



# **The Ignored Risk of Employees' Use of Internet Applications**

---

**Sponsored by  
Palo Alto Networks**

Independently conducted by Ponemon Institute LLC

Publication Date: October 15, 2008

## The Ignored Risk of Employees' Use of Internet Applications

Prepared by Dr. Larry Ponemon, October 15, 2008

*The Ignored Risk of Employees' Use of Internet Applications* study reveals that employees with workplace computer access are putting their organizations at risk by using certain applications that could involve the sharing of sensitive and confidential information. Employees are using these applications to access important information from both the office and home. When confronted with a security or privacy breach due to use of an Internet application, 45% did nothing and continued to use the product. Further, 19% responded by simply decreasing their use of the application.

In the same study, 78% of IT security practitioners said that their organizations have policies prohibiting the use of specific applications, however almost half (48%) of respondents are not certain if employees are using these products that are not allowed. As a result, IT security practitioners don't know how vulnerable their organizations are to such risks as increased infection of malware and viruses, disclosure of confidential or sensitive company information and external threats to networks. If they do know, it is through network surveillance (46%), informal observations (43%), device scanning (28%) and periodic monitoring and auditing (21%).

Conducted by Ponemon Institute and sponsored by Palo Alto Networks, this is the first study to benchmark 649 end-users or employees who have Internet access as part of their role and 301 IT security practitioners in the same 193 U.S. based organizations on their use of Internet applications in the workplace. We focused on the following topics:

- Have employees ever experienced the loss of privacy or security when using one or more Internet applications? If so, what was their response?
- How pervasive is employees' use of instant messaging, Web-based email, social networks or other Internet applications?
- What Internet applications are most commonly used and which ones are most risky?
- Are organizations addressing this risk with policies? If so, are employees aware of the policies and are they complying with them?
- How do IT practitioners determine if Internet applications not permitted in the workplace are still being used?
- Do any of these applications involve the sharing of company confidential information such as customer names, location of business meetings, business confidential documents and so forth?

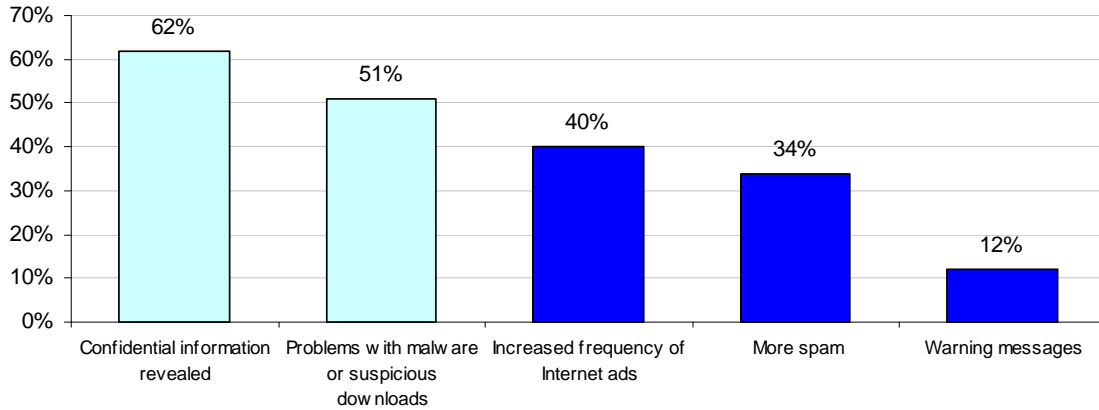
Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as the Appendix to this paper.

### **Many employees seem unconcerned about the loss of their personal information when using Internet applications.**

According to the study, 33% of employees have experienced privacy or security issues when using one or more of these Internet applications. Bar Chart 1a shows the most common consequences of the privacy or security breach. As reported, 62% say that the issue was the leakage of confidential information. Another 51% report that they experienced suspicious

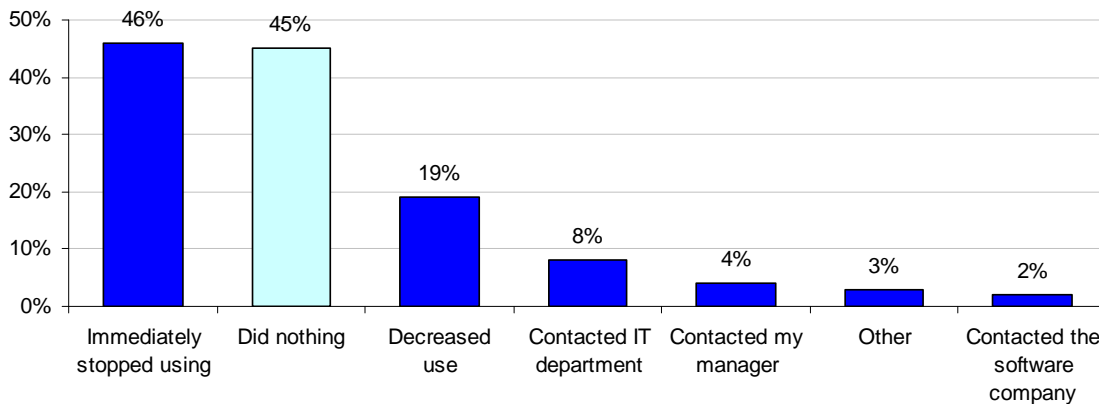
software downloads followed by 41% who report that it increased the frequency of Internet ads (spyware or malware) 34% received more spam and 12% say that they received warning messages from security applications or operating system.

Bar Chart 1a  
Privacy & security problems employees experienced



While 46% immediately stopped using the application, almost half (45%) did nothing as a result of having this experience as shown in Bar Chart 1b. This suggests that if so many seem unconcerned about their own personal privacy, it might affect their attitude about protecting their organizations' privacy.

Bar Chart 1b  
How employees responded to privacy & security problems



**Employees are using Internet applications that their organization prohibits.**

Bar Chart 2 shows some of the Internet applications IT security respondents say their organization prohibits employees from using and the percentage of employees in our study who use them at work and home. As shown, the most frequently used applications include iTunes, Webex and Google desktop search. More than 60% are frequent or very frequent users of these applications.

