IDC
Analyze the Future

WHITE PAPER

Insider Risk Management: A Framework Approach to Internal Security

Sponsored by: RSA, The Security Division of EMC

Brian E. Burke Christian A. Christiansen

August 2009

IDC OPINION

Internal security risks are a complex challenge facing organizations of all industries and in all regions. Unfortunately, no single technology will solve the wide range of risks posed by "insiders."

Insiders are authorized users with legitimate access to corporate networks, applications, and data. They include, but are not limited to, employees, executives, board members, business managers, IT, consultants, outsourcers, contractors, and business partners.

As organizations build strategies to better secure their business, establishing a framework for managing insider risk should be a top priority for CISOs, CSOs, and other C-level executives globally. IDC believes a comprehensive risk management framework is the only way to effectively manage operational risk, secure competitive advantage, reduce vulnerabilities, manage misconfigurations, reduce the growing number of regulatory compliance violations, and control high-profile incidents of information leaks.

The exposure of confidential information is now the single greatest threat to enterprise network security, according to IDC's 2008 *Enterprise Security Survey*. Data loss prevention (DLP) has garnered lots of attention as a way to mitigate the risk of information leaks and comply with various regulations. However, IDC believes that DLP is only one piece of the puzzle.

We believe organizations should look at insider risk as a holistic problem that requires a holistic solution. In response to these beliefs, IDC and RSA embarked on a study to further understand the sources and challenges of insider risk management. We also wanted to identify the framework of policies, procedures, and best practices needed to effectively address the problem. Our research shows that CXOs across the United States, the United Kingdom, France, and Germany are dealing with a wide range of internal risks, including:

- The majority of organizations (52%) characterized their incidents arising from insider threats as predominantly accidental. We found that only 19% believed insider threat incidents were primarily deliberate and 26% believed they were an equal combination. Whether the threats are accidental or deliberate, the costs are still the same. Disclosure of sensitive information results in regulatory actions, failed audits, litigation, public ridicule, and competitive disadvantages. Organizations risk substantial and ongoing damage when sensitive information, such as customer and employee personally identifiable information (PII), design plans, source codes, and other types of intellectual property, is accidentally exposed.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

- Over the past 12 months, surveyed organizations experienced an average of 14.4 incidents of unintentional data loss through employee negligence. Contractors and temporary staff represented the greatest insider risk to organizations. As a by-product of the recession and its slow recovery, many companies are increasing the use of contractors, temporary staff, and outsourcers. While not employees, they need access to corporate networks. This creates a burden for IT staff who are tasked with managing their access rights, monitoring their activities, and deprovisioning their accounts when their contracts expire while still protecting sensitive information and complying with privacy regulations.

- Out-of-date and/or excessive privilege and access control rights for users are viewed as having the most financial impact on organizations. This is clear evidence that identity management and granular access control policies must be part of any risk management framework. In years past, IDC has estimated that as many as 60% of all accounts on most systems are expired. This large number of expired accounts means that insiders who no longer have a relationship with the firm continue to use the firm's IT resources (e.g., network, email, applications, and data). Other insiders can also use these expired accounts to misrepresent themselves and/or harass other employees, defraud the firm, or commit illegal acts against the firm's partners. Needless to say, expired accounts are a significant issue in failed audits. Because large companies are now audited separately for a variety of regulations (e.g., SOX, EU privacy laws, HIPAA, PCI), expired accounts can cause multiple failed audits.

METHODOLOGY

This study presents a summary and analysis of a survey conducted by IDC and RSA. This comprehensive study was designed with the aim of revealing, understanding, analyzing, and presenting the predominant issues relating to perceptions about internal security risks. The survey was conducted online by IDC; following the data collection, the analysis took place in February and March 2009. IDC surveyed a total of 400 respondents — 100 each in the United States, the United Kingdom, France, and Germany. Respondents to this in-depth survey are very high-level individuals from organizations of various sizes, including:

- CIOs and heads of IT accounted for 71% of respondents.

- CSOs, CISOs, and VPs/heads of information security accounted for 22% of respondents.

- Organizations with 5,000+ employees accounted for 36% of respondents.

- Organizations with 1,000–5,000 employees accounted for 50% of respondents.

- Organizations with fewer than 1,000 employees accounted for 14% of respondents.

 ©2009 IDC

KEY RESEARCH FINDINGS

Good People Doing Bad Things

Historically, the term "insider threat" was used to describe malicious employees who were engaging in criminal activity, stealing information, and sabotaging corporate systems. IDC defines this group of employees as renegades and rogues and believes they represent only a very small percentage of an organization's overall staff. Although renegades and rogues can represent a serious threat to an organization, they have recently taken a back seat to the risk of good employees doing bad things, inadvertently and/or deliberately.

The growing number of incidents in which employees inadvertently violate corporate policy has become the most serious "insider threat." In fact, our research found that organizations experienced an average of 14.4 incidents of unintentional data loss through employee negligence in the past 12 months, as shown in Figure 1. The majority of organizations (52%) characterized their insider threat incidents as predominantly accidental. We found that only 19% believed insider threat incidents were primarily deliberate and 26% believed the incidents were an equal combination, as shown in Figure 2.

The growing number of incidents in which employees inadvertently violate corporate policy has become the most serious "insider threat."

