

# 2009 Security Mega Trends Survey

---

**Sponsored by**

**Lumension**

Independently conducted by Ponemon Institute LLC

Publication Date: November 2008

## 2009 Security Mega Trends Survey Executive Summary

By Dr. Larry Ponemon

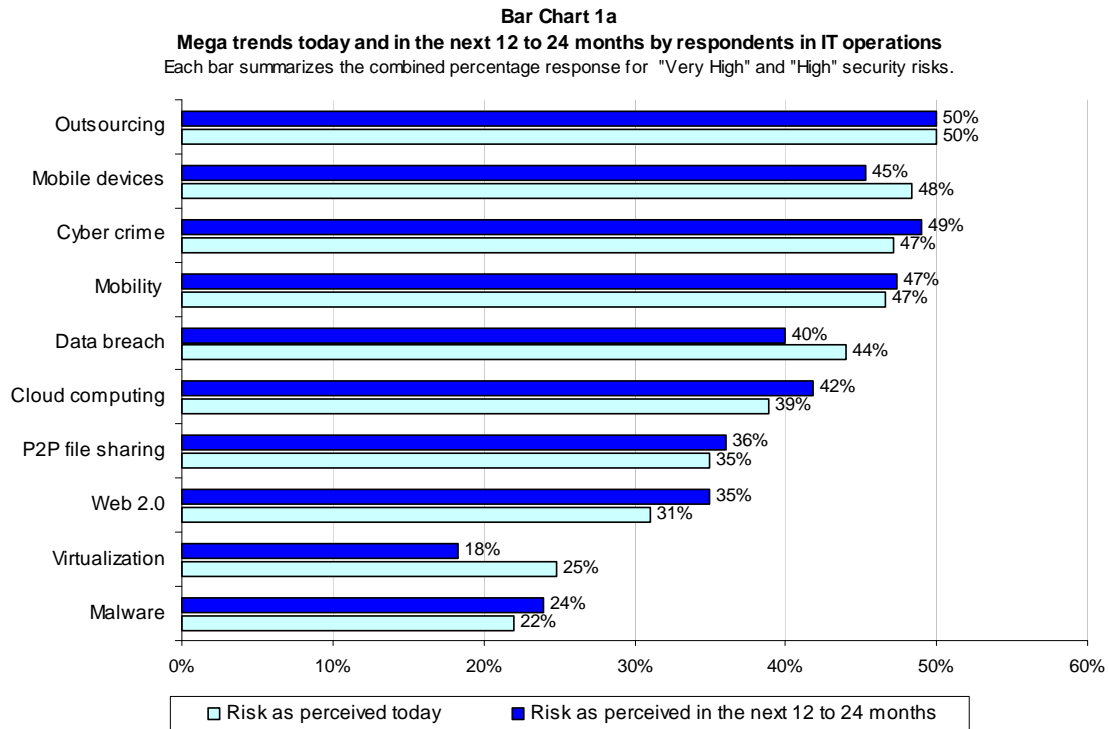
What will be the biggest threats to an organization's sensitive and confidential data over the next 12 to 24 months? According to 825 respondents in IT operations, it is outsourcing of sensitive information to third parties, the external threat of organized cyber criminal syndicates and a mobile workforce armed with portable data-bearing devices. In contrast, 577 respondents in IT security worry most about stopping data breaches, access to cloud computing and outsourcing of sensitive data assets to third parties.

*The 2008 Security Mega Trends Survey* was conducted by Ponemon Institute and sponsored by Lumension to better understand if certain publicized IT risks to personal and confidential data are, or should be, more or less of a concern for organizations. We asked respondents in IT operations and IT security to consider how eight Security Mega Trends affect organizations today and during the next 12 to 24 months.

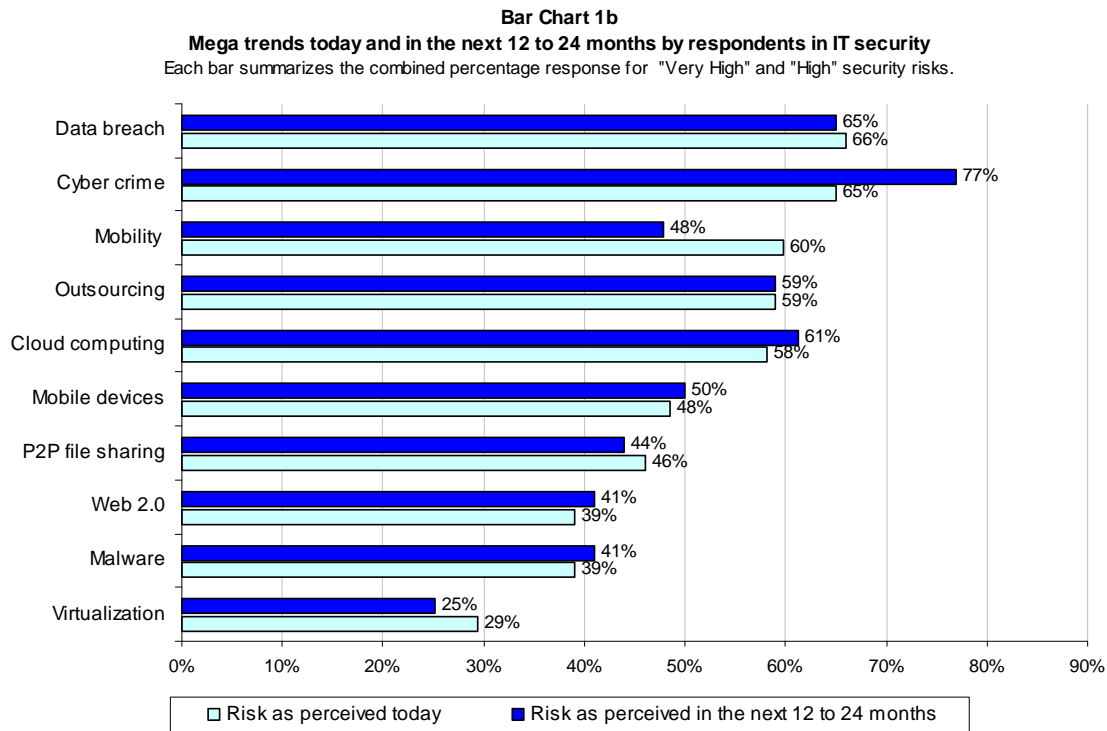
We believe the results of the study will be helpful to organizations struggling to understand how they should allocate resources to help ensure their information assets are safeguarded.

Based on interviews with IT experts in operations and information security, we selected the following eight Mega Trends for this study: cloud computing, virtualization, mobility and mobile devices, cyber crime, outsourcing to third parties, data breaches and the risk of identity theft, peer-to-peer file sharing and Web 2.0

Bar Chart 1a lists the security risks identified by respondents in IT operations as perceived today and over the next 12 to 24 months.



Bar Chart 1b lists the security risks identified by the IT security practitioners as perceived today and over the next 12 to 24 months.



We asked respondents in IT operations and IT security to respond to questions about the following topics:

- What security threats do they worry most about today? Do respondents have different perceptions about these threats?
- Are these security threats decreasing or increasing in severity over time?
- What are the most significant risks associated with each of these threats?
- How many organizations have experienced a cyber criminal attack?
- How confident are IT operations and IT security professionals that they can prevent the loss or theft of sensitive data?

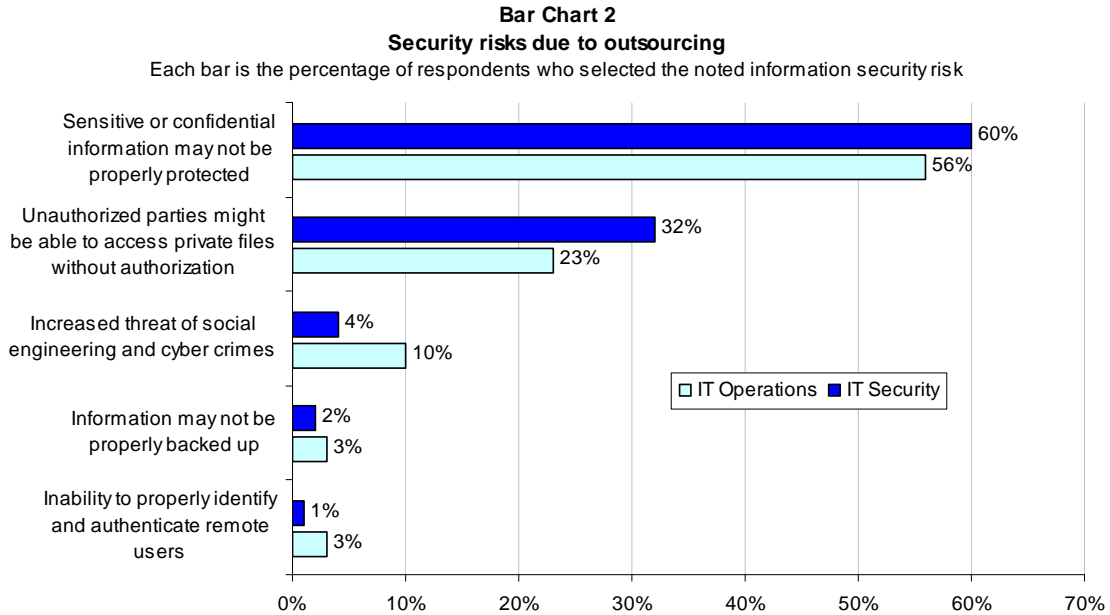
Following are the most salient findings of this survey research. Please note that most of the results are displayed in a bar or line chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as Appendix I to this paper.

