

Sponsored by:

**TIV**ERSA™

Independently Conducted by



**Presents**

# **The Ignored Crisis in Data Security: P2P File Sharing**

**Published by Ponemon Institute LLC**

**April 21, 2008**

# The Ignored Crisis in Data Security: P2P File Sharing

Executive Summary by Larry Ponemon, April 21, 2008

## I. What is the crisis?

What if you knew that sensitive and confidential documents about your organization were publicly available on the Internet? What if you knew that trusted employees, vendors, partners and even customers were leaking these documents on the Internet? What would you do if you learned that criminals, the media, competitors and foreign governments were accessing and using your most sensitive documents and profiting from them?

This is precisely what is happening on Peer-to-Peer or P2P file-sharing networks today. Beginning with Napster, which enables users to share music and music, P2P file-sharing networks have grown explosively over the past nine years. Today over 450 million people have access to these networks and make more than 1.5 billion requests for files per day. That is almost 10 times more than what Google processes for the World-wide Web.

Unfortunately, when users put software on their computers to share music and movies, they can easily share their whole hard drive and all its contents. At the same time, P2P's ease of use has lowered the skills needed for criminals to access the contents of these exposed hard drives. No longer is there a need to hack or phish – just issue a search for “credit card,” “audit” or “medical records” and the files of auditors, attorneys, physicians, executives, or home users can be found without the victims' knowledge.

What this means is that every day the leakage of sensitive documents occurs and no commercial or government organization is fully immune despite current IT measures. In one well-publicized case, an employee at a global pharmaceutical company downloaded unauthorized file sharing software on a corporate laptop and caused the disclosure of Social Security numbers and personal data of 17,000 current and former employees. In another incident, a TV reporter used a widely used P2P file sharing program to obtain a confidential document discussing a terrorist threat on Chicago and 34 other cities. The maliciousness of this practice for monetary gain is exemplified by the arrest and conviction of a Seattle man for ID theft and fraud using P2P file sharing networks to obtain his victims' information.

Sponsored by Tiversa, Ponemon Institute conducted this study, *The Ignored Crisis in Data Security: P2P File Sharing*, to better understand the level of awareness among IT security practitioners about the risks posed by P2P file-sharing applications that reside on workplace, remote and home computers. What was learned is that IT security practitioners seem to be only partially aware of or underestimate the risk, despite high profile cases that have illustrated the impact of disclosing even one file. It is also difficult to understand why this crisis goes ignored when 76% of IT security practitioners in our study admit that their organization has had a data breach involving the loss or theft of confidential information over the Internet.

We believe contributing to the crisis are the following six trends occurring in the private and public sector:

- ✓ Virtualization of the workforce. Employees, contractors and other third parties are now able to work virtually anywhere. As a result, confidential documents are often downloaded on computers with P2P file-sharing applications in homes and third-party offices. This has resulted in the leakage of confidential documents.
- ✓ Outsourcing of projects and data to third parties. Most large organizations have thousands of vendors with access to sensitive documents and would not be aware of the third parties use of P2P file-sharing applications.
- ✓ Failure to monitor the extended enterprise to guard against disclosure of information on P2P file-sharing networks. The tendency is for IT practitioners to believe that all risk is contained

within their “four walls” and the use of firewalls is what is needed to protect sensitive data from P2P file-sharing networks.

- ✓ Evolving technologies that can make security tools ineffective in protecting data – especially as fraudsters, hackers, and ID thieves have become more sophisticated and focused on financial gain.
- ✓ Younger employees and contractors increasing use of portable technologies and file-sharing applications for music and games. These technologies can unleash sensitive data over P2P networks. P2P file-sharing networks are large, not part of the web and operate differently. Further, P2P has millions of users and is larger in activity than many well-known web brands.
- ✓ A growing generation gap among IT practitioners. An older generation of IT practitioners lacks real-world experience with P2P file-sharing networks. P2P file-sharing networks are confused with the web and are dismissed as unimportant or near extinction and, therefore, the risk is not worth addressing.

In this study, Ponemon Institute surveyed 767 IT security practitioners with an average of more than eight years experience in the information technology (IT) or IT security fields. A description of respondents is provided in Section IV of this report. According to 63% of these respondents, their organizations forbid the use of P2P file-sharing networks in the workplace. However, organizations don’t seem to be communicating the risk posed by P2P file sharing effectively through the enterprise. More than 26% are uncertain about whether or not their organization has a policy concerning the prohibition of P2P file-sharing networks.

The survey asked questions about the following issues:

- Do IT security practitioners truly understand P2P file-sharing applications?
- Do IT security practitioners understand the inherent risk of P2P file sharing in their organizations and throughout their extended enterprise?
- What would be the negative impact if certain sensitive information in the workplace was leaked and shared on the Internet (via P2P)?
- What is the likelihood that sensitive information could be leaked and then disclosed on the internet (via P2P)?
- How do organizations monitor the disclosure of confidential or sensitive documents and data that may be inadvertently shared in the P2P environment? How does this compare to other modes of information disclosure?

## II. Key findings

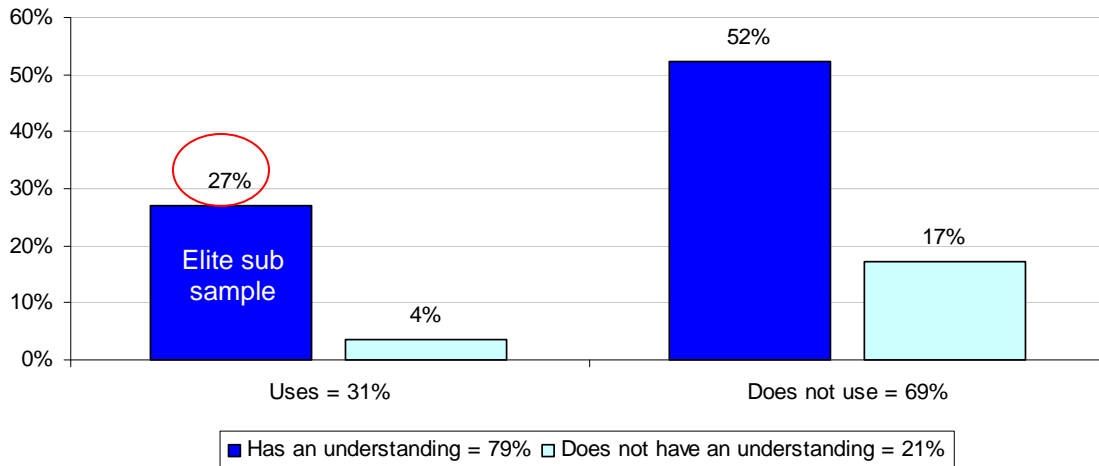
**Only 31% of IT practitioners say they are users of P2P applications, but 79% state that they understand how P2P file-sharing applications work.**