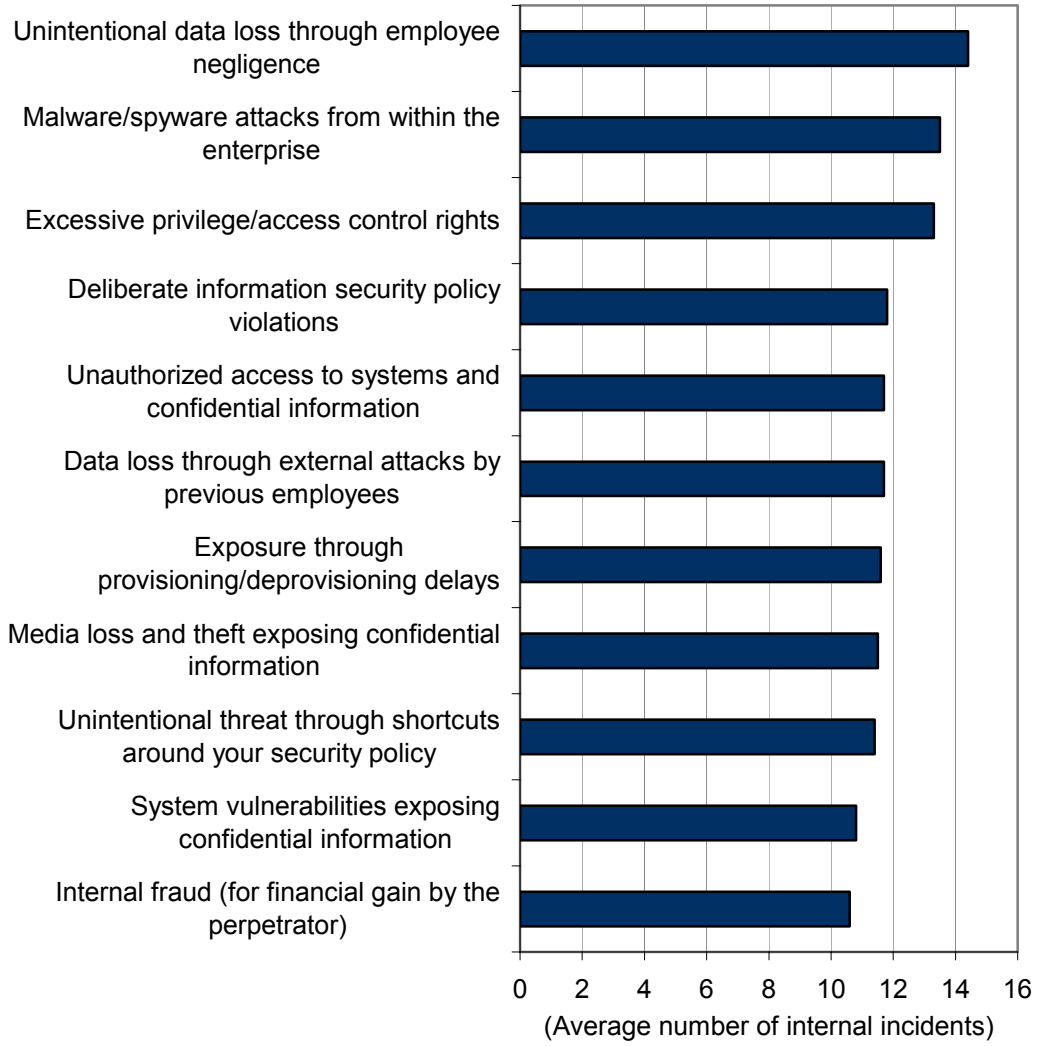
Malware and spyware attacks are another example of the risk of good employees doing bad things. Employees have become very casual about the Web sites they visit during the workday. The practice of using URL filtering to prevent employees from visiting nonbusiness Web sites during the workday is no longer sufficient. Compromises of legitimate Web sites by hackers to install malicious code and steal personal or business confidential information have become increasingly more common. Various studies have shown that up to 80% of Web sites containing malware are legitimate businesses. Moreover, Microsoft estimated in an April 2009 report that the total number of legitimate Web pages being compromised per month is more than 1 million.

What's even more alarming about the survey data that follows is that organizations are experiencing almost 1 incident per month from each threat. The difference between the top incident of unintentional data loss (14.4 per year) and the bottom incident of internal fraud (10.6 per year) is a clear sign that no single solution is the answer to addressing internal security risks. Given the current recession, the global economy will impact many different sorts of insider threats — for example, causing the number of incidents of internal fraud to rise.

The difference between the top incident of unintentional data loss (14.4 per year) and the bottom incident of internal fraud (10.6 per year) is a clear sign that no single solution is the answer to addressing internal security risks.

FIGURE 1

Average Number of Internal Incidents per Year

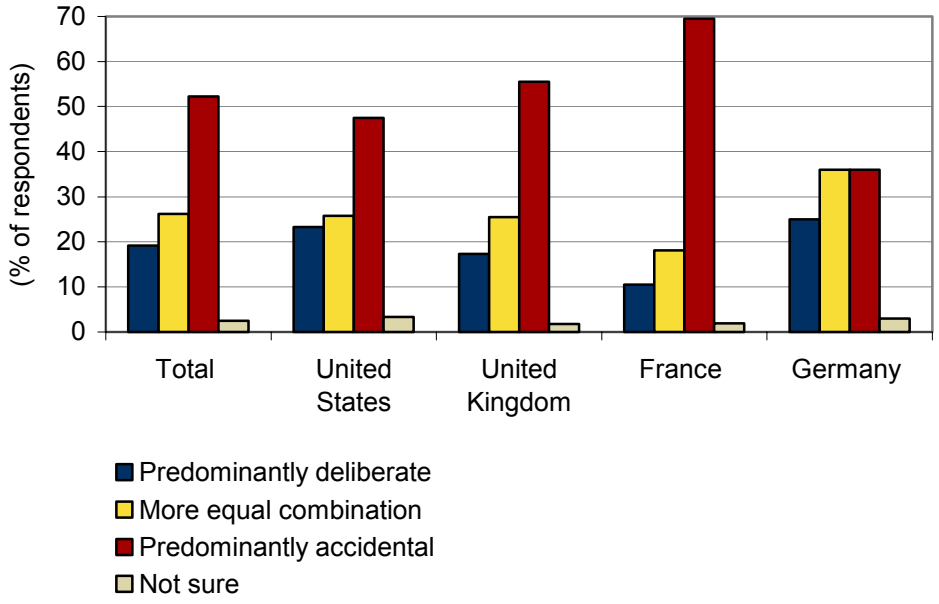


Source: IDC, 2009

 ©2009 IDC

FIGURE 2

Accidental Versus Deliberate Incidents by Country



Source: IDC, 2009

The incidents of internal security breaches vary dramatically by vertical industry, as shown in Table 1. Our research shows that:

- Unintentional data loss through employee negligence had the highest number of incidents in the financial (13.7), public (14.5), and healthcare (14.5) sectors.
- The telecommunications sector indicated that the highest number of incidents per year (18) came from malware/spyware attacks from within the enterprise.
- IT outsourcing indicated that the highest number of incidents per year (16.3) came from exposure through provisioning/deprovisioning delays. IDC believes this finding is based on the high turnover and lack of infrastructure within the IT outsourcing sector to handle deprovisioning.
- The technology sector indicated that the highest number of incidents per year (17.9) came from media loss and theft exposing confidential information. IDC has observed that participants in the technology sector often use multiple devices. In fact, one of the authors of this white paper always travels with the following items: a laptop, two cell phones, 5–10 USB memory sticks, a digital camera, and an MP3 player. Given that all these devices contain significant data storage capacity, this collection represents a serious internal security risk if the devices are not managed effectively.

TABLE 1

Total Number of Internal Incidents per Year by Vertical Industry

	Financial	Manuf.	Telco	Public	Healthcare	IT Outsourcing	Technology	Other
Unintentional data loss through employee negligence	1,154	1,380	628	853	494	930	567	238
Malware/spyware attacks from within the enterprise	1,039	1,134	721	818	345	715	608	450
Excessive privilege/access control rights	1,089	1,422	618	634	298	844	541	348
Deliberate information security policy violations	1,023	1,308	633	455	242	783	464	270
Unauthorized access to systems and confidential information	950	1,080	545	593	337	750	523	275
Data loss through external attacks by previous employees	957	1,226	574	434	250	875	535	230
Exposure through provisioning/ deprovisioning delays	893	1,085	574	499	234	964	547	244
Media loss and theft exposing confidential information	840	1,271	521	541	255	798	610	175
Unintentional threat through shortcuts around your security policy	952	1,181	556	432	309	820	541	186
System vulnerabilities exposing confidential information	944	974	531	411	250	717	580	273
Internal fraud (for financial gain by the perpetrator)	826	1,092	515	400	263	784	523	199
Other insider attacks	5	50	21	20	0	5	62	10
Valid n	84	104	40	59	34	59	34	22
Total incidents per country by respondents	10,667	13,152	6,416	6,071	3,277	8,979	6,037	2,886

Source: IDC, 2009

 ©2009 IDC

Information Protection Priorities

Sophisticated data breaches executed by determined and skillful criminals are a nightmare, but Table 1 highlights that inadvertent mistakes, misconfigurations, and inattention to proper IT disciplines gnaw at operational integrity to a greater degree than deliberate malicious attacks. Once again, our survey data outlines the wide range of insider risks, be they malicious or inadvertent, and calls for a comprehensive set of solutions to help reduce risk. Our findings show that:

Sophisticated data breaches executed by determined and skillful criminals are a nightmare, but Table 1 highlights that inadvertent mistakes, misconfigurations, and inattention to proper IT disciplines gnaw at operational integrity to a greater degree than deliberate malicious attacks.

- Remediating internal risk guards against lost laptops, USB drives, and smartphones by controlling the information on these devices; encrypting sensitive data (at rest and in motion); and managing access to networks, devices, applications, and data.
- Antimalware is always a critical component of any internal security, but controlling access is equally important.
- Excessive privilege and access rights are controlled with provisioning, periodic review of privileges, and partitioning excessively powerful administrative rights.
- The same identity and access management techniques can significantly reduce unauthorized access to confidential data and applications.

As noted in Figure 1, insider threats are not just inadvertent incidents. Internal security risk contains a high incidence of deliberately malicious activity by current and past employees. Privileged users at senior levels (executive, IT, business unit managers, etc.) will probe systems for unauthorized access, co-opt other users' access privileges, and attack systems for a variety of reasons (disgruntlement, spite, revenge, competitive advantage, blackmail, etc.). The fact that these users already have access rights makes detection very difficult.

However, solutions include controlling access rights, reviewing activity, analyzing anomalous behaviors, monitoring inbound and outbound traffic for confidentiality violations, and encrypting data. In both cases (accidental and deliberate), the goals are the same: prevent most incidents, respond quickly and accurately to any problems, run forensics after incidents, and feed the results back into the prevention mechanisms.

While insider risk management is important to compliance, the benefits are greater than just satisfying regulations and industry requirements. Safeguarding intellectual property continues to gain importance. Organizations in various industries, especially telecommunications and manufacturing, are extremely concerned with protecting patents, trademarks, brands, trade secrets, designs, architectures, copyrights, algorithms, software code, hardware schematics, inventions, business processes, and many other corporate assets (see Figure 3).