Bar Chart 2  
Employees' use of prohibited Internet applications at home and work

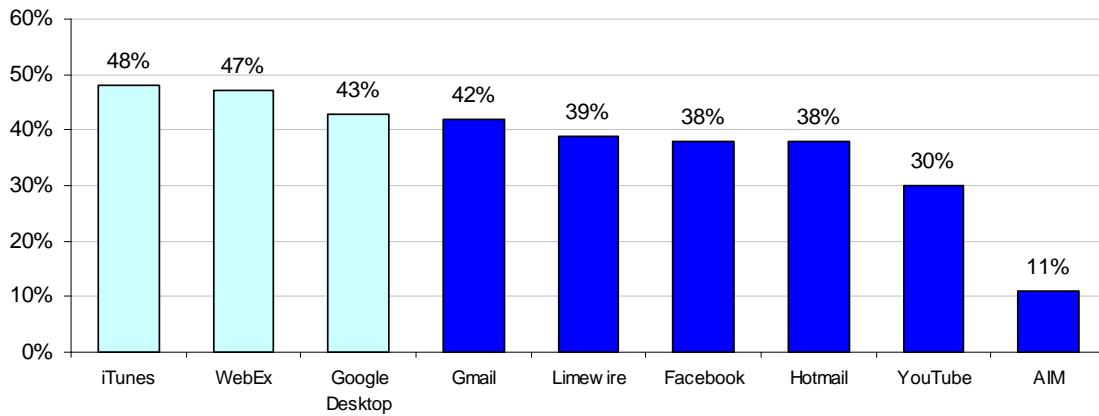


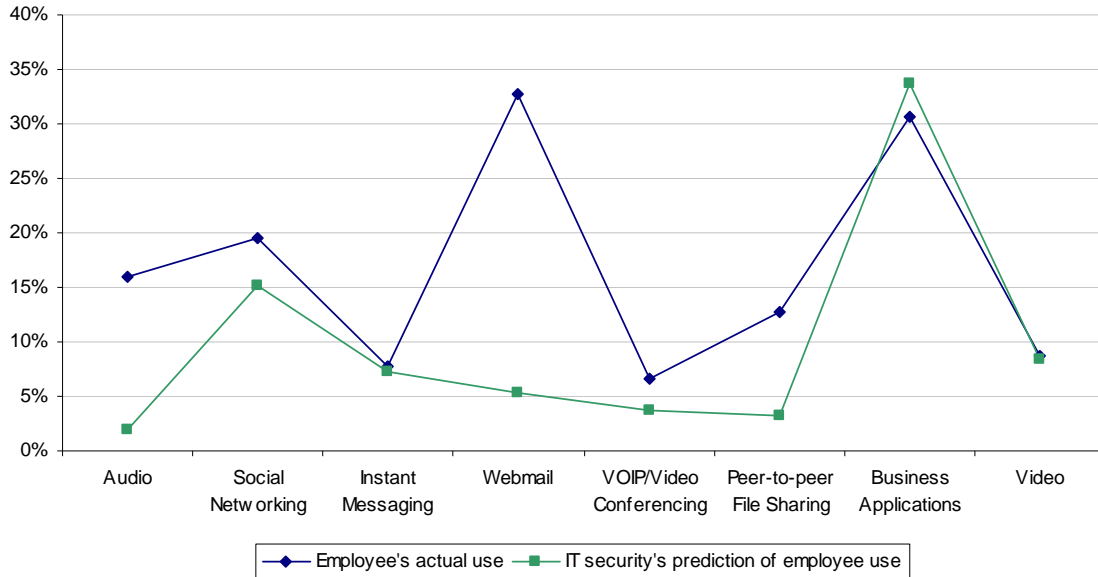
Table 1 shows the applications IT security practitioners believe are most risky to use. This risk score is a weighted average value ranging from 1 = highest risk to 5 = lowest risk. As can be seen, the 10 applications listed have an average risk score that is below 2.5 (the risk level median value). This suggests a high level of concern among IT security practitioners with respect to the use of these Internet applications by employees within their organizations.

Application	Average Risk Score (1=highest risk)
Limewire	1.67
YouTube	1.73
Gmail	1.92
Hotmail	1.96
MySpace	2.15
Facebook	2.21
Skype	2.30
Google Desktop Search	2.35
AIM	2.38
Google Talk	2.45

Many of these applications are prohibited from being used and believed to pose a serious risk to sensitive and confidential information. However, almost half of IT security practitioners don't know if employees are using these applications.

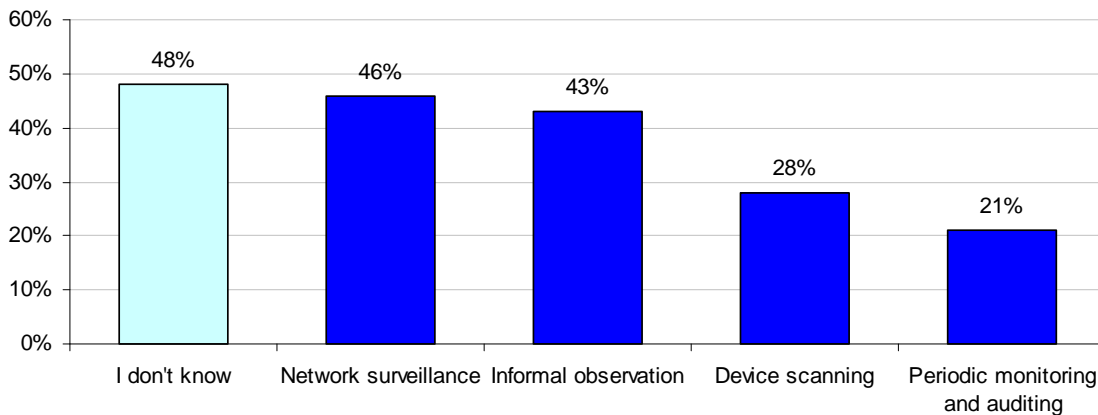
In the case of several of the prohibited applications, there is a significant gap between what employees self-report as using in the workplace and what IT security practitioners believe they are using in the workplace. Line Graph 1 shows the gap, especially in employees' use of audio (iTunes, Pandora and Ruckus) and Webmail (Gmail, Yahoo Mail and Hotmail) applications.

**Line Graph 1**  
**Gap analysis between employees' use of Internet applications in the workplace and IT security's prediction of employee use.**  
 Average percentage usage frequencies are reported by application category



Bar Chart 3 shows the methods that IT security practitioners use to determine if employees are using certain Internet applications. It is interesting to see that over 48% of IT security practitioners in our study do not know what applications are being used by employees.