As noted in Bar Chart 1, 27% (207 respondents) say they understand and use P2P file-sharing applications. Fifty-five percent of respondents understand but do not use P2P applications. Seventeen percent do not use P2P and do not understand how they work. Only 4% uses P2P file-sharing applications without understanding how they work.

For purposes of this study, respondents who both understand and use P2P are referred to as our Elite subsample. We believe this group is most likely to recognize the inherent information risks

associated with the use of P2P networks on computers containing the organization's confidential information.<sup>1</sup>

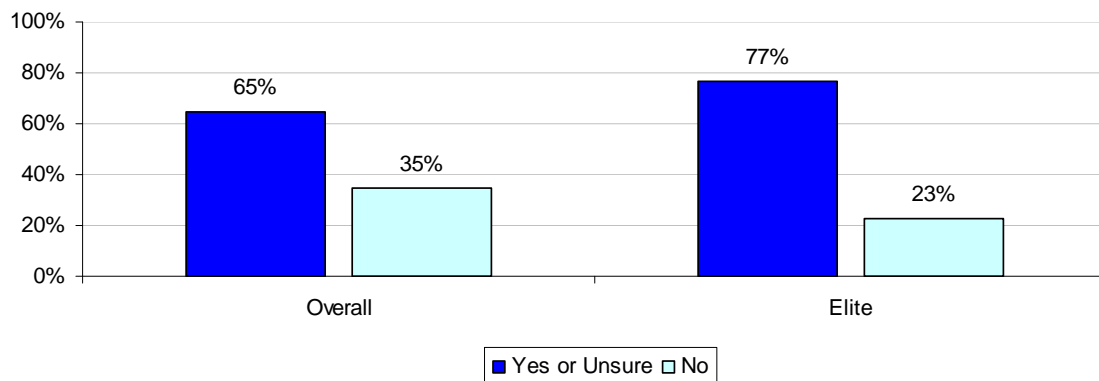
Bar Chart 1  
What is your level of understanding of P2P file sharing applications?



**Sixty-five percent of all respondents and 77% of Elite respondents respond Yes or Unsure to the question that asks whether P2P file-sharing networks can result in the inadvertent leakage of confidential information.**

Bar Chart 2 shows less than 35% of IT security practitioners and 23% of Elite respondents do not believe P2P file-sharing networks can cause inadvertent transfers and disclosures of documents that reside on company computers and laptops.

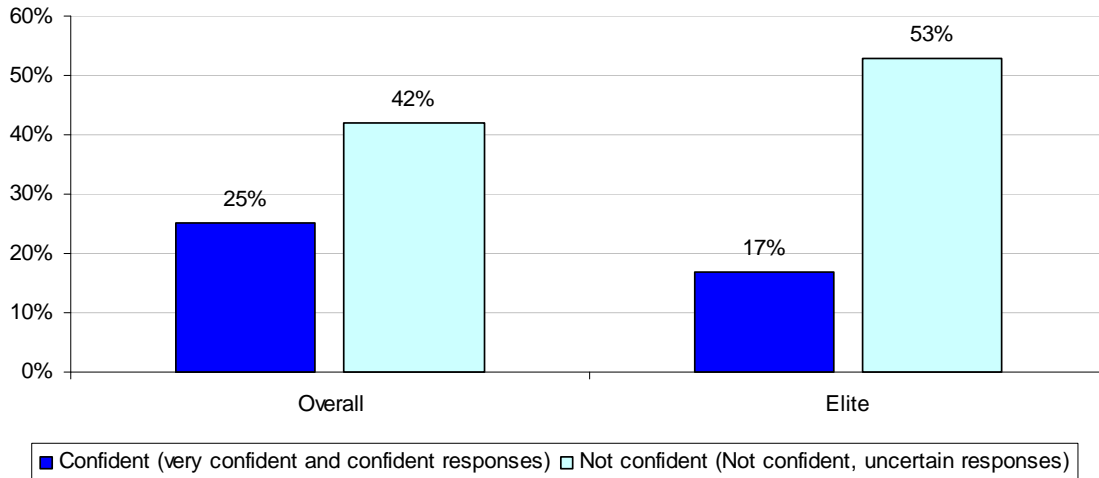
Bar Chart 2  
Do you believe that P2P file sharing networks can result in the inadvertent transfer and disclosure of documents that reside on company computers and laptops?



<sup>1</sup> The use of P2P file sharing may suggest an age gap between younger and older participants. We did not collect age demographics for respondents; however, it is our belief that older IT practitioners tend not to be as familiar with the various ways these applications work. The best way to understand P2P file-sharing applications is to use them because they typically are not well documented, consist of 250 different client applications, and often have non-publicized features that create significant security risks.

As shown in Bar Chart 3, only 25% of all respondents and 17% of Elite respondents are confident that their organizations' IT security systems and controls will prevent P2P file-sharing networks from inadvertently transferring and disclosing documents residing on company computers and laptops.

Bar Chart 3  
How confident are you that your organization's information security will prevent P2P file sharing networks from leaking confidential documents that reside on company computers?

