




Data Protection Solutions at Midsize Organizations

DATA LEAK PREVENTION 

 **Study Results from
Data Leakage Business Survey**

An IDG Business Study Sponsored by Trend Micro
February 2008

Data Protection Solutions at Midsize Organizations

 **TABLE OF CONTENTS**

OVERVIEW.....3

PROFILE OF RESPONDENTS.....3-5

EXECUTIVE SUMMARY.....6

DATA LEAKAGE AND PROTECTION AGAINST INFORMATION SECURITY BREACHES.....6

REASONS FOR DATA LEAKS.....7

PROTECTION AGAINST DATA LEAKS.....7

LEVEL OF CONCERN ABOUT DATA LEAKAGE FROM VARIOUS SOURCES.....8

ACTUAL DATA LEAKS AT RESPONDENTS' ORGANIZATIONS.....9

MEASURES TAKEN TO PREVENT DATA LEAKS.....10

PROTECTING MOBILE DATA.....10

SECURING REMOTE ACCESS TO THE COMPANY NETWORK.....11

SECURING MISSION-CRITICAL WEB APPLICATIONS.....11

SPENDING FOR DATA LEAKAGE PREVENTION.....12

CONCLUSION.....12

Data Protection Solutions at Midsize Organizations

OVERVIEW

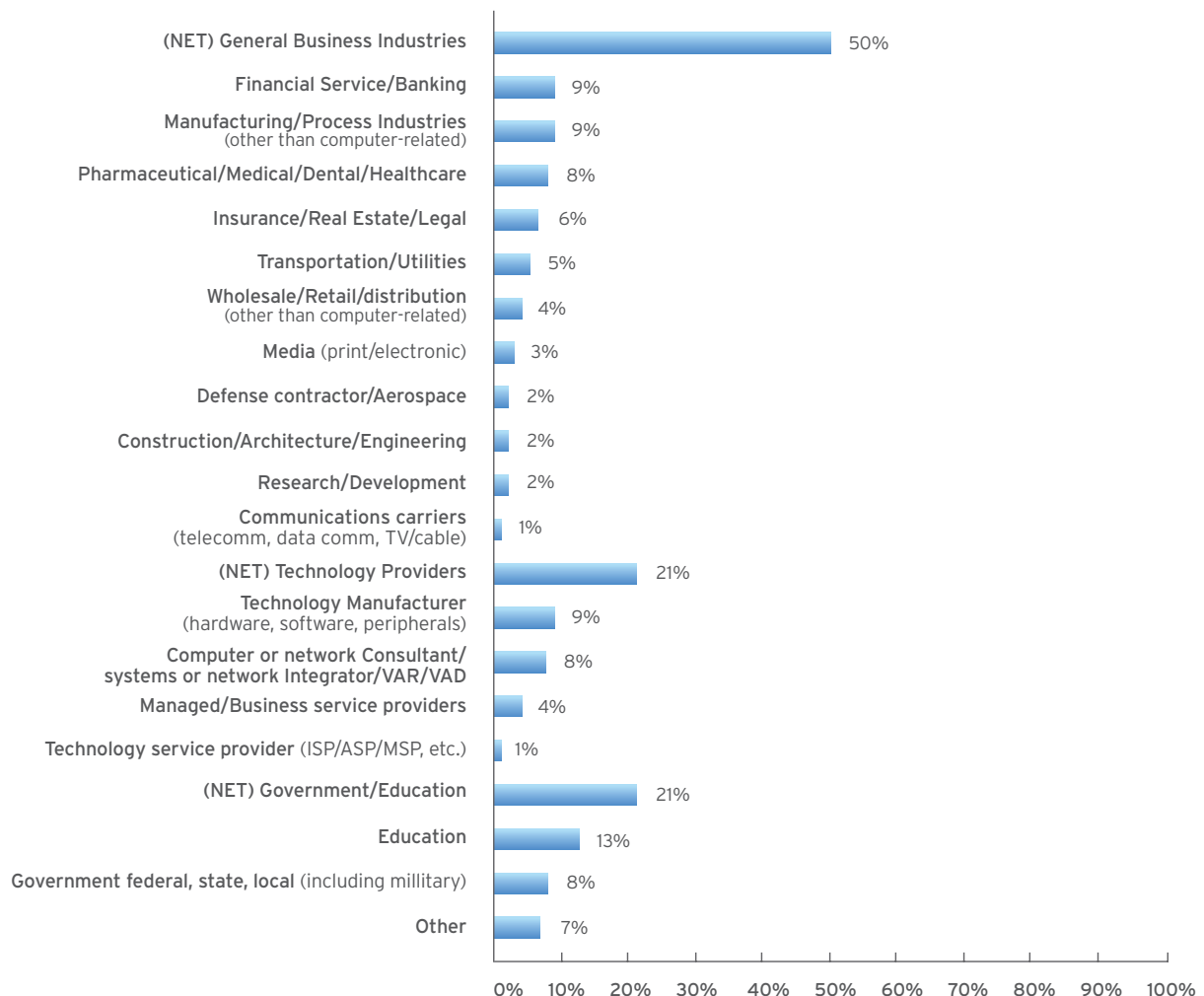
In January of 2008, a random sample of online technical newsletter subscribers at midsize companies (100-5,000 employees) received an email invitation to participate in a survey about data protection solutions use at their organizations. The goal of the survey was to identify sources of and/or reasons for information security breaches, and to better understand how businesses are planning to protect themselves against data leaks. The following report presents top line results of the study.