**Bar Chart 3**  
 How IT security determines employees' use of prohibited Internet applications

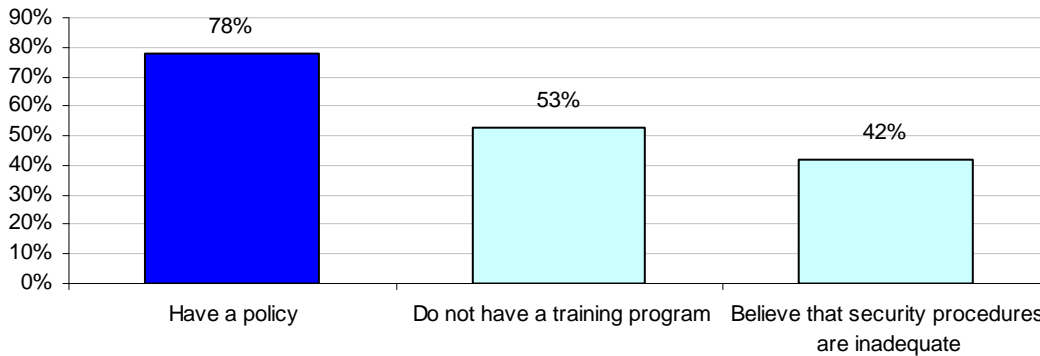


When asked if they use these applications, 48% of employees say they use Internet applications on a desktop, laptop, PDA, iPhone or other comparable mobile device in the workplace. Further, 55% admit to not having permission from their supervisors to use these applications.

**Policies to stop the use of risky Internet applications seem to be ineffective. Moreover, IT security practitioners don't believe their security procedures are adequate.**

As shown in Bar Chart 4, 78% of IT practitioners say their company has a policy, however about half (53%) have a training and awareness program to make sure employees understand and comply with the policy.

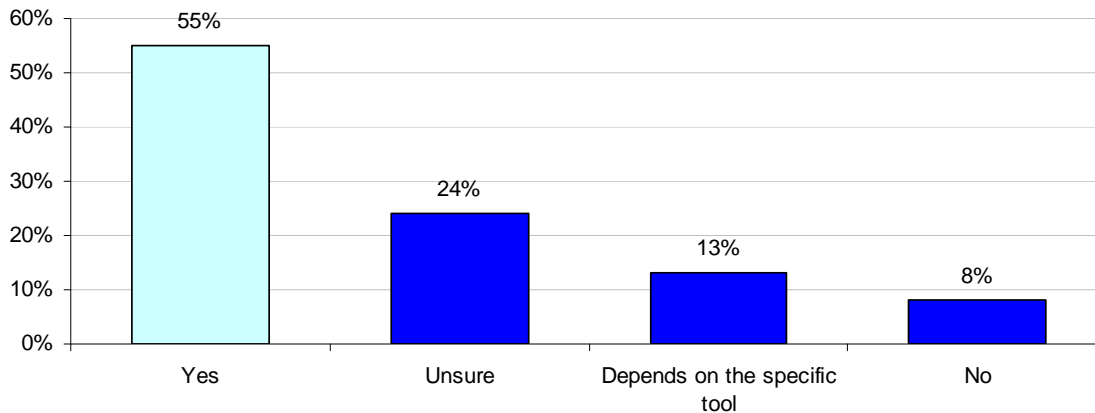
Bar Chart 4  
Percentage of companies that have a policy and training program that restricts or forbids the use of Internet applications



Also as shown, of those who responded that there is a policy, 42% say their security procedures are inadequate to reduce any risks associated with these applications.

Far fewer employees realize there is a policy. Only 41% of employees surveyed say there is a policy restricting or forbidding the use of these Internet tools in the workplace. As shown in Bar Chart 5, when asked if they would discontinue their use if such a policy existed, 55% say they would and 24% are unsure. The other 21% say it would depend on the specific tool (13%) and 8% say no. Only 40% report that their supervisor has given permission to use these applications in the workplace.

Bar Chart 5  
Would employees follow a policy restricting use of Internet applications?

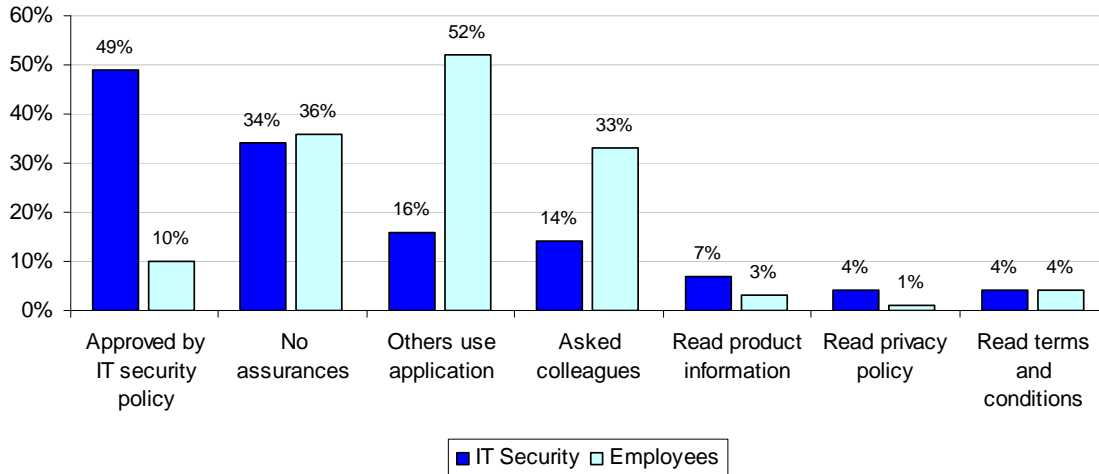


**IT security practitioners are more likely to make sure the Internet application is approved for use in their organization.**

As shown in Bar Chart 6, almost half (49%) of Internet security practitioners make sure the Internet application is approved by the company's IT security policy. However, 34% have no

assurances. Only 4% read the privacy policy or read the terms and conditions in end user licensing agreements.

Bar Chart 6  
Assurances relied upon when using Internet applications

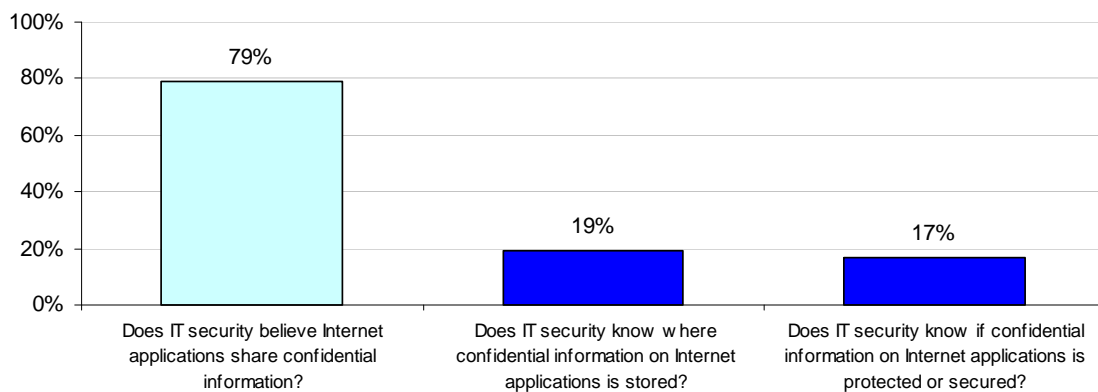


In contrast, as also illustrated in Bar Chart 6, more than half (52%) of employees believe that because others use these tools without incident it is fine to use them, and 36% have no assurance that the application can be used without risk. Only 10% of employees determine if the Internet application is approved for use. Just like IT security practitioners, however, only 4% read the terms and conditions in the end user licensing agreement and 3% obtained product information from the Internet before using the application. As a further indication of their attitude about privacy, only 1% read the applications' privacy policy.