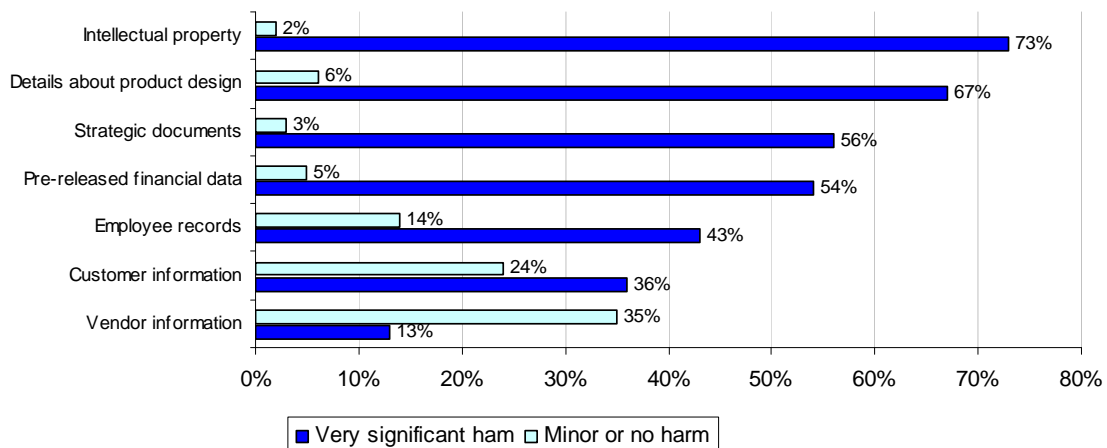


Taken together, Bar Charts 2 and 3, suggest IT practitioners acknowledge the threat and control gaps that may prevent their organization from properly detecting and preventing the leakage of sensitive or confidential because of P2P file-sharing applications. Elite users cite greater acknowledgement of these gaps.

**IT security practitioners worry most about the loss of intellectual property and are less concerned about the leakage of customer information.**

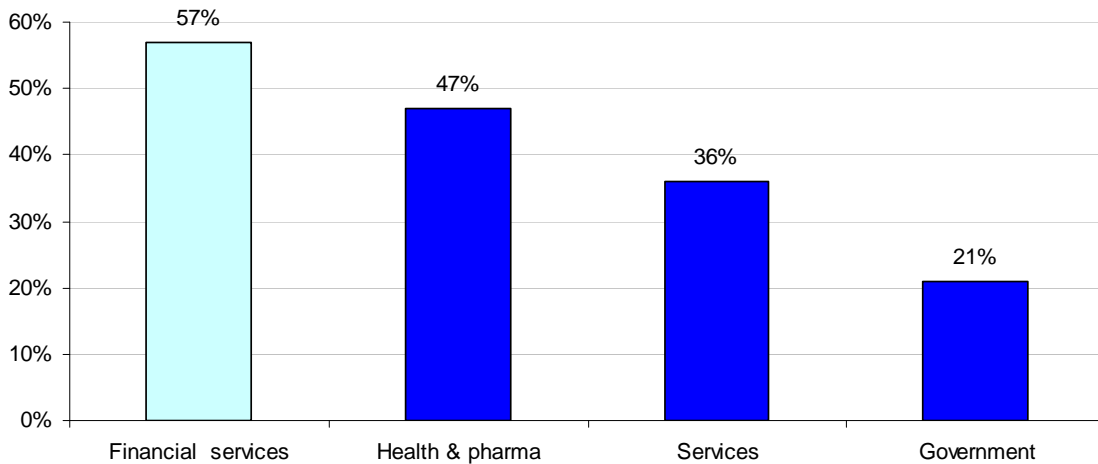
As shown in Bar Chart 4a, respondents believe the inadvertent disclosure of intellectual property (73%) and product design documents (67%) would bring about the greatest harm to their organization. Other data categories that would be extremely harmful if lost or stolen include: strategic documents such as information about mergers and acquisitions (56%), pre-released financial information and forecasts (54%) and employee records (43%).

Bar Chart 4a  
What data types would cause the greatest harm if disclosed?



Thirty-six percent of respondents believe disclosure of customer information as a result of P2P file sharing would have a very significant negative impact on their organization. This is an interesting finding given that the disclosure of unprotected customer or consumer information often requires notification of individuals in compliance with state data breach laws and is often most likely to cause significant brand damage. Bar Chart 4b reports differences by industry sector for customer/consumer information being inadvertently disclosed through P2P file sharing. Fifty-seven percent of respondents in the financial services industry see the loss of customer information as having a very negative impact on their organizations. In contrast, only 21% of respondents in government see it as being extremely harmful to the organization.

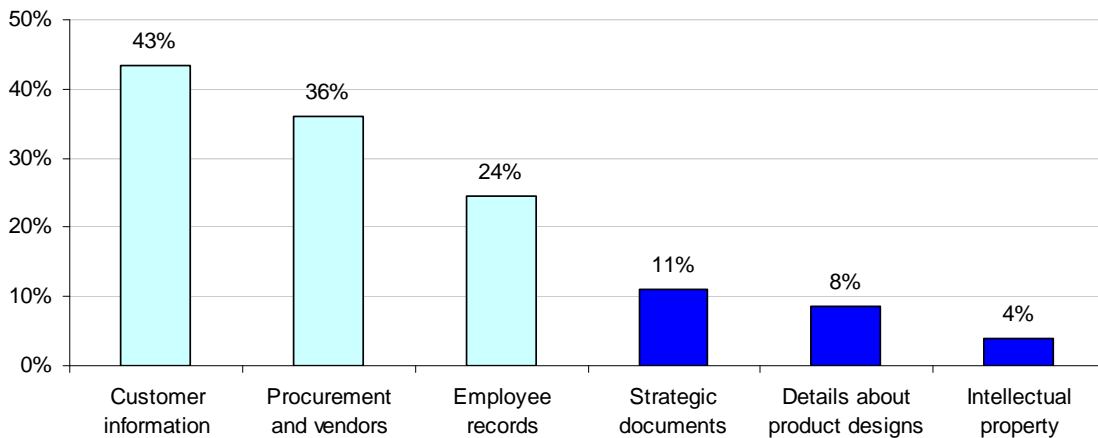
Bar Chart 4b  
Belief that the loss of customer/consumer information would cause a very significant negative impact for financial services, health care, services and government sectors



**IT security practitioners understand the risk that leakage of these information categories could pose to the organization, but believe it is highly unlikely to occur.**

According to Bar Chart 5, less than 4% of respondents believe intellectual property could be leaked through P2P file-sharing networks, 8% believe product design details could be revealed and 11% think strategic documents could be leaked.