PROFILE OF THE RESPONDENTS (Total respondents: 131)

All 131 respondents were required to have involvement in the acquisition or implementation of data protection solutions at companies with between 100 and 5,000 employees worldwide. The following charts provide a more specific breakdown of key respondent demographics.

PRIMARY BUSINESS OR INDUSTRY

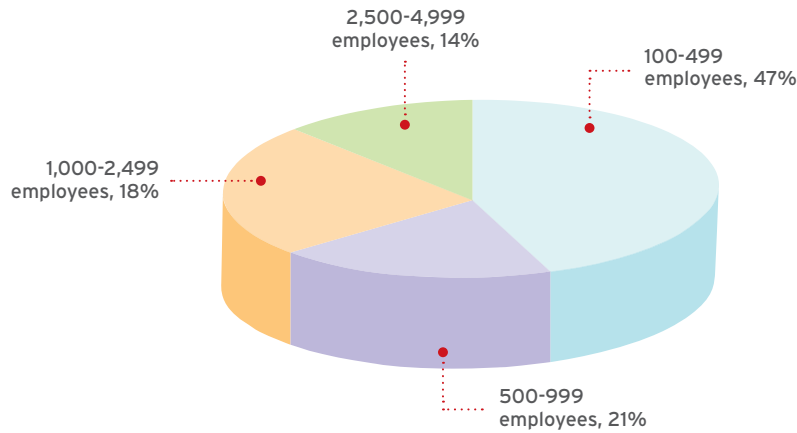
- Which of the following best describes your company's primary business or industry?