**IT security practitioners recognize that these applications involve the sharing of confidential information; employees do not.**

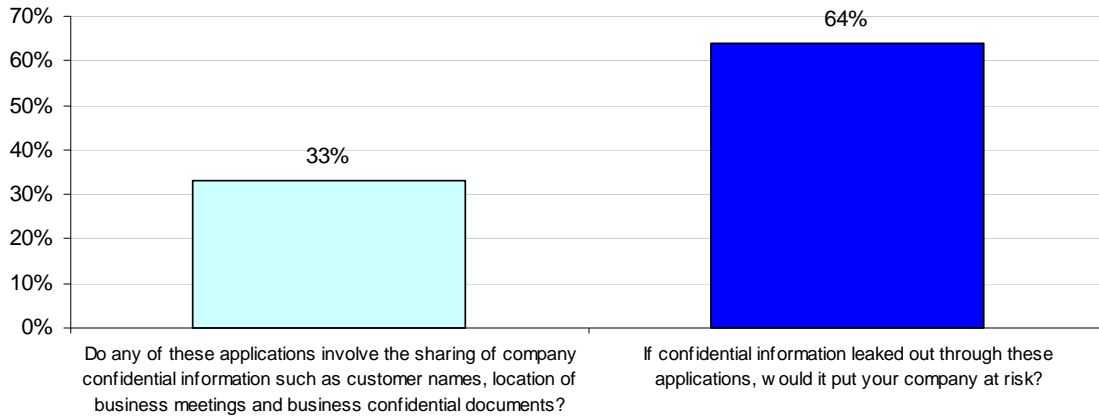
As shown in Bar Chart 7, 79% percent of IT security practitioners know that these applications can involve the sharing of confidential information such as customer names, location of business meetings and other business confidential documents. However, very few respondents know where the information is stored (19%) and if the information is protected or secured (17%).

Bar Chart 7  
Yes response to questions about sharing, storage and protection of confidential information on Internet applications



As illustrated in Bar Chart 8, only 33% of employees know if these applications involve sharing of confidential information. But 64% understand that the leakage of this information could pose a risk.

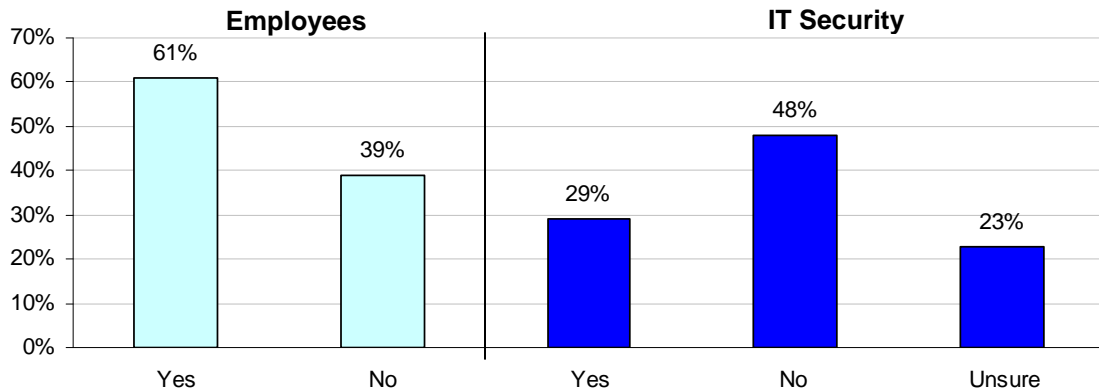
Bar Chart 8  
Do employees believe these Internet applications share confidential information?



**Employees believe Internet applications make them more efficient, but IT practitioners are skeptical.**

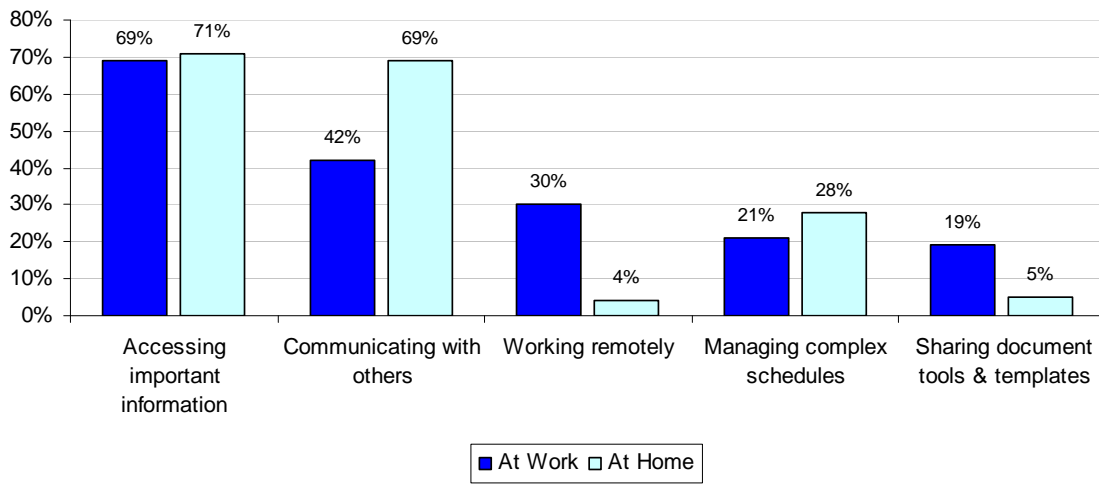
As shown in Bar Chart 9, 61% of employees believe they are more productive in the workplace when they are using Internet applications whereas only 29% of IT practitioners believe that these tools increase their job performance or productivity and 23% are unsure.

Bar Chart 9  
Do Internet applications improve productivity?



