The Risk of Insider Fraud

U.S. Study of IT and Business Practitioners

Sponsored by Attachmate

Independently conducted by Ponemon Institute LLC

Publication Date: October 2011

The Risk of Insider fraud

Ponemon Institute, October 2011

Part 1. Introduction

Ponemon Institute and Attachmate are pleased to present the results of *The Risk of Insider Fraud*. According to Ponemon Institute research, insider negligence and maliciousness can be one of the major causes of a costly and reputation damaging data breach. As reported in the Ponemon Institute's most recent *Cost of Data Breach* study, malicious insiders cause 31 percent of all data breaches and the average cost of such a breach is $318 per lost record. We believe this study is important because it reveals how prevalent insider fraud is in the organizations we studied, the consequences of fraud and how much money is needed to reduce the risk.

In our study, we defined insider fraud as the malicious or criminal attacks perpetrated upon business or governmental organizations by employees, temporary employees and contractors. Typically, the objective of such attacks is the theft of financial or information assets – which include customer data, trade secrets and intellectual properties. Sometimes the most dangerous insiders are those who possess strong IT skills or have access to your organization's critical applications and data. Other risks with potentially severe consequences are the intentional or accidental data misuse or policy violation.

The recent case involving a 31-year-old UBS trader illustrates how costly and potentially damaging to an organization's reputation insider fraud can be. According to the *Financial Times,* Kweku Adoboli was charged with fraud by abuse of position and two counts of false accounting. The total loss to UBS as a result of his "unauthorized" activity is $2 billion.[1]

Using survey methods, we implemented an objective study about how highly experienced individuals in IT, security, compliance and other business fields deal with the risk of fraud perpetrated by malicious insiders. This study attempts to ascertain what these individuals perceive to be the most serious vulnerabilities in their organizations and how they can improve IT, governance and control practices that reduce fraud and ensure compliance with regulations.

Our sample consists of 707 individuals (respondents) who have more than 10 years of experience and the vast majority is positioned at or above the manager level within their organizations. Sixty-two percent of respondents are in IT-related roles. While all respondents are located in the United States, many of their organizations are multinational or with operations in other countries.

Some of the most salient findings from this study are the following:

- Employee-related incidents of fraud, on average, occur weekly in participating organizations.
- Sixty-four percent of the respondents in this study say the risk of insider fraud is very high or high within their organizations.
- CEO's and other C-level executives may be ignoring the threat, according to respondents.
- The majority of insider fraud incidents go unpunished, leaving organizations vulnerable to future such incidents.
- The threat vectors most difficult to secure and safeguard from insider fraud are mobile devices, outsourced relationships (including cloud providers) and applications.
- The majority of respondents do not believe their organization has the appropriate technologies to prevent or quickly detect insider fraud, including employees' misuse of IT resources.

[1] M. Murphy & M. Gill, "UBS Trader in Custody after Fraud Charge" Financial Times, September 16, 2011.

Part 2. Key Findings

Following is a summary of key findings. We have organized this paper according to the following major themes or topics: prevalence of insider fraud in organizations, how organizations are responding to insider fraud and the efforts taken to combat insider fraud and mitigate the consequences.

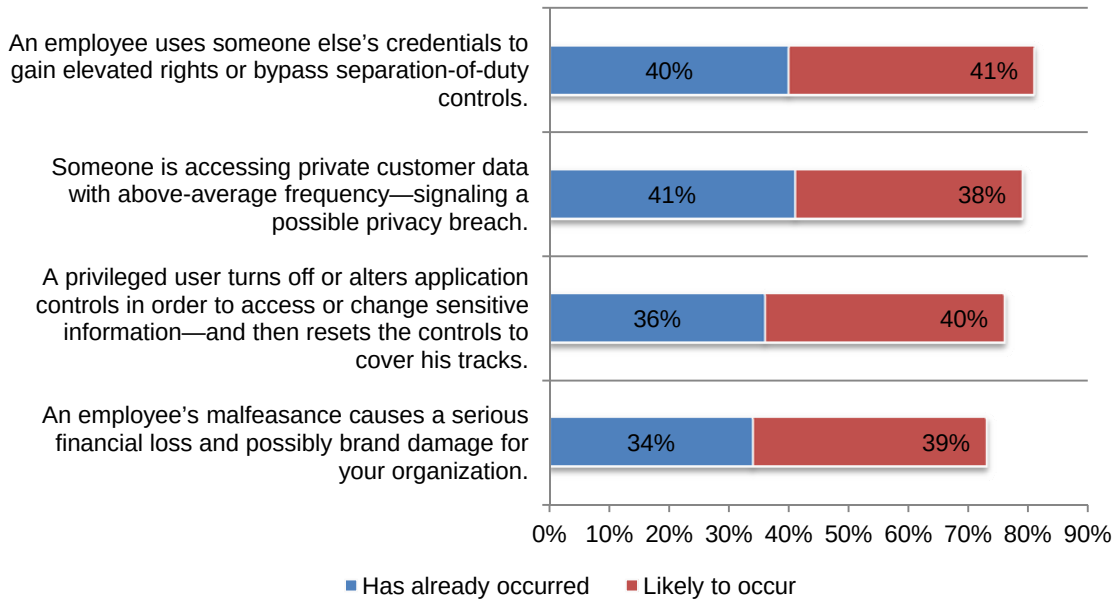
Prevalence of Insider Fraud

Insider fraud is a common occurrence. On average, organizations have had approximately 53 employee-related incidents of fraud. This translates to about one fraud event perpetrated by a malicious insider per week.

Bar Chart 1 shows that according to 41 percent of respondents, their organizations already have experienced someone accessing private customer data with above-average frequency—signaling a possible data breach and 40 percent say they already had an employee use someone else's credentials to gain elevated rights or to bypass separation-of-duty controls.