**The most serious security threats in the next 12 to 24 months, according to respondents in IT operations**

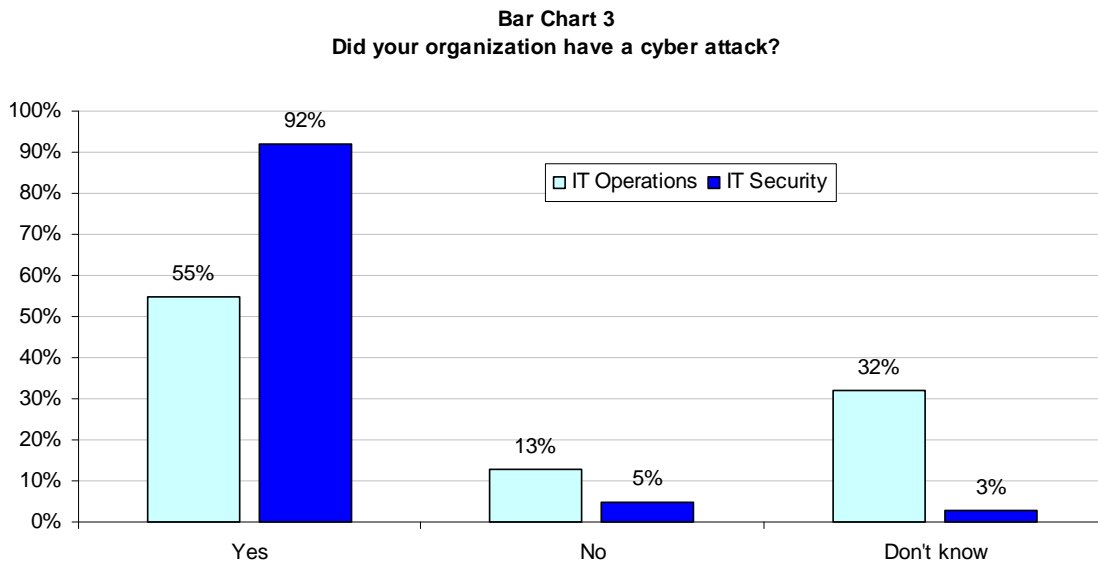
The largest percentage of IT operations professionals participating in our study (50%) believes that outsourcing will be a very high or high risk to organizations. Possibly contributing to the concern about outsourcing is that only 12% of respondents believe that their organizations will decrease the outsourcing of sensitive and confidential information to third parties.

Organizations outsource sensitive and confidential customer and employee data to vendors and other third parties to reduce processing costs and improve operating efficiencies. These purposes

can include (but are not limited to): marketing and sales campaigns, software application development, call center operations, and mortgage and other credit application processing. According to Bar Chart 2, the primary risks associated with outsourcing concern an organization's inability to properly protect sensitive or confidential information followed by unauthorized parties who might be able to access private files without authorization.



The next greatest threat for respondents in IT operations is increasingly sophisticated attacks from cyber criminals. More than half (55%) report that their organization has had a cyber crime attack and almost a third (32%) are uncertain. However, as shown in Bar Chart 3, 92% of IT security practitioners report their organization had a cyber criminal attack.

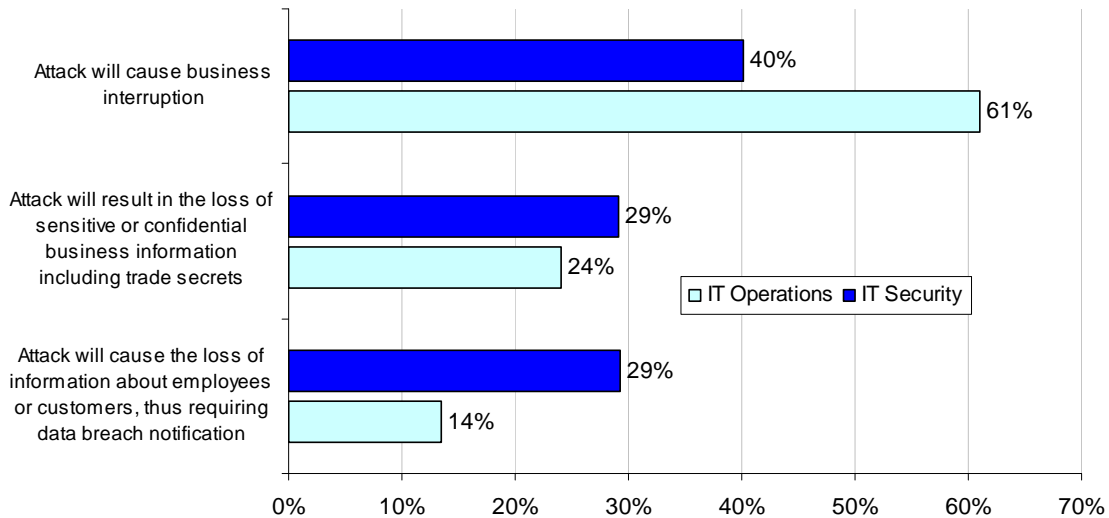


For purposes of this study, cyber crime usually describes criminal activity in which the computer or network is an essential part of the illegal criminal activity. This term also is used to include traditional crimes in which computers or networks are used to enable the illicit activity. As shown in Bar Chart 4, 40% of respondents in IT operations fear that an external attack will cause

business interruptions and could result in the loss of sensitive or confidential business information, including trade secrets. They also worry about such an attack resulting in the loss of employee or customer information that would require data breach notifications.

**Bar Chart 4**  
**Security risks due to cyber crime**

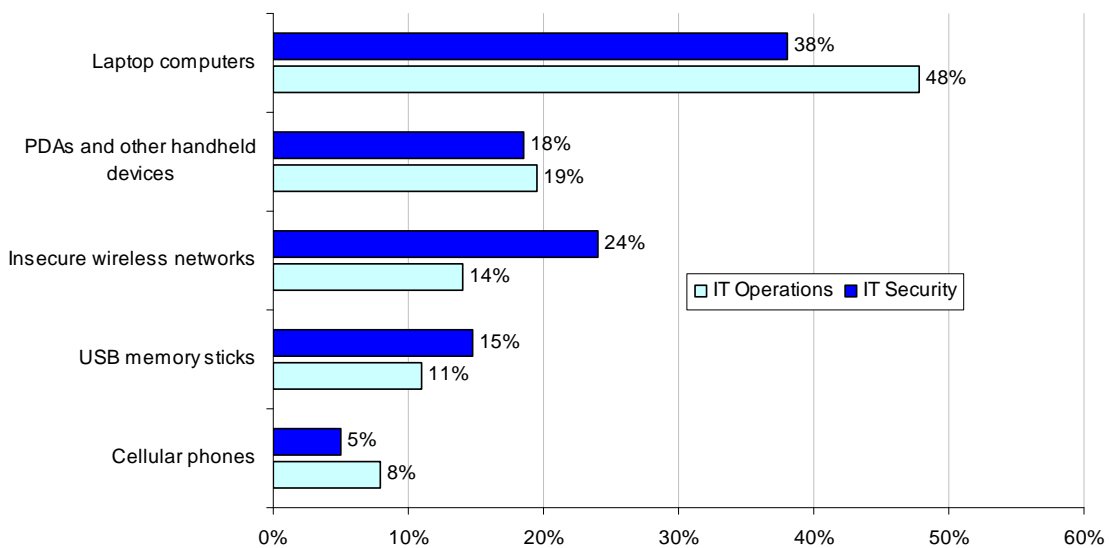
Each bar is the percentage of respondents who selected the noted information security risk



