

Introduction

SECTION 01

Awareness and Exposure

SECTION 02

Intent: Malicious or Unintentional

SECTION 03

Employee Resignations

SECTION 04

Taking Punitive Actions

SECTION 05

A High Price to Pay

Conclusion

Appendix



Data loss is a burning issue that should be on the mind of every C-level executive and board member—if it isn't already. Every day we read about companies suffering millions of dollars in losses due to security breaches. Those losses directly hurt the innocent stakeholders of those companies, including hardworking employees and shareholders.

Opportunity for data loss is everywhere, and intentional or otherwise, data that ends up in the wrong place can do tremendous harm. It might be at the hands of a single disgruntled employee with a flash drive, or a forgetful member of your finance department leaving a CD-ROM on the subway. But however it happens, data loss can be devastating, and it's only a matter of time before a high-profile company, perhaps a squeaky clean one bursting with integrity and good will, is brought to its knees by a breach.

There are several pieces of legislation in place to prevent this from happening, but is that enough? Awareness of the issue is also very high, but that doesn't seem to be enough either. Are companies doing enough to protect themselves from becoming the first true poster child for data loss?

We decided to take a hard look at those questions and partnered with Datamonitor to find out what IT decision makers at over 1,400 large organizations around the world thought about the issue. What did we find? Read on for details, but we were surprised to learn that despite all the publicity, regulations, and technology around the issue, 60 percent of the companies we surveyed had experienced a loss of confidential data—just in the past year. And even more frightening than that, a full third of them believe a major breach could put them out of business.

Those results are startling and not something we take lightly at McAfee. We are committed to protecting your valuable data, whether you're an enterprise with valuable trade secrets, or a grandmother worried about identity theft. And we know that technology alone is not always the answer.

We hope you find this report insightful. To my mind, it's a big wake-up call if we're to avoid the next Enron-style corporate scandal from happening.

Dave DeWalt
McAfee president and CEO

Datamonitor's global research into enterprises' experiences of data leakage highlights a problem that should be increasingly prevalent in IT decision making—a problem that impacts them through numerous channels and sources. Perhaps most significantly, it is a problem that could lead to extremely serious financial consequences. Though most enterprises are aware of this, many appear to be complacent in the way that they are addressing the issue.

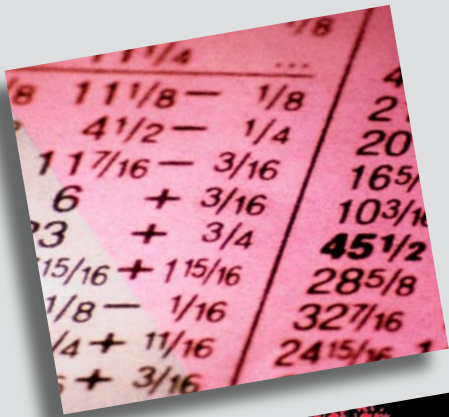
The study indicates that IT decision makers are far from confident about their ability to track data leakage: only six percent of enterprises are in a position to categorically state that they have not experienced any data loss in the last two years. Given this, Datamonitor sees data loss from the enterprise as a ubiquitous problem.

Respondents see the primary threat coming from inside rather than outside the organization, although the vast majority recognize that leakage occurs to some extent on both sides of the firewall. Malicious data loss represents an especially serious concern: the finding that 23 percent of all data loss is considered to be malicious is higher than Datamonitor anticipated, indicating the scale of the threat that enterprises face.

In terms of financial impact, the survey's findings are stark. Those enterprises that are able to provide an estimate believe that data leakage costs their organizations \$1.82 million on average per year. The potential effect of a data breach is even more serious: 33 percent of respondents believe that a major breach could potentially put them out of business, while 70 percent believe that a major breach could seriously damage their company's brand.