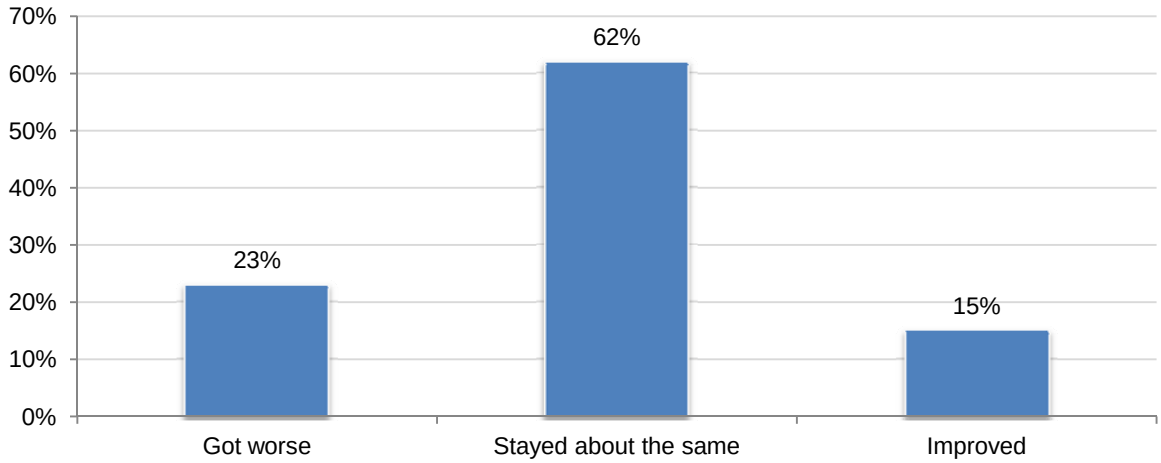
When asked what incidents are most likely to occur, 41 percent are concerned about the use of someone else's credentials and 40 percent say it is likely that a privileged user will turn off or alter application controls in order to access or change sensitive information and then resets the controls to cover his or her tracks.

Bar Chart 1: Has this ever happened or will it happen in your organization?
Has already occurred or is likely to occur



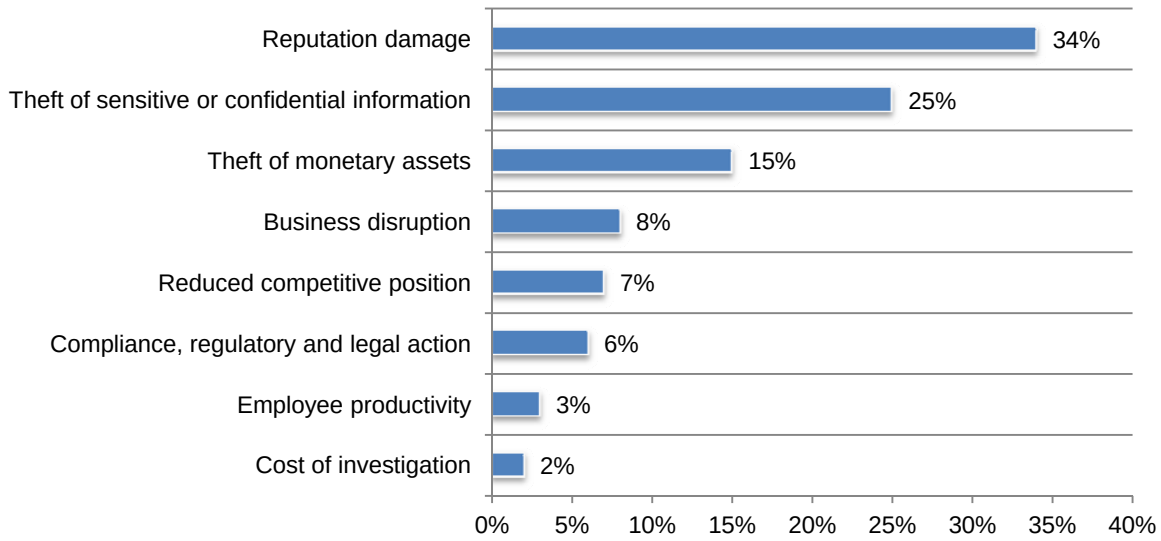
In addition to the awareness that fraudulent incidents are occurring or will occur, 64 percent of respondents say that the risk in their organizations is either very high or high. Moreover, respondents believe the current state of insider fraud will continue. According to Bar Chart 2, 23 percent say the risk has actually worsened and 62 percent say it has stayed the same. Only 15 percent believe their organization has been able to improve the insider threat. The individuals considered most responsible for preventing and quickly detecting insider fraud are: business unit managers (26 percent), CISOs (14 percent) and fraud prevention unit leaders (13 percent).

Bar Chart 2: How has insider fraud risk changed over the past 12 to 24 months?



Insider fraud risk may not be a high priority in many organizations. Insider fraud may not be on the radar screen of CEOs and C-level executives. Respondents say that only 16 percent of this group in their organizations view insider risk as very significant and 19 percent say it is significant. In addition, less than half (47 percent) strongly agrees or agrees that their organization considers the prevention of insider fraud as a top security priority. When asked what CEOs and other C-level executives would think is the worst possible consequence of insider fraud, 34 percent of respondents say it would be reputation damage, as shown in Bar Chart 3. Only 25 percent say it would be theft of sensitive or confidential information.

Bar Chart 3: In the opinion of respondents, what do CEOs & C-level executives believe is the one worst consequence of insider fraud?