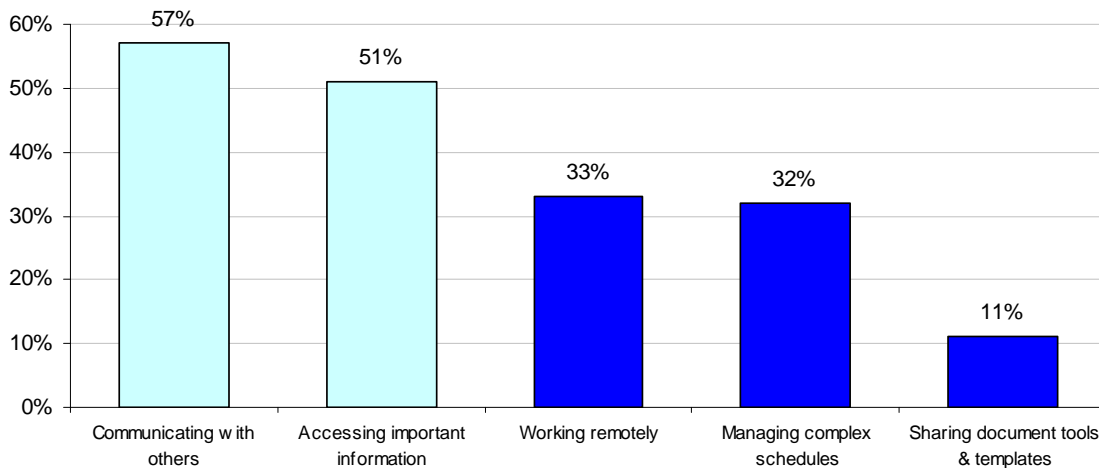
Employees believe that these applications make them more productive because they are able to access important information, communicate with others and work remotely (see Bar Chart 10a).

Bar Chart 10a  
How Internet applications make employees more productive at home and work



This is similar to the reasons cited by IT security practitioners: these tools enable them to access important information, communicate with contacts and work remotely (see Bar Chart 10b),

Bar Chart 10b  
How Internet applications make IT security more productive



### Implications for Organizations

Organizations' sensitive and confidential information is at risk because of the widespread use of Internet applications both at home and at the office. These are applications used for downloading music, social networking, instant messaging, Webmail, VOIP/video conferencing, business applications and video. The risk is created by employees who seem to be indifferent about the loss of personal and confidential information, and many IT security practitioners don't believe their security procedures are adequate to reduce the threat.

IT practitioners recognize the risk of Internet applications usage in the workplace. However, they don't seem to be taking the steps necessary to reduce this risk such as making sure employees are trained to follow policies prohibiting the use of these applications and the risk they pose to

sensitive and confidential information. In addition, only 49% check to make sure the Internet application they use is approved by their organization, and 34% don't have any such assurance.

Despite the prevalence of publicized data breaches, employees in our study seem to be apathetic about the possibility of losing confidential business information that could include customer names. While 64% of employee respondents recognize that if confidential information were leaked through these applications it would put their organization at risk, they do little to determine the safety of the applications, such as of making sure they are approved for use by the IT security policy and pursuing other assurances. For many respondents in our study, this apathy extends to their own personal privacy.

Employees see the value of using these applications at work outweighing security issues. Organizations need to communicate the importance of protecting sensitive and confidential data—even if it results in some loss of worker efficiency. A significant number of employees in our study see these tools as positive because they contribute to job performance and productivity. Employees should be made aware that while productivity is important, protecting sensitive and confidential data they handle is critical.

Organizations should understand the security practices needed to protect the organization from risks posed by these tools. The study revealed that the majority of IT security practitioners don't know or are unsure about where the confidential information on these applications is stored and don't know or are unsure if this data is protected or secured.

According to IT security practitioners, the procedures necessary to reduce the disallowed Internet applications in the workplace are: training and education of employees, limited use of portable devices, enhanced perimeter controls such as firewalls, network surveillance, access controls and device scanning.

### **Survey Caveats**

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the benchmark list is representative of U.S. companies and individuals who are typical IT security practitioners or employees/end users. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

### **Benchmark Sample**

This study utilized a benchmark sampling method. More than four thousand U.S.-based companies were included in our proprietary sampling frame. As shown in Table 2, 193 public or

private sector organizations participated in this research.<sup>1</sup> Within each organization, we selected representative samples of respondents from two target groups – namely, IT security practitioners and employees who have desktop or laptop access as a normal part of their job or function. In total, 301 IT security practitioners and 649 end-users (employees) completed usable survey responses.

Responses were captured using a web-based survey instrument and no personally identifiable information was collected. All respondents were located in the United States.<sup>2</sup> More than 95% of all respondents completed the survey instrument within 14 minutes.

<b>Table 2</b> Description of sample	Freq.	Pct%
Total companies	4,207	100.0%
Total responses	330	7.8%
Companies that lacked matching criteria	137	3.3%
Benchmark sample of separate companies	193	4.6%
Sample of IT security practitioners with 193 companies	301	
Sample of employees (end-users) within 193 companies	649	

Following are self-reported key demographics and organizational characteristics for respondents. Table 3a reports the position level of IT security respondents and Table 3b reports the position level for employees (end-users). The majority of respondents in both groups are at the director, manager or associate/technician/staff levels (60%).

<b>Table 3a</b> Position levels for IT security	Pct%
Executive	0%
Vice President	2%
Director	25%
Manager	42%
Associate/technician/staff	30%
Other	1%
Total	100%

<b>Table 3b</b> Position levels for employees	Pct%
Executive	2%
Vice President	4%
Director	22%
Manager	43%
Associate/Staff	29%
Other	0%
Total	100%

As shown in Table 4, on average, IT security respondents have 10.24 years of overall work experience and 4.01 of years in current position. Employees (end-users) have 11.70 years of overall work experience and 3.21 years in current position.

<b>Table 4</b> Experience	IT Security	Employees
Total years of experience	10.24	11.70
Total years in current position	4.01	3.21

Pie Chart 1 reports the industry distribution of 193 organizations participating in our benchmark study in descending order by size. As shown, the largest groups of respondents are employed by banking institutions, retailers and government entities.

<sup>1</sup> A total of 37 companies did not match benchmark criteria because they did not have fully dedicated employees in IT security.

<sup>2</sup> Respondents were given nominal compensation to complete survey questions.