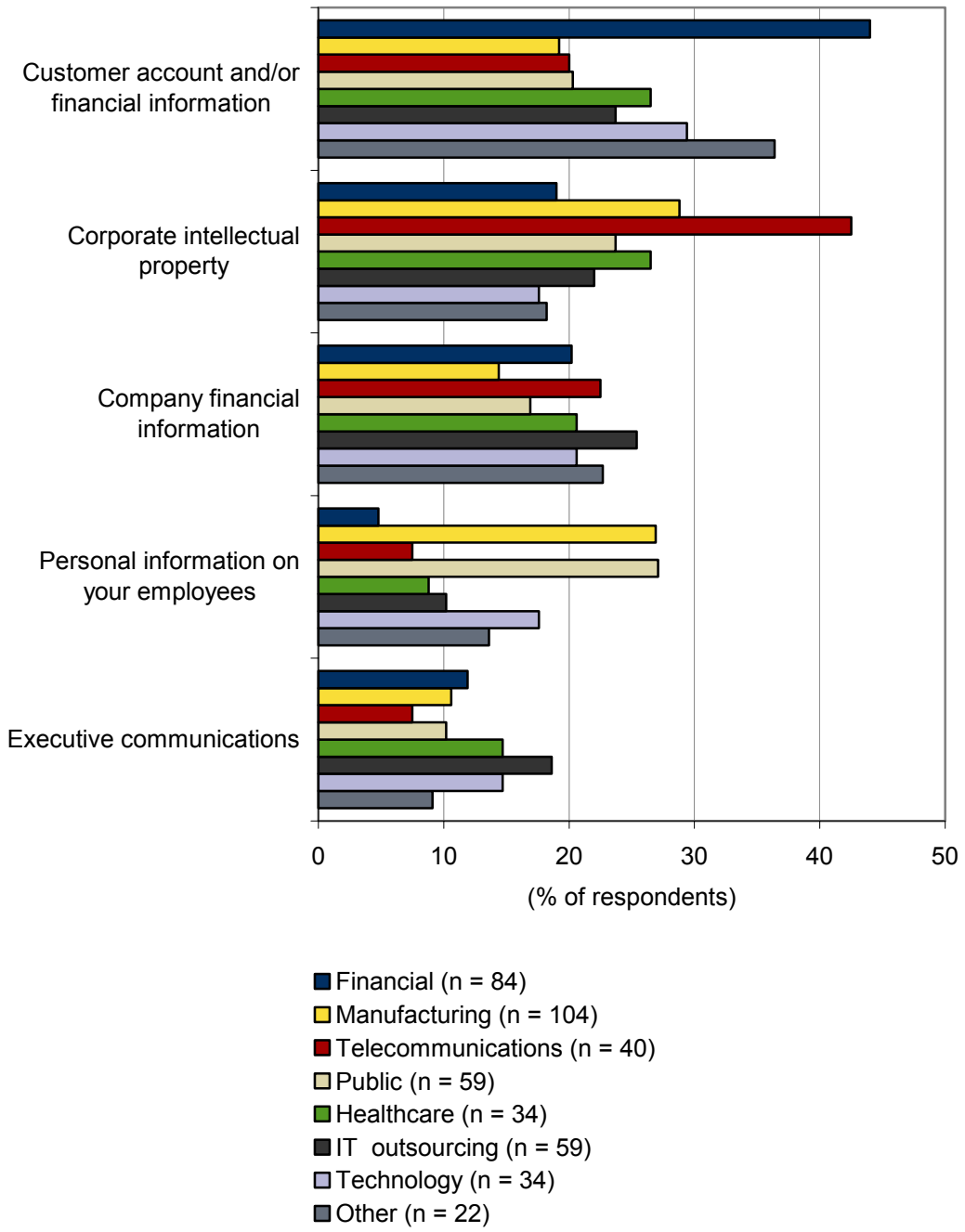
While insider risk management is important to compliance, the benefits are greater than just satisfying regulations and industry requirements.

The truth is that every business, regardless of industry, has some sort of intellectual property that has value. IDC believes intellectual property needs to be protected whether at rest, in motion, or in use. It's critical that organizations know where intellectual property is being stored, who has access to it, how it is being used, if it is being sent outside the organization, and who it is being sent to. This requires a

comprehensive approach to internal security that goes well beyond the capabilities of some of the point solutions in the market today. In today's economic climate, the risk of deliberate IP theft increases as many organizations reduce staff and freeze promotions.

FIGURE 3

Information Protection Priorities by Vertical Industry



Source: IDC, 2009

 ©2009 IDC

Insider Risks: The Financial Impact by Region

The financial impact of insider risks varies dramatically by region and by vertical industry, as shown in Figures 4–6.

- The United States views internal fraud for financial gain as having the greatest financial impact. In light of the current recession, this finding is not surprising. Now more than ever, organizations must take appropriate steps to mitigate insider risk. The increased pressure on employees, due to personal financial worries or concern about keeping their jobs, often results in greater levels of fraud. As the current financial crisis unfolds, IDC expects more fraudulent activities to be uncovered.

- In France, unintentional data loss through employee negligence has the greatest financial impact. IDC believes that the vast majority of data violations are inadvertent. However, unintentional data loss can still devastate an organization. The risk of damage to an organization's brand reputation, exposure of proprietary information, and loss of trust in partners and client relationships can be devastating to companies of all sizes.