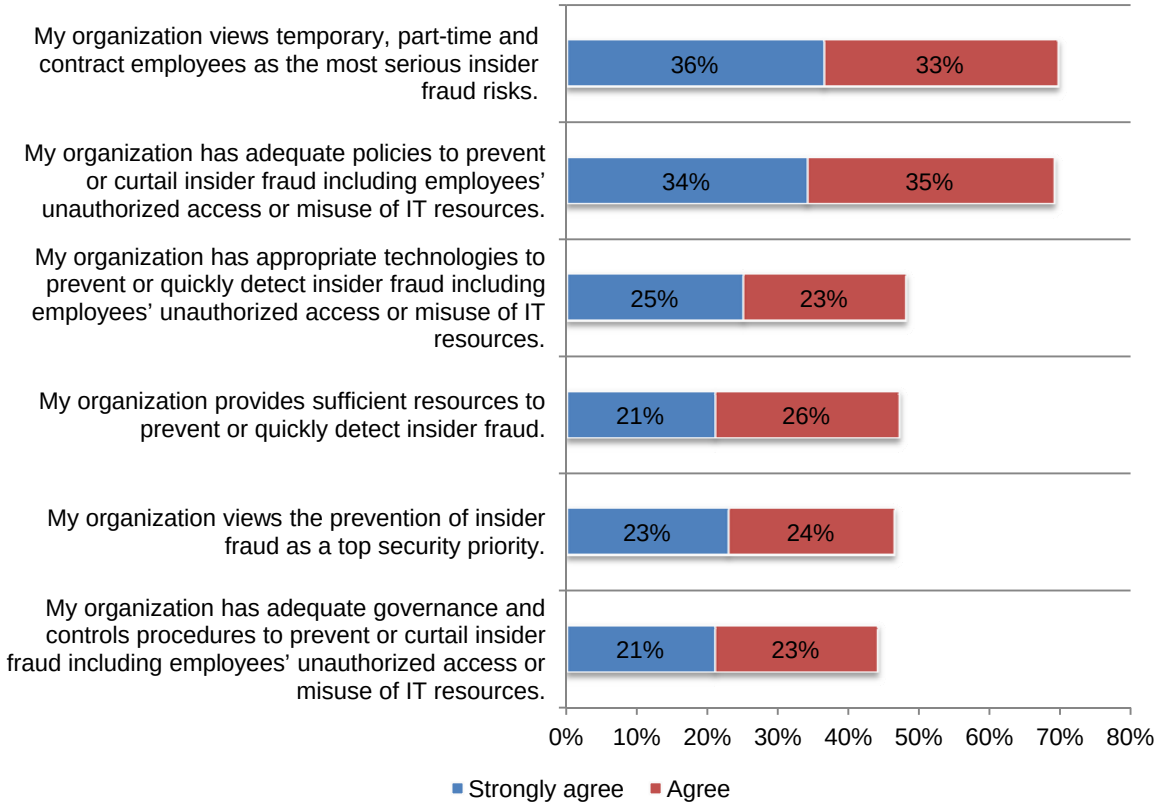


Bar Chart 4 reveals the perceptions respondents have about insider fraud mitigation efforts in their organizations. The highest level of agreement (69 percent) among respondents is that their organization views temporary, part-time and contract employees as the most serious insider fraud risks.

The most favorable perception among respondents is that organizations' policies for prevention of insider fraud are adequate. As shown, 69 percent of respondents strongly agree and agree that organizations' policies used to prevent or curtail insider fraud, including unauthorized access or misuse of IT resources are adequate.[2]

Less favorable are those perceptions about technologies, controls and resources to deal with insider fraud. Specifically, less than half (48 percent) of respondents believe their organization has the appropriate technologies to prevent or quickly detect insider fraud, including employees' misuse of IT resources. Forty-seven percent agree they have sufficient resources to prevent or quickly detect inside fraud and 44 percent believes that their organizations have adequate governance and controls procedures to prevent or curtail insider fraud including employees' unauthorized access or misuse of IT resources.

Bar Chart 4: Six attributions about insider fraud mitigation efforts in respondents' organizations.
Strongly agree and agree response



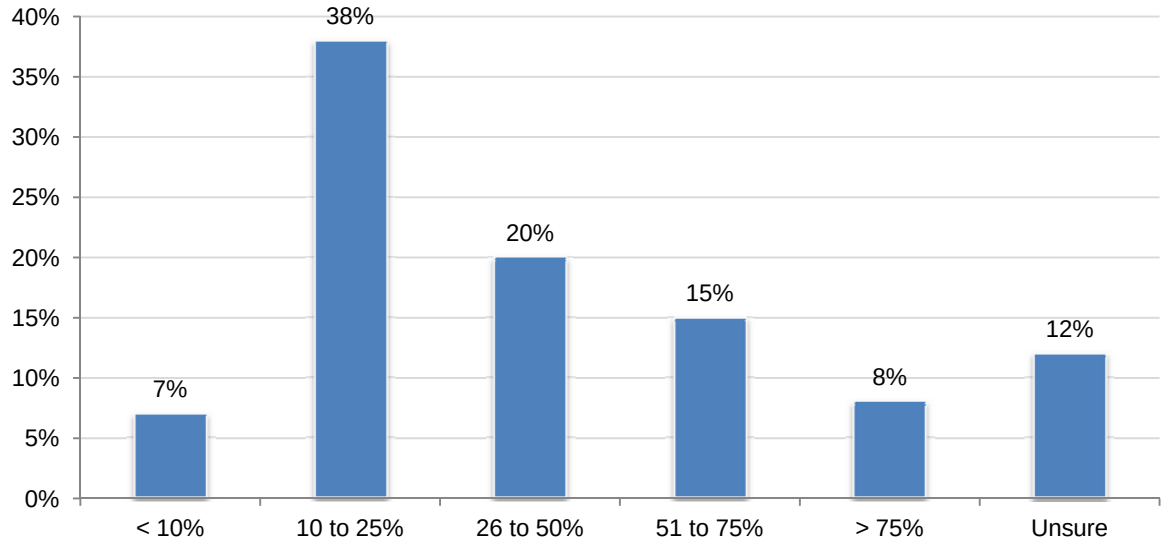
[2]We measure respondents' perceptions using a five-point scale from strongly agree to strongly disagree to each attribution or statement. A **favorable rating** is defined as a strongly agree and agree response of more than 50 percent. An **unfavorable rating** is a strongly disagree, disagree and unsure combined response at or below 50 percent.

Organizations' Response to Insider Fraud

Insider fraud investigations are a long and tedious process. On average, it takes 89 days to first recognize that insider fraud has occurred and another 96 days or more than three months to determine the root cause of the insider fraud incident and the consequences to the organization.

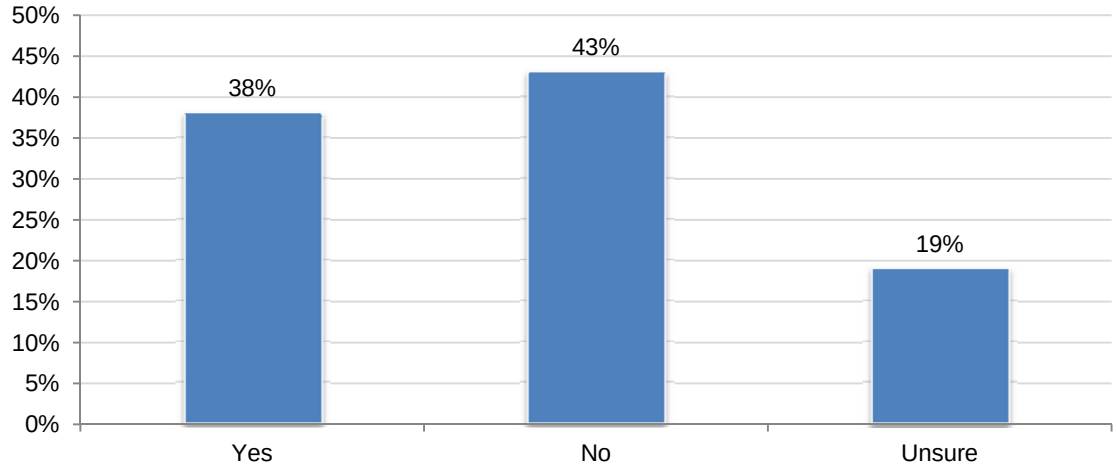
Bar Chart 5 reveals that on average about one-third (34 percent as the extrapolated value) of these investigations result in actionable evidence against the perpetrators, which means the majority of these incidents go unpunished making organizations vulnerable to more such incidents.

Bar Chart 5: Approximately what percentage of insider fraud investigations result in actionable evidence against the perpetrators?
Extrapolated value = 34 percent



The cost to organizations is difficult to determine. Bar Chart 6 shows that the financial impact and associated costs of insider fraud cannot be assessed according to 43 percent of respondents and 19 percent are unsure.

