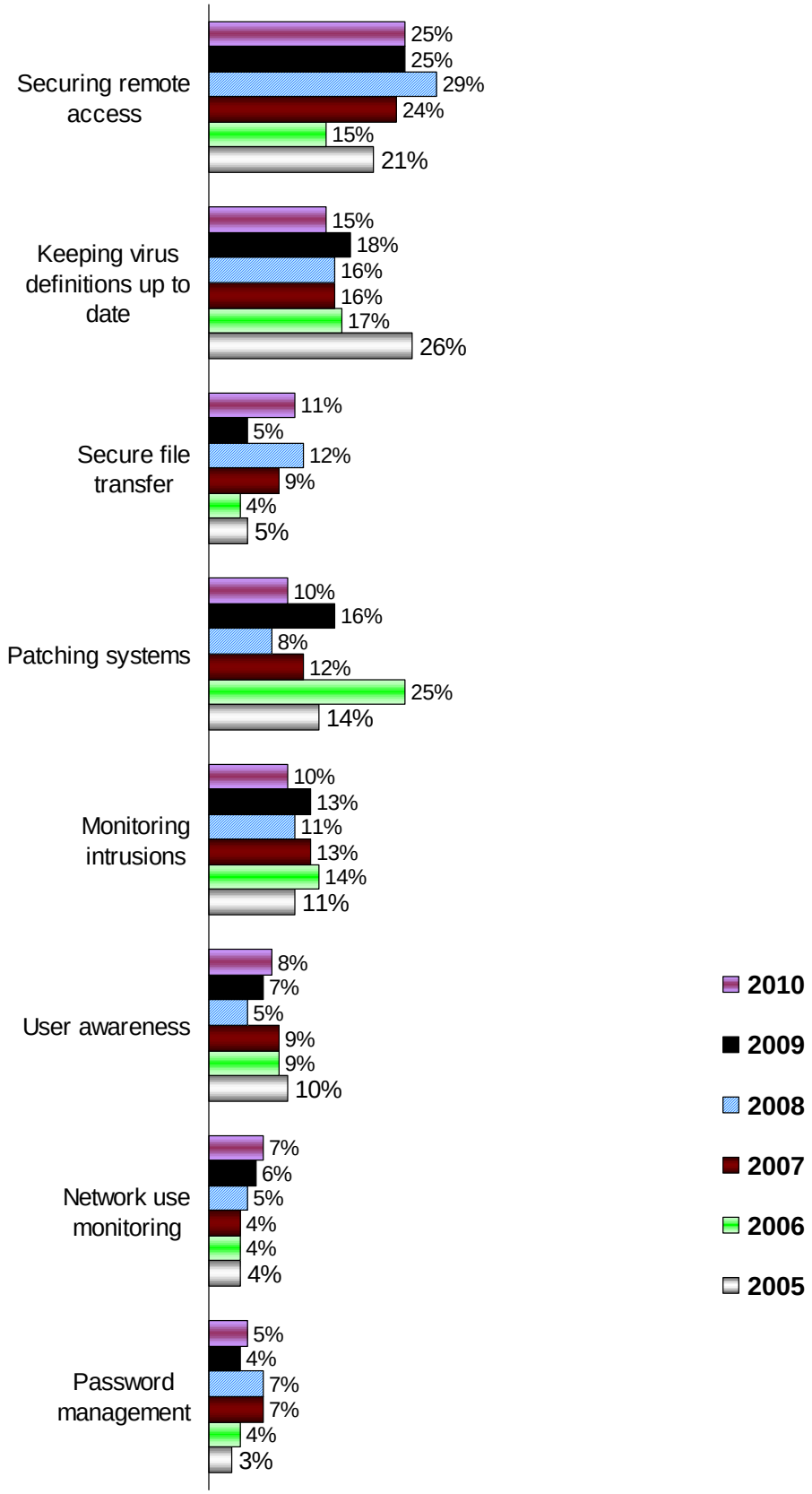
Security Management Priorities

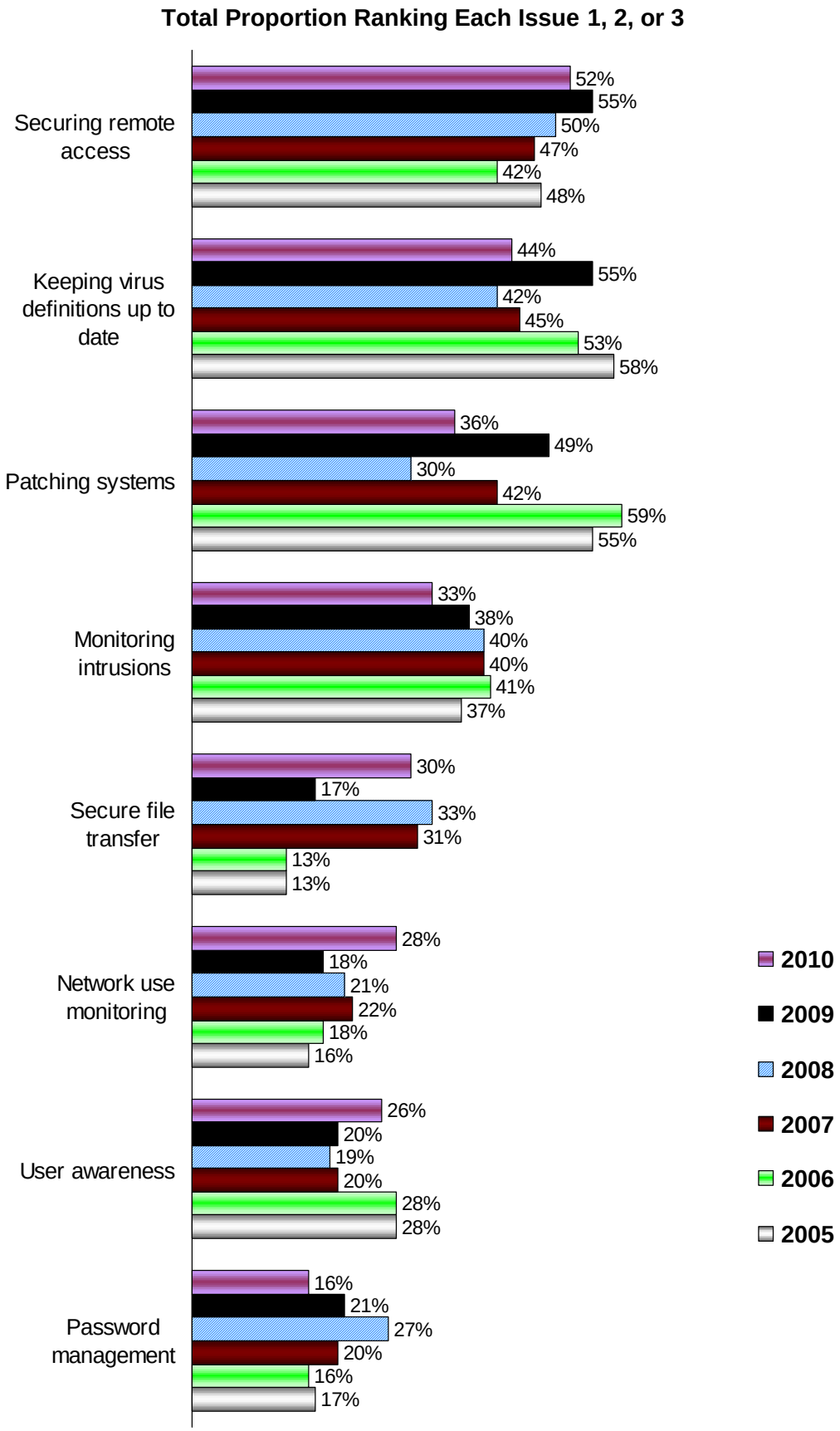
- To help understand security management priorities, network administrators were asked to rank the top three issues facing their company / organization from a list of 11 items. The best way to begin examining the results is to first focus on the 2010 survey results, as shown below. For example, 25% indicated that "securing remote access" is the #1 most important security management issue facing their organization. Another 15% gave "securing remote access" a rank of #2, and 12% gave it a rank of #3. In the end, 52% ranked "securing remote access" either 1, 2, or 3 in importance from the list of 11 items that are included in the chart below.



