

Sponsored by

**ArcSight**

Independently Conducted by



**Presents**

**National Survey of Managing Insider  
Threats**

Published by Ponemon Institute, LLC

Target Report Date, August 31, 2006

**Private & Confidential Document. Please Do Not Quote Without Express Permission.**

## National Survey on Managing the Insider Threat

By Dr. Larry Ponemon, August 31, 2006

Many of the data security breaches occurring today are caused by negligent or malicious employees, contractors or others with access to an organization's sensitive information. Ponemon Institute conducted the first National Survey on Managing the Insider Threat to learn what information security professionals believe organizations can do to better prevent and detect data security breaches.

The survey was sponsored by ArcSight, an enterprise security management company, and queried 461 respondents who are employed in corporate IT departments within U.S.-based organizations. For purposes of this survey, we define the "*insider threat*" as the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data, by employees, contractors and others. Insider threats occur because of human error such as mistakes, negligence, reckless behavior, and sometimes even corporate sabotage. Our survey sought to answer the following three questions.

1. What are the root causes of insider threats and how do information security practitioners respond to this pervasive IT and business risk?
2. What technologies, practices and procedures are employed by organizations to reduce or mitigate insider-related risks?
3. What are the issues, challenges and possible impediments to effectively detecting and preventing insider threats?

### Executive Summary

In a Ponemon Institute study, "What a Data Breach Costs a Company" conducted in October 2005, it was determined that an organization's direct and indirect costs of responding to a data breach total \$138.39 per data subject. These costs included: the internal investigation; legal, audit and consulting services; notification of the victims of the data breach; remediation activities and the loss of customers. In this survey on "Managing the Insider Threat," respondents reported that while an organization can expect to spend an average of \$3.4 million annually to deal with the security breaches caused by insiders, most are investing less than \$1 million in preventative measures.

Because of the enormous impact a data breach can have on the bottom line, we believe it is important to examine the causes of a breach and determine what companies can do to prevent and detect a breach. We decided to focus our research on the IT professionals because they would seem to have the most understanding about the current practices of organizations attempting to mitigate the insider threat to personal and sensitive information. Accordingly, their responses to our survey were valuable in better understanding how much time IT professionals allocate to the insider risk, which category of insider poses the greatest threat, the cost associated with insider-related security problems, the root causes of insider threats and organizations' experiences managing this data security risk.

The following are the most salient findings in our study.

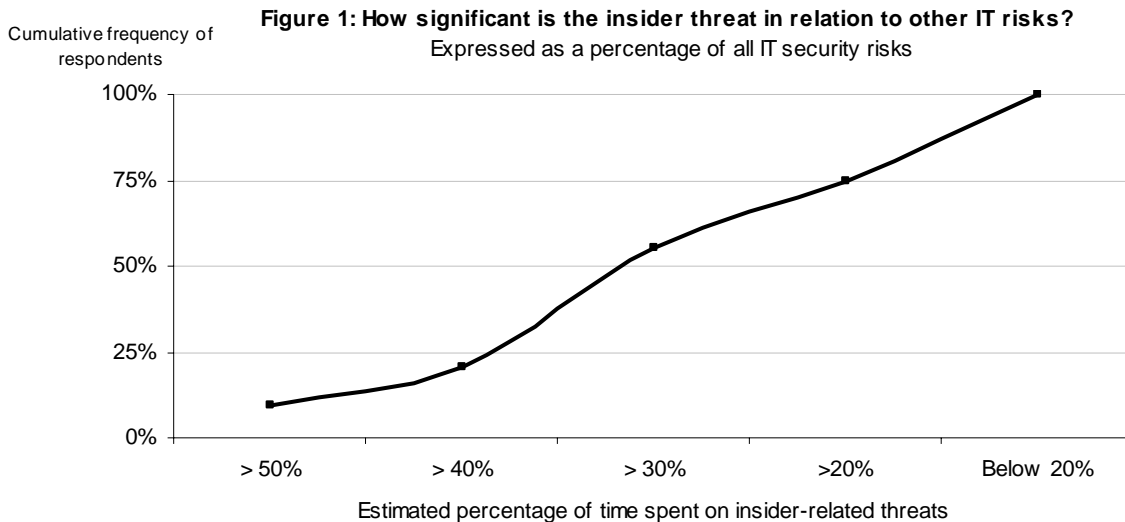
**Data breaches go unreported.** While we seem to be inundated with reports of data breaches, we may not know the full extent of the problem. More than 78% of respondents said that there

has been at least one and possibly more unreported insider-related security breaches within their company.