Data Protection Solutions at Midsize Organizations

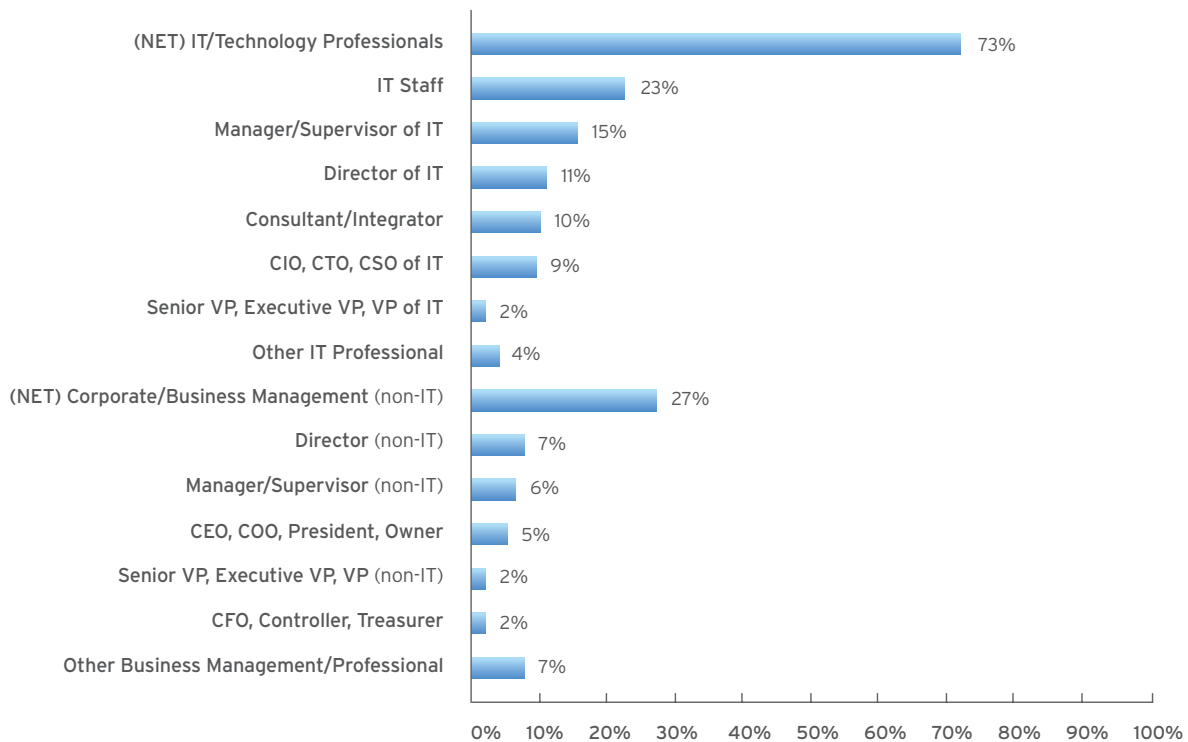
COMPANY SIZE

- How many people are employed in your entire company, including all branches, divisions and subsidiaries?



JOB TITLE

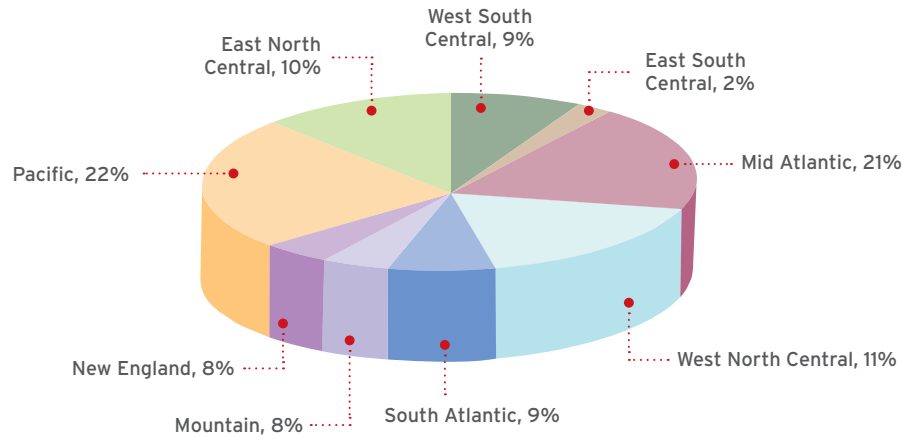
- What is your title?