With such potentially damaging consequences, it is surprising that so many enterprises have put so few practices in place to prevent data leakage. Clearly, enterprises' approach to data leakage is still far from reaching maturity. Enterprises must therefore engage with third-party specialists to ensure that both the correct security solutions, as well as effective policies and procedures, are put in place.

Tim Gower, Director of Research, Datamonitor





The motivation may be malicious, and the consequences can be disastrous.

A tarnished reputation. Weakened market position. Financial loss. Stiff fines and even jail sentences. And finally—complete meltdown.



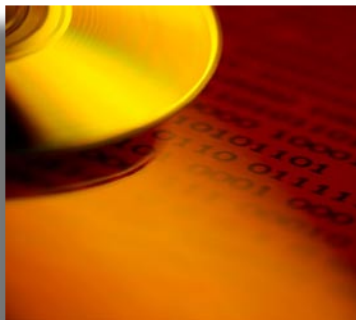
Data leakage. Just about everyone is aware of it, but is it the next wave of impending disaster that could sweep the global enterprise landscape? More than 60 percent of enterprises surveyed have experienced it within the last year, and 33 percent believe it could put them out of business. It has the potential to change the face of business and the global economy if it continues to go unchecked.

themselves and the companies' reputations, but also shareholders who suffered monetary losses and employees who lost their retirement savings and their jobs. Today, there is regulatory legislation in place in the United States and around the world to prevent financial fraud and nondisclosure of accounting practices, including the U.S. Sarbanes-Oxley Act (SOX), signed into law on July 30, 2002. But are government and industry regulations enough?



Loss of confidential company data has far-reaching ramifications that can potentially change the way business is done all over the world. The problem of data loss is growing exponentially. According to the Privacy Clearinghouse¹ Web site, nearly 150 million records containing sensitive personal information have been involved in data breaches in the United States alone. Since 2004, there has been a 1700 percent increase in data loss incidents.² In December 2006, the number of data loss incidents hit 100 million; by spring of 2007, the number grew to 150 million.

Eight years into the 21st century, the spotlight has shifted away from the executive ranks, and a new threat has emerged. Today virtually anyone can be an intentional or unintentional perpetrator. A disgruntled employee who decides to leave the company can steal confidential data and sell it to a competitor for a hefty price. A well-intentioned CFO can have his laptop containing vital financial data stolen from his rental car at the airport. Or a conscientious HR manager decides to copy and paste sensitive information into a message she's sending via her own webmail account, so that she can work on the material on her home computer over the weekend. No matter how data loss occurs, many individuals could be hurt as a result.



A large-scale data breach could be the next corporate scandal of the new century. Shortly after the turn of the century, the fraudulent financial practices of a handful of unscrupulous executives brought down some once-powerful companies. Their actions hurt not only

It is a watershed moment for large organizations all over the world. And with increasing pressure to stay compliant, they need to start taking proper precautions to prevent the floodgates from bursting.



1 SOURCE: <http://www.privacyrights.org>
 2 SOURCE: <http://www.privacyrights.org>

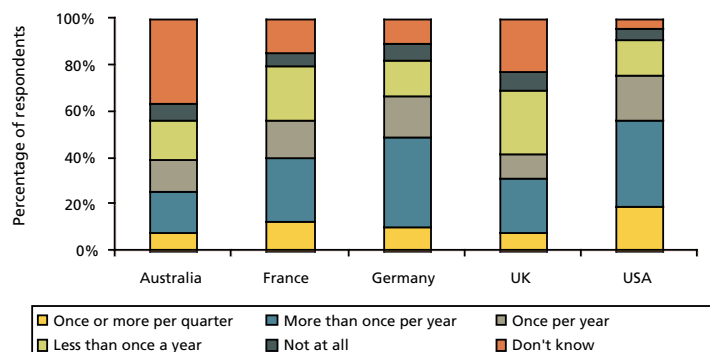
Awareness and Exposure

There's no question that there's a high level of awareness about security breaches involving exposure of confidential company data—customer financial information, employee Social Security numbers, intellectual property, and medical records, to name a few. The media's focus on regulatory compliance, along with its coverage of high-profile incidents, has certainly opened everyone's eyes, but awareness of the issue also comes from direct experience. In fact, only six percent of enterprises surveyed can state without hesitation that they've had no data leakage problems in the last two years. Geographical differences are also worth noting. In the United States and Germany, 80 percent of enterprises surveyed have experienced data leaks, while in the United Kingdom and Australia, the percentages hover in the 60 percent range.