**Who’s accountable?** Lack of resources and leadership makes it difficult to address the insider threat. Approximately 93% believe that the number one barrier to addressing this risk is lack of sufficient resources and 80% believe that it is the lack of leadership. Another contributing factor to this threat to data is the fact that 31% of respondents report that no one person has overall responsibility for managing insider threats.

As further evidence of this lack of accountability, less than half of respondents (49%) believe that their CEOs think the insider threat is serious. In contrast, 89% of our respondents believe that it should be taken seriously.

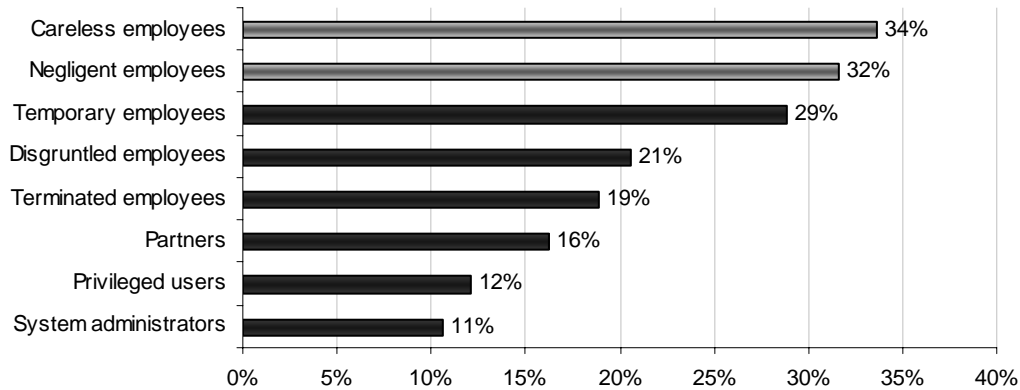
**Are an organization’s insider threats more or less serious than other information security risks?** Figure 1 shows how much effort respondents spend on insider threats, which is reported as a percentage of all IT security risk management. This specific finding suggests that respondents devote a considerable amount of their efforts helping to prevent or control insider threats as part of their company’s IT security risk management program. As shown in the figure, approximately 10% of respondents report that they spend more than half of their time on insider-related risks. About 55% of respondents state that they spend more than 30% of their time helping to manage inside-related issues.<sup>1</sup>



<sup>1</sup> The computed average about of time spent on managing insider-related risk management (as a perception of total IT security risk management) is 26%.

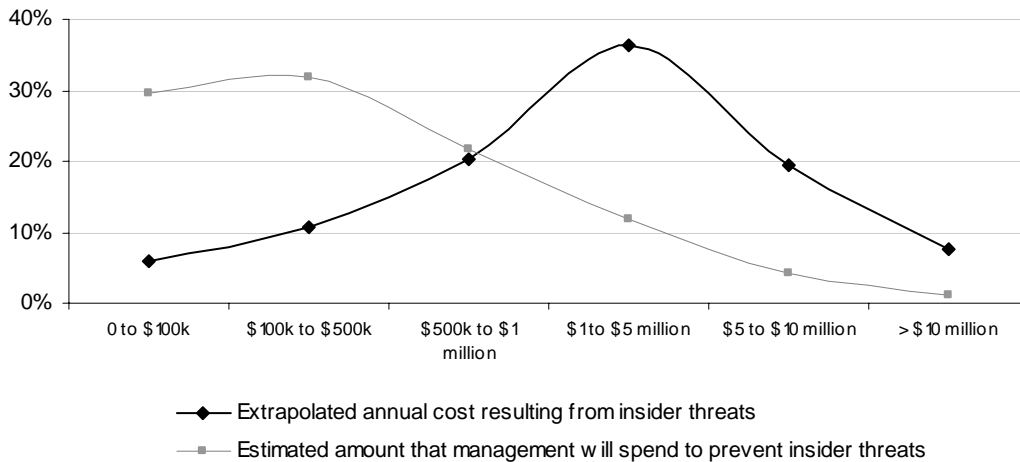
**Who within the organization presents the greatest insider security threat?** Figure 2 shows that careless or negligent employees represent the highest risk to companies participating in our survey. In contrast, system administrators and other privileged users represent a much lower insider risk to organizations.