Data Protection Solutions at Midsize Organizations

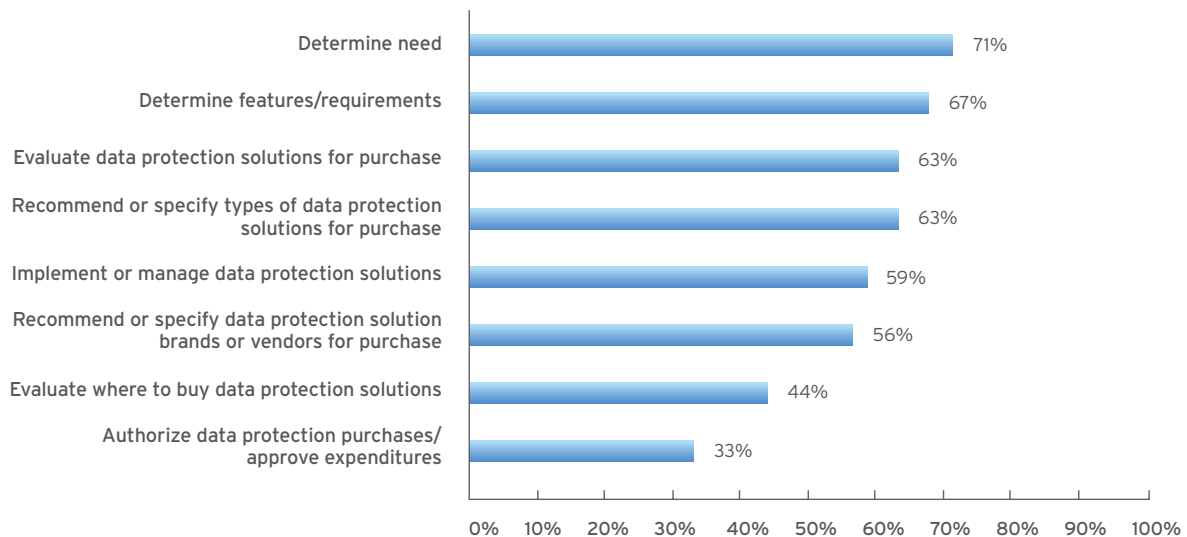
PRIMARY LOCATION

- What is your primary office location?



INVOLVEMENT WITH THE ACQUISITION OR IMPLEMENTATION OF DATA PROTECTION SOLUTIONS

- In which of the following ways are you personally involved in the acquisition or implementation of data protection solutions for your company?



Data Protection Solutions at Midsize Organizations

EXECUTIVE SUMMARY

Data leakage continues to be a major concern for businesses nationwide. Undoubtedly, the traditional workplace landscape is changing in ways that make protecting data more and more challenging. With a growing number of businesses now able to offer employees remote access to their company networks and infrastructure, the need to secure mobile technologies has increased dramatically.

Although there is always the potential threat of malicious outsiders hacking into company systems and gaining access to proprietary or confidential information, businesses generally feel well protected against these intruders with traditional firewalls and anti-virus software. Companies are finding that the most challenging sources of data leakage are internal, most often as a result of employee mistakes or carelessness. Without the proper security measures in place, employees can unknowingly put extremely important data at a very high risk of accidental exposure.

Fortunately, organizations are becoming increasingly aware of the data risks posed by internal sources, and are taking the appropriate measures to minimize the occurrence of such breaches.

DATA LEAKAGE AND PROTECTION AGAINST INFORMATION SECURITY BREACHES

Data leakage, not surprisingly, is a major source of apprehension to organizations. For the purposes of this survey, respondents were asked to rate how well each of the following statements define the term data leakage.

Definition 1:

"Data leakage is a physical or virtual breach of confidential or proprietary content occurring either as a result of malicious intent or mistake."

- • • 86% agree that this statement defines data leakage well (rating 4 or 5 on a 5-point scale where 5 = defines very well)

Definition 2:

"Data leakage is when content meant only for need-to-know individuals falls into the hands of someone who is not classified as need to know."

- • • 76% agree that this statement defines data leakage well (rating 4 or 5 on a 5-point scale where 5 = defines very well)

Definition 3:

"Data leakage is when confidential content has breached a pre-defined restricted area."

- • • 65% agree that this statement defines data leakage well (rating 4 or 5 on a 5-point scale where 5 = defines very well)

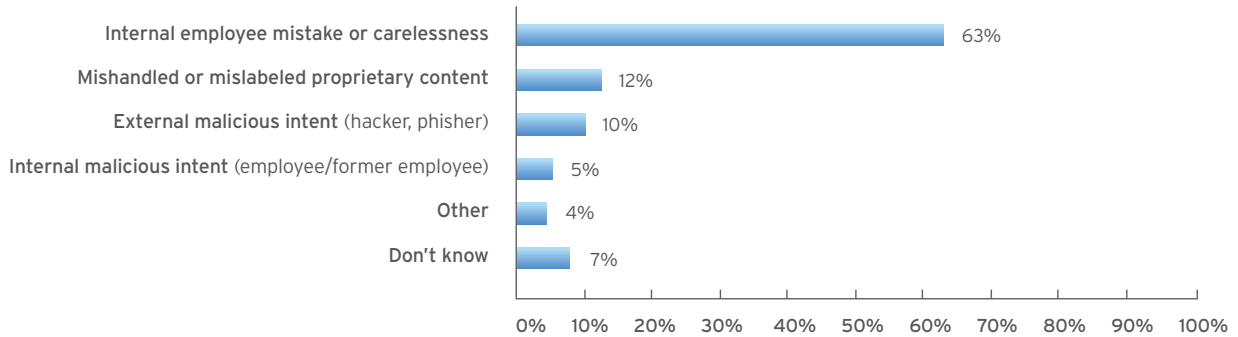
Roughly two-thirds of the respondents (66%) rate data leakage as a serious concern (rating "4" or a "5" on a 5-point scale where "5" is a very serious concern). Just one respondent indicates that data leakage is of no concern at all to his organization.