Bar Chart 5  
Percentage of respondents who believe information could be leaked as a result of P2P file sharing for six data categories

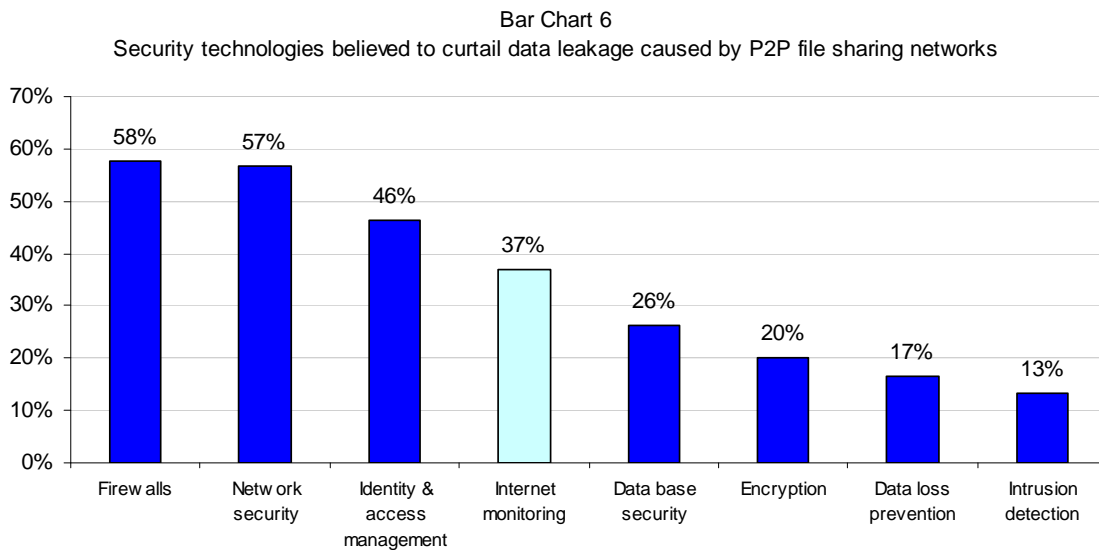


More than 43% of respondents believe customer information and 36% believe vendor information is at risk for inadvertent leakage as a result of P2P file-sharing applications.

**IT security practitioners fail to fully understand the risks posed by extra-perimeter P2P sourced data leaks and the inherent nature of P2P file-sharing applications to subvert many perimeter control technologies.**

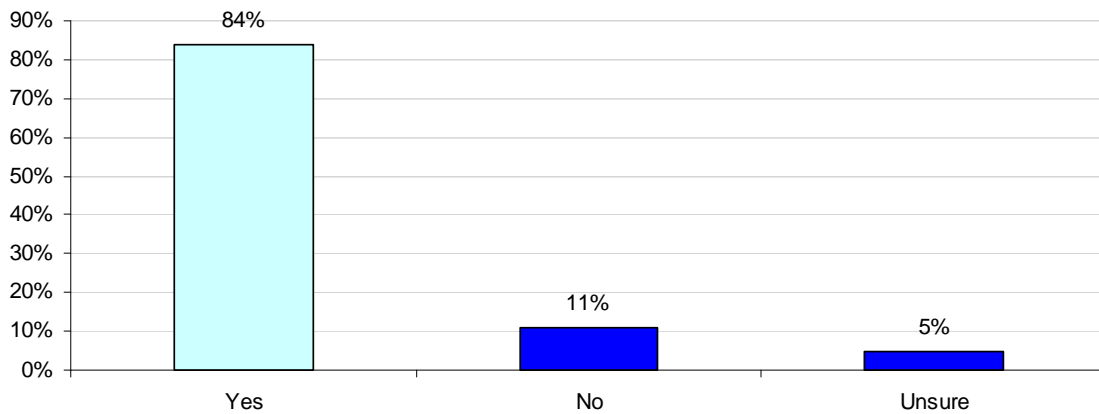
As noted in Bar Chart 6, IT security practitioners choose firewalls (58%), network security (57%) and identity & access management (46%) as the most important tools for curtailing data leakage through P2P file-sharing networks. Tools that are less important include Internet monitoring (37%), data base security (26%), encryption (20%), data loss prevention (17%) and intrusion detection (13%).

The fact that respondents choose perimeter, network and access controls as the primary tools to combat data loss in the P2P file-sharing network is an indication that they do not comprehend this problem. Empirical data shows that between 40%-60% of P2P sourced leaks originate from suppliers, contractors, or partners of organizations outside their firewalls. In addition, P2P file-sharing applications have built in methods to defeat firewalls and extrude networks, not intrude.



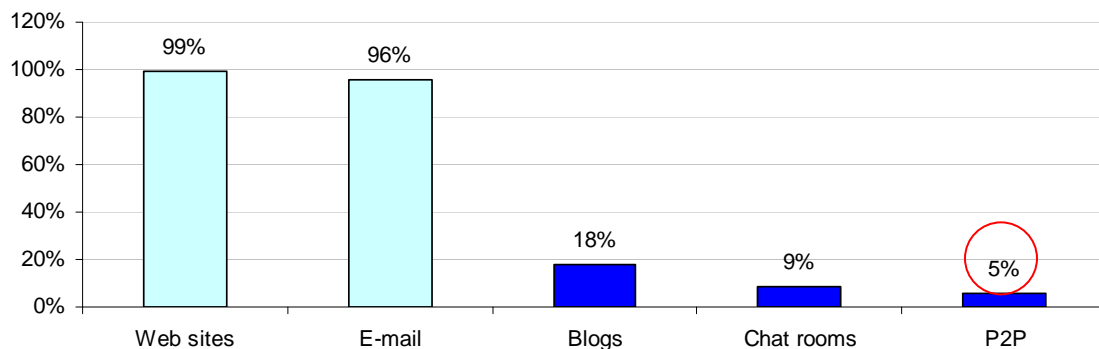
As shown in Bar Chart 7a, 84% of respondents report that they monitor the Internet for the disclosure of confidential or sensitive documents and data.