**Pie Chart 1: Distribution of the Benchmark Sample**

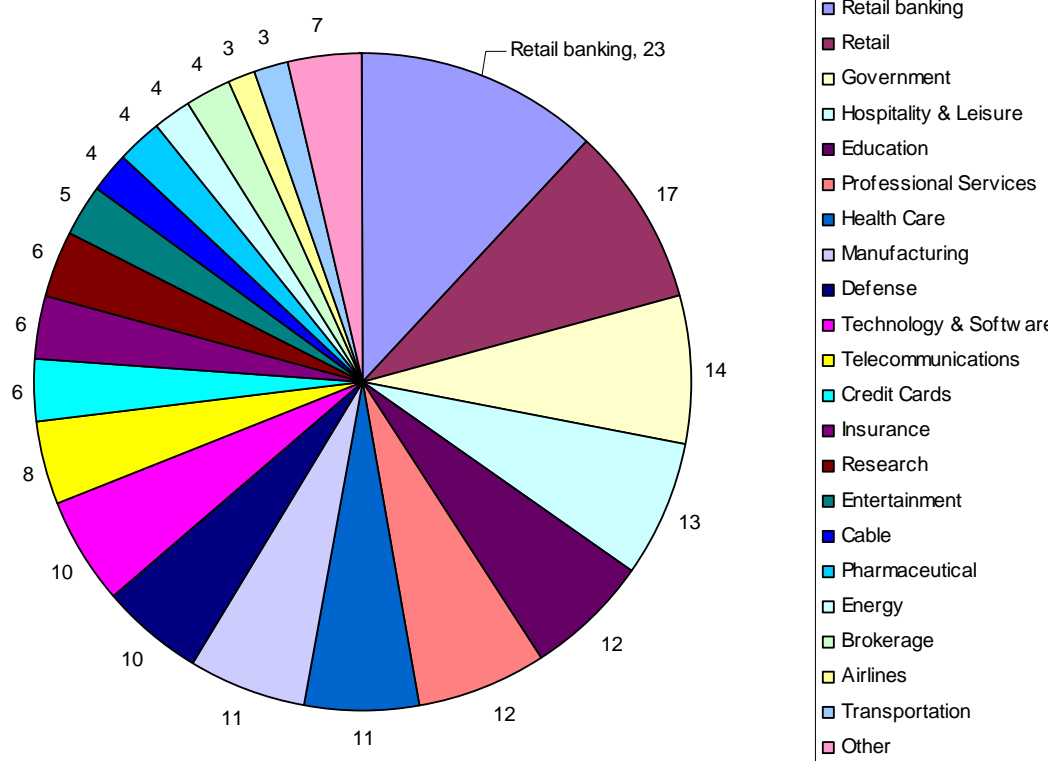


Table 5a shows the location of respondents' companies in the United States. Table 5b provides the approximate headcounts of these organizations. As can be seen, 71% of respondents are employed by larger-sized organizations with more than 5,000 employees.

Geographic location	Pct%
Northeast	20%
Mid-Atlantic	19%
Midwest	19%
Southeast	12%
Southwest	14%
Pacific	16%
Total	100%

Organizational headcount	Pct%.
Less than 500 people	3%
500 to 1,000 people	6%
1,001 to 5,000 people	19%
5,001 to 25,000 people	36%
25,001 to 75,000 people	24%
More than 75,000 people	11%
Total	100%

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC  
 Attn: Research Department  
 2308 US 31 North  
 Traverse City, Michigan 49686  
 1.800.887.3118  
[research@ponemon.org](mailto:research@ponemon.org)

## **Ponemon Institute** LLC

*Advancing Responsible Information Management*

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

## Appendix I: End-User Study

Benchmark sample of workplace Internet users: Sample size = 649 individuals from 193 U.S. companies

	Q1	Q4
	You use app either at home or at work	You use app in the workplace
Please check those applications employees are not allowed to use in the workplace.		
<b>Audio:</b>		
iTunes	48%	20%
Pandora	19%	12%
Ruckus	18%	16%
<b>Social Networking:</b>		
Facebook	38%	27%
MySpace	34%	29%
StumbleUpon	4%	2%
<b>Instant Messaging:</b>		
Aim	11%	10%
Yahoo!	8%	7%
GoogleTalk	8%	6%
<b>Webmail:</b>		
Gmail	42%	40%
Yahoo Mail	29%	26%
Hotmail	38%	32%
<b>VOIP/Video Conferencing:</b>		
Skype	19%	13%
Yahoo voice/Webcam	9%	6%
MSN voice/Video	2%	1%
<b>Peer-to-peer File Sharing:</b>		
BitTorrent	14%	11%
Limewire	39%	20%
eMule	11%	7%
<b>Business Applications:</b>		
Salesforce.com	7%	7%
WebEx	47%	45%
Google Desktop Search	43%	40%
<b>Video:</b>		
YouTube	30%	19%
Hulu	19%	6%
Sling	3%	1%
Average	22%	17%

Q2. For the applications checked above, how would you define your level of use?	Pct%
Very frequent	17%
Frequent	43%
Occasional	28%
Rare	12%
Total	100%

Use of Internet apps	Pct%	Median	Average
None	29%	0	0
Between 1 to 3	14%	2	0.3
Between 4 to 6	22%	5	1.1
Between 7 to 9	13%	8	1.0
Between 10 to 12	6%	11	0.7
Between 13 to 15	7%	14	0.9
Between 16 to 18	6%	17	1.0
Between 18 to 20	2%	19	0.4
More than 20	2%	22	0.3
Total	100%		5.7

Q3. Please list up to five Internet applications that you use most frequently? 1 = the most frequently used.	Freq.	Forced Rank
iTunes	48%	1
WebEx	47%	2
Desktop	43%	3
Gmail	42%	4
Limewire	39%	5

Q4. Please list up to five Internet applications you know are the <b>greatest</b> security risks to your company? . 1 = the highest risk level.	Average Risk Score	Forced Rank
Limewire	1.67	1
YouTube	1.73	2
Gmail	1.92	3
Hotmail	1.96	4
MySpace	2.15	5
Facebook	2.21	6
Skype	2.30	7
Google Desktop Search	2.35	8
AIM	2.38	9
Google Talk	2.45	10

Q5. Do you use any of the applications listed above on a desktop, laptop, PDA, iPhone or other comparable mobile device in the workplace?	Pct%
Yes	48%
No	52%
Total	100%

Q6a. Do these applications increase your job performance or productivity?	Pct%
Yes	61%
No	39%
Total	100%

If yes, how do they make you more productive?	Q6b at Work	Q6c at Home
Accessing important information	69%	71%
Communicating with contacts and colleagues	42%	69%
Working remotely	30%	4%
Managing complex schedules	21%	28%
Sharing tools and templates for documents and presentations	19%	5%
Other	3%	2%
Total	185%	179%

Q7. Do you have permission from your supervisor or manager to use these applications in the workplace?	Pct%
Yes	40%
No	55%
Unsure	5%
Total	100%

Q8. Do any of these applications involve the sharing of company confidential information such as customer names, location of business meetings, business confidential documents and so forth?	Pct%
Yes	33%
No	28%
Unsure	39%
Total	100%