Data Protection Solutions at Midsize Organizations

REASON FOR DATA LEAKS

Internal employee mistakes or carelessness (63%) is by far the most frequently cited reason for data leakage at respondents' organizations. This is distantly followed by mishandled or mislabeled proprietary information (12%), external malicious intent (10%) and internal malicious intent (5%).

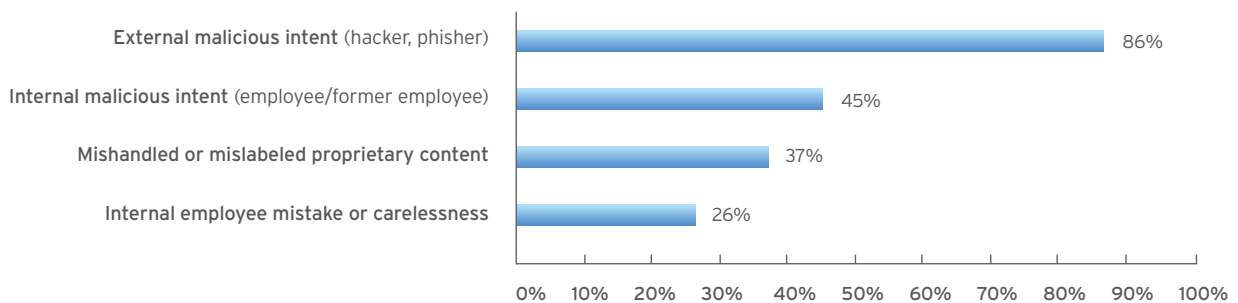
- What is the primary reason for data leaks at your company?



PROTECTION AGAINST DATA LEAKS

While 86% of respondents believe that they are extremely or well protected against external malicious intent (hackers, phishers, etc.), only one-quarter of respondents (26%) feel protected against internal employee mistakes or carelessness.

- How well protected do you feel your company is against each of the following types of data leaks?