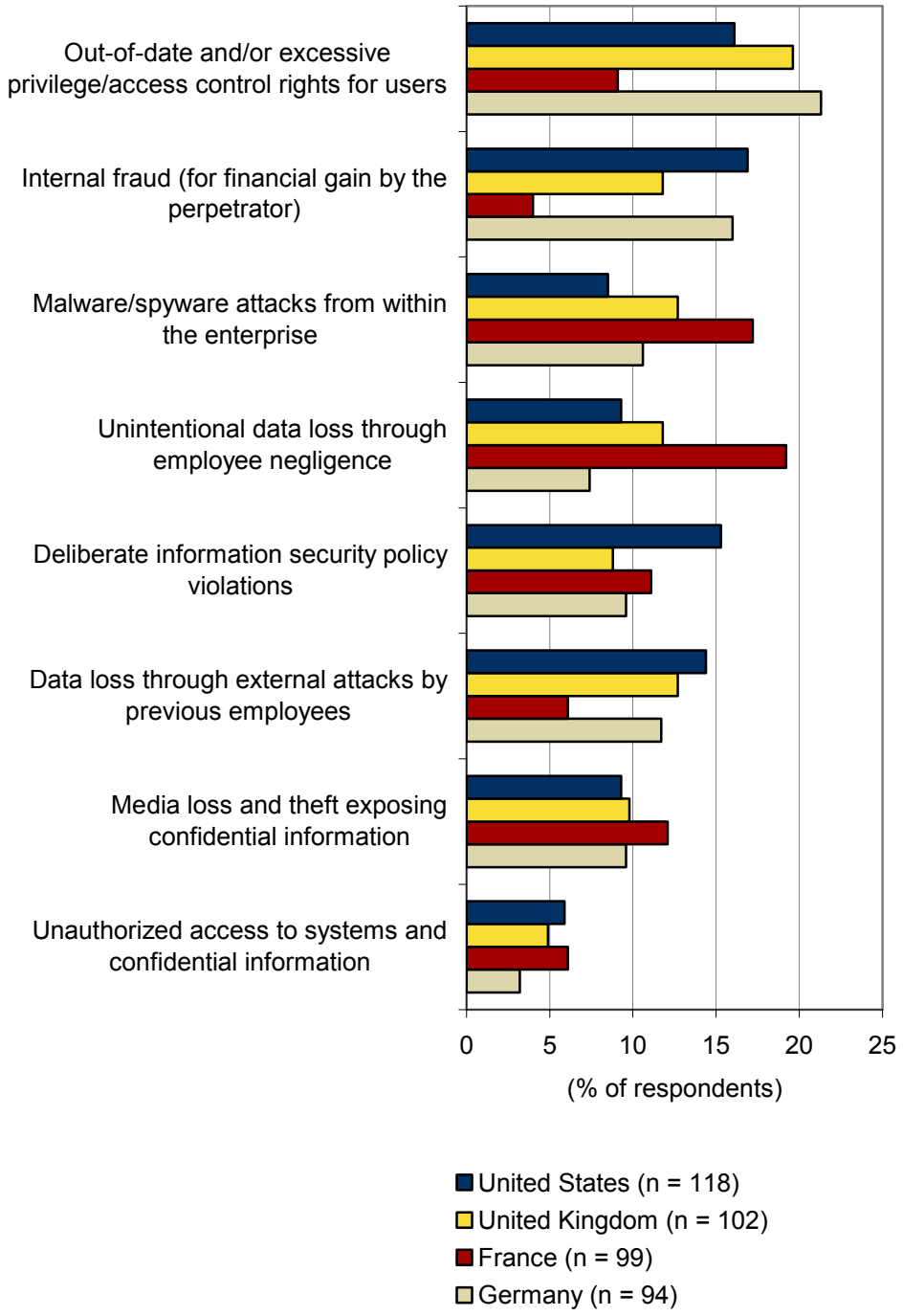
The risk of damage to an organization's brand reputation, exposure of proprietary information, and loss of trust in partners and client relationships can be devastating to companies of all sizes.

- In Germany and the United Kingdom, out-of-date and/or excessive privilege and access control rights for users have the greatest financial impact. Organizations with out-of-date or misconfigured identity management and provisioning policies risk losing serious dollars. IDC believes organizations must consider identity, access control, and provisioning as part of an internal risk management framework that provides management of employees, business partners, customers, and temporary staff from initial provisioning to deprovisioning.

FIGURE 4

Financial Impact of Internal Risk by Country (Top 8)