Bar Chart 6: Is your organization able to assess the financial impact and associated costs of insider fraud?



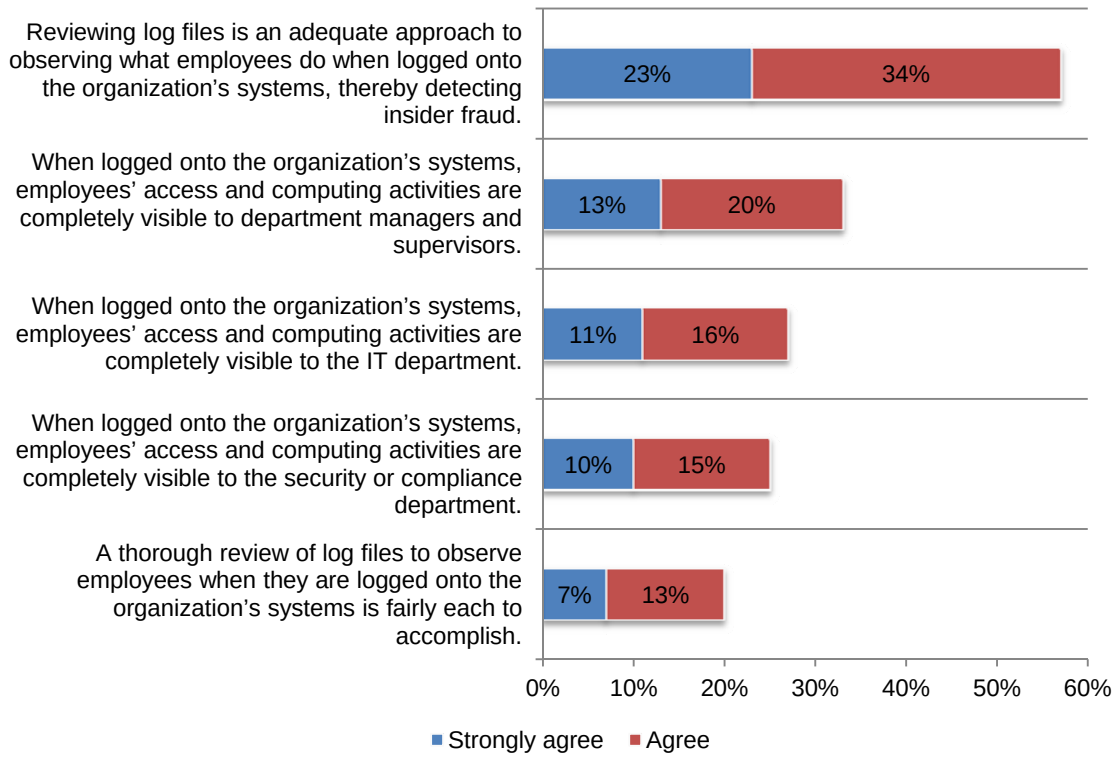
On average, organizations in our study are investing $8 million on security such as technologies, staffing, overhead and other related costs. According to respondents, on average organizations are spending 26 percent of the $8 million (approximately $2.1 million annually) on insider fraud prevention. This level of spending is expected to stay the same, according to 65 percent of respondents. Only 14 percent say it will increase and 8 percent say it will increase significantly. As previously discussed, less than half (47 percent) of respondents say their organization provides sufficient resources to prevent or quickly detect insider fraud.

Efforts to Reduce the Risk of Insider Fraud

Organizations face multiple challenges in their efforts to reduce insider fraud risks. These challenges are: availability of technology solutions, employee awareness, leadership and accountability, resources and executive-level priority. The threat vectors most difficult to secure are mobile devices, outsourced relationships (including cloud) and applications.

A lack of visibility into employees' access and computing activities is a deterrent to reducing insider fraud, according to Bar Chart 8.[3] However as shown, only 20 percent of respondents say a thorough review of log files to observe employees when they are logged onto the organization's systems is fairly easy to accomplish. Twenty-seven percent of respondents agree that when they are logged into the organization's systems, employees' access and computing activities are completely visible to the IT department. This level of agreement is similar for security and the business unit (33 percent and 25 percent, respectively).

Bar Chart 8: Five attributions about the visibility of insider fraud within respondents' organizations.
Strongly agree and agree response