**Figure 2: Which categories of your staff pose the greatest risk of an insider threat (top two choices per respondent)?**



**How much do insider threats cost organizations?** Figure 3 reports the estimated annual cost associated with insider-related security problems. The graph also shows the estimated dollar amount that the organization’s management is willing to spend to reduce or prevent insider threats. According to respondents, the average cost impact of the insider threat is about \$3.4 million per year. The estimated amount that the company’s management spends to manage insider threats is less than \$1 million.

**Figure 3: The expected annual cost of an insider threat and the amount companies will pay to prevent risks**



The more than \$2.4 million average estimated cost difference or gap between the two line graphs suggests that companies are under-funding the management of insider-related risks and vulnerabilities.

**What are the root causes of insider threats?** According to more than 61% of respondents, accidental data leaks occur “frequently” or “very frequently” because employees or contractors

lack sufficient knowledge about preventative measures. Over 66% of respondents state that accidental data leaks occur “frequently” or “very frequently” because employees or contractors are careless.

Less than half (48%) of respondents claim that corporate sabotage (such as the deliberate destruction of IT equipment) occurs “frequently” or “very frequently” because employees or contractors are malicious or disgruntled.

**What are organizations’ experiences in managing insider threats?** The top three IT security risks that respondents face are: (1) missed or failed security patches on critical applications, (2) insider threats and (3) virus, malware or spyware infections on networks or enterprise systems. To address these risks, respondents use both manual controls and technologies.

The top three manual controls that respondents believe mitigate or reduce insider threats include (1) supervision and management, (2) training and awareness activities, and (3) independent audits. The most frequently used technologies for reducing insider threats are identity and access management solutions and encryption. The two most effective technologies for managing insider threats are content filtering and data leak detection and prevention solutions.

## Caveats to this Survey

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 security practitioners. We also acknowledge that the results may be biased by external events such as media coverage of recent data breaches.. 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

A random sampling frame of 5,796 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 three national mailing lists of information security professionals. In total, 546 respondents completed their survey results during within a 10 day research period. Of returned instruments, 85 survey forms were rejected because of reliability checks. A total of 461 surveys were used as our final sample. This sample represents a 8.6% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is  $\leq 3\%$ .

Over 80% of respondents completed all survey items within 13.5 minutes. Respondents were given the following instruction before starting the survey.

Your participation is completely confidential. No personally identifiable or company identifiable information is requested. All responses will be compiled, analyzed, and distributed at an aggregate level.

The purpose of this study is to provide important information about how organizations enforce, detect and prevent insider threats. If you have specific questions or issues regarding this survey, please contact Ponemon Institute at 800.877.3118. Or, send an e-mail to [research@ponemon.org](mailto:research@ponemon.org).

Following are demographics and organizational characteristics for 461 respondents. Table 1a reports the most frequently cited job titles of respondents (Top 5 list). Table 1b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (29%) or director (21%) levels, respectively.

Table 1a: Job Titles (Top 5)	Freq.	Pct%
Manager, information security	58	13%
Manager, information systems	50	11%
Information security auditor	42	9%
Director, network security	39	8%
Information security specialist	36	8%
All other titles	236	51%
Total	461	100%

Table 1b: Organizational levels	Freq.	Pct%
Senior Executive	12	3%
Vice President	18	4%
Director	97	21%
Manager	134	29%
Supervisor	65	14%
Associate/Staff	85	18%
Other	50	11%
Total	461	100%

On average, respondents have more than five years of experience in the information security field, and over four years of experience in their current position. In total, 78% of respondents were males and 22% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the information security field in North America.

Over 31% of respondents state that their job function or position is located within the corporate CIO department. About 21% state that they report to the organization's information security leader (CISO or CSO), and 12% state that they report to the company's compliance or internal audit departments.

Pie Chart 1 reports the percentage distribution of respondents by major industry classification. As shown below, over 22% of respondents are employed in financial service companies. About 14% of the sample works for governmental organizations including the military.