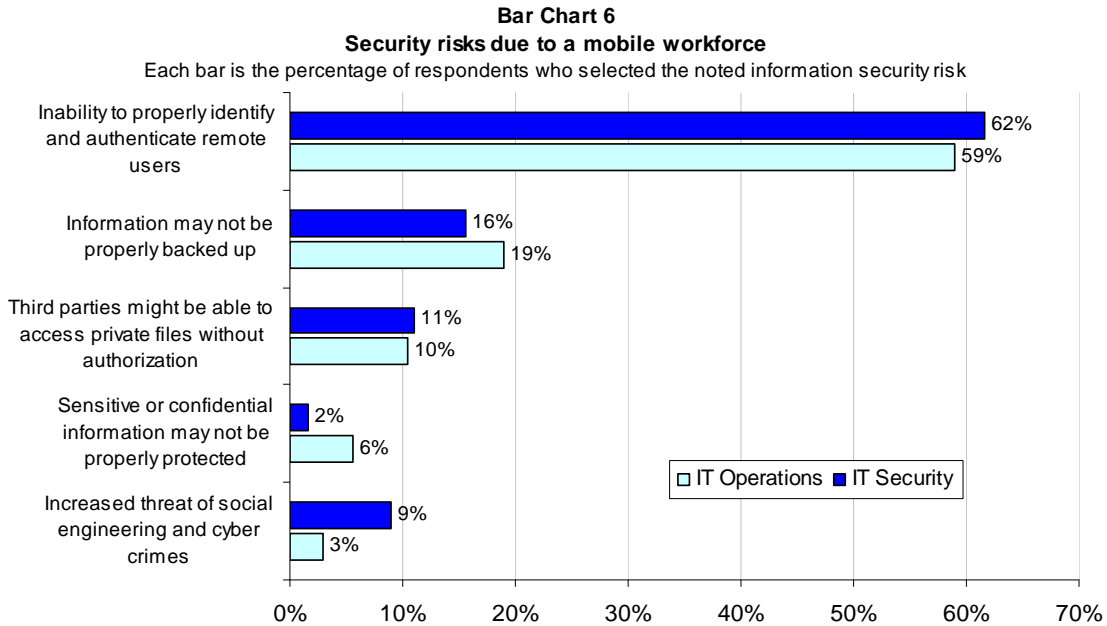
The third greatest threat, according to IT operations is the growth of a mobile workforce and the use of portable data-bearing devices. According to 34% of respondents, more than half of their workforce in their organizations is mobile. Organizations have become increasingly dependent upon a mobile workforce with access to information no matter where they work or travel. Typically, employees or contractors can use the following mobile devices when they travel or work at home: laptops, VPN, PDAs, cell phones and memory sticks. Bar Chart 5 compares IT operations and IT security professionals' perceptions about which mobile devices are most risky.

**Bar Chart 5**  
**Most risky mobile devices**

Each bar is the percentage of respondents who selected the device as their highest risk

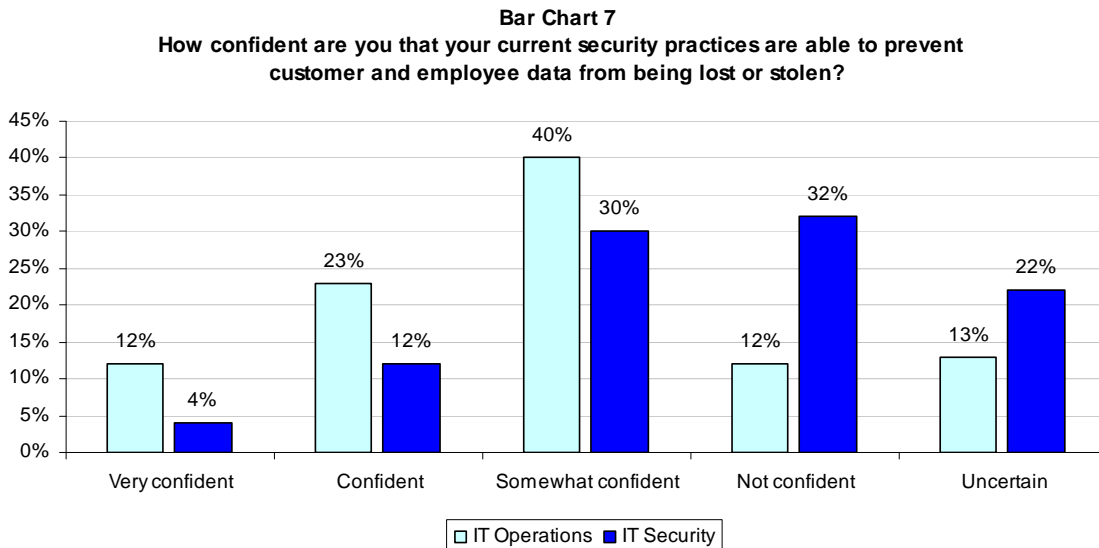


As shown in Bar Chart 6, the most significant security threat associated with a mobile workforce is the inability to properly identify and authenticate multiple systems followed by the concern that third parties might be able to access private files without authorization. Only 1% of respondents are worried about information being properly backed up. With respect to security risks posed by mobile devices, the number one concern is the inability to properly identify and authenticate remote users and that the sensitive or confidential information may not be properly protected or backed up.

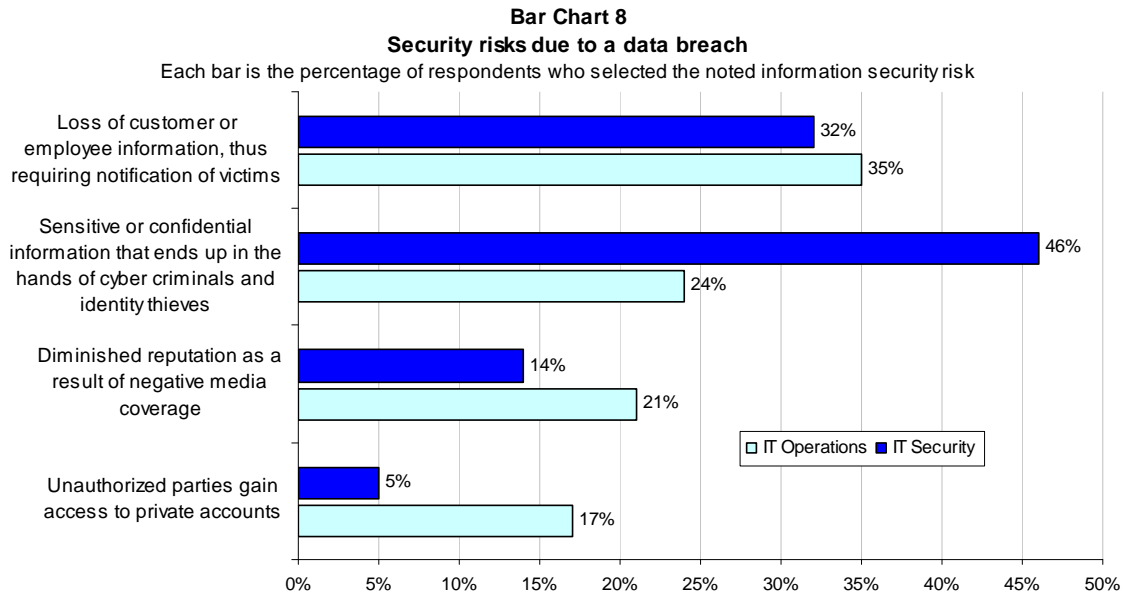


**The most serious security threats in the next 12 to 24 months, according to IT security professionals**

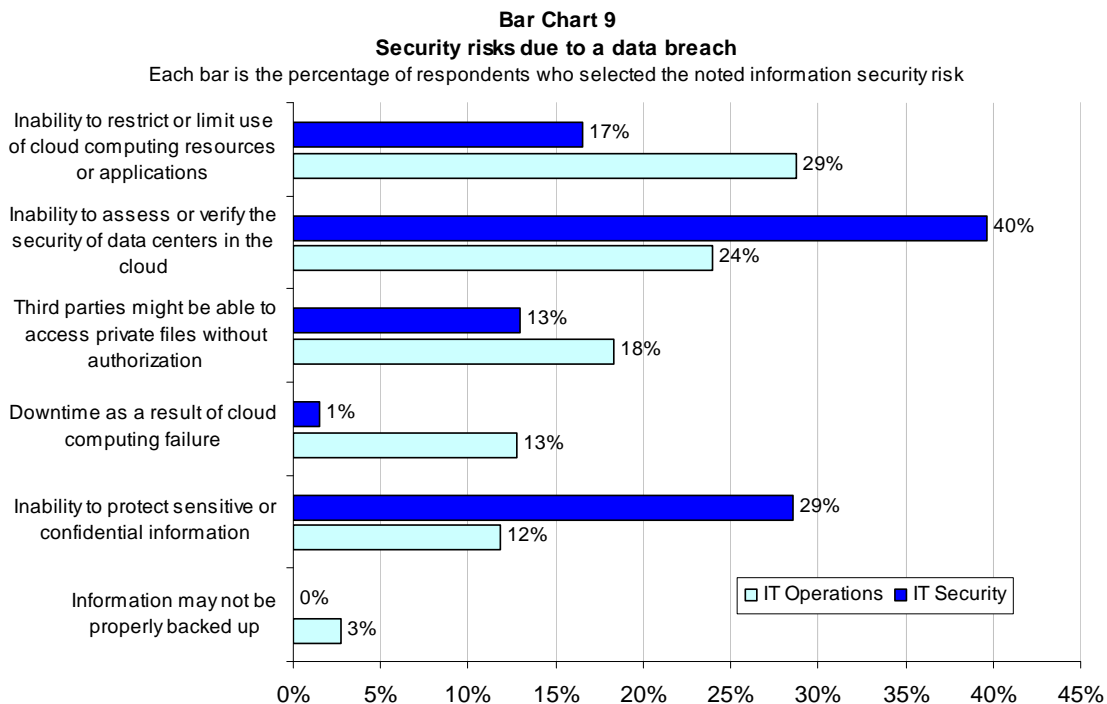
Eighty-three percent of IT security professionals surveyed report their organization experienced a data breach because customer or employee information was lost or stolen. A slightly smaller percentage (79%) of respondents in IT operations report their organization had a data breach.