Q9. If confidential information leaked out through these applications, would it put your company at risk?	Pct%
Yes	64%
No	16%
Unsure	20%
Total	100%

Q10. What assurance do you have that the Internet applications you use can be <u>trusted</u> to protect your information (including company information provided by you)?	Total%
Others in my organization use it successfully or without incident, so it is okay	52%
No assurances	36%
Asked colleagues who use the application about safety and security features	33%
Approved by the company's IT security policy	10%
Read terms and conditions in end user licensing agreement	4%
Obtained product information from the Internet before using it	3%
Read privacy policy	1%
Other	1%
Total	139%

Q11a. Have you ever experienced the loss of your privacy or security when using one or more of these Internet applications?	Pct%
Yes	33%
No	67%
Total	100%

Q11b. If yes, what was the privacy or security issue? Please check all that apply.	Total%
Confidential information or secrets revealed to others without my permission	62%
Technical problems with computer, laptop or other devices used because of malware or other suspicious downloads	51%
Increased frequency of Internet ads	40%
Increased frequency of spam (email or IM)	34%
Warning message from security applications or operating system	12%
Total	199%

Q11c. If yes, what did you do as a result of these privacy and security problems?	Total%
Stopped using the product immediately	46%
Did nothing (continued using the product)	45%
Decreased frequency or level of use	19%
Contacted my IT or security department	8%
Contacted my immediate supervisor or manager	4%
Contacted the software company to express concern	2%
Other (please specify)	2%
Contacted outside parties such as attorney, regulator or law enforcement	1%
Total	127%

Q12. Does your company's IT or security department have a policy that restricts or forbids the use of these Internet tools?	Pct%
Yes	41%
No	33%
Unsure	26%
Total	100%

Q13. If your company's security policy restricts or forbids the use of these Internet tools you currently use, would you stop using them?	Pct%
Yes	55%
Depends on the specific tool	13%
Unsure	24%
No	8%
Total	100%

## Organizational Characteristics & Demographics, End-Users

What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	4%
Director	22%
Manager	43%
Associate/Staff	29%
Other	0%
Total	100%

Check the <b>Primary Person</b> you or your supervisor reports to within your organization. (too many security titles here)	Pct%
CEO/Executive Committee	2%
Chief Financial Officer	7%
Chief Information Officer	17%
Compliance Officer	10%
Chief Privacy Officer	0%
Marketing VP	8%
Sales VP	16%
Manufacturing VP	3%
Operations VP	15%
Director of Internal Audit	3%
General Counsel	1%
Chief Technology Officer	4%
Human Resources VP	6%
Chief Security Officer	0%
Chief Risk Officer	1%
Other	8%
Total	100%

Check the country or U.S. region where your company's <b>primary</b> headquarters is located.	Pct%
Northeast	21%
Mid-Atlantic	19%
Midwest	18%
Southeast	13%
Southwest	14%
Pacific	15%
Total	100%

Educational and career background:	Pct%
Sales & marketing	23%
Communications	3%
Engineering	14%
Research & development	8%
Information Technology & security	22%
Legal/compliance	6%
Accounting & finance	7%
Transportation & logistics	6%
Administration	3%
General management	4%
Other technical field	4%
Other non-technical field	1%
Total	100%

Experience	Mean
Total years of business experience	11.70
Total years in current position	3.21

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount? (Not appropriate here)	Pct%
Less than 10 people	4%
Between 10 to 50 people	7%
Between 50 to 100 people	7%
Between 100 to 500 people	12%
Between 500 to 1,000 people	11%
Between 1,000 to 2,000 people	26%
Over 2,000 people	21%
Unknown	12%
Total	100%

What industry best describes your organization's industry concentration or focus?	Pct%
Airlines	3%
Automotive	2%
Agriculture	0%
Brokerage	1%
Cable	3%
Chemicals	3%
Credit Cards	3%
Defense	4%
Education	4%
Entertainment	2%
Services	1%
Health Care	6%
Hospitality & Leisure	7%
Manufacturing	5%
Insurance	3%

Internet & ISPs	0%
Government	8%
Pharmaceutical	1%
Professional Services	6%
Research	3%
Retail	7%
Banking	8%
Energy	2%
Telecommunications	4%
Technology & Software	5%
Transportation	1%
Wireless	6%
Total	100%

What best describes your role in managing privacy and data protection risks within your organization? Check all that apply. (Not appropriate here)	Total%
Setting priorities	12%
Managing budgets	12%
Selecting vendors and contractors	6%
Determining privacy and data protection strategy	2%
Evaluating program performance	5%
Total	37%

What is the worldwide headcount of your organization?	Pct%
Less than 500 people	2%
500 to 1,000 people	7%
1,001 to 5,000 people	21%
5,001 to 25,000 people	36%
25,001 to 75,000 people	24%
More than 75,000 people	11%
Total	100%

## Appendix II: IT Security Study

Benchmark sample of IT security practitioners: Sample size = 301 individuals from 193 U.S. companies

	Q1	Q2	Q10a
Please check those applications employees are not allowed to use in the workplace.	Your company has a policy restricting use of the app	You believe that employees use this app in the workplace	You use this app in the workplace
<b>Audio:</b>			
iTunes	87%	3%	3%
Pandora	81%	2%	1%
Ruckus	80%	1%	1%
<b>Social Networking:</b>			
Facebook	88%	23%	12%
MySpace	87%	21%	9%
StumbleUpon	74%	2%	2%
<b>Instant Messaging:</b>			
Aim	76%	5%	3%
Yahoo!	77%	8%	5%
GoogleTalk	74%	9%	3%
<b>Webmail:</b>			
Gmail	89%	10%	1%
Yahoo Mail	89%	3%	2%
Hotmail	88%	3%	1%
<b>VOIP/Video Conferencing:</b>			
Skype	60%	5%	5%
Yahoo voice/Webcam	63%	3%	2%
MSN voice/Video	58%	3%	3%
<b>Peer-to-peer File Sharing:</b>			
BitTorrent	84%	3%	1%
Limewire	85%	4%	1%
eMule	82%	3%	1%
<b>Business Applications:</b>			
Salesforce.com	11%	9%	0%
WebEx	50%	55%	30%
Google Desktop Search	63%	37%	18%
<b>Video:</b>			
YouTube	90%	9%	4%
Hulu	81%	9%	2%
Sling	73%	7%	1%
Average	75%	10%	5%

Q3. Please list up to five Internet applications that you know are <b>used most frequently</b> by employees within your company? 1 = the most frequently used.	Employee Use	Forced Rank
WebEx	55%	1
Google Desktop Search	37%	2
MySpace	21%	3
Facebook	23%	4
Gmail	10%	5