While 60 percent of enterprises surveyed are cognizant of the problem because they've had data leakage issues, they are not 100 percent confident about their ability to track data leakage. In fact, most companies rate the effectiveness of their policies and solutions at 2.84 on a scale of one to four, with four indicating total confidence in their data loss prevention practices.

UK and Australian enterprises experience less data leakage

Approximately how often have data leaks, either intentional or accidental, occurred in your organization over the past two years?



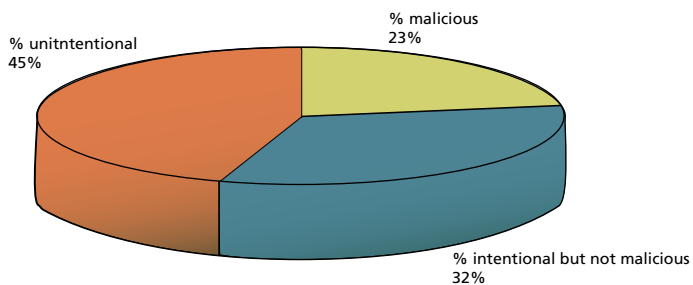
- Analysis of the trends by geography indicates German and US enterprises are the most likely to have experienced data leaks in the last year.
- Enterprises in the UK and Australia appear to have had the least experience of data leakage.

Intent: Malicious or Unintentional?

Today, data travels around the world and back again in seconds through many different channels. Global commerce, mobility, and data sharing with partners, contractors, and remote employees are a given for most enterprises, so opportunities for data leakage abound. Survey respondents identified removable storage devices—USB drives, CD-ROMs, and even MP3 players, along with corporate email and mobile devices or wireless access—as the main channels for data loss. This finding raises the question of what kinds of controls and technologies should organizations implement to prevent sensitive information from walking out the door and inviting catastrophe?

Malicious data leakage represents a serious problem

What percentage of data leakage do you think is malicious, what percentage is intentional but not malicious, and what percentage is unintentional?



- Enterprise IT decision makers believe that 55% of data leakage from their organizations is intentional. However, 58% of intentional data leakage is not malicious, such as emailing files to a home computer to work from home.
- Regardless, the finding that 23% of all data leakage is considered to be malicious is higher than Datamonitor anticipated, providing an indication of the scale of the threat that enterprises face.

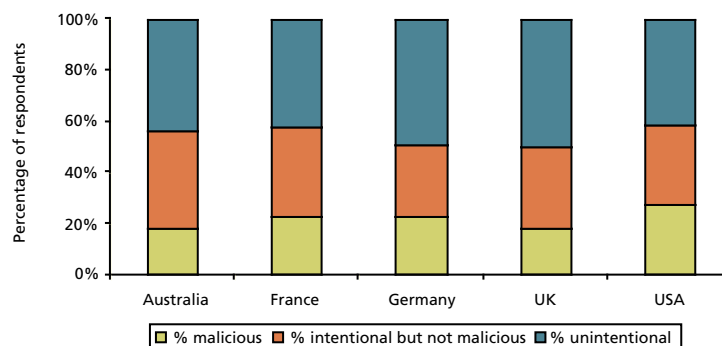
a textbook example of malicious data leakage that occurred at their own company, an Australian manufacturing firm with more than 10,000 employees. The night before a sales representative gave notice that he was leaving the company to join a competitor, he sent confidential pricing information to several customers via remote access.