As shown in Bar Chart 7, only 16% of IT security professionals are very confident or confident that current security practices are able to prevent customer and employee data from being lost or stolen. In contrast, 35% of respondents in IT operations are very confident or confident that they can prevent the loss of customer or employee data. Therefore, it is understandable why the majority of respondents in IT security believe data breaches pose a high and very high security threat to their organizations. Bar Chart 8 shows security risks due to the threat of data breach. Their primary fear is that sensitive or confidential information will end up in the hands of cyber criminals and identity thieves and that the loss of data will impact their company's reputation.



The next security threat that poses a high or very high risk to organizations according to 61% of IT security respondents is cloud computing.

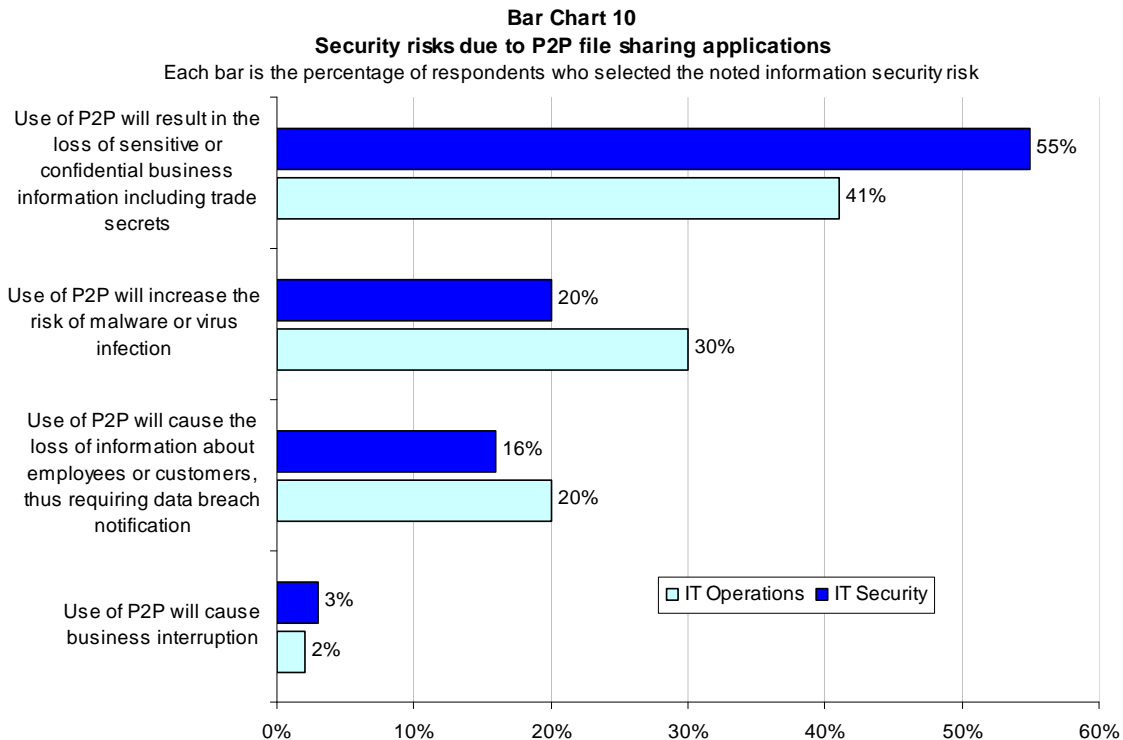


Cloud computing refers to distributed computing solutions owned by third-parties on data center locations outside the end-user company's IT infrastructure. Consumers of cloud computing services purchase capacity on-demand and are not concerned with the underlying technologies used to increase computing capacity. As shown in Bar Chart 9, the main concern for IT security professionals is the inability to assess or verify the security of data centers in the cloud and the inability to protect sensitive information.

The third most significant threat is outsourcing. More than half (59%) of IT security professionals agree with IT operations that outsourcing is a serious risk to an organization's information assets. They also concur that it is the difficulty in protecting sensitive or confidential information and the possibility that unauthorized parties might be able to access private files without authorization. Similar to IT operations, only 12% see outsourcing of sensitive and confidential information decreasing in their organizations.

**IT security perceives the risks from P2P file sharing, Web 2.0, malware attacks and virtualization higher than respondents in IT operations**

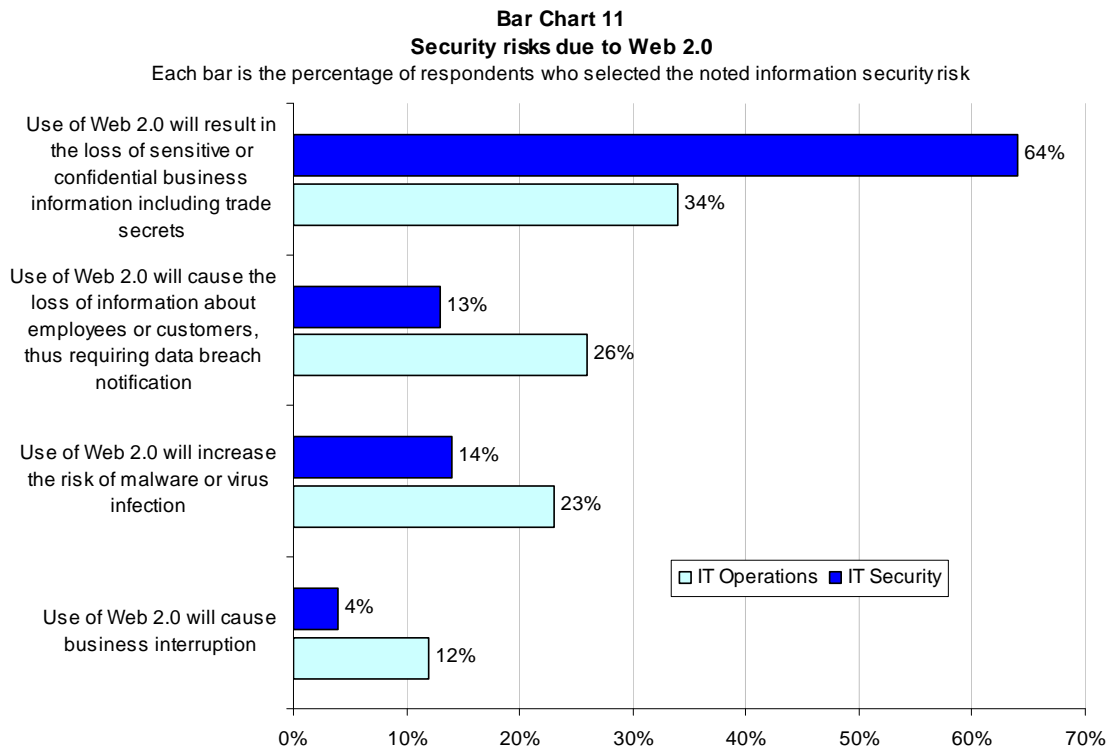
Only 36% of IT operations practitioners believe P2P file sharing poses high or very high security risks. Forty-four percent of IT security practitioners consider P2P a high or very high risk. P2P file sharing networks allow a group of computers to connect with each other and directly access files from one another's hard drives. P2P file sharing networks started with Napster by enabling Internet users to share music files.



P2P file-sharing networks can cause inadvertent transfers and disclosures of documents that reside on an organization's computers and laptops. File sharing networks where inadvertent file sharing typically occurs include networks. For example, a sales representative downloads a peer-to-peer music sharing application onto his company assigned notebook computer. This P2P file sharing network exposes confidential business documents contained on his computer. As shown in Bar Chart10, both agree that the risk associated with P2P is that it could result in the loss of

sensitive or confidential business information including trade secrets followed by the risk of malware or virus infection.

Forty-one percent of respondents in IT security as opposed to 39% in IT operations consider Web 2.0 a high or very high risk. Web 2.0 refers to a plethora of Internet tools that enhance information sharing and collaboration among users. These concepts have led to the evolution of web-based communities and hosted services, such as social networking sites, wikis and blogs. This term does not refer to an update to any technical specifications, but to changes in the ways software developers and end-users use the World Wide Web. As shown in Bar Chart 11, both groups agree that biggest risk is the loss of sensitive or confidential business information including trade secrets, followed by the increase in the risk of malware or virus infection and the loss of information about employees or customers thus requiring data breach notification.