**Pie Chart 1: Percentage Sample Distribution by Industry**

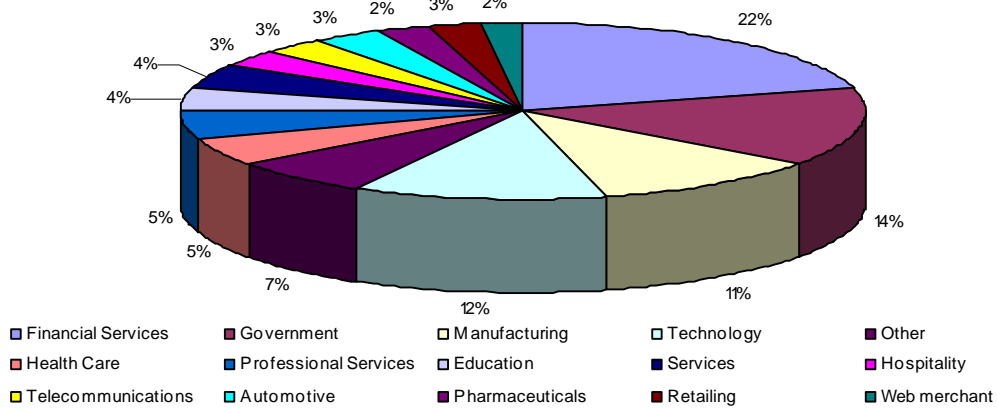


Table 2a reports the global footprint of organizations that employ respondents. Table 2b provides the approximate headcounts of these companies. As can be seen, over 57% of respondents are employed by larger-sized organizations (with more than 25 thousand employees).

Corporate locations	Freq.	Total%
United States	458	99%
Canada	52	11%
Europe	265	57%
Asia-Pacific	230	50%
Latin America (including Mexico)	162	35%
Other	13	3%

Corporate headcount	Freq.	Pct%
Less than 500 people	10	2%
500 to 1,000 people	15	3%
1,001 to 5,000 people	55	12%
5,001 to 25,000 people	121	26%
25,001 to 75,000 people	127	28%
More than 75,000 people	133	29%
Total	461	100%

**Detailed Results**

The detailed findings are reported below. Survey frequencies and percentage frequencies are reported in tabular format. The abbreviation “Pct%” denotes that the tabled percentages sum to the sample total. The column heading “Total%” means that the table percentages sum to the response sample total (which is greater than the sample total if a given question allows more than one response).

As shown in Table 3, there does not appear to be one functional area that has responsibility for managing or controlling the company’s insider threats. Over 31% of respondents state that there is no one person charged with this responsibility. Over 17% state that the responsibility is owned by the company’s CISO or CSO. Another 10% of respondents state that the company’s CIO has overall responsibility for managing insider-related IT security risks.

Table 3 Who within your organization is responsible for managing the insider threat?	Freq.	Pct%
No one has this responsibility	144	31%
CISO/CSO	80	17%
Chief Information Officer	48	10%
Chief Risk Officer	42	9%
Chief Privacy Officer	33	7%
Compliance/Ethics Officer	32	7%
General Counsel	26	6%
CEO/Executive Committee	23	5%
Chief Financial Officer	14	3%
Other	14	3%
Human Resources VP	5	1%
Total	461	100%

Table 4 reports the distribution of respondents based on how much effort they spend on insider-related problems as part of the overall IT security risk management (also shown in Figure 1). As shown below, more than 55% of respondents state that insider-related problems represent more than 30% of their company's overall risk management activities. About 25% of the sample state that insider threats represent less than 20% of their company's overall IT security risk.

Table 4 In relation to other IT risks, how significant is the insider threat (expressed as a percentage of all IT security risks the company might experience over the next 12 months)?	Freq.	Pct%
Insider Threat represents more than 50% of my IT security risk	44	10%
Insider Threat represents more than 40% of my IT security risk	51	11%
Insider Threat represents more than 30% of my IT security risk	159	34%
Insider Threat represents more than 20% of my IT security risk	90	20%
Insider Threat represents less than or equal to 20% of my IT security risk	117	25%
Total	461	100%

Table 5 reports the ranking of six known IT security risks. Results show that respondents view missed or failed security patches as the number one threat that they face today. The number two threat concerns insider-related problems. Denial of services and hacker attacks are viewed as a much less serious risk by a majority of respondents.