Q. Which type of insider threat had the most financial impact?

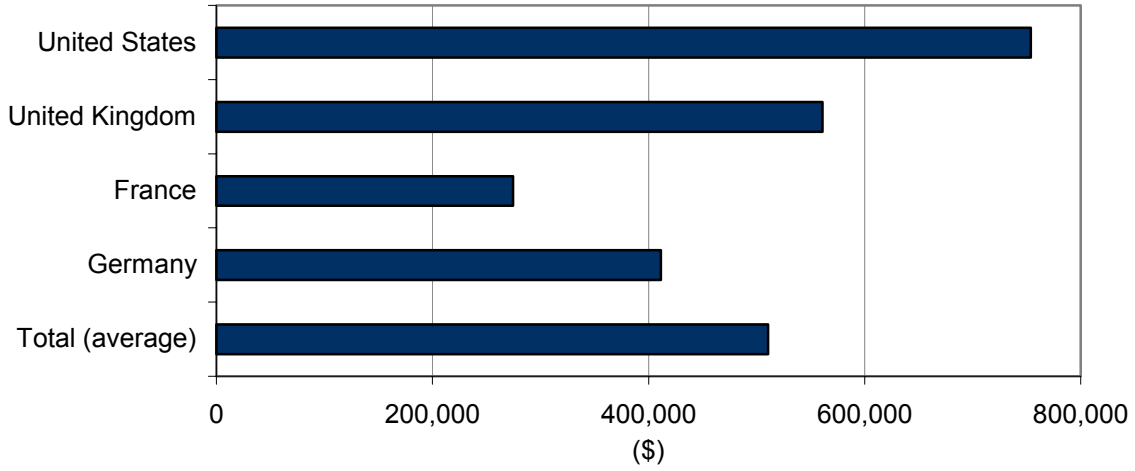


Source: IDC, 2009

 ©2009 IDC

FIGURE 5

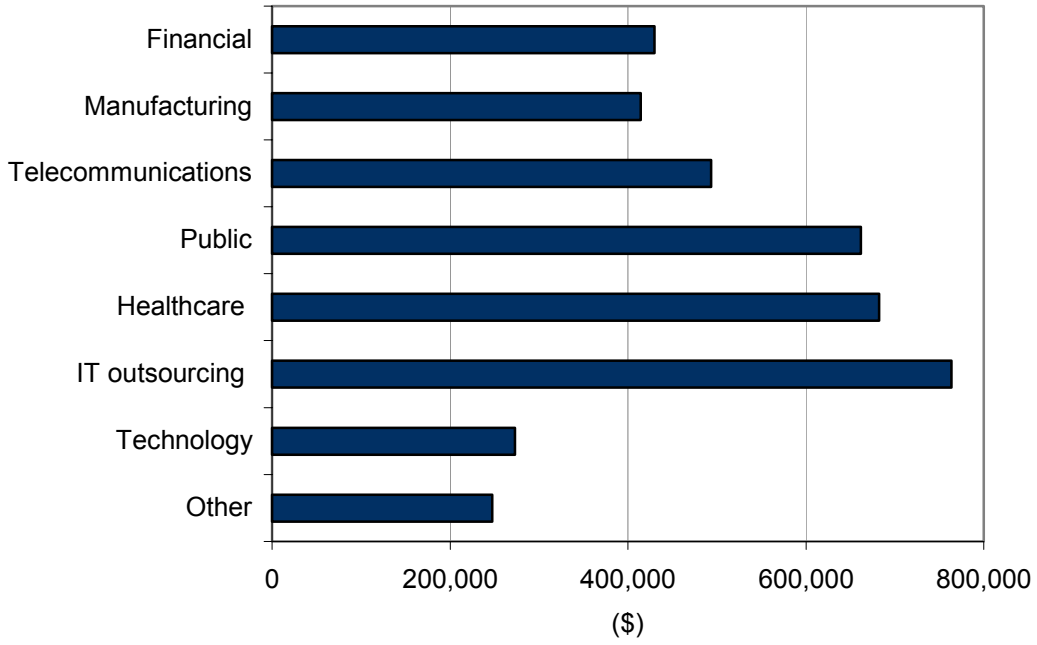
Annual Financial Loss from Insider Incidents per Organization by Region



Source: IDC, 2009

FIGURE 6

Annual Financial Loss from Insider Incidents per Organization by Vertical Industry



Source: IDC, 2009

We Have Seen the Enemy and He Is Us

Our research found that contractors and temporary staff represent the greatest insider risk to organizations, followed by technical staff and IT administrators, as shown in Table 2 and Figure 7.

- Our results show that contractors and temporary staff represent the greatest internal risk or organizations. This is true particularly in the healthcare industry, where almost 40% of respondents view contractors and temporary staff as the greatest risk. Doctors and other healthcare professionals are often associated with several different hospitals. The complexities of managing multiple accounts names, passwords, and authentication methods can cause a general disregard for security protocols, resulting in inadvertent information breaches. In the current economy, IDC believes a growing number of organizations are leveraging temporary staff and contractors to fill voids in staffing from executives, IT managers, and general line-of-business workers. This creates a nightmare for policy management and risk mitigation to ensure that temporary staff or contractors don't have access to sensitive information that is not pertinent to their role or responsibility.

- The technology industry indicated more concern about technical staff and IT administrators. The breadth of access and control of critical systems and information is highest with technical staff and IT managers. The question is, Who watches the watchers? The fact is that IT has access to the most sensitive business and personal information in all organizations. Over the years, many IT administrators have turned rogue to get even with executives, business managers, and other employees to draw attention to security weaknesses. While there is a certain logic to their action, the results are generally bad for all concerned.

- We found a high percentage of accidental issues from contractors and temporary staff, which is not surprising. These workers have only a casual understanding of a firm's security policies. Because they are paid by the project, they are focused on hitting deadlines, not complying with internal security policies. They strongly believe that compliance is someone else's problem. We have heard of many instances of contractors creating multiple accounts designed to expire at different times, although we don't have any survey data to support these claims. Typically, there is no malicious intent. The contractors simply want an active account so they can start work immediately the next time they get a contract. While this attitude is somewhat admirable, it is misguided because it clearly violates internal security policies and will certainly draw auditors' ire.

- The financial industry's concern about outsourcers and "cloud-based" service providers is a growing issue. We recently heard about an incident of a West Coast healthcare firm outsourcing patient record processing to a U.S. firm in the Southwest. This company subcontracted to an East Coast business that distributed the work to independent contractors in Pakistan. When the East Coast firm failed to pay a Pakistani contractor, she emailed the healthcare provider, included some patient records, and threatened to expose the data. While the contractor wanted only $250 and promised to destroy all records, this incident illustrates that unprotected patient information may still be circulating in the wild. This represents a potential exposure in the future.