While hacker attacks and exploits are certainly a cause for concern, 61 percent of respondents believe that data leakage is the doing of insiders. For the first time ever, Datamonitor has gathered facts and figures that offer insight into IT's perception of intent. Pointing the finger primarily at insiders, a surprisingly high 23 percent of all respondents said that the data loss was malicious (e.g., employees stealing company secrets or customer databases). Thirty-two percent of all interviewees said it was intentional but not malicious (e.g., copying a confidential legal agreement to a USB drive, so that one could work on it at home). And 45 percent of the total stated that it was unintentional (e.g., leaving a laptop or USB drive unattended in a public place). One of the interviewees described

Geographical analysis shows that the perception of intentional data leakage is higher in the United States and France (close to 30 percent) than in enterprises located in other countries (20 percent or lower). This could be a result of a more mobile workforce that travels frequently or works at home and routinely uses remote access, PDAs, laptops and cell phones.

US & French enterprises experience more intentional leakage

What percentage of data leakage do you think is malicious, what percentage is intentional but not malicious and what percentage is unintentional?



- Analysis of trends by geography suggests that the problem of intentional data leakage is slightly higher in the USA and France.
- Responses mirror trends in the regularity of data leakage more generally, with the UK and Australia appearing to be less likely to experience malicious data leakage.

Employee Resignations: An Overlooked Source of Information Leaks

DuPont, Duracell, and other corporations that are household names have been victimized by employees who have one foot out the door and one hand on sensitive company data. Employee resignations are, in fact, an often overlooked cause of data breaches, and it is a fair assumption that this high-risk group is responsible for a large proportion of malicious information leaks. It appears that many organizations don't take proper precautions when employees give notice. While 74 percent of enterprises provide training programs to increase employee awareness of data leakage, only 54 percent debrief and monitor employees before they leave the company. By failing to impose and enforce strict security policies and procedures, most enterprises are not walking their talk when it comes to monitoring and educating employees.

CASE STUDIES

Without Internal Controls, Insider Threats Flourish

In 2006 a DuPont employee stole \$400 million worth of proprietary information from his employer's database, but nobody realized it until he left DuPont for a rival firm. Later, it was discovered that he had accessed more than 15 times as many documents as the most active user of the system. He pleaded guilty.¹

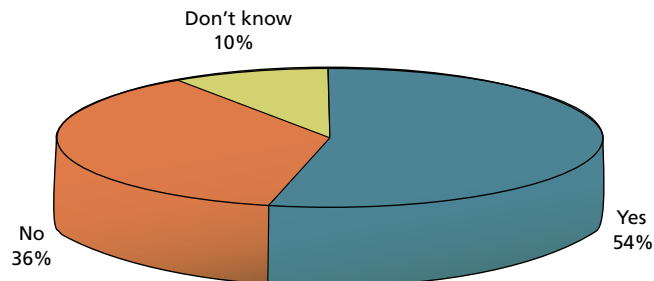
In a similar scenario, a cell development technologist at battery maker Duracell stole proprietary product research and emailed the information to his home computer. He then forwarded it to two Duracell competitors—presumably with the intention of cashing in on brokering the confidential information.²

¹ SOURCE: <http://www.eweek.com>

² SOURCE: <http://computerworld.com>

Enterprises are complacent about employee resignations

Do you take any special precautions against data leakage when an employee gives notice that he/she is leaving the company?



- Only 54% of enterprises take precautions against employees that are set to leave the company. This suggests a high degree of complacency among enterprises, given the risks that this group poses.
- Essentially, this finding suggests that data leakage policies and procedures are still far from reaching maturity among enterprises.

1. Locate and classify sensitive data. Confidential information—e.g., credit card information, Social Security numbers, trade secrets, product specifications—can be found just about anywhere in most organizations and in databases that reside on central servers, on laptops, in email inboxes, and even on USB drives. Enterprises need to know where their data is.