- After examining the 2010 results above, the next step is to make comparisons to previous years. The chart on the next page shows the proportion giving a #1 ranking for each issue each year. The chart on the page after that shows the proportions ranking each item #1 *or* #2 *or* #3 (i.e., among their top three). (In both charts the 3 lowest percentage items were excluded to enhance readability.) Perhaps the most interesting finding from these charts is that securing remote access has continued to have a higher proportion selecting it (as #1 priority and as among the top 3) than other issues.

Proportion Ranking Each Issue #1 in Importance




Total Proportion Ranking Each Issue 1, 2, or 3
Securing remote access
52%
55%
50%
47%
42%
48%
Keeping virus definitions up to date
44%
55%
42%
45%
53%
58%
Patching systems
36%
49%
30%
42%
59%
55%
Monitoring intrusions
33%
38%
40%
40%
41%
37%
Secure file transfer
30%
17%
33%
31%
13%
13%
Network use monitoring
28%
18%
21%
22%
18%
16%
User awareness
26%
20%
19%
20%
28%
28%
Password management
16%
21%
27%
20%
16%
17%
2010
2009
2008
2007
2006
2005

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 devices / aspects of IT security.

2010: How satisfied are you with the current security at your company for:

	Very dissatisfied	Somewhat dissatisfied	Neutral	Somewhat satisfied	Very satisfied	Not applicable
Legend	**1**	**2**	**3**	**4**	**5**	**6**
Desktop PCs	6 1.7%	26 7.37%	44 12.46%	145 41.08%	127 35.98%	5 1.42%
Laptops	12 3.4%	54 15.3%	49 13.88%	125 35.41%	99 28.05%	14 3.97%
Handheld devices (e.g., Palm, PocketPC, Blackberry)	14 3.97%	40 11.33%	75 21.25%	114 32.29%	58 16.43%	52 14.73%
Data center / Server farm	4 1.13%	11 3.12%	41 11.61%	93 26.35%	184 52.12%	20 5.67%
Wireless LAN	7 1.98%	25 7.08%	66 18.7%	113 32.01%	104 29.46%	38 10.76%
Remote access by employees, customers, and/or partners	11 3.12%	23 6.52%	51 14.45%	152 43.06%	100 28.33%	16 4.53%
Physical security (facility and workstation access)	15 4.25%	24 6.8%	47 13.31%	110 31.16%	153 43.34%	4 1.13%
Virtual machines	5 1.42%	12 3.4%	69 19.55%	95 26.91%	112 31.73%	60 17.0%

- Since the table above shows the exact number and percentage for all response choices, "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 ("very" or "somewhat") with the security of each item, as shown below.

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

	2004	2005	2006	2007	2008	2009	2010
Datacenter / server farm	82%	80%	86%	84%	74%	81%	83%
Desktop PCs	76%	71%	74%	77%	74%	75%	78%
Physical security	71%	61%	75%	71%	66%	72%	75%
Remote access	64%	66%	68%	70%	66%	67%	75%
Virtual machines	na	na	na	na	na	63%	71%
Wireless LAN	55%	49%	60%	63%	66%	68%	69%
Laptops	58%	50%	58%	62%	67%	59%	66%
Handheld devices	45%	33%	44%	45%	52%	37%	57%

- Last year there was particular concern about a drop between 2008 and 2009 in the proportion satisfied with the security of laptops and handheld devices used at their company. In 2010, however, results improved for both items, especially for handheld devices.

- On other items in the table above, the proportion satisfied was slightly higher in 2010 than in 2009, although some of these increases were too small to be statistically significant.

    - The following items in the table above had increases in 2010 that were statistically significant: remote access (from 67% in 2009 to 75% in 2010), virtual machines (63% to 71%), and handheld devices (37% to 57%).