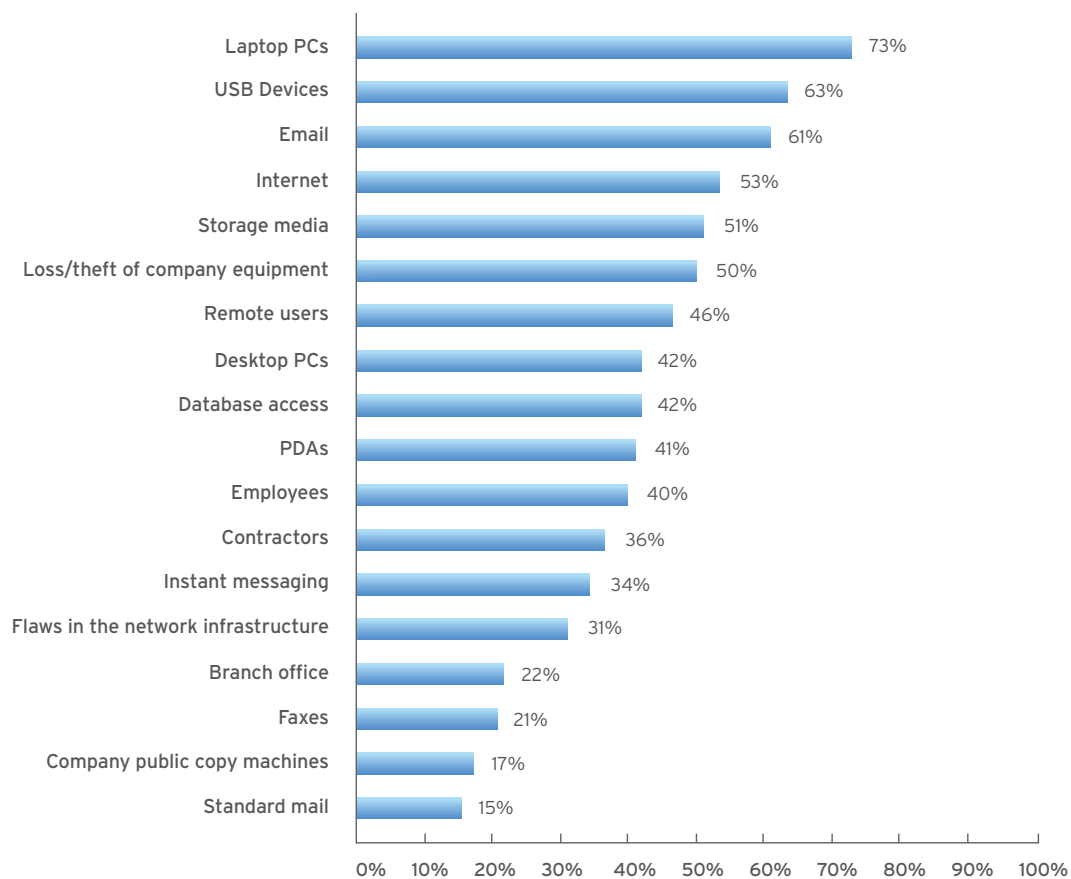


Data Protection Solutions at Midsize Organizations

LEVEL OF CONCERN ABOUT DATA LEAKAGE FROM VARIOUS SOURCES

Companies are most concerned about data leaks from mobile devices such as Laptops and USB devices. Because organizations also tend to be apprehensive about entities that do not have a permanent physical location, email and Internet fall close behind. Other top sources of concern include storage media, loss/theft of equipment and remote users. Interestingly, because so few businesses rely heavily on standard mail, it is less likely to be considered as a major concern for data leaks.

- Please rate how concerned your organization is about data leakage from each of the following sources



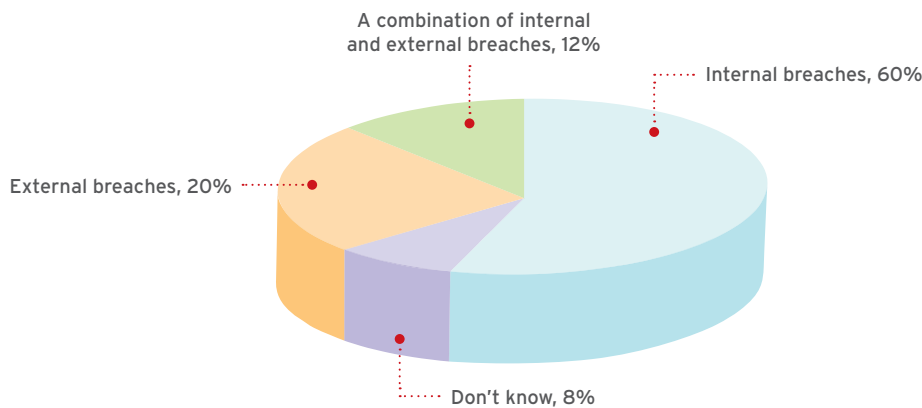
Data Protection Solutions at Midsize Organizations

ACTUAL DATA LEAKS AT RESPONDENTS' ORGANIZATIONS

While one in five respondents (19%) report that their companies have experienced data leakage over the past 12 months, 32% are unsure. Among those who have experienced data leaks, almost two-thirds (60%) report that these breaches were from internal sources.

- What was the primary source for the data leaks?