Bar Chart 7a  
Do you monitor the Internet for disclosure of confidential documents?



According to Bar Chart 7b, only 5% of respondents say they monitor P2P file-sharing networks. The top two areas for Internet monitoring are employees' use of web sites (99%) and e-mail (96%).<sup>2</sup> Despite recognizing that P2P file-sharing networks pose a significant risk to their information, few IT practitioners monitor P2P file-sharing networks.

Bar Chart 7b  
Which areas of the Internet do you monitor?

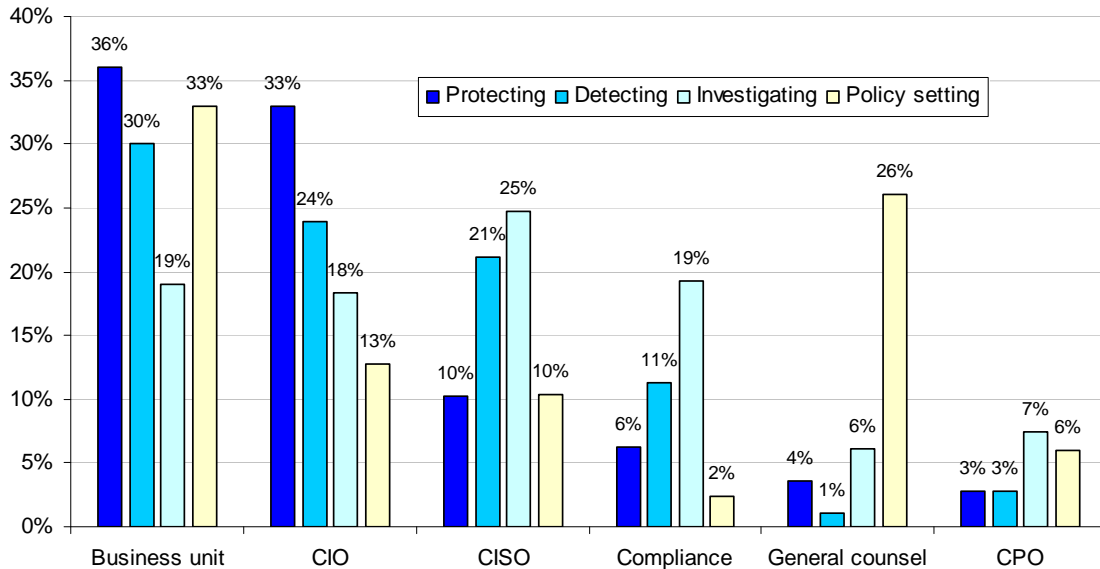


**Business units are believed to be most responsible for the governance of sensitive information.**

As shown in Bar Chart 8, 36% of respondents believe that business unit management is the responsible party for protecting sensitive data and 30% believe the same group is accountable for detecting data leakage. However, the responsibility for investigating data loss or theft is assigned to the CISO (25%) followed by the business unit management (19%) and the compliance/audit staff (also 19%).

<sup>2</sup> It is our belief that IT practitioners often associate Internet with Web and confuse Web and P2P file sharing as one control activity. Web and P2P operate on the Internet, but P2P operates separately from Web.

Bar Chart 8  
Who is most responsible for the governance of sensitive information?

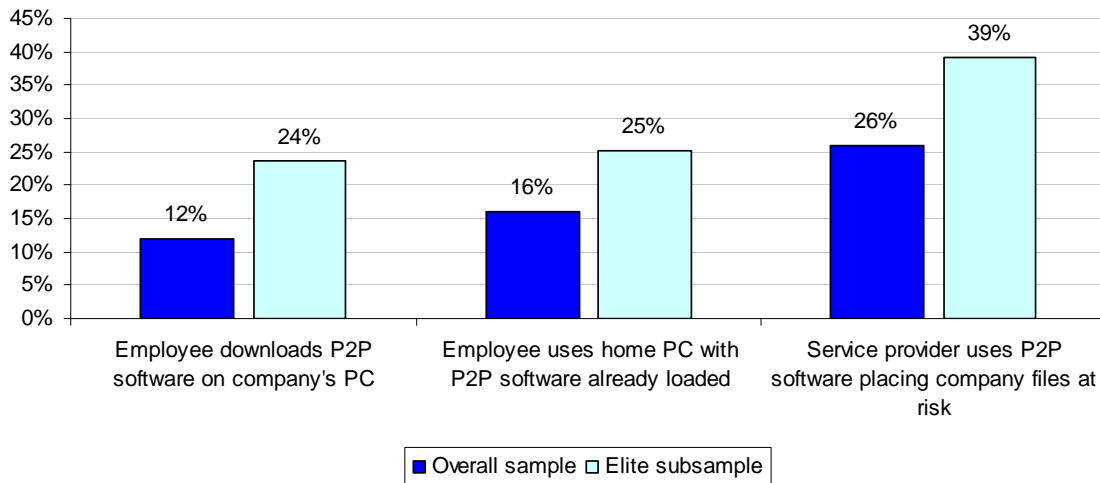


Respondents believe business units are the most responsible for data protection policies. Only 13% of respondents believe that the CIO is responsible for setting policy to protect data and 10% believe it is the CISO. According to 33%, the business unit manager sets policy followed by legal. In general, Bar Chart 8 suggests there is no one person or group in-charge of data governance. It also shows that chief privacy officers are not fully engaged in data governance activities.

**Trusted service providers can increase the risk of data leakage from P2P filing sharing.**

Bar Chart 9 clearly shows differences between the overall sample and respondents in the Elite subsample. Accordingly, Elite respondents are more likely to rate each one of the three scenarios as likely or very likely to occur.

Bar Chart 9  
Belief that scenario is likely or very likely to occur



According to 26% of all respondents (and 39% of Elite respondents) a contractor, consultant, auditor, attorney or other trusted service provider are very likely or likely to use a file-sharing

program during the next 24 months. Elite respondents also seem to be more aware of the human risk factors that can result in the disclosure of information via P2P file-sharing networks.