Malware infections create a security risk within an organization, according to 89% of IT operations and 92% of IT security professionals. Both groups see the risk of malware as resulting in the loss of sensitive or confidential business information including trade secrets or the attack will cause the loss of sensitive or confidential information. Only 21% of IT operations and 39% of IT security professionals consider it a high or very high risk with the risk increasing slightly over the next 12 to 24 months, 24% and 41% respectively.

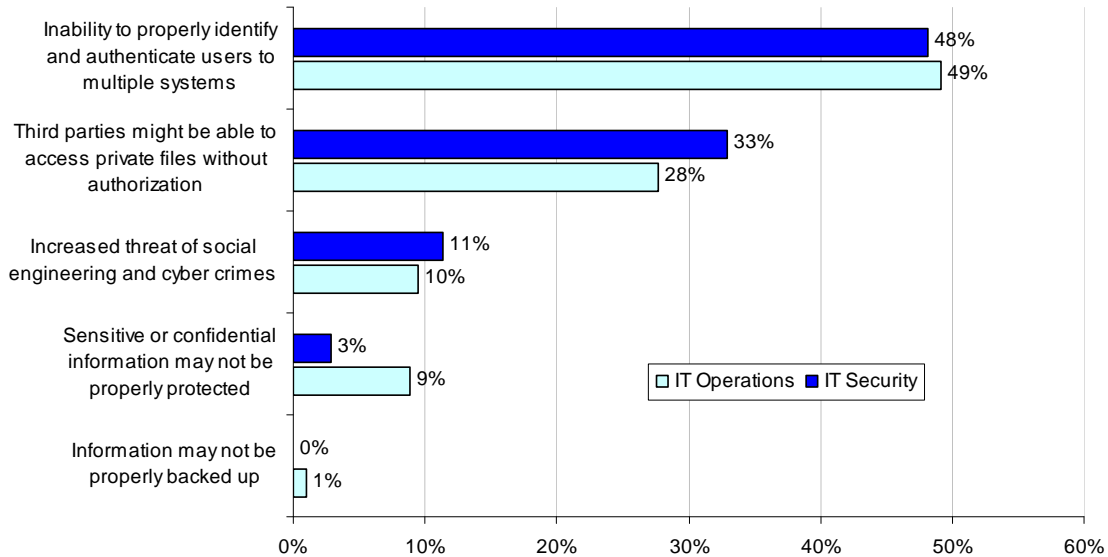
Virtualization is at the bottom of the risk list for both IT operations (18%) and IT security (25%) practitioners. Virtualization technology allows end-users to access multiple secure networks from a single computer, wherein the PC or laptop essentially acts as a hardware authentication token. With one computer, the end-user is able to gain access to separate virtual devices or machines. Virtualization makes server and operating system deployments more flexible and improves the use of storage and systems resources.

As shown in Bar Chart 12, both groups agree that the most significant risk associated with virtualization is the inability to properly identify and authenticate users to multiple systems and third parties access to private files without authorization.

**Bar Chart 12**

**Security risks due to virtualization**

Each bar is the percentage of respondents who selected the noted information security risk



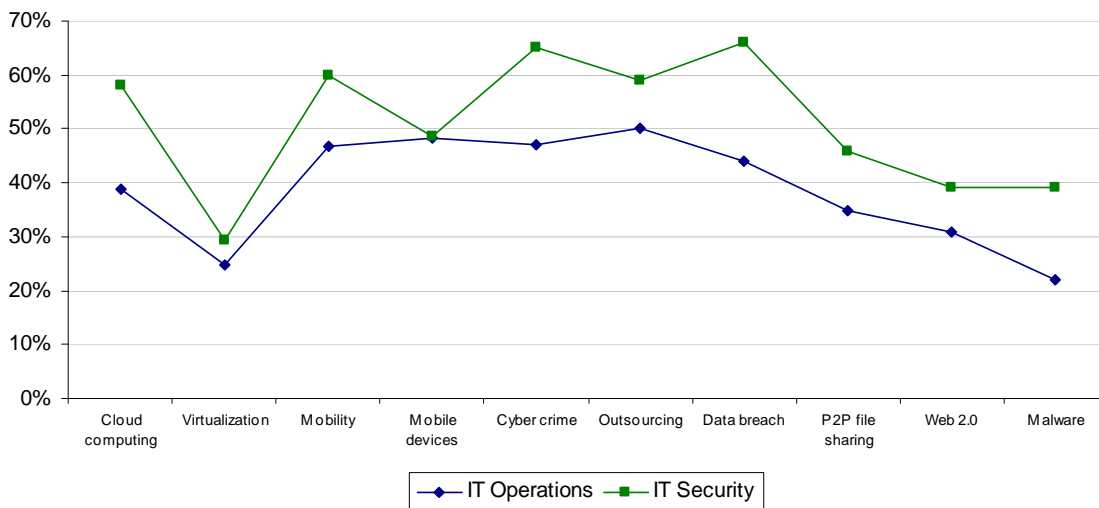
**Information security practitioners consistently perceive threats as higher than their colleagues in IT operations.**

It is interesting to note that respondents in IT security rate each one of the mega trends as posing a higher security risk than respondents in IT operations.. As shown in Line Graph 1a, the biggest gaps in perceptions concern cloud computing, cyber crime, and data breach. In contrast, they are closely aligned with virtualization and mobile devices.

**Line Graph 1a**

**Security mega trends as perceived today for both samples**

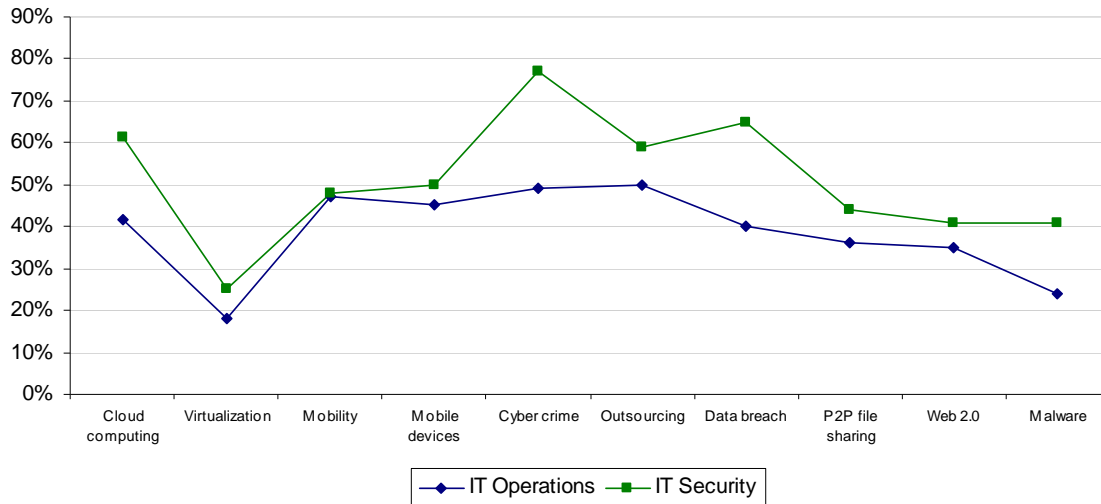
Each point reflects the percentage responses for very high or high security risks at present



Line Graph 1b shows how respondents in IT operations and IT security view security mega trends over the next two years. In general, the same pattern exists, wherein IT security practitioners

consistently rate each threat as a higher security level than respondents in IT operations. Also, the widest gaps concern cloud computing, cyber crime and data breach.

**Line Graph 1b**  
**Security mega trends as perceived 12 to 24 months for both samples**  
 Each point reflects the percentage responses for very high or high security risks at present



### Implications for organizations

Organizations are faced with a plethora of security threats to their confidential and sensitive data assets. We asked IT operations and security practitioners to rank those they believe have a high or very high risk to sensitive and confidential information. Based on the risks associated with each of these threats, we believe organizations should consider the following solutions:

- Create and enforce policies that ensure access to private data files is restricted to authorized parties only.
- Secure corporate endpoints to protect against data leakage and malware.
- Make sure third parties who have access to your sensitive and confidential information take appropriate security precautions.
- Train employees and contractors to understand their responsibility in the protection of data assets.
- Ensure that mobile devices are encrypted and that employees understand the organizations' policies with respect to downloading sensitive information and working remotely.
- Understand precautions that should be taken when traveling with laptops, PDAs and other data bearing devices.

We believe the findings from this study provide organizations with guidance on which threats are more critical than others to address. IT operations and IT security professionals identified outsourcing of sensitive information to third parties, external threat of organized cyber criminal syndicates, a mobile workforce, data breaches and access to cloud computing as the most significant

## 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 in IT operations and IT security, 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 sample is representative of individuals in the IT operations and IT security fields. We also acknowledge that the results may be biased by external events. 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.