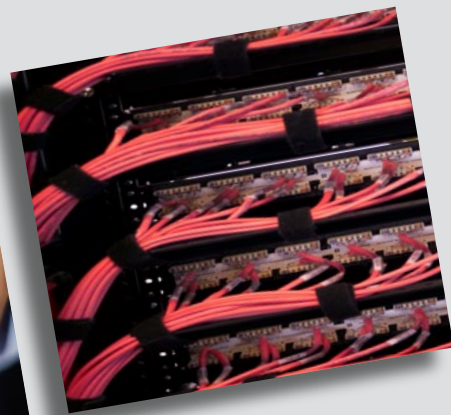
2. Take control of corporate data. Organizations must implement tools that can scan data according to where it lives and what type of data it is. Based on this information, they must set appropriate controls on how the information is used and who is allowed to use it.

3. Monitor endpoints. In today's mobile world, data travels far and wide on laptops that have remote access, USB drives, CD-ROMs, and even MP3 players. Organizations should deploy agent-based security solutions that maintain a constant vigil on desktops, tracking and blocking sensitive data.

4. Keep an eye on data flow. Organizations need to monitor where data is coming from and where it is going in the normal course of daily business with gateway and host solutions. It is critical to find out what information is leaving the network via email, instant messaging, webmail, and FTP. Gateway tools issue alerts when they detect sensitive data that is about to leave the network and can go a step further by blocking or encrypting it.

5. Enforce policies. Staff must be trained and educated on a regular basis on the importance of data leakage prevention through classes and distribution of updated best practices and security policies. Employees who have given notice must be tracked and thoroughly debriefed at exit interviews before they walk out the door for the last time. And employees must be made aware that there will be disciplinary action for infractions of policy.

6. Store critical data in a central location. Work with the IT department to create a secure repository for confidential information on a central server with airtight, permission-based access. By storing key data in a central location, it is easier to monitor its whereabouts with centralized management solutions that provide detailed reporting and monitoring.



Taking Punitive Action

Nearly half of the enterprises surveyed are oblivious to the potential for data loss at the hands of employees who resign. Only 54 percent debrief employees when they leave the company. But significantly, 88 percent have opened their eyes to the seriousness of the issue after the fact and have considered taking punitive action against partners, contractors and staff who have engaged in this serious form of theft. And 55 percent of enterprises in all geographical locales have disciplined an employee, contractor, or staff member once a data leak has been discovered. **Up to 60 percent have gone so far as to dismiss employees.** With its weaker labor protection laws, it is not surprising that the United States scored the highest in disciplining employees for malicious data loss incidents.

Third parties—partners, contractors, and vendors—that do business with enterprises on a daily basis are also a cause for concern. **Sixty-five percent of enterprises surveyed keep partners at arm's length, imposing conditions on them as a way of minimizing data loss.** More than a quarter of the companies in this study choose not to share any data at all with partners which illustrates the extent to which data leakage is taken seriously.

STEAL DATA, GET FIRED!

In the United States, employees who steal confidential data are more likely to lose their jobs than their French and German counterparts. Sixty percent of American enterprises terminated employees who were involved in data loss incidents, compared to 40 percent of companies in France and Germany.

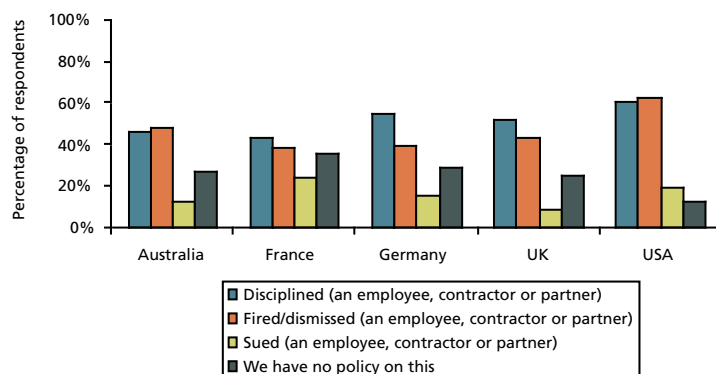
DATA LOSS PREVENTION CONSIDERATIONS

The high level of data leakage activity by insiders raises a host of questions that enterprises need to consider:

- ➔ Is security technology robust, appropriate and far-reaching enough to provide host and network data loss prevention? Does it offer adequate monitoring with a centralized view of security status, and easy-to-access reporting capabilities?
- ➔ Are data security policies and best practices updated and communicated to employees on a regular basis?
- ➔ Are policies being enforced?
- ➔ If IT suspects that a large portion of employees are engaged in corporate data theft, then how many insiders are actually getting away with it?

Employee dismissals are greatest in the US

Has your organization ever disciplined, fired or sued an employee, contractor or partner because confidential data was leaked?



- Perhaps unsurprisingly, given its weaker labor regulations, employee discipline relating to data leakage appears to be more widespread in the US than in other geographies.
- Generally, however, enterprises in all geographies are prepared to act on this issue.

A High Price to Pay

There's a good reason why 33 percent of enterprises surveyed believe a data breach can shut down their businesses. Breaches are extremely costly in dollars and cents, and there's also the less tangible, but equally important cost to brand and reputation. The majority—77 percent—were unable to track and audit losses after a data breach. Based on the responses of the 23 percent of respondents who could provide an estimate, the average cost of a data leakage incident was \$1.82 million.



LOST IN TRANSIT

Recently, a CD containing the private data—names, birth dates, and Social Security numbers—of 2.9 million Medicaid recipients was lost in transit. Officials at the Georgia Department of Community Health could not say for certain whether the data was encrypted, and they do not currently know the name of the transportation company that shipped the disk.

SOURCE: <http://www.computerworld.com>

Most high-profile stories in the media today address the type of data loss that affects people on a personal level—credit cards, Social Security numbers and other private personal information. Indeed, this is something we should all be concerned about. Identity theft takes a toll on economies worldwide. In the United Kingdom, the Home Office estimates the cost of identity theft at \$3.2 billion during the last three years. The Australasian Centre for Policing Research places the cost of identity theft at \$3 billion annually. And while the costs are high for the individual, breaches involving customers' personal information can be financially damaging for enterprises as well. On average, companies spend \$268,000 just to inform their customers when such disasters occur.

SECTION 05

With large enterprises, there is even more cause for concern, but it is something rarely covered in the news and may be underreported to corporate stakeholders as well. Intellectual property and financial information are rated as the two most valuable classes of data—\$1.68 million on average. This figure covers loss of potential revenues that could result if a competitor got its hands on proprietary product specifications and went to market first. It also covers IT costs, including policy changes, investment in new security technologies, time invested in auditing and monitoring, and compliance fines. If this is what keeps IT personnel awake at night, clearly the issue is not getting much media attention and not enough management attention.



The lack of attention placed on protecting these two critical types of data calls into question a company's fiduciary responsibility. Intellectual property and financial data are the lifeblood of an enterprise—and are tied to the bottom line. If these assets are at risk, the company's share price and valuation are at risk, and shareholder confidence is likely to plummet. It doesn't take much imagination to visualize the inevitable conclusion if this should occur.