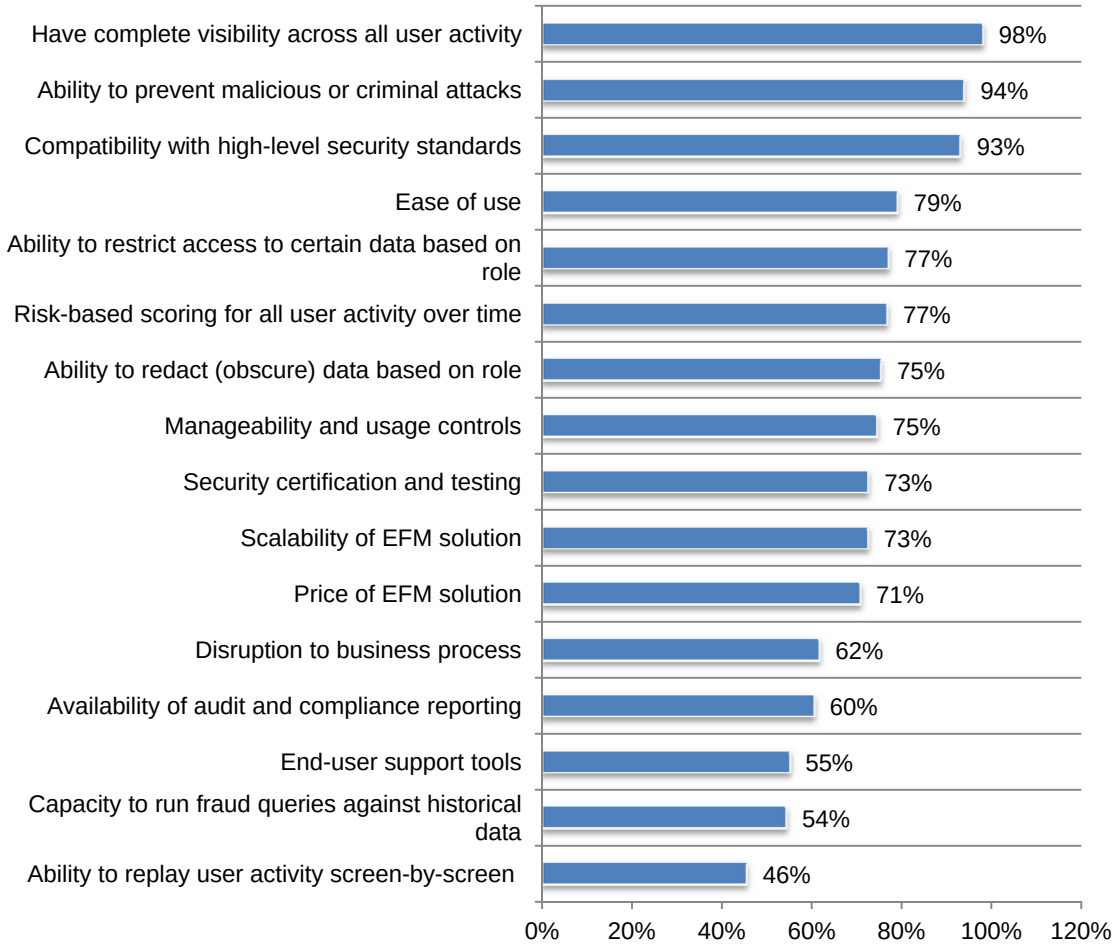
[3] Ibid, Footnote 2

The main drivers for deploying an enterprise fraud management solution focus on detection, compliance and damage control. Respondents surveyed are looking for solutions that enable them to correctly identify insider fraud, comply with regulations and laws, and minimize damage from malicious attacks are the main reasons for deploying enterprise fraud management solutions.

The majority of respondents (75 percent) believe log files for raising the level of visibility into what employees do when logged onto the organization's network or enterprise system is either very important or important. However, 78 percent believe the manual review of log files is an inadequate method for observing questionable or suspicious employee access and computing activities. This belief about the inadequacy is due to the difficulty in observing employee fraud, misuse or policy violations.

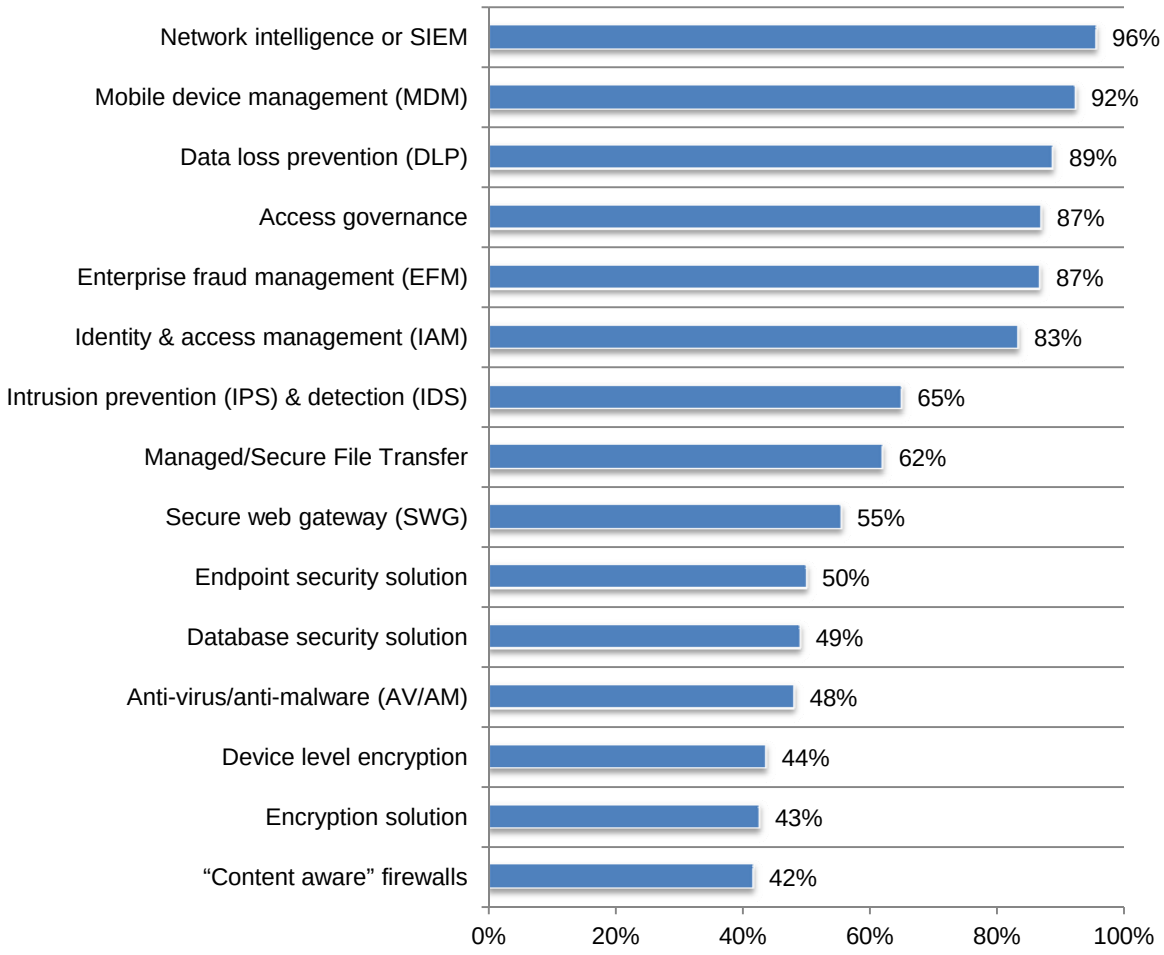
Bar Chart 9 reveals the most important factors or features when selecting an enterprise fraud management solution. Clearly the most important factors are complete visibility across all user activity, ability to prevent malicious or criminal attacks and compatibility with high-level security standards.

Bar Chart 9: What are the most important factors for evaluating and selecting an enterprise fraud management (EFM) solution within your organization?
Very important and important responses



As a strategy to combat insider fraud, respondents say their organizations have implemented enabling security technologies and governance and control practices. Bar Chart 10 lists the technologies their organizations consider very important or important. Most popular are network intelligence or SIEM, mobile device management, data loss prevention, access governance, enterprise fraud management & identity and access management.

Bar Chart 10: How important is each one of the following enabling security technologies at reducing or mitigating the threat of insider fraud?
Very important and important response



Part 3. Methods

A random sampling frame of 19,089 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of highly experienced IT and certain non-IT practitioners with bona fide credentials. As shown in Table 1, 788 respondents completed the survey. Of the returned instruments, 81 surveys failed reliability checks. This resulted in a final combined sample of 707 qualified individuals or a response rate of 3.7 percent.