According to 16% of respondents (and 25% of Elite respondents), it is very likely or likely that employees will use e-mail or a USB storage device to bring their work home and download it on a home computer that has a file-sharing program for sharing music and movies. Only 12% of respondents (and 24% of Elite respondents) believes it would be very likely or likely that an employee would download a software program on a company-assigned computer that would enable the sharing of files residing on the computer to others on the Internet sometime during the next 24 months.

### III. 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 list is representative of individuals who are information technology practitioners. 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 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.

### IV. Sample

A random sampling frame of 13,032 adult-aged individuals who reside within the United States was used to recruit participants to this web survey. Our randomly selected sampling frame was selected from two national mailing lists of IT security professionals. In total, 865 respondents completed their survey results within an eight-day holdout period. Of returned instruments, 98 survey forms were rejected because of reliability issues. A total of 767 surveys were used as our final sample. This sample represents a 5.9% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is  $\leq 5\%$ .

Over 91% of respondents completed all survey items within 10 minutes. Following are key demographics and organizational characteristics for U.S. respondents.

Table 1a describes the reporting chain for survey respondents, with 41% reporting through their organization's security or IT security leader. About 40% are located within the CIO organization. Table 1b provides their self-reported organizational levels. As can be seen, the majority of respondents are at the manager (35 %) or technician (34 %) levels, respectively. As such, these individuals represent primarily IT personnel and those responsible for information security and represent individuals on the "front-line" doing the day-to-day work.

Table 1a. Where do you report in the organization?	Pct%
To the CFO	6%
To the CTO	2%
To the CIO	40%
To the CSO/CISO	41%
To the CPO	2%
Compliance leader	6%
Other	4%
Total	100%

Table 1b: Organizational levels	Pct %
C-Level Senior Executive	2%
Vice President	2%
Director	19%
Manager	35%
Technician or staff	34%
Consultant	6%
Other	3%
Total	100%

On average, respondents have more than eight years of experience in the information management or security fields and over four years of experience in their current position. In total, 65% of respondents were males and 35% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields in North America.

Pie Chart 1 reports the percentage age distribution of respondents by their organization’s primary industry classification. As shown, 21% of respondents are employed by financial service companies including insurance, banking, credit cards, brokerage and investment management and 19% work for federal or local government. Another 13% work in the services sector, including research and professional services.

Pie Chart 1: Industry Distribution of the Panel

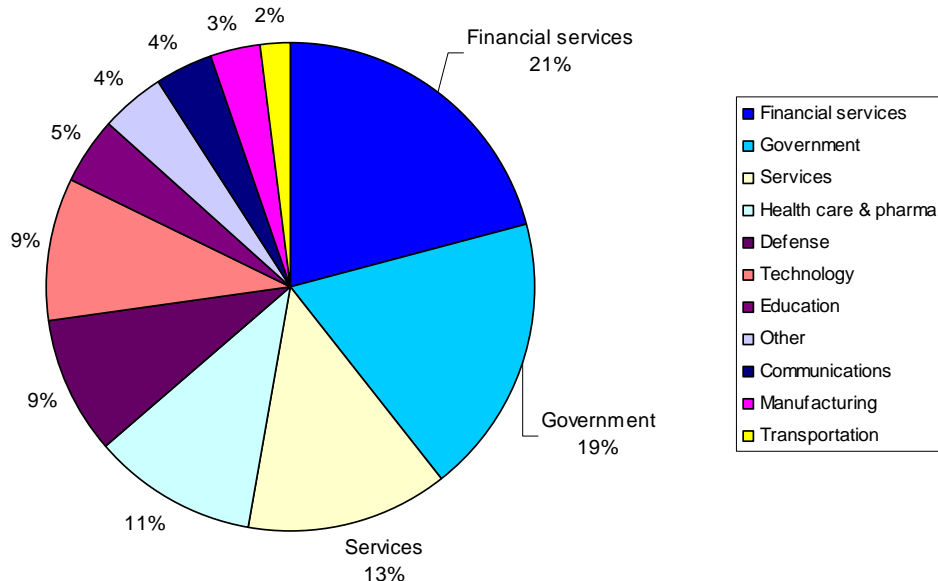


Table 2a reports the organization’s economic structure, showing that the majority of respondents’ companies (52%) work for organizations that are publicly traded on a major exchange such as NYSE or NASDAQ.

Table 2b provides the approximate headcounts of these organizations. As can be seen, 60% of respondents are employed by larger-sized organizations with more than 5,000 employees.

Table 2a. Economic structure	Pct%
Major exchange (NYSE, NASDAQ)	52%
Minor exchange	15%
Not publicly traded	33%
Total	100%

Table 2b. Corporate headcount	Pct%.
Less than 500 people	13%
500 to 1,000 people	12%
1,001 to 5,000 people	15%
5,001 to 25,000 people	21%
25,001 to 75,000 people	26%
More than 75,000 people	13%
Total	100%

## V. Implications for organizations

Following are the most salient implications suggested by this research:

- There appears to be a lack of understanding about the significant risk to confidential data in the extended enterprise resulting from P2P file-sharing networks. We find this surprising given the fact that 76% of respondents report that their organizations have had a data breach involving the loss or theft of confidential information over the Internet.
- There is a perception gap between IT security practitioners who actually use P2P networks (Elites) and those who claim to understand P2P, but don't use it. The Elites are more aware of the risk of data loss or theft associated with the expanded enterprise (and especially involving contractors and other outsourced partnerships).
- A vast majority of respondents monitor the web for data leakage, but only 5% monitor P2P networks. This indicates a lack of awareness about the reality that the leakage of confidential data such as intellectual property is occurring over P2P networks and a potential confusion over that fact that P2P file-sharing networks, the web and the internet are not the same networks.
- Respondents are uncertain about who sets policy governing the use of P2P networks and many are not sure if policies actually exist. Sixty-three percent report that their organizations forbid P2P file sharing. However, 26% don't know if a policy prohibiting this practice exists in their organizations. As a result, many employees and contractors are not being made aware of the risks inherent in P2P file-sharing applications and that their use is prohibited. There is also confusion about who sets policy. Thirty-three percent of respondents report it is the business unit's responsibility, 26% say it is the general counsel followed by the CIO at 13%.
- IT practitioners are looking at the wrong set of tools to solve the data leak problem caused by P2P file-sharing networks
- Trusted service providers and employees' (or their families) working from home are more likely to use P2P networks and are putting the organizations they work with at risk.
- IT practitioners are not as concerned about the leakage of customer/consumer data despite the data breach notification laws. However, this finding appears to be related to industry, wherein respondents in the financial services industry and healthcare are most concerned about the loss of customer or consumer data.