## Sample

Two random sampling frames of adult-aged individuals who reside within the United States was used to recruit participants to this web survey.<sup>1</sup> Our randomly selected sampling frames were selected from three national lists of IT, security, compliance and data protection professionals.

Table 1 Sample description	IT Operations	IT Security
Total sampling frame	14518	11506
Bounce-back	3957	2109
Total returns	915	658
Rejected surveys	90	81
Final sample	825	577
Response rate	5.7%	5.0%

Table 1 shows 825 respondents in IT operations and 577 respondents in information security completed the survey within an eight-day research period. Of returned instruments, less than 1% was omitted because of reliability tests. The final samples represent a 5.7% net response rate for IT operations and 5.0% net response rate for IT security. The margin of error on all adjective scale and Yes/No/Unsure responses is  $\leq 3.0$  percent.

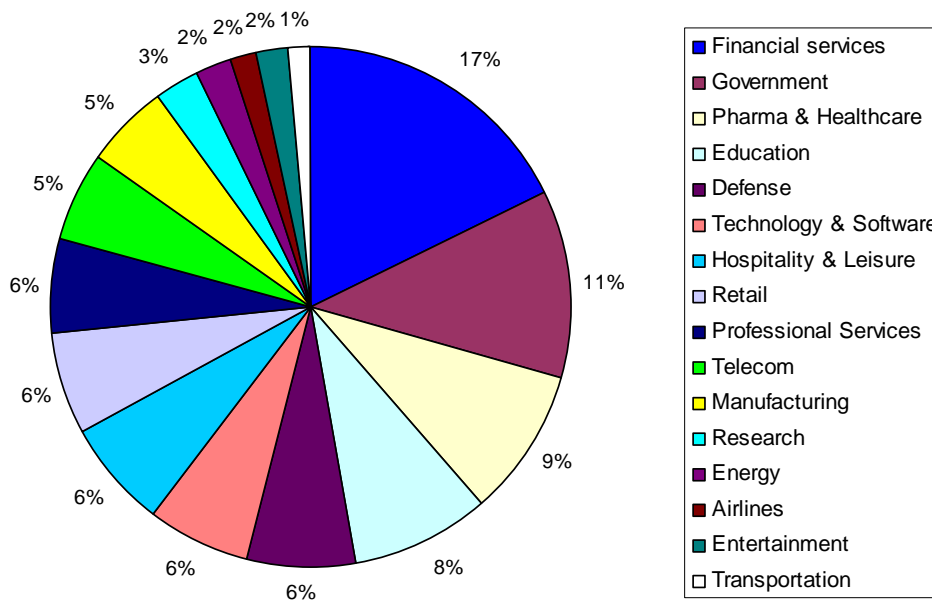
The mean experience level for the IT operations sample is 8.9 years and for the IT security sample is 9.4 years. Over 95% of respondents completed all survey items within 20 minutes. Following are key demographics and organizational characteristics for U.S. respondents. Table 2 reports the organizational level of respondents in both samples. As can be seen, the majority of respondents in both samples are at the director, manager or supervisor levels.

<sup>1</sup> Respondents were given nominal compensation to complete all survey questions.

Table 2 What organizational level best describes your current position?	IT Operations	IT Security
Senior Executive	1%	0%
Vice President	2%	2%
Director	21%	24%
Manager	24%	26%
Associate/Staff/Technician	45%	39%
Consultant	4%	6%
Other	2%	3%
Total	100%	100%

Pie Chart 1 reports the average distribution of respondents in both samples by their organization’s primary industry classification. As shown, 17% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 11% work for federal or local government.

**Pie Chart 1**  
Industry distribution of the combined IT operations and IT security samples



In total, 60% of respondents were males and 40% 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.

Table 3a reports the respondent organization’s geographic location within the United States for both samples combined. Table 3b provides the approximate full time equivalent headcount of these organizations. As can be seen, 82% of respondents are employed by larger-sized organizations (with more than 5,000 employees).

Table 3a Geographic location	Pct%
Northeast	20%
Mid-Atlantic	19%
Midwest	19%
Southeast	13%
Southwest	14%
Pacific	17%
Total	100%

Table 3b. Organizational headcount	Pct%.
Less than 500 people	2%
500 to 1,000 people	4%
1,001 to 5,000 people	12%
5,001 to 25,000 people	29%
25,001 to 75,000 people	34%
More than 75,000 people	19%
Total	100%

Appendix II provides additional organizational characteristics and demographics for respondents in IT operations and IT security.

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 1: Detailed Survey Results

Field work completed on September 14, 2008

The following table describes the sample response from two independent panels consisting of 825 practitioners in IT operations and 577 IT security professionals. By design, at the time of this survey, all respondents were employed by organizations located in the United States.

Sample description	IT Operations	IT Security
Total sampling frame	14518	11506
Bounce-back	3957	2109
Total returns	915	658
Rejected surveys	90	81
Final sample	825	577
Response rate	5.7%	5.0%

Mega Trend 1: Cloud computing		
Q1a. How familiar are you with cloud computing?	IT Operations	IT Security
Very familiar	28%	29%
Familiar	41%	46%
Not familiar	31%	25%
Total	100%	100%

Q1b. Does your organization access cloud computing resources or applications?	IT Operations	IT Security
Yes	38%	33%
No	39%	58%
Unsure	23%	9%
Total	100%	100%

Q1c. Do you believe that cloud computing increases the information security risks within your company?	IT Operations	IT Security
Yes	43%	67%
No (Go to Q2a)	57%	33%
Total	100%	100%

Q1d. If yes, what is the most significant security risk associated with cloud computing? Please check only one choice:	IT Operations	IT Security
Inability to assess or verify the security of data centers in the cloud	24%	40%
Inability to protect sensitive or confidential information	12%	29%
Inability to restrict or limit use of cloud computing resources or applications	29%	17%
Third parties might be able to access private files without authorization	18%	13%
Information may not be properly backed up	3%	0%
Downtime as a result of cloud computing failure	13%	1%
Other (please specify)	2%	1%
Total	100%	100%

Q1e. If yes, please rate the security risk presented by cloud computing within your organization today.	IT Operations	IT Security
Very low	12%	4%
Low	15%	11%
Moderate	34%	27%
High	20%	32%
Very high	19%	26%
Total	100%	100%

Q1e. If yes, please rate the security risk presented by cloud computing in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	11%	4%
Low	14%	11%
Moderate	33%	24%
High	22%	33%
Very high	20%	28%
Total	100%	100%

### Mega Trend 2: Virtualization

Q2a. How familiar are you with virtualization?	IT Operations	IT Security
Very familiar	47%	51%
Familiar	43%	42%
Not familiar	10%	7%
Total	100%	100%

Q2b. Does your organization utilize virtualization technologies?	IT Operations	IT Security
Yes	75%	74%
No	19%	19%
Unsure	6%	7%
Total	100%	100%

Q2c. Do you believe that virtualization increases the information security risks within your company?	IT Operations	IT Security
Yes	36%	61%
No (Go to Q3a)	64%	39%
Total	100%	100%

Q2d. If yes, what is the most significant security risk associated with virtualization? Please check only one choice:	IT Operations	IT Security
Inability to properly identify and authenticate users to multiple systems	49%	48%
Sensitive or confidential information may not be properly protected	9%	3%
Third parties might be able to access private files without authorization	28%	33%
Information may not be properly backed up	1%	0%
Increased threat of social engineering and cyber crimes	10%	11%
Other (please specify)	4%	5%
Total	100%	100%

Q2e. If yes, please rate the security risk created by virtualization within your organization today.	IT Operations	IT Security
Very low	17%	14%
Low	27%	22%
Moderate	32%	35%
High	20%	22%
Very high	5%	7%
Total	100%	100%

Q2f. If yes, please rate the security risk created by virtualization in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	17%	15%
Low	28%	25%
Moderate	36%	35%
High	16%	16%
Very high	2%	9%
Total	100%	100%

### Mega Trend 3a: Mobility

Q3a. What percentage of your organization's employees is mobile?	IT Operations	IT Security
Less than 5%	2%	2%
Between 5 to 10%	2%	3%
Between 10 to 20%	8%	7%
Between 20 to 30%	10%	9%
Between 30 to 40%	10%	10%
Between 40 to 50%	7%	6%
Over 50%	34%	35%
None	4%	4%
Don't know	22%	23%
Total	100%	100%

Q3b. Do you believe the workplace mobility increases the information security risks within your company?	IT Operations	IT Security
Yes	91%	96%
No (Go to Q3f)	9%	4%
Total	100%	100%

Q3c. If yes, what is the most significant security risk associated with a mobile workforce? Please check only one choice:	IT Operations	IT Security
Inability to properly identify and authenticate remote users	59%	62%
Sensitive or confidential information may not be properly protected	6%	2%
Third parties might be able to access private files without authorization	10%	11%
Information may not be properly backed up	19%	16%
Increased threat of social engineering and cyber crimes	3%	9%
Other (please specify)	3%	1%
Total	100%	100%