Table 1: Survey response	Freq.	Pct%
Total sample frame	19,089	100.0%
Total invitations sent	18,113	94.9%
Total returned surveys	788	4.1%
Rejected surveys	81	0.4%
Final sample	707	3.7%

Table 2 reports the respondent's organizational level within participating organizations. By design, 86 percent of respondents are at or above the supervisory levels. On average, respondents had 10.65 years of overall experience in either the IT or IT security fields.

Table 2: Respondents' organizational level	Pct%
Senior Executive	3%
Vice President	7%
Director	24%
Manager	34%
Supervisor	18%
Technician	5%
Staff	3%
Contractor	4%
Other	2%
Total	100%

Table 3 shows that the most frequently cited reporting channels among respondents are the CIO (39 percent), CISO (17 percent) and compliance officer (9 percent). Sixty-two percent of respondents say they are mostly involved in IT-related activities.

Table 3: Respondents' primary reporting channel	Pct%
Chief Information Officer	39%
Chief Information Security Officer	17%
Compliance Officer	9%
Chief Risk Officer	7%
Chief Financial Officer	6%
Human Resources VP	6%
CEO/Executive Committee	5%
Chief Security Officer	5%
General Counsel	4%
Other	2%
Total	100%

Table 4 reports the worldwide headcount of participating organizations. It reports that 50 percent of respondents are located in organizations with more than 5,000 employees.

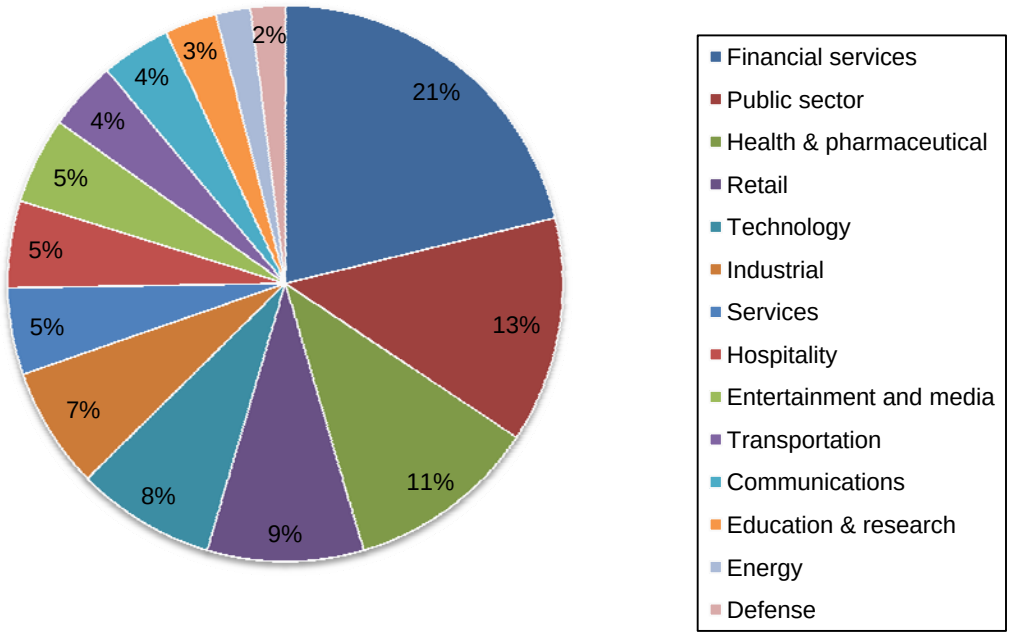
Table 4: Worldwide headcount of respondents' organizations	Pct%
Less than 500 people	11%
500 to 1,000 people	15%
1,001 to 5,000 people	23%
5,001 to 25,000 people	29%
25,001 to 75,000 people	14%
More than 75,000 people	8%
Total	100%

Table 5 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States.

Table 5: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	69%
Europe	67%
Middle East & Africa	26%
Asia-Pacific	53%
Latin America (including Mexico)	49%

Pie Chart 1 reports the industry distribution of respondents' organizations. As shown, financial services (including retail banking, insurance, brokerage and payments), public sector (federal, state and local), and healthcare and pharmaceuticals are the three largest industry segments.

Pie Chart 1: Industry distribution of respondents' organizations



Part 5. 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 non-IT practitioners located in the United States, 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 or perceptions about data protection activities 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, IT security and other related fields. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents 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 certain respondents did not provide accurate responses.

Part 5. Conclusion

Organizations today face a variety of serious threats to their networks and IT infrastructure. As a result, understanding how best to allocate limited resources to achieve their security goals is a challenge. Our goal in this research is to share the barriers and solutions of other organizations and provide guidance on the growing risk of insider fraud.

Following are five essential steps organizations might consider to help them identify and curtail the inherent risk caused by insider fraud.

Know your insiders. Organizations need to do a thorough job checking the backgrounds of all employees and contractors before giving them access to information assets and IT resources.

Vigorously monitor the workplace. Establish governance and risk management procedures that help supervisory and management personnel detect unusual employee activities, especially when it involves privileged users. The scope of monitoring should also include activities outside the traditional workplace such as employees or contractors working from remote locations such as a home office.

Deploy appropriate technologies. Our research shows that visibility is critical to the proactive management of insider risks. To achieve visibility requires enabling security technologies to detect and quickly contain suspicious activities or actual fraud incidents.

Create employee awareness. Fraud prevention requires a high level of awareness among employees, temporary employees and contractors. Thus, organizations need to educate all employees about how to identify and escalate insider risks they observe both within and outside the workplace.

Establish appropriate policies. In our opinion, the risk of insider fraud can be substantially decreased in organizations that clearly set the limits to acceptable practices to all employees.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of all survey questions completed by 707 qualified respondents. Please note that the fielding of this research including debriefing interviews concluded in September 2011.

Survey response	Freq.	Pct%
Total sample frame	19,089	100.0%
Total invitations sent	18,113	94.9%
Total returned surveys	788	4.1%
Rejected surveys	81	0.4%
Final sample	707	3.7%

Part 1. Perceptions about insider fraud

Q1. Has this ever happened within your organization? Please use the scale below each scenario based on your knowledge and experience. Has already occurred or is likely to occur.	Has occurred	Likely to occur
Q1a. A privileged user turns off or alters application controls in order to access or change sensitive information—and then resets the controls to cover his tracks.	36%	40%
Q1b. An employee uses someone else's credentials to gain elevated rights or bypass separation-of-duty controls.	40%	41%
Q1c. Someone is accessing private customer data with above-average frequency—signaling a possible privacy breach.	41%	38%
Q1d. An employee's malfeasance causes a serious financial loss and possibly brand damage for your organization.	34%	39%