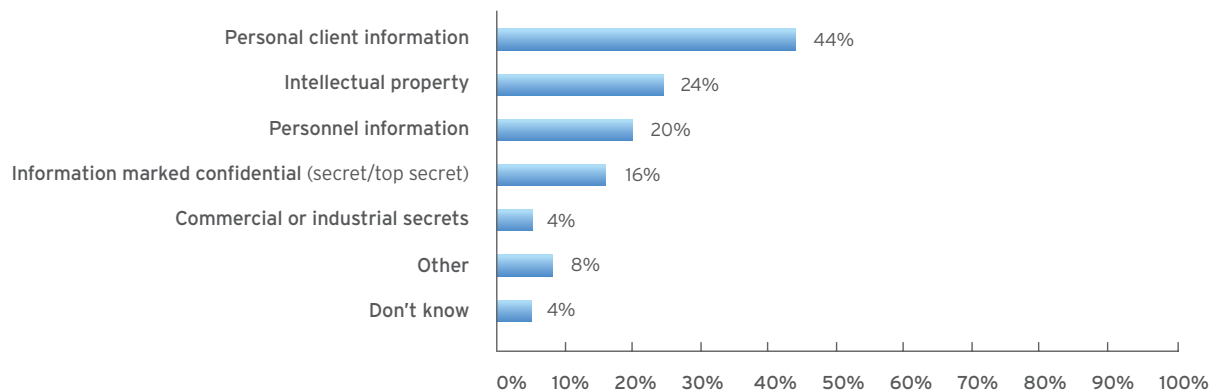
(Among the 25 respondents whose companies have experienced data leakage over the last 12 months)



Among respondents whose companies have experienced data leakage in the past year, personal client information was the type of data most likely to be compromised, followed by intellectual property and personnel information. While 4% are unsure of what type of information was leaked, commercial or industrial secrets appear to be the most well-guarded types of information.

- What type of information has been leaked?

(Among the 25 respondents whose companies have experienced data leakage over the last 12 months)

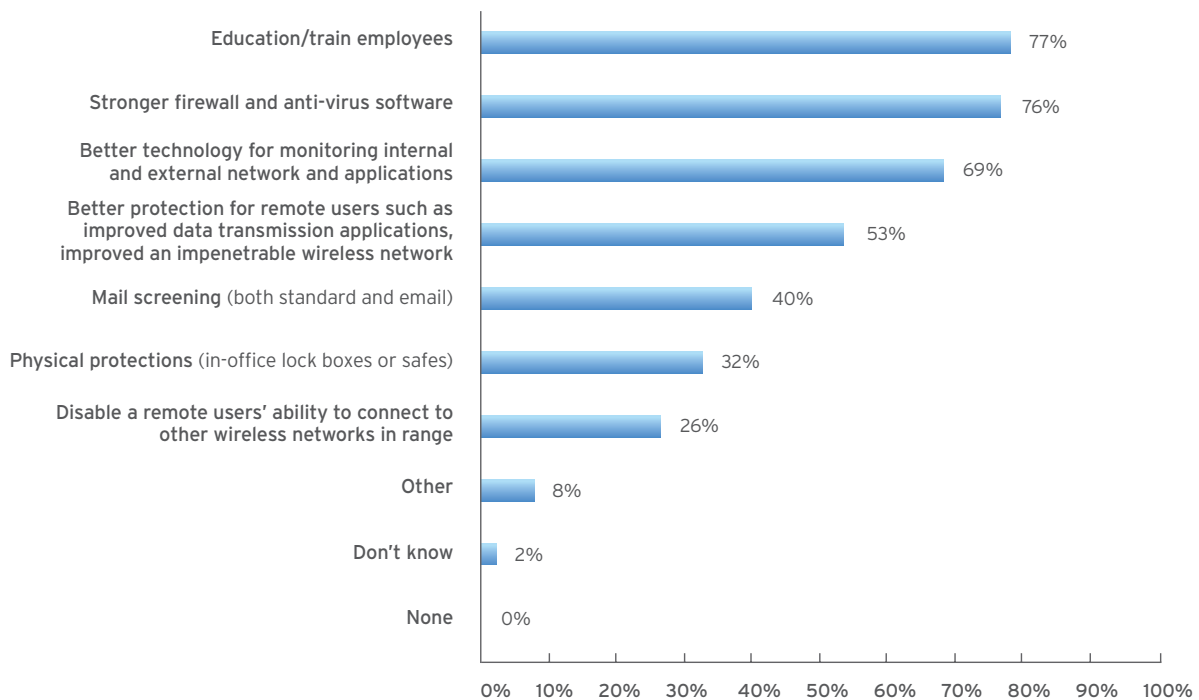


Data Protection Solutions at Midsize Organizations

MEASURES TAKEN TO PREVENT DATA LEAKS

Companies are becoming more and more vigilant in their pursuit to prevent data leakage. Some of the ways in which businesses are attempting to minimize the occurrence of data leakage include: education and training for employees, stronger firewall and anti-virus software, and implementing better technology for monitoring internal and external networks and applications. All of the respondents indicate that their organizations are taking some type of measure to prevent data leakage, as illustrated on the following chart.