Table 5 Rank order of known IT security risks within the respondent's organization.	Average Rank	Forced Rank
Missed or failed security patches	2.61	1
Insider threats	2.64	2
Virus, malware or spyware infection	2.95	3
Bugs or software misconfigurations	3.00	4
Hacker attacks (penetration)	3.78	5
Denial of service	3.81	6
Average	3.13	

Table 6 shows careless employees (a.k.a. “cowboys”) and well-meaning employees who are unaware of security policies as the most likely cause of insider-related security risk. Over 29% of respondents state that temporary employees, contractors and consultants are a source of insider-related security risk. About 21% of subjects state that disgruntled employees, and 19% state that terminated employees, create insider-related problems within their organizations.

Table 6 Which categories of your staff pose the greatest risk of an insider threat within your organization?	Freq.	Total%*
Careless employees or “cowboys” (aware of policies but careless)	155	34%
Well meaning employees who are unaware of security policies (negligence or ignorance)	146	32%
Temporary employees, Contractors or consultants	133	29%
Disgruntled employees	95	21%
Terminated employees, contractors or consultants	87	19%
Partners	75	16%
Privileged users (business application administrators, finance, and others)	56	12%
System administrators	49	11%
Other	13	3%

\*Please note that respondents can provide two choices.

Table 7 shows that over 59% of respondents believe that insider-related problems are more likely to occur outside of their departments or organizational units.

Table 7 <b>Attribute:</b> <i>The greatest risk of an insider threat is outside my department (or organizational unit).</i>	Freq.	Total%
Strongly agree	98	21%
Agree	173	38%
Unsure	70	15%
Disagree	69	15%
Strongly disagree	51	11%
Total	461	100%

Table 8 shows that 35% of respondents view the most negative impact of insider-related security risks is remediation. Sixteen percent state that the most serious impact is the cost of incident response.

Table 8 Which one of the categories below has the most significant negative impact to your organization as a result of insider threats?	Freq.	Pct%
Remediation efforts	163	35%
Incident response and investigations	74	16%
System outages	54	12%
Diminished company brand	50	11%
Loss of revenue (ecommerce)	38	8%
Customer turnover or churn	33	7%
Media coverage and public disclosure	26	6%
Decline in stock price	23	5%
Total	461	100%

Table 9 provides the cost impact associated with insider-related security risks on an annual basis. The extrapolated average cost based on these data is \$3.371 million (also, please see Figure 3).

Table 9 Approximately what are the total dollars lost by your organization each year as a result of insider negligence or abuse?	Freq.	Pct%
Between 0 and \$100k	27	6%
Between \$100k to \$500k	49	11%
Between \$500k to \$1 million dollars	94	20%
Between \$1 million to \$5 million dollars	167	36%
Between \$5 million to \$10 million dollars	89	19%
Greater than \$10 million dollars	35	8%
Total	461	100%

Table 10 shows the amount that management would pay to prevent or mitigate insider-related security risks. The extrapolated average amount based on these data is \$978,000 (also shown in Figure 2).

Table 10 Approximately how much would management pay to avoid a documented or publicly visible insider attack?	Freq.	Pct%
Between 0 and \$100k	136	30%
Between \$100k to \$500k	147	32%
Between \$500k to \$1 million dollars	100	22%
Between \$1 million to \$5 million dollars	54	12%
Between \$5 million to \$10 million dollars	19	4%
Greater than \$10 million dollars	5	1%
Total	461	100%

Table 11 reports that over 78% of respondents know of an insider-related security incident that was not publicly disclosed.

Table 11 Do you know of an insider-related incident in your organization (or any other organization in your industry) which was not disclosed to the public or to law enforcement?		
	Freq.	Pct%
Yes	358	78%
No	40	9%
Unsure	63	14%
Total	461	100%

Figures 4, 5 and 6 show the types of insider threats that an organization is most likely to experience. Respondents were asked to provide their answers using a 5-point ordinal scale (1) Very frequent, (2) Frequent, (3) Not frequent, (4) Rarely, and (5) Never happens.

Figure 4 shows responses when the insider threat is based on the employee’s lack of knowledge. As can be seen, the most frequently cited consequence is accidental data leakage. Under this scenario, fraud and corporate sabotage are unlikely events. As shown below, over 61% state that accidental data leaks occurs “frequently” or “very frequently” because employees lack sufficient knowledge.