While there is recognition among IT security practitioners that the disclosure of certain confidential information on the Internet could have devastating consequences for organizations, only 37% report the use of Internet monitoring tools and only 5% for P2P. Further, while they believe the risk of having sensitive documents disclosed over the Internet through P2P file-

sharing applications is minimal, most concur that existing controls could not reduce or mitigate the risk.

It is not clear who has responsibility for establishing policies and practices to protect confidential information and detect the misuse of data. The greatest percentage of respondents believes it is the business unit followed by those who believe it is the CIO.

With respect to holding the business unit accountable for the protection of sensitive data, IT security practitioners may think responsibility should rest with those who oversee and manage projects that use sensitive data. Another possible reason why business units should be held accountable is because they often hire the vendors who then have access to sensitive data. In any event, there seems to be the lack of a strong governance process which could explain why IT security practitioners in our study do not believe that controls are in place to stop the leakage of sensitive information.

In order to address this crisis, organizations should first understand the risks created by P2P file-sharing networks. While many in our study report that they understand how P2P file-sharing applications work, they need to actually use them to realize the risks inherent in their proliferation across the Internet. IT security professionals need to work closely with their business users to explain the threats to confidential data. The goal would be to have organizations make better outsourcing decisions and to have appropriate policies and processes in place to protect confidential data in the extended enterprise. Finally, organizations should monitor P2P file-sharing networks at a level equivalent to other Internet risks.

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: Percentage Frequencies for all Survey Items

Following are the audited results of a survey completed in February 2008 involving a United States sample of 767 corporate IT and information security practitioners. The following results are presented in a percentage frequency format.

The sample response rate is 5.9%, which is determined as follows:

Sampling plan	Totals
Total sample frame	13032
Total bounce backs	1197
Total response	865
Rejected surveys	98
Final sample	767
	Response rate
	5.9%

The survey results are summarized in the following tables:

### Screening questions

S1. Has your organization experienced a data breach involving the loss or theft of confidential information over the internet?	Pct%
Yes	76%
No	11%
Uncertain	13%
Total	100%

S2. What is your level of familiarity with privacy and data protection regulations?	Pct%
Very familiar	37%
Somewhat familiar	51%
Not familiar	12%
Total	100%

### Survey questions

Q1. What would be the negative impact (if any) to your organization if sensitive information were leaked and shared on the Internet? Please rate the following data categories using this five-point scale: 1 - very significant impact, 2 - significant impact, 3 - some impact, 4 - minor impact, 5 - no impact.	1	2	3	4	5	Total%
Minutes of executive or board meetings	35%	32%	21%	9%	3%	100%
Details about new product designs	67%	25%	2%	5%	1%	100%
Employee records including salaries and benefits	43%	19%	24%	7%	7%	100%
Management accounting reports and budgets	38%	26%	15%	16%	5%	100%
Legal and/or audit documents	39%	21%	15%	15%	10%	100%
HR and employee correspondence	23%	14%	37%	20%	6%	100%
Customer information (could include personally identifiable information)	36%	19%	21%	20%	4%	100%

Strategic documents (including information about mergers and acquisitions)	56%	19%	22%	2%	1%	100%
Procurement and vendor lists	13%	12%	40%	26%	9%	100%
Pre-released financial information and forecasts	54%	20%	21%	5%	0%	100%
Intellectual property, formulae, source code, trade secrets, etc	73%	10%	15%	2%	0%	100%
Average	43%	20%	21%	12%	4%	100%

Q2. What is the likelihood that sensitive information could be leaked and then disclosed on the Internet? Please rate the following 10 data categories using the five-point scale below each item: 1 - a leak will occur, 2 - a leak is likely to occur, 3 - a leak is somewhat likely to occur, 4 - a leak is not likely to occur, and 5 - uncertain that a leak will occur	1	2	3	4	5	Total%
Minutes of executive or board meetings	3%	3%	7%	67%	19%	100%
Details about new product designs	8%	13%	21%	33%	24%	100%
Employee records including salaries and benefits	24%	13%	17%	32%	13%	100%
Management accounting reports and budgets	4%	8%	26%	33%	30%	100%
Legal and/or audit documents	12%	15%	13%	28%	32%	100%
HR and employee correspondence	13%	19%	20%	23%	25%	100%
Customer information (could include personally identifiable information)	43%	26%	24%	3%	5%	100%
Strategic documents (including information about mergers and acquisitions)	11%	11%	16%	42%	20%	100%
Procurement and vendor lists	36%	22%	4%	15%	24%	100%
Pre-released financial information and forecasts	1%	1%	4%	84%	10%	100%
Intellectual property, formulae, source code, etc	4%	9%	7%	71%	9%	100%
Average	15%	13%	14%	39%	19%	100%

Q3a. Who in your organization is responsible for <b>protecting and securing</b> sensitive data? Please select the function that is <b>most</b> responsible for protecting this kind of data.	Pct%
CIO/Information Technology	33%
CISO/Information security	10%
CPO/Privacy office	3%
Compliance/audit	6%
General Counsel/Legal	4%
Human resources	2%
Business unit management	36%
Do not know	5%
Other (please specify)	1%
Total	100%

Q3b. Who in your organization is responsible for <b>detecting</b> misuse of data? Please select the function that is <b>most</b> responsible for protecting this kind of data.	Pct%
CIO/Information Technology	24%
CISO/Information security	21%
CPO/Privacy office	3%
Compliance/audit	11%
General Counsel/Legal	1%
Human resources	0%
Business unit management	30%
Do not know	7%
Other	2%
Total	100%