 ©2009 IDC

TABLE 2

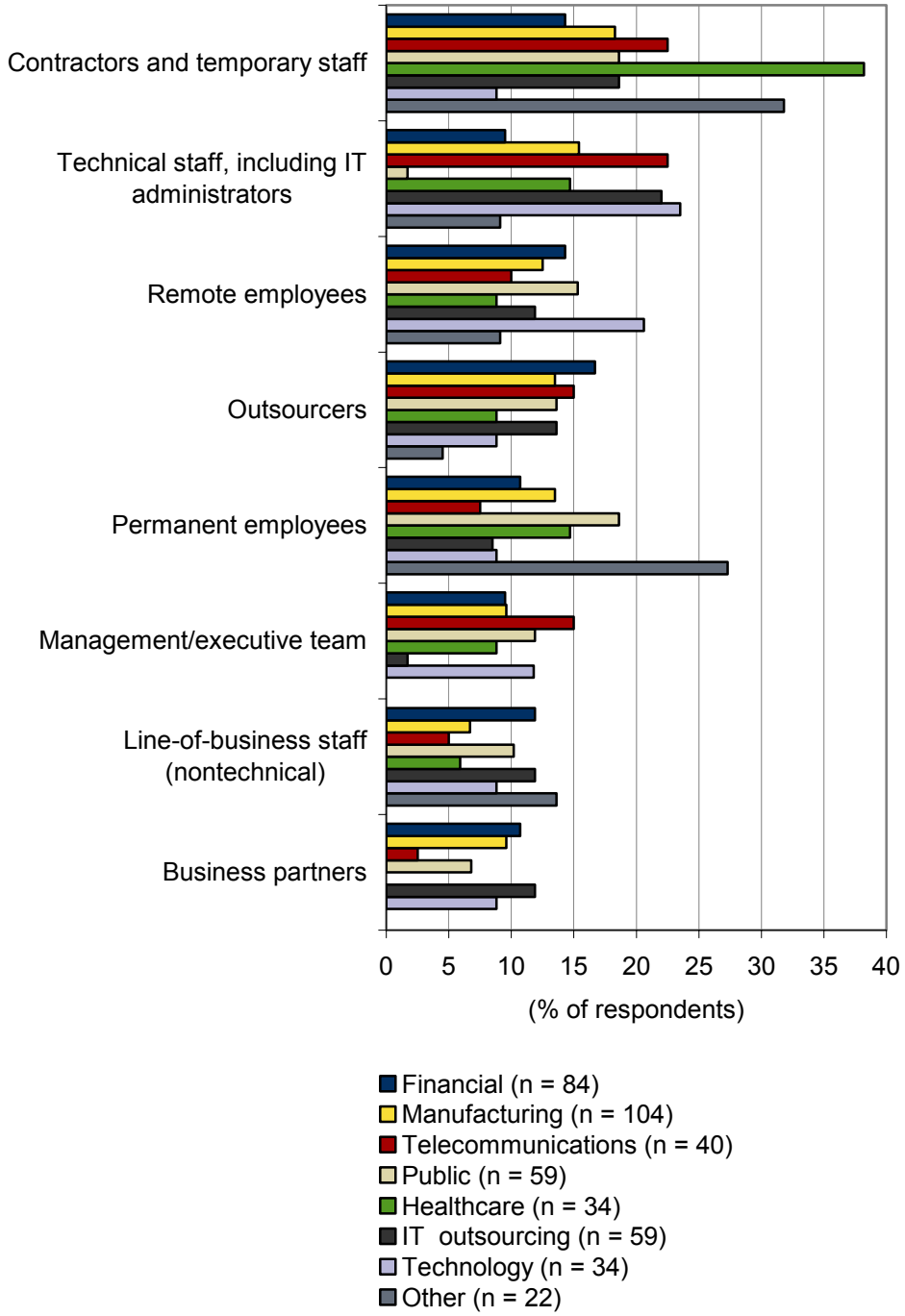
Insider Risks: Accidental Versus Deliberate (% of Respondents)

	Total	Predominantly Deliberate	Predominantly Accidental	Equal	Not sure
Contractors and temporary staff	19.5	13.3	23.3	16.7	27.3
Permanent employees	12.7	13.3	13.2	12.3	
Management/executive team	9.1	8.4	9.3	7.9	18.2
Technical staff, including IT administrators	14.1	22.9	9.3	17.5	9.1
Line-of-business staff (nontechnical)	9.1	14.5	7.9	6.1	27.3
Remote employees	13.2	8.4	13.7	17.5	
Business partners	7.7	8.4	6.2	10.5	9.1
Outsourcers	13.2	10.8	15.0	10.5	9.1
Other	1.4		2.2	0.9	
Valid n =	440	83	227	114	11

Source: IDC, 2009

FIGURE 7

Insider Risks by Employee Role



Source: IDC, 2009

 ©2009 IDC

FUTURE OUTLOOK

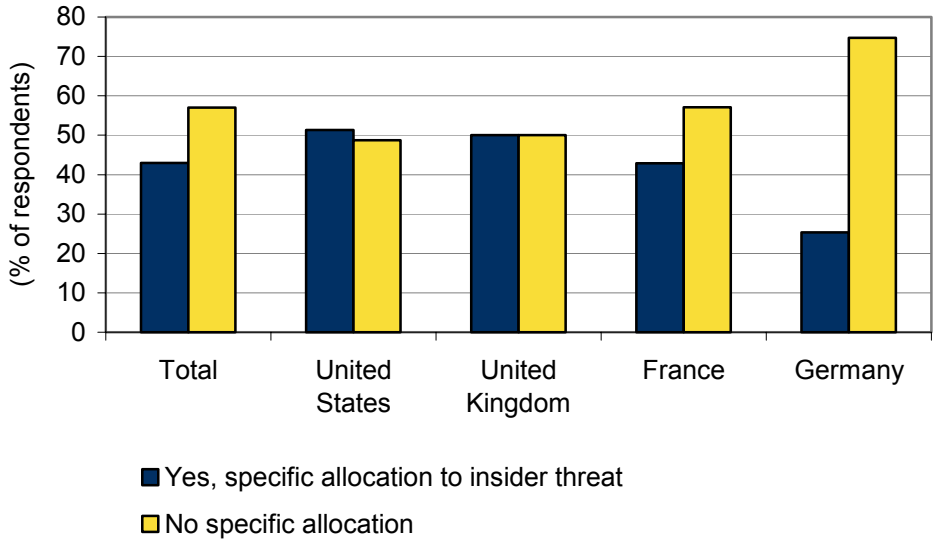
Security Budgets for Insider Risk Management

Our survey found that 43% of organizations have a specific budget allocated for internal security risks (see Figure 8). The United States had the highest percentage (51%), followed by the United Kingdom (50%), France (43%), and Germany (25%).