**Figure 4: Insider threat occurs because employee lacks knowledge, which results in fraud, sabotage or accidental data leaks**

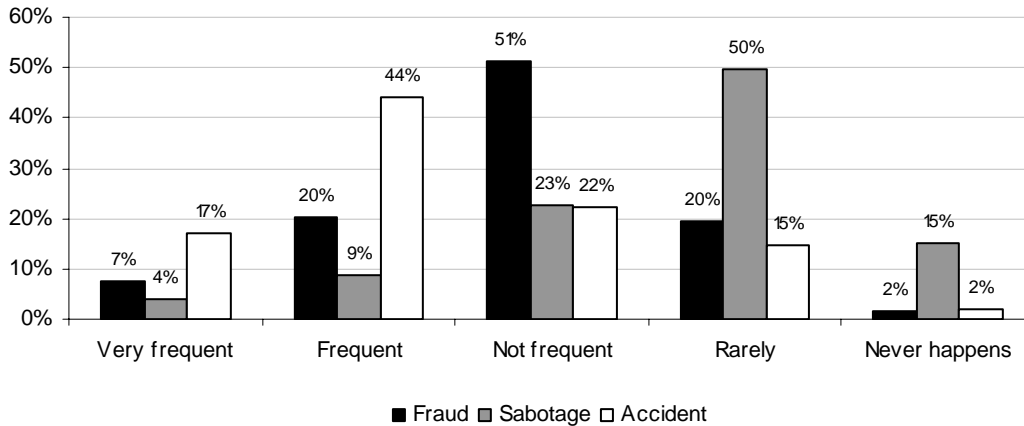


Figure 5 shows responses when the insider threat is based on the employee’s careless actions. Similar to above, the most frequently cited consequence is accidental data leakage. Under this scenario, fraud and corporate sabotage are still infrequent events. As noted below, 66% of respondents state that accidental data leaks occurs “frequently” or “very frequently” because employees or contractors are careless.

**Figure 5: Insider threat occurs because employee is careless, which results in fraud, sabotage or accidental data leaks**

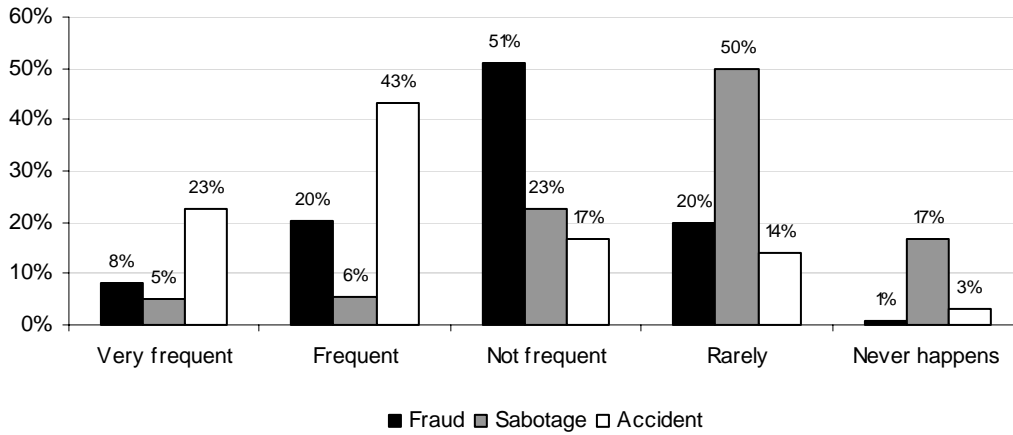


Figure 6 shows responses when the employee is believed to be malicious. Here the frequency of sabotage and fraud rise considerably from the other two scenarios. Forty-eight percent of respondents report that corporate sabotage (such as the deliberate destruction of data or IT assets) occurs “frequently” or “very frequently” because employees are angry or disgruntled. In addition, over 28% stat the fraud occurs “frequently” or “very frequently” because of malicious employees.

**Figure 6: Insider threat occurs because employee is malicious, which results in fraud, sabotage or accidental data leaks**