Q3c. Who in your organization is responsible for <b>investigating</b> the misuse of data? Please select the function that is <b>most</b> responsible for protecting this kind of data.	Pct%
CIO/Information Technology	18%
CISO/Information security	25%
CPO/Privacy office	7%
Compliance/audit	19%
General Counsel/Legal	6%
Human resources	1%
Business unit management	19%
Do not know	3%
Other	1%
Total	100%

Q3d. Who in your organization is responsible for <b>setting policy</b> for protection of data? Please select the function that is <b>most</b> responsible for protecting this kind of data.	Pct%
CEO	3%
Board of Directors	1%
CIO/Information Technology	13%
CISO/Information security	10%
CPO/Privacy officer	6%
Compliance/audit director	2%
General Counsel/Legal	26%
Human resources	1%
Business unit management	33%
Do not know	2%
Other	2%
Total	100%

Q4. What is your level of understanding of P2P file-sharing applications? Please choose the one response that best describes your level of understanding or familiarity.	Pct%
I am a user of P2P file-sharing applications, and <b>I understand</b> how P2P file sharing works	27%
While I do not use P2P file-sharing applications, <b>I understand</b> how P2P file sharing works	52%
While I am a user of P2P file-sharing, <b>I do not understand</b> how P2P file sharing works	4%
I am not a user of P2P file-sharing applications and <b>I do not understand</b> how P2P file-sharing works	17%
Total	100%

Q5. Does your organization have a policy that forbids P2P file-sharing networks from company computers and laptops?	Pct%
Yes	63%
No	11%
Unsure	26%
Total	100%

Q6. Do you believe that P2P file-sharing networks can result in the inadvertent transfer and disclosure of documents that reside on company computers and laptops?	Pct%
Yes	34%
No	35%
Unsure	31%
Total	100%

Q7. How confident are you that your organization's information security systems and controls prevent P2P file-sharing networks from inadvertently transferring and disclosing documents that reside on company computers and laptops?	Pct%
Very confident	9%
Confident	16%
Somewhat confident	33%
Not confident	27%
Uncertain	15%
Total	100%

<b>Q8. An employee of your organization downloads a software program onto her company-assigned computer. The software enables the sharing of files residing on the computer to others on the Internet. The employee possesses highly confidential and sensitive data.</b>	
Q8a. What would be the impact on the organization's information security efforts if this scenario occurred?	Pct%
Very significant impact	30%
Significant impact	25%
Some impact	18%
Minor impact	20%
No impact	7%
Total	100%

Q8b. What is the likelihood this scenario could occur within your organization during the next 24 months at least once?	Pct%
Very likely to occur	3%
Likely to occur	9%
Somewhat likely to occur	37%
Not likely to occur	41%
Uncertain	11%
Total	100%

Q8c. What regulations do you believe will be violated if this scenario occurred in your organization? Please check all that apply:	Total%
Breach notification state statutes	62%
Sarbanes-Oxley	52%
Payment Card Industry (PCI) requirements	5%
Gramm-Leach-Bliley Act	5%
FTC Safeguards Rule	4%
Health Insurance Portability & Accountability Act	1%
Federal Privacy Act	3%
Don't know	31%
Total	164%

<b>Q9. An employee of your organization uses a file-sharing software program on his home computer for sharing music and movies. Using email or a USB storage device he brings job-related information home to work on his personal computer. The file-sharing software enables others on the Internet to share files residing on his computer.</b>	
Q9a. What would be the impact on the organization's information security efforts if this scenario occurred?	Pct%
Very significant impact	29%
Significant impact	27%
Some impact	19%
Minor impact	17%
No impact	8%
Total	100%

Q9b. What is the likelihood this scenario could occur within your organization during the next 24 months at least once?	Pct%
Very likely to occur	5%
Likely to occur	11%
Somewhat likely to occur	35%
Not likely to occur	29%
Uncertain	20%
Total	100%

Q9c. What regulations do you believe will be violated if this scenario occurred in your organization? Please check all that apply:	Total%
Breach notification state statutes	66%
Sarbanes-Oxley	59%
Payment Card Industry (PCI) requirements	0%
Gramm-Leach-Bliley Act	5%
FTC Safeguards Rule	1%
Health Insurance Portability & Accountability Act	1%
Federal Privacy Act	3%
Don't know	39%
Total	174%

<b>Q10. A trusted service provider to your organization (i.e. a contractor, consultant, auditor or attorney) uses a file-sharing software program on her computer. This software enables the sharing of files residing on the computer to others on the Internet.</b>	
Q10a. What would be the impact on the organization's information security efforts if this scenario occurred?	Pct%
Very significant impact	33%
Significant impact	30%
Some impact	15%
Minor impact	11%
No impact	11%
Total	100%

Q10b. What is the likelihood this scenario could occur within your organization during the next 24 months at least once?	Pct%
Very likely to occur	7%
Likely to occur	19%
Somewhat likely to occur	23%
Not likely to occur	21%
Uncertain	30%
Total	100%

Q10c. What regulations do you believe will be violated if this scenario occurred in your organization? Please check all that apply:	Total%
Breach notification state statutes	67%
Sarbanes-Oxley	53%
Payment Card Industry (PCI) requirements	0%
Gramm-Leach-Bliley Act	6%
FTC Safeguards Rule	0%
Health Insurance Portability & Accountability Act	0%
Federal Privacy Act	3%
Don't know	46%
Total	175%

Q11. Please check the security technologies or tools that you believe reduce or mitigate the threat of inadvertent P2P file sharing of sensitive or confidential information? Check all that apply.	Total%
Firewalls	58%
Intrusion prevention and detection	13%
Data loss prevention (DLP)	17%
Encryption	20%
Network security (including VPN)	57%
Data base security tools (including scanners)	26%
Identity and access management	46%
Internet monitoring	37%
Other (please specify)	13%
Total	287%

Q11a. As part of your organization's information security or privacy program, do you monitor the Internet for the disclosure of confidential or sensitive documents and data?	Pct%
Yes	84%
No	11%
Unsure	5%
Total	100%

Q11b. If yes, which areas of the Internet do you monitor?	Total%
Blogs	18%
Web sites	99%
Chat rooms	9%
E-mail	96%
P2P	5%
Other (Please specify)	3%
Total	229%