The responsibility to safeguard key assets rests not only with IT, but also with executive management and the board of directors. Sixty-three percent of interviewees believe that their board of directors provides them with adequate resources to protect valuable company data. On the other hand, a large percentage—37 percent of respondents—do not feel that their board of directors is supporting them in their endeavors to reduce data loss. Does this suggest that a large percentage of boards are apathetic when it comes to data loss? Does it mean that those at the helm are lulled into a false sense of complacency; perhaps they feel that since no one else is solving the problem and they are doing the best they can, why worry? Most IT budgets constitute four to five percent of a company's total spend at most. Of the five percent invested in IT, only 10 percent of that is allocated to security. With such a small percentage of dollars invested in data security, perhaps IT decision makers feel that they cannot fight a losing battle that no one wants to acknowledge as important. After examining the financial losses and the potential damage to reputation and erosion of customer confidence, isn't it time everyone in the boardroom sat up and took notice?

CONCLUSION

A single data breach can run a prosperous, well-respected company into the ground virtually overnight. There's not a shadow of a doubt that most enterprises are aware of the magnitude of damage that information leakage can leave in its wake, as this new research has revealed. Awareness is an important first step, but it is not enough to forestall disaster. **Every enterprise needs to make data loss preparedness a priority.** It is up to the key decision makers—board members, C-level executives, and IT—to allocate sufficient resources and follow best practices for proper corporate governance. They owe it to all their stakeholders—shareholders, employees, suppliers, customers, partners and the community at large. By establishing data loss prevention policies, educating employees, and implementing technologies that automate and simplify enforcement and monitoring tasks, large organizations can prevent data breaches and focus on their business goals. It is only by taking responsibility that enterprises can maintain a global commerce environment that is flexible, collaborative and innovative. **It is not too late—at least not yet.**

WHILE THEY WERE SLEEPING...

Information stolen from \$16 billion retailer TJX, parent company of TJ MAXX (known as TK MAXX in Europe), was being used fraudulently in an \$8 million gift card scheme. TJX officials didn't learn of the breach until a month later, in December 2006. The mega-retail chain said that a large portion of the information was accessed as early as 2005, and the data went as far back as 2003. What went wrong? TJX relied solely on encryption to protect customer credit card data, but obviously this wasn't enough.

SOURCE: <http://www.eweek.com>



Scope of the Research

FOCUS OF THE SURVEY

In April 2007, McAfee commissioned Datamonitor to measure IT perception about data leakage in large enterprises of 250 or more employees as a way of gauging how much of a threat this problem poses to businesses worldwide.

The aim of the survey was to determine the prevalence of data loss incidents—both accidental and malicious—and to assess the level of awareness, perceived costs, and proactive measures that organizations are taking in the face of this serious security issue. Datamonitor defines data leakage as “the accidental or malicious loss of confidential data.” In the context of this research, data leakage was not associated with loss of data due to failed backups or erased hard drives.

DEMOGRAPHICS AND METHODOLOGY

Datamonitor conducted an online survey to gather information from 1,408 IT decision makers and other key stakeholders at major enterprises to gain insight into their views about data leakage.

THE MARKETS:

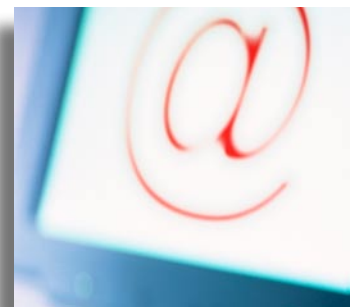
- United States
- United Kingdom
- France
- Germany
- Australia

THE ORGANIZATIONS

- Revenues ranging from US\$10 million to more than \$1 billion
- A minimum of 250 employees, with 75 percent of the companies having 1,000 or more employees
- A broad cross-section of vertical industries, from nonprofits and healthcare to manufacturing and financial services
- Interview respondents comprised IT decision makers, including IT directors, network administrators, database administrators, developers, and others

DATAMONITOR

McAfee selected Datamonitor to conduct this research based on its best-practice methodologies and its reputation as one of the world’s leading providers of online data, analytic and forecasting platforms for key vertical sectors. The global research company has tracked the IT, business and market dynamics of more than 10,000 corporate clients in six industry sectors.





McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 - 2007 McAfee, Inc. All rights reserved. Datagate-bro-0407