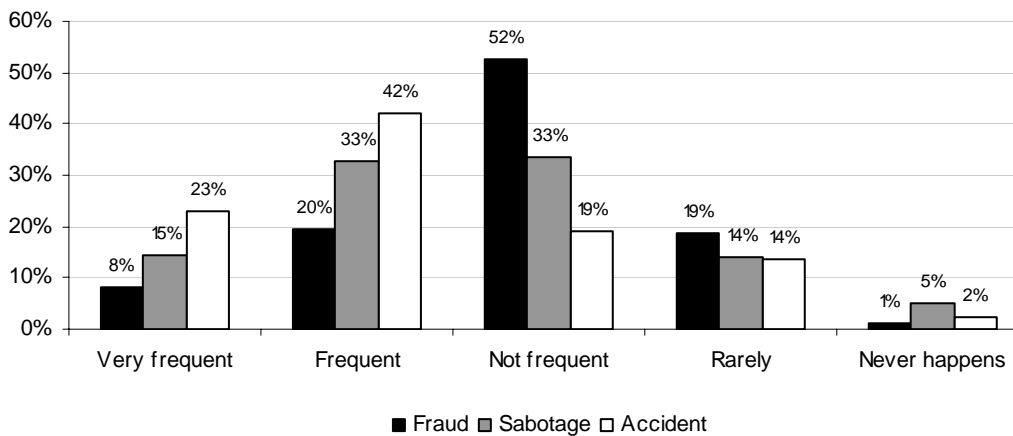


Table 12 reports the technologies most frequently used to prevent or lessen insider-related security threats. As shown, identity and access management systems and encryption are the two most deployed solutions.

Table 12 Top five technologies that organizations use to manage the insider-related security risks	Freq.	Total%*
Identity and access management systems	279	61%
Encryption technologies	220	48%
Intrusion detection systems (IDS)	182	39%
Configuration management systems	134	29%
Security information and event management	105	23%

\*Please note that respondents can provide more than one response.

Table 13 reports the five top ranked technologies that are believed to be most effective at mitigating or reducing insider-related security threats. Content filtering and data leak detection/prevention systems are viewed as the top two solutions.

Table 13 Top five technologies in terms of effectiveness at mitigating insider-related security risks	Average Score	Forced Rank*
Content filtering technologies	1.87	1
Data leak detection/prevention systems	1.89	2
Encryption technologies	2.06	3
Identity and access management systems	2.23	4
Intrusion prevention systems (IPS)	2.48	5

\*Please note that the ranking was performed on a list of 12 different technology categories.

Table 14 shows how respondents view different manual procedures or controls with respect to mitigating or reducing insider threats. The top three manual practices are supervision, training and independent audit. The least effective practices are employee background checks and security policies.

Table 14 Manual practices and procedures deemed to be most effective at mitigating or reducing insider-related security threats.	Average Rank	Forced Rank
Supervision and management	2.24	1
Training and communication programs	2.32	2
Independent audits	3.01	3
Data classification	3.03	4
Policies	3.24	5
Background checks	3.25	6

Table 15 shows the barriers that respondents believe impact the management of insider threats. The number one concern is the lack of resources. The second most frequently cited concern is the lack of coherent leadership over this pervasive security risk.

Table 15 What are the barriers to achieving a high level of comfort about these controls? Check all that apply.	Freq.	Total%
Sufficient resources (budget, time and headcount) to enforce compliance	430	93%
Leadership to manage insider-related threats	367	80%
Security technologies that perform better	302	66%
Support from senior management	269	58%
Other	23	5%

Table 16 reports that 89% of respondents view insider threats as a significant business risk for their companies.

Table 16 Do you and your colleagues within your department see the insider threat problem as a serious business risk?	Freq.	Pct%
Yes	412	89%
No	49	11%
Total	461	100%

In contrast to the above result, Table 17 reports that respondents believe that only 49% of their organization's leaders (CEOs) view insider threats as serious business risk.

Table 17 Do your company's leaders (CEO) see the insider threat problem as a serious business risk?	Freq.	Pct%
Yes	227	49%
No	234	51%
Total	461	100%

## Conclusion

This study reports a generally consistent set of findings about insider threats. First, we find that most information security practitioners in our study view the insider threat as a very serious business risk within their organizations. However, many respondents believe they don't have adequate resources to effectively manage insider-related security problems. Findings also suggest that organizations may not have the right leadership or accountability structure to ensure coherent management of this pervasive problem.

It is noteworthy that the most likely root cause of insider-related problems is the employee's lack of knowledge. Thus, organizations may find that training and awareness programs may be the most effective way of reducing the problem. Our results also show that technology-based solutions such as content filtering, data leak detection/prevention systems and encryption solutions may be helpful in mitigating or reducing the insider threat.

Please note that these observations are preliminary and believe that further research about how organizations manage the insider threat is needed.

---

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 email:

Ponemon Institute, LLC  
Attn: Research Department  
212 River Street  
Post Office Box 601  
Elk Rapids, Michigan 49629  
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.