Q4. Please list up to five Internet applications you know are the <b>greatest</b> security risks to your company? . 1 = the highest risk level.	Average Risk Score	Forced Rank
Limewire	1.67	1
YouTube	1.73	2
Gmail	1.92	3
Hotmail	1.96	4
MySpace	2.15	5
Facebook	2.21	6
Skype	2.30	7
Google Desktop Search	2.35	8
AIM	2.38	9
Google Talk	2.45	10

Q5. What are the security risks associated with the use of Internet applications by employees in the workplace?	Total%
Increases infection of malware and viruses	75%
Reduces employee productivity	61%
Disclosure of confidential or sensitive information	48%
Increases external threats to networks	39%
Loss of confidential or sensitive information	34%
Other	12%
Total	269%

Q6. How do you know if employees are using Internet applications that are not permitted in the workplace? Select up to three choices.	Total%
I really don't know if employees are using these applications	48%
Network surveillance	46%
Informal observations	43%
Device scanning	28%
Periodic monitoring and auditing	21%
Discovered while system is exchanged, repaired or refurbished	19%
Security reporting systems	11%
Employee reported misuse	8%
Other	7%
Total	231%

Q7. Please rank the following security controls or procedures in terms of their ability to reduce the use of disallowed Internet applications in the workplace? 1 = most important security control or procedure and 7 = least important security control or procedure.	Average Rank	Forced Rank
Training and education of employees	1.65	1
Limited use of portable devices	2.36	2
Enhanced perimeter controls such as firewalls	3.00	3
Network surveillance	3.60	4
Access controls	3.86	5
Device scanning	3.89	6
Policy	5.95	7
Average	3.47	

Q8. How pervasive is the use of Internet applications by your company's employees?	Pct%
More than 75% of all employees with computer access	12%
Between 50 to 75% of all employees with computer access	15%
Between 25 to 50% of all employees with computer access	34%
Between 10 to 25% of all employees with computer access	26%
Between 5 to 10% of all employees with computer access	10%
Less than 5% of all employees with computer access	3%
Total	100%

Q9a. Does your company have a policy that restricts or forbids the use of Internet applications by employees in the workplace?	Pct%
Yes	78%
No	22%
Total	100%

Q9b. If yes, do you take steps to raise awareness or educate employees about security risks associate with the use of these applications by employees in the workplace?	Pct%
Yes	47%
No	53%
Total	100%

Q9c. If yes, do you believe your security procedures are adequate to reduce any risks associated with the use these Internet applications by employees in the workplace?	Pct%
Yes	58%
No	42%
Total	100%

Q10b. If yes, do any of these Internet applications increase your job performance or productivity in the workplace?	Pct%
Yes	29%
No	48%
Unsure	23%
Total	100%

Q10c. If yes, how do they make you more productive?	Total%
Communicating with contacts and colleagues	57%
Accessing important information	51%
Working remotely	33%
Managing complex schedules	32%
Sharing tools and templates for documents and presentations	11%
Other	5%
Total	189%

Q11a. Do any of these applications involve the sharing of company confidential information such as customer names, location of business meetings, business confidential documents and so forth?	Pct%
Yes	79%
No	10%
Unsure	11%
Total	100%

Q11b. If yes, do you know where this confidential information is stored?	Pct%
Yes	19%
No	40%
Unsure	41%
Total	100%

Q12. Do you know how this confidential information is protected or secured?	Pct%
Yes	17%
No	60%
Unsure	23%
Total	100%

Q13. What assurance do you have that the Internet applications you use can be <u>trusted</u> to protect your information (including company information provided by you)?	Total%
Approved by the company's IT security policy	49%
No assurances	34%
Others in my organization use it successfully or without incident, so it must be okay	16%
Asked colleagues who use the application about safety and security features	14%
Obtained product information from the Internet before using it	7%
Read privacy policy	4%
Read terms and conditions in end user licensing agreement	4%
Other	0%
Total	128%

## Organizational Characteristics & Demographics, IT Security

What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	2%
Director	25%
Manager	42%
Associate/Staff	30%
Other	1%
Total	100%

Check the <b>Primary Person</b> you or your supervisor reports to within your organization. (too many security titles here)	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	6%
Chief Information Officer	54%
Compliance Officer	6%
Chief Privacy Officer	2%
Director of Internal Audit	2%
General Counsel	1%
Chief Technology Officer	10%
Human Resources VP	0%
Chief Security Officer	16%
Chief Risk Officer	1%
Other	2%
Total	100%

Check the country or U.S. region where your company's <b>primary</b> headquarters is located.	Pct%
Northeast	20%
Mid-Atlantic	19%
Midwest	19%
Southeast	12%
Southwest	14%
Pacific	16%
Total	100%

Educational and career background:	Pct%
Compliance (auditing, accountant, legal)	10%
IT (systems, software, computer science)	68%
Security (law enforcement, military, intelligence)	11%
Other non-technical field	10%
Other technical field	1%
Total	100%

Experience	Mean
Total years of business experience	10.24
Total years in IT or data security	8.96
Total years in current position	4.01

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount? (Not appropriate here)	Pct%
Less than 10 people	3%
Between 10 to 50 people	8%
Between 50 to 100 people	8%
Between 100 to 500 people	11%
Between 500 to 1,000 people	12%
Between 1,000 to 2,000 people	25%
Over 2,000 people	23%
Unknown	10%
Total	100%

What industry best describes your organization's industry concentration or focus?	Pct%
Airlines	2%
Automotive	1%
Agriculture	0%
Brokerage	1%
Cable	2%
Chemicals	2%
Credit Cards	3%
Defense	5%
Education	6%
Entertainment	2%
Services	1%
Health Care	6%
Hospitality & Leisure	8%
Manufacturing	6%
Insurance	3%
Internet & ISPs	0%
Government	10%
Pharmaceutical	2%
Professional Services	6%
Research	3%
Retail	7%
Banking	9%
Energy	2%
Telecommunications	4%
Technology & Software	5%
Transportation	1%
Wireless	1%
Total	100%

What best describes your role in managing privacy and data protection risks within your organization? Check all that apply. (Not appropriate here)	Pct%
Setting priorities	54%
Managing budgets	49%
Selecting vendors and contractors	39%
Determining privacy and data protection strategy	39%
Evaluating program performance	43%
Total	224%

What is the worldwide headcount of your organization?	Pct%
Less than 500 people	3%
500 to 1,000 people	6%
1,001 to 5,000 people	19%
5,001 to 25,000 people	36%
25,001 to 75,000 people	24%
More than 75,000 people	11%
Total	100%