We found that almost 40% of organizations plan to increase spending on internal security risks over the next 12 months and only 6% have plans to decrease spending (see Figure 9). In light of the current economy and the fact that many organizations are slashing IT budgets across the board, this is clear evidence that internal security risks are a top priority. The growth in the number of internal security breaches is forcing organizations to increase spending to combat these incidents.

FIGURE 8

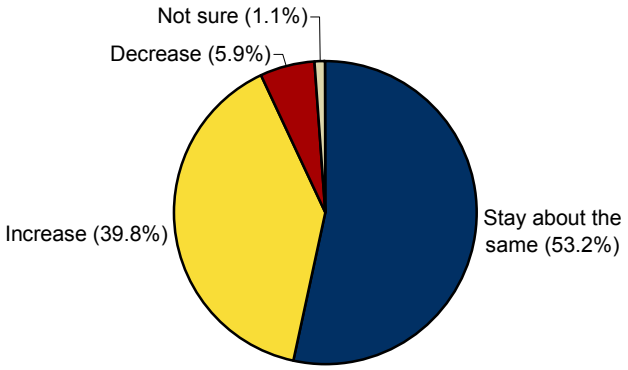
Security Budget for Internal Risks



Source: IDC, 2009

FIGURE 9

Future Spending on Internal Security Risks



Source: IDC, 2009

CHALLENGES AND RECOMMENDATIONS

The risk posed by the high percentage of employees with laptops, mobile phones, PDAs, multiple email accounts, and access to applications and databases makes addressing the insider threat a substantial challenge. Moreover, this situation creates far more risk to an organization through negligent and accidental acts than the 1–3% of insiders that commit deliberate, malicious acts.

Reducing the vulnerabilities posed by internal users needs to be a key priority in a CXO's information security strategy. The foundation of this strategy should be to implement world-class technologies in an information risk management framework. While many firms already adhere to elements of this strategy, a true risk mitigation strategy should address the whole:

1. Risk assessment should be the first priority. Organizations must understand the scope of the problems and prioritize remediation through policy and procedure and identify key security controls around network, access, data, applications, and audit.

2. Review and update information security policy on an annualized basis. For the sake of auditors and regulators, thoroughly document any changes and underlying reasoning; ensure the policy clearly demonstrates enforcement of security controls, such as data and access controls, as well as monitoring and reporting capabilities; and update the policy to include new threats such as spyware, malware, social networking, etc.

3. Educate employees on policy changes. Consider making security education a required element in annual performance reviews. Automate employee notification of violations, reiterate policy, and log all incidents.

 ©2009 IDC

4. Define insider threats by determining the value of customer accounts, intellectual property, confidential financial information, employee data, executive communications, and other confidential information to the firm. Calculate the cost of this data and the impact if it is exposed, leaked to competitors, and/or corrupted.

5. Classify and search for all high-risk data, determine where the data is and if it is secure in its current location, and determine which individuals are accessing it and if their access is appropriate. With full consideration for avoiding disruptions to critical business practices, consider data loss prevention and other data controls to protect and enforce policy on the data itself (such as quarantining data from being emailed, deleting data from endpoints, encrypting) and not just protecting the location (e.g., laptops, PDAs, databases, file servers).

6. Audit all active internal user accounts — employees, contractors, partners, customers, and other legitimate account holders. Expunge the dead accounts (up to 50–60% of accounts in poorly managed environments) and, in some cases for contractors and other semiregular workers, freeze inactive accounts.

7. Provide strong security controls for *all* your internal users (not just remote users) to access network and critical information in order to ensure that only legitimate users are accessing corporate resources. This also provides audit ability for any investigation or remediation activity following a breach.

8. Identify high-risk internal users, such as systems admins, users with access to critical business applications or customer data, job leavers, users turned down for promotion, etc. Monitor and review their activity on a regular basis, such as log-in attempts, and correlate that activity with insider risk patterns. Automatically alert on out-of-character or suspicious activity. Develop and test an incident/event management plan for prompt remediation.

9. Reconcile the access privileges of all users, starting with high-risk users, for their *current* role and job description, and immediately revoke excessive privileges. This is especially important for contractors and temporary staff who are generally given the same access rights as permanent employees when they don't need it.

10. Implement regulatory reporting on compliance with a focus on internal security policy and meeting key performance metrics.

11. Make all these steps a continuous process with regular reports on any exceptions sent to IT, compliance officers, risk officers, HR, and senior management.

IDC CONCLUSION

The internal threat landscape is a complex environment with multiple risks that are currently being managed by multiple point technologies. Internal security risks represent a wide range of deliberate and accidental incidents. The scope of the problem only intensifies as the complexity of the modern business model continues to evolve with increased mobility, a growing mix of users, and geographically diverse

business offices. IDC believes a framework approach will provide improved efficiencies, better visibility, and effective security for the internal risks outlined in this paper. The challenge of managing insider risks is too complicated and complex for a single point solution, such as DLP or authentication, to manage alone. IDC believes organizations should adopt a framework of technologies that manage internal risks across the entire infrastructure (such as endpoints, networks, applications, databases, storage, etc.). Technologies include encryption, information classification and discovery, identity management and assurance, data loss prevention, and security and event information management.

Although our survey shows that spending for internal security risks will increase, budgets remain under tight control and security investments are being cautiously managed. Budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure, especially related to the insider threat.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.