Q2. Please rate the following six statements using the scale provided below each item. Strongly agree and agree.	Strongly agree	Agree
Q2a. My organization views the prevention of insider fraud as a top security priority.	23%	24%
Q2b. My organization provides sufficient resources to prevent or quickly detect insider fraud.	21%	26%
Q2c. My organization has adequate governance and controls procedures to prevent or curtail insider fraud including employees' unauthorized access or misuse of IT resources.	21%	23%
Q2d. My organization has adequate policies to prevent or curtail insider fraud including employees' unauthorized access or misuse of IT resources.	34%	35%
Q2e. My organization has appropriate technologies to prevent or quickly detect insider fraud including employees' unauthorized access or misuse of IT resources.	25%	23%
Q2f. My organization views temporary, part-time and contract employees as the most serious insider fraud risks.	36%	33%

Part 2. Insider fraud experience

Q3. On average, how long does it take to investigate an insider fraud incident within your organization?	Pct%	
Less than one day	0%	
One day	1%	
One week	15%	
One month	29%	
Three months	25%	
Six months	11%	
One year	6%	
More than one year	3%	
Cannot determine	10%	Avg days
Total	100%	95.8

Q4. Approximately what percentage of insider fraud investigations result in actionable evidence against the perpetrators?	Pct%	
Less than 10%	7%	
10 to 25%	38%	
26 to 50%	20%	
51 to 75%	15%	
More than 75%	8%	
Cannot determine	12%	Avg pct%
Total	100%	34%

Q5. How many incidents regarding employee fraud, including the misuse of assets and policy violations, did your organization uncover in the last 12 months?	Pct%	
None	1%	
1 to 5 incidents	6%	
6 to 10 incidents	11%	
11 to 20 incidents	12%	
21 to 50 incidents	17%	
51 to 100 incidents	20%	
More than 100 incidents	24%	
Cannot determine	9%	Average #
Total	100%	52.8

Q6. On average, how long do incidents regarding insider fraud (including the misuse of assets and policy violations) exist **before** they are uncovered by your organization?	Pct%	
Less than one day	1%	
One day	4%	
One week	15%	
One month	29%	
Three months	25%	
Six months	11%	
One year	5%	
More than one year	3%	
Cannot determine	7%	Avg days
Total	100%	88.9

Q7. How does your organization investigate insider fraud, including the misuse of assets and policy violations?	Pct%
Cross function team conducts independent investigation	18%
Anti-fraud or forensic specialists conduct independent investigation	27%
Internal auditors conduct independent investigation	32%
Outside auditors conduct independent investigation	19%
Other (please specify)	4%
Total	100%

	Very high	High
Q8a. Using the following scale, how would you rate the insider fraud risk level within your organization today? Very high and high.	31%	33%

Q8b. How has insider fraud risk changed over the past 12 to 24 months?	Pct%
Worsened	23%
Stayed about the same	62%
Improved	15%
Total	100%

Q9. Is your organization able to assess the financial impact and associated costs of insider fraud?	Pct%
Yes	38%
No	43%
Unsure	19%
Total	100%

	Very significant	Significant
Q10. In your opinion, how do your organization's CEO and other C-level executives view the risk of insider fraud? Very significant and significant.	16%	19%

Q11. In your opinion, what is the one **worst** consequence of insider fraud in the eyes of your organization's CEO and other C-level executives?	Pct%
Theft of monetary assets	15%
Theft of sensitive or confidential information	25%
Cost of investigation	2%
Business disruption	8%
Employee productivity	3%
Reputation damage	34%
Reduced competitive position	7%
Compliance, regulatory and legal action	6%
Other (please specify)	0%
Total	100%

Q12. What steps does your organization take today to mitigate or minimize insider fraud risk? Please rank each step using the following scale: 1 = most important to 6 = least important for mitigating or minimizing insider fraud risk.	Pct%
Enabling security technologies	2.18
Employee background checks (screening)	3.41
Employee education and training	4.43
Governance and control procedures	2.50
Security and privacy policies	5.39
Monitoring and supervision	3.04
Average	3.49

Q13. Following is a list of eight areas that require security safeguards for most organizations. With respect to the prevention of insider fraud, please rank these areas from 1 = most difficult to secure to 8 = least difficult to secure within your organization today.	Pct%
Wireless (mobile) devices and communications	1.55
Applications	2.69
Databases	5.03
Networks	4.28
Storage devices	5.90
Paper records	6.39
Endpoints	2.55
Outsourced or contract services	2.12
Physical IT infrastructure (data center and remote locations)	7.09
Total	4.18

Q14. What are the most serious challenges your organization faces with addressing insider fraud? Please select only the top three choices.	Pct%
Resources	47%
Executive priority	43%
Conflicting priorities	17%
Leadership and accountability	46%
Available technologies	52%
Employee awareness	51%
Policies and procedures	10%
Monitoring and enforcement	34%
Total	300%

Q15. What types of sensitive or confidential information are most at risk because of insider fraud? Please select only the top three choices.	Pct%
Consumer data	32%
Customer data	67%
Employee records	59%
Non-financial confidential documents	24%
Financial confidential documents	22%
Source code	9%
Trade secrets	18%
Other intellectual properties	65%
Other (please specify)	4%
Total	300%

Q16. What compliance regulations are most important to your organization's insider fraud prevention activities? Please rate each regulation using the following scale: Very important and important.	Very important	Important
Various state regulations on privacy and data protection	33%	46%
Health Insurance and Portability & Accountability Act (HIPAA)	24%	12%
Payment Card Industry Data Security Standards (PCI-DSS)	56%	39%
Federal Information Security Management Act (FISMA)	12%	10%
Sarbanes-Oxley (SOX)	55%	33%
NIST Security Standards	10%	9%
NERC Security Standards	2%	2%
Gramm-Leach-Bliley Act (GLBA)	15%	11%
European Union Privacy Directive	9%	13%
FFIEC	8%	15%
Red Flag Rule	26%	13%
Other (please specify)	25%	24%
Average	23%	19%

Q17. Who in your organization is **most responsible** for preventing or quickly detecting insider fraud?	Pct%
Chief information officer	8%
Chief information security officer	14%
Chief security officer	9%
Chief compliance officer	9%
Risk management leader	8%
Fraud prevention unit leader	13%
Business unit management	26%
Chief executive officer	0%
Chief financial officer	7%
Other (please specify)	6%
Total	100%

Q18. Please rate the following statements using the scale provided below this item. Strongly agree and agree.	Strongly agree	Agree
Q18a. When logged onto the organization's systems, employees' access and computing activities are **completely visible** to the security or compliance department.	10%	15%
Q18b. When logged onto the organization's systems, employees' access and computing activities are **completely visible** to the IT department.	11%	16%
Q18c. When logged onto the organization's systems, employees' access and computing activities are **completely visible** to department managers and supervisors.	13%	20%
Q18d. Reviewing log files is an adequate approach to observing what employees do when logged onto the organization's systems, thereby detecting insider fraud.	23%	34%
Q18e. A thorough review of log files to observe employees when they are logged onto the organization's systems is fairly each to accomplish.	7%	13%