Q3d. If yes, please rate the security risk created by workplace mobility within your organization today.	IT Operations	IT Security
Very low	8%	4%
Low	17%	12%
Moderate	29%	24%
High	30%	32%
Very high	17%	28%
Total	100%	100%

Q3e. If yes, please rate the security risk created by workplace mobility in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	8%	6%
Low	18%	15%
Moderate	27%	31%
High	27%	31%
Very high	20%	17%
Total	100%	100%

**Mega Trend 3b: Mobile devices**

Q3f. Do you believe portable mobile devices increase the information security risks within your company?	IT Operations	IT Security
Yes	79%	90%
No (Go to Q4a)	21%	10%
Total	100%	100%

Q3g. If yes, is the most significant security risk associated with portable mobile devices? Please check only one choice:	IT Operations	IT Security
Inability to properly identify and authenticate remote users	31%	26%
Sensitive or confidential information may not be properly protected	26%	32%
Third parties might be able to access private files without authorization	12%	11%
Information may not be properly backed up	22%	20%
Increased threat of social engineering and cyber crimes	2%	4%
Other (please specify)	7%	8%
Total	100%	100%

Q3h. If yes, please rate the security risk created by portable mobile devices within your organization today.	IT Operations	IT Security
Very low	9%	8%
Low	19%	17%
Moderate	24%	26%
High	23%	21%
Very high	25%	27%
Total	100%	100%

Q3i. If yes, please rate the security risk created by portable mobile devices in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	10%	8%
Low	20%	18%
Moderate	25%	24%
High	22%	24%
Very high	23%	26%
Total	100%	100%

<b>IT Operations</b> Q3j. What mobile devices present the greatest security risk to your organization? Please rank from 1=highest risk to 5=lowest risk.	Average	Rank
Laptop computers	2.28	1
PDA's and other handheld devices	3.17	4
Cellular phones	4.05	5
USB memory sticks	3.00	3
Insecure wireless networks	2.52	2

<b>IT Security</b> Q3j. What mobile devices present the greatest security risk to your organization? Please rank from 1=highest risk to 5=lowest risk.	Average	Rank
Laptop computers	2.28	1
PDA's and other handheld devices	2.95	3
Cellular phones	4.22	5
USB memory sticks	2.98	4
Insecure wireless networks	2.56	2

**Mega Trend 4: The external threat of organized cyber criminal syndicates**

Q4a. How familiar are you with cyber crime?	IT Operations	IT Security
Very familiar	51%	89%
Familiar	30%	10%
Not familiar	19%	1%
Total	100%	100%

Q4b. Have cyber criminals ever attacked your organization?	IT Operations	IT Security
Yes	55%	92%
No	13%	5%
Don't know	32%	3%
Total	100%	100%

Q4c. Do you believe the external threat (cyber criminals) increases the information security risks within your company?	IT Operations	IT Security
Yes	93%	98%
No (Go to Q5a)	7%	2%
Total	100%	100%

Q4d. If yes, what is the most significant security risk associated with cyber crime? Please check only one choice:	IT Operations	IT Security
Attack will cause business interruption	61%	40%
Attack will result in the loss of sensitive or confidential business information including trade secrets	24%	29%
Attack will cause the loss of information about employees or customers, thus requiring data breach notification	14%	29%
Other (please specify)	1%	1%
Total	100%	100%

Q4e. If yes, please rate the security risk created by external threats (cyber criminals) within your organization today.	IT Operations	IT Security
Very low	7%	3%
Low	7%	7%
Moderate	39%	25%
High	13%	31%
Very high	34%	34%
Total	100%	100%

Q4f. If yes, please rate the security risk created by external threats in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	7%	2%
Low	6%	7%
Moderate	38%	14%
High	15%	34%
Very high	34%	43%
Total	100%	100%

#### Mega Trend 5: Outsourcing to third parties

Q5a. Does your organization outsource sensitive and confidential data to third parties?	IT Operations	IT Security
Yes	73%	72%
No	11%	12%
Unsure	16%	16%
Total	100%	100%

Q5b. Do you believe the outsourcing of customer and employee data increases the information security risks to your company?	IT Operations	IT Security
Yes	63%	89%
No (Go to 6)	37%	11%
Total	100%	100%

Q5c. If yes, what is the most significant security risk associated with outsourcing? Please check only one choice:	IT Operations	IT Security
Inability to properly identify and authenticate remote users	3%	1%
Sensitive or confidential information may not be properly protected	56%	60%
Unauthorized parties might be able to access private files without authorization	23%	32%
Information may not be properly backed up	3%	2%
Increased threat of social engineering and cyber crimes	10%	4%
Other (please specify)	5%	1%
Total	100%	100%

Q5d. If yes, please rate the security risk created by outsourcing customer and employee data to your organization today.	IT Operations	IT Security
Very low	2%	2%
Low	5%	4%
Moderate	43%	35%
High	21%	23%
Very high	29%	36%
Total	100%	100%

Q5e. If yes, please rate the security risk created by outsourcing customer and employee data to your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	2%	3%
Low	6%	4%
Moderate	42%	34%
High	22%	23%
Very high	28%	36%
Total	100%	100%

Q5f. Do you see outsourcing increasing or decreasing within the next 24 months?	IT Operations	IT Security
Increasing	34%	32%
Decreasing	12%	12%
Staying the same	54%	56%
Total	100%	100%

Q5g. Has your organization ever experienced a security incident or data breach as a result of outsourcing?	IT Operations	IT Security
Yes	54%	47%
No	46%	53%
Total	100%	100%

**Mega Trend 6: Data breaches involving personal information are increasing and so is the risk of identity theft**

Q6a. Has your organization suffered a data breach because customer or employee information was lost or stolen?	IT Operations	IT Security
Yes	79%	83%
No	21%	17%
Total	100%	100%

Q6b. How confident are you that your current security practices are able to prevent customer and employee data from being lost or stolen?	IT Operations	IT Security
Very confident	12%	4%
Confident	23%	12%
Somewhat confident	40%	30%
Not confident	12%	32%
Uncertain	13%	22%
Total	100%	100%

Q6c. What is the most significant security risk associated with data breach? Please check only one:	IT Operations	IT Security
Loss of customer or employee information, thus requiring notification of victims	35%	32%
Sensitive or confidential information that ends up in the hands of cyber criminals and identity thieves	24%	46%
Unauthorized parties gain access to private accounts	17%	5%
Diminished reputation as a result of negative media coverage	21%	14%
Other	3%	3%
Total	100%	100%

Q6d. Please rate the security risk created by the inability to protect customer and employee data from being lost or stolen to your organization today.	IT Operations	IT Security
Very low	2%	1%
Low	4%	4%
Moderate	50%	29%
High	32%	25%
Very high	12%	41%
Total	100%	100%

Q6e. Please rate the security risk created by the inability to protect customer and employee data from being lost or stolen to your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	2%	1%
Low	6%	4%
Moderate	52%	30%
High	30%	26%
Very high	10%	39%
Total	100%	100%

**Mega Trend 7: Peer-to-peer file sharing**

Q7a. How familiar are you with peer-to-peer file sharing?	IT Operations	IT Security
Very familiar	49%	49%
Familiar	35%	36%
Not familiar	16%	15%
Total	100%	100%

Q7b. Do you believe the use of P2P file sharing networks in the workplace creates a security risk within your organization?	IT Operations	IT Security
Yes	49%	58%
No (Go to 8)	51%	42%
Total	100%	100%

Q7c. If yes, what is the most significant security risk associated with P2P file sharing applications? Please check only one choice:	IT Operations	IT Security
Use of P2P will cause business interruption	2%	3%
Use of P2P will increase the risk of malware or virus infection	30%	20%
Use of P2P will result in the loss of sensitive or confidential business information including trade secrets	41%	55%
Use of P2P will cause the loss of information about employees or customers, thus requiring data breach notification	20%	16%
Other	7%	6%
Total	100%	100%

Q7d. If yes, please rate the security risk created by P2P file sharing within your organization today.	IT Operations	IT Security
Very low	3%	3%
Low	14%	15%
Moderate	48%	36%
High	26%	35%
Very high	9%	11%
Total	100%	100%

Q7e. If yes, please rate the security risk created by P2P file sharing in the workplace in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	3%	3%
Low	15%	15%
Moderate	46%	38%
High	27%	34%
Very high	9%	10%
Total	100%	100%

### Mega Trend 8: Web 2.0

Q8a. How familiar are you with Web 2.0?	IT Operations	IT Security
Very familiar	68%	67%
Familiar	24%	26%
Not familiar	8%	7%
Total	100%	100%

Q8b. Do you believe that employee use of Web 2.0 creates a security risk within your organization?	IT Operations	IT Security
Yes	65%	81%
No (Go to Q8h)	35%	19%
Total	100%	100%