	Very important	Important
Q19. How important are log files for raising the level of visibility into what employees do when logged onto the organization's network or enterprise system? Very important and important.	37%	38%

	Very difficult	Difficult
Q20. How difficult is it to use log files to observe employee fraud, misuse or policy violations when logged onto the organization's network or enterprise system? Very difficult and difficult.	41%	37%

Q21. In your opinion, how important is each one of the following enabling security technologies at reducing or mitigating the threat of insider fraud? Please indicate your opinion using the following scale: Very important and important.	Very important	Important
Enterprise fraud management (EFM)	48%	38%
Mobile device management (MDM)	37%	55%
Data loss prevention (DLP)	53%	35%
Anti-virus/anti-malware (AV/AM)	23%	25%
Intrusion prevention (IPS) & intrusion detection (IDS)	33%	32%
"Content aware" firewalls	17%	25%
Access governance	50%	37%
Identity & access management (IAM)	49%	34%
Managed/Secure File Transfer	30%	32%
Endpoint security solution	19%	31%
Database security solution	25%	24%
Device level encryption	24%	19%
Network intelligence or SIEM	47%	49%
Encryption solution	24%	19%
Secure web gateway (SWG)	20%	35%
Other (please specify)	27%	50%
Average	33%	34%

Q22. What are the three most important factors for evaluating and selecting an enterprise fraud management (EFM) solution within your organization? Please indicate your opinion using the following scale: Very important and important.	Very important	Important
Price or EFM solution	34%	37%
Ease of use	55%	24%
Scalability of EFM solution	46%	26%
End-user support tools	25%	30%
Disruption to business process	26%	35%
Ability to prevent malicious or criminal attacks	54%	40%
Ability to restrict access to certain data based on role	44%	33%
Ability to redact (hide or obscure) data based on role	42%	34%
Have complete visibility across all user activity	50%	48%
Availability of audit and compliance reporting	35%	26%
Risk-based scoring for all user activity over time	28%	49%
Ability to replay user activity screen-by-screen	21%	24%
Capacity to run fraud queries against historical data	24%	31%
Compatibility with high-level security standards	45%	48%
Manageability and usage controls	52%	23%
Security certification and testing	38%	35%
Other (please specify)	35%	30%
Total	41%	32%

Q23. What are the two main drivers for deploying an enterprise fraud management (EFM) solution within your organization?	Pct%
Comply with regulations and laws	44%
Minimize damage resulting from malicious or criminal attacks	39%
Identify insider fraud and misuse	50%
Comply with vendor or business partner agreements	8%
Avoid harms to customers, employees and other stakeholders	18%
Minimize the cost of data breach	9%
Improve security posture	32%
Other (please specify)	0%
Total	200%

	Very important	Important
Q24. With respect to your organization's CIO, how important is the prevention of insider fraud relative to other IT priorities? Very important and important.	19%	20%

Q25. What cost range best describes your organization's current annual budget or investment in information security? Please include technologies, staffing, overhead and other related costs. Your best guess is welcome.	Pct%	
Less than $1 million	8%	
$1 to $5 million	29%	
$6 to $10 million	41%	
$11 to $20 million	11%	
Over $20 million	11%	Avg budget
Total	100%	8.2

Q26. What percentage best describes your organization's current annual spending on insider fraud prevention relative to total spending for information security? Your best guess is welcome.	Pct%	
Less than 10%	26%	
10 to 25%	36%	
26 to 50%	21%	
51 to 75%	9%	
More than 75%	8%	Avg spend
Total	100%	26%

Q27. In terms of this year's cost of insider fraud prevention activities, how will spending change in the next 12 to 24 months? Your best guess is welcome.	Pct%
Significant decrease	2%
Decrease	11%
Stay about the same	65%
Increase	14%
Significant increase	8%
Total	100%

Q28a. Do you presently have an enterprise fraud management (EFM) solution deployed within your organization?	Pct%
Yes, fully deployed in my organization	15%
Yes, partially deployed in my organization	23%
No, but we plan to deploy it within the next 12-24 months	19%
No	43%
Total	100%

Q28b. If yes, in terms of mitigation or minimizing insider fraud, how would you rate return on investment (ROI) resulting from the deployment of EFM within your organization?	Pct%
The ROI is very significant	22%
The ROI is significant	34%
The ROI is not significant	21%
No favorable ROI realized	23%
Total	100%

Q29. What departments or operating units within your organization are most responsible for evaluating, implementing, and managing EFM solutions? Please select only one department per column.	Evaluating EFM	Managing EFM
IT operations	11%	32%
IT security	13%	7%
Business units	35%	40%
Risk management	6%	0%
Privacy office	0%	0%
Compliance & legal	11%	6%
Procurement	15%	0%
Data center management	9%	15%
Other (please specify)	0%	0%
Total	100%	100%

Part 3. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	7%
Director	24%
Manager	34%
Supervisor	18%
Technician	5%
Staff	3%
Contractor	4%
Other	2%
Total	100%

D2. What best defines your role/relationship to the IT department?	Pct%
I am mostly involved in IT-related activities	62%
I am most involved in non-IT or business activities	38%
Total	100%

D3. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	Pct%
Chief Information Officer	39%
Chief Information Security Officer	17%
Compliance Officer	9%
Chief Risk Officer	7%
Chief Financial Officer	6%
Human Resources VP	6%
CEO/Executive Committee	5%
Chief Security Officer	5%
General Counsel	4%
Other	2%
Total	100%

D4. Experience	Mean	Median
Total years of experience in IT or security	10.65	11.25
Total years in your present position	4.78	4.50

D5. Gender	Pct%
Female	24%
Male	76%
Total	100%

D6. What industry best describes your organization's industry focus?	Pct%
Communications	4%
Defense	2%
Education & research	3%
Energy	2%
Entertainment and media	5%
Financial services	21%
Health & pharmaceutical	11%
Hospitality	5%
Industrial	7%
Public sector	13%
Retail	9%
Services	5%
Technology	8%
Transportation	4%
Other	1%
Total	100%

D7. Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	69%
Europe	67%
Middle East & Africa	26%
Asia-Pacific	53%
Latin America (including Mexico)	49%

D8. What is the worldwide headcount of your organization?	Pct%	
Less than 500 people	11%	
500 to 1,000 people	15%	
1,001 to 5,000 people	23%	
5,001 to 25,000 people	29%	
25,001 to 75,000 people	14%	
More than 75,000 people	8%	Avg size
Total	100%	18,287

Ponemon Institute

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.