Q8c. If yes, what is the most significant security risk associated with Web 2.0? Please check only one choice:	IT Operations	IT Security
Use of Web 2.0 will cause business interruption	12%	4%
Use of Web 2.0 will increase the risk of malware or virus infection	23%	14%
Use of Web 2.0 will result in the loss of sensitive or confidential business information including trade secrets	34%	64%
Use of Web 2.0 will cause the loss of information about employees or customers, thus requiring data breach notification	26%	13%
Other	5%	5%
Total	100%	100%

Q8d. If yes, please rate the security risk created by employees' use of Web 2.0 applications within your organization today.	IT Operations	IT Security
Very low	3%	4%
Low	10%	12%
Moderate	56%	45%
High	23%	30%
Very high	8%	9%
Total	100%	100%

Q8e. If yes, please rate the security risk created by employees' use of Web 2.0 applications in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	5%	4%
Low	11%	14%
Moderate	49%	41%
High	27%	30%
Very high	8%	11%
Total	100%	100%

Q8f. Have you had a security incident or data breach as a result of Web 2.0 applications?	IT Operations	IT Security
Yes	12%	28%
No	56%	51%
Unsure	32%	21%
Total	100%	100%

Q8g. How familiar are you with widgets and malware?	IT Operations	IT Security
Very familiar	46%	56%
Familiar	35%	36%
Not familiar	19%	8%
Total	100%	100%

Q8h. Do you believe that malware infection creates a security risk within your organization?	IT Operations	IT Security
Yes	89%	92%
No (Go to 9)	11%	8%
Total	100%	100%

Q8i. If yes, what is the most significant security risk associated with malware infections? Please check only one:	IT Operations	IT Security
Attack will cause business interruption	29%	18%
Attack will result in the loss of sensitive or confidential business information including trade secrets	35%	42%
Attack will cause the loss of information about employees or customers, thus requiring data breach notification	34%	39%
Other	2%	1%
Total	100%	100%

Q8j. If yes, please rate the security risk presented by malware infection within your organization today.	IT Operations	IT Security
Very low	5%	4%
Low	13%	14%
Moderate	60%	43%
High	13%	21%
Very high	9%	18%
Total	100%	100%

Q8l. If yes, please rate the security risk presented by malware infection in your organization within the next 12 to 24 months.	IT Operations	IT Security
Very low	5%	4%
Low	13%	15%
Moderate	58%	40%
High	14%	23%
Very high	10%	18%
Total	100%	100%

**Other survey items**

Q9. Who are the decision-makers or influencers within your organization when purchasing IT security products? Please check all that apply.	IT Operations	IT Security
Chief information security officer	35%	59%
Chief privacy officer	4%	10%
Chief financial officer	46%	54%
Business unit leaders	68%	67%
Application developers	23%	23%
Application architects	7%	8%
Enterprise IT architect	21%	6%
Information security team	43%	60%
Compliance or internal audit teams	23%	28%
Other (please specify)	1%	2%
Total	271%	318%

Q10. Approximately, what percentage of the 2008 IT budget will go to data protection activities?	IT Operations	IT Security
Less than 5%	3%	2%
Between 5% to 10%	7%	6%
Between 11% to 20%	27%	25%
Between 21% to 30%	20%	21%
Between 31% to 40%	27%	28%
Between 41% to 50%	13%	14%
Between 51% to 60%	1%	2%
Between 61% to 70%	0%	1%
Between 71% to 80%	1%	0%
Between 81% to 90%	1%	1%
Between 91% to 100%	0%	0%
Total	100%	100%

Q11. Is your organization planning to increase your security budget next year?	IT Operations	IT Security
Yes	35%	37%
No	36%	38%
Will stay the same (no change)	29%	25%
Total	100%	100%

Q12. Who within your organization has the greatest influence on the IT security budget decision?	IT Operations	IT Security
Chief information security officer (leader)	11%	12%
Chief privacy officer (leader)	0%	1%
Chief information officer (CIO)	23%	20%
Chief technology officer (CTO)	6%	7%
Chief financial officer (CFO)	19%	20%
Business unit leaders	41%	39%
Other (please specify)	1%	0%
Total	100%	100%

Q13. Which regulations are most influential to your organization's IT security compliance? Please check all that apply.	IT Operations	IT Security
CA 1386 or other state breach notification statutes	21%	56%
Sarbanes-Oxley	35%	24%
Payment Card Industry (PCI) requirements	35%	51%
Gramm-Leach-Bliley Act	8%	8%
FTC Safeguards Rule	2%	6%
European Union Privacy Directive	2%	11%
Health Insurance Portability & Accountability Act	4%	20%
CANSPAM Act	2%	6%
Other	1%	0%
Total	109%	182%

<b>IT Operations</b> Q14. For each one of the eight mega trends listed above, please rank order them according to security risks within your organization. 1= Highest security risk area for your company today and 8 = Lowest security risk area for your company today.	Average risk score	Rank
Cloud computing	3.19	5
Virtualization	5.14	8
Mobility	2.28	2
External threats	2.55	3
Outsourcing	2.19	1
Data breach	2.94	4
P2P filing sharing	3.33	6
Web 2.0	4.39	7

<b>IT Security</b> Q14. For each one of the eight mega trends listed above, please rank order them according to security risks within your organization. 1= Highest security risk area for your company today and 8 = Lowest security risk area for your company today.	Average risk score	Rank
Cloud computing	3.04	5
Virtualization	4.15	7
Mobility	2.74	3
External threats	2.41	2
Outsourcing	2.82	4
Data breach	2.08	1
P2P filing sharing	4.29	8
Web 2.0	3.19	6

Q15. Please check all the elements that you believe define the endpoints to your organization's IT infrastructure?	IT Operations	IT Security
Wireless networks that are used for remote connectivity	74%	72%
Laptop or notebooks	96%	100%
Hand held PDAs including iPhone	91%	84%
USB memory sticks	68%	64%
Home computers used occasionally for business	38%	56%
Other	6%	5%
Total	264%	390%

## Appendix II: Organizational Characteristics

The following table describes the sample characteristics from two independent panels consisting of 825 practitioners in IT operations and 577 IT security professionals. By design, at the time of this survey, all respondents were employed by organizations located in the United States.

What organizational level best describes your current position?	IT Operations	IT Security
Senior Executive	1%	0%
Vice President	2%	2%
Director	21%	24%
Manager	24%	26%
Associate/Staff/Technician	45%	39%
Consultant	4%	6%
Other	2%	3%
Total	100%	100%

Where does your department report in the organization?	IT Operations	IT Security
To the CFO	2%	8%
To the CTO	14%	0%
To the CIO	66%	41%
To the CSO/CISO	1%	26%
To the CPO	0%	1%
Compliance leader	4%	14%
Other business unit head or leader	9%	6%
Other	4%	4%
Total	100%	100%

Experience (means reported)	IT Operations	IT Security
Total years of business experience	8.98	9.37
Total years in IT or data security	7.61	8.05
Total years in current position	3.42	3.25

How many network connections (nodes) do you have in your organization's IT environment?	IT Operations	IT Security
Less than 50	1%	1%
50 to 250	4%	5%
250 to 500	18%	17%
500 to 1,000	38%	33%
1,000 to 2,500	29%	36%
More than 2,500	9%	8%
Total	100%	100%

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?	IT Operations	IT Security
Less than 50 people	2%	0%
50 to 100 people	2%	1%
101 to 500 people	4%	5%
501 to 1,000 people	18%	16%
1,001 to 5,000 people	43%	47%
Over 5,000 people	31%	30%
Total	100%	100%

What is the worldwide headcount of your organization?	IT Operations	IT Security
Less than 500 people	2%	1%
500 to 1,000 people	4%	3%
1,001 to 5,000 people	11%	12%
5,001 to 25,000 people	30%	29%
25,001 to 75,000 people	34%	34%
More than 75,000 people	19%	20%
Total	100%	100%

What industry best describes your organization's industry concentration or focus?	IT Operations	IT Security
Airlines	2%	2%
Automotive	1%	2%
Brokerage	1%	2%
Cable	2%	1%
Chemicals	2%	1%
Credit Cards	3%	4%
Defense	5%	7%
Education	6%	10%
Entertainment	2%	1%
Services	1%	3%
Health Care	6%	6%
Hospitality & Leisure	8%	4%
Manufacturing	6%	4%
Insurance	3%	2%
Internet, ISP and Wireless	1%	2%
Government	10%	12%
Pharmaceutical	2%	3%
Professional Services	6%	5%
Research	3%	2%
Retail	7%	5%
Banking	9%	9%
Energy	2%	2%
Telecommunications	4%	3%
Technology & Software	5%	7%
Transportation	1%	1%
Total	100%	100%

Check the country or U.S. region where your company's <b>primary</b> headquarters is located.	IT Operations	IT Security
Northeast	20%	20%
Mid-Atlantic	19%	19%
Midwest	19%	18%
Southeast	12%	13%
Southwest	14%	13%
Pacific	16%	17%
Total	100%	100%