- What measures is your company taking to prevent data leaks?



PROTECTING MOBILE DATA

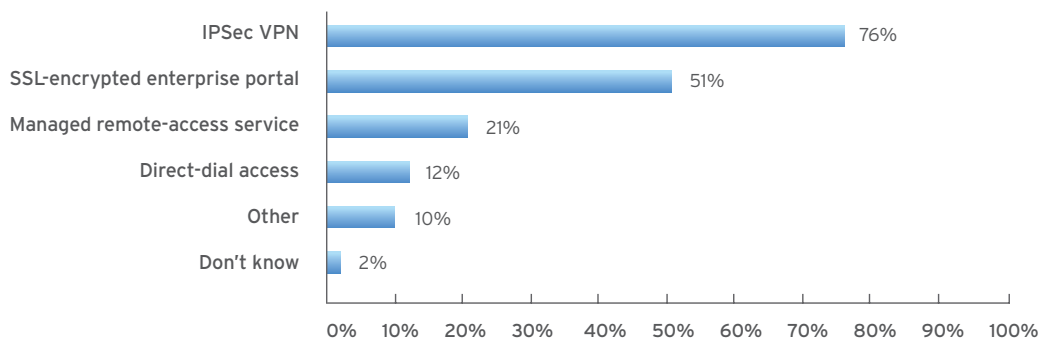
One quarter of respondents (24%) claim to have measures in place today that are above the level of encryption, while 57% say they do not, and 19% are unsure. Respondents report that mobile workers make up 22% of the workforce, on average. Just over one-half (53%) of respondents' companies have existing policies in place for protecting mobile data. Strikingly, despite the growing number of mobile employees, 40% of respondents' companies still do not have such policies in place.

Data Protection Solutions at Midsize Organizations

SECURING REMOTE ACCESS TO THE COMPANY NETWORK

Over three-quarters of respondents (76%) indicate that their companies secure remote access to their network through IPSec VPN. Other ways companies secure remote access include SSL-encrypted portals, managed remote-access service, and direct-dial access.

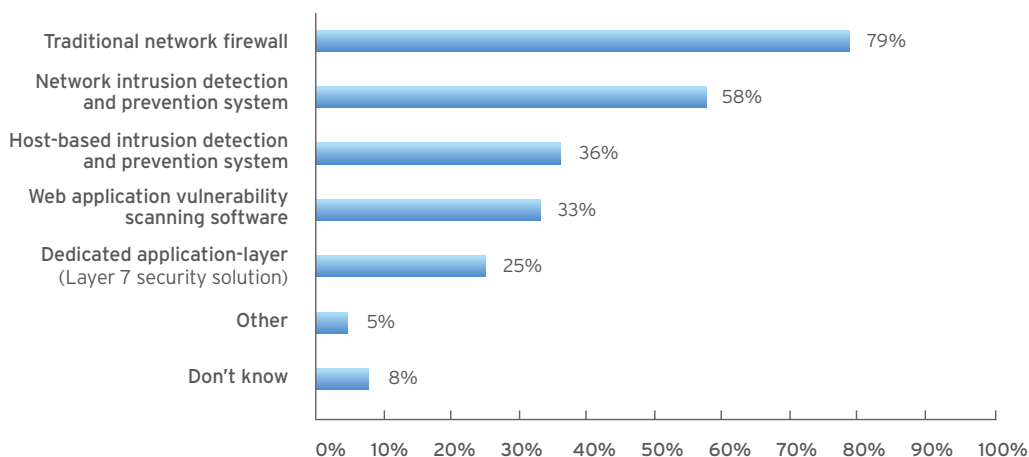
- How does your company secure remote access to the company network?



SECURING MISSION-CRITICAL WEB APPLICATIONS

Respondents typically secure their mission-critical Web applications by using traditional network firewalls (79%), while 58% use network intrusion detection and prevention systems. Other methods used by respondents' companies to secure mission-critical Web applications are presented in the chart below.

- How does your company secure mission-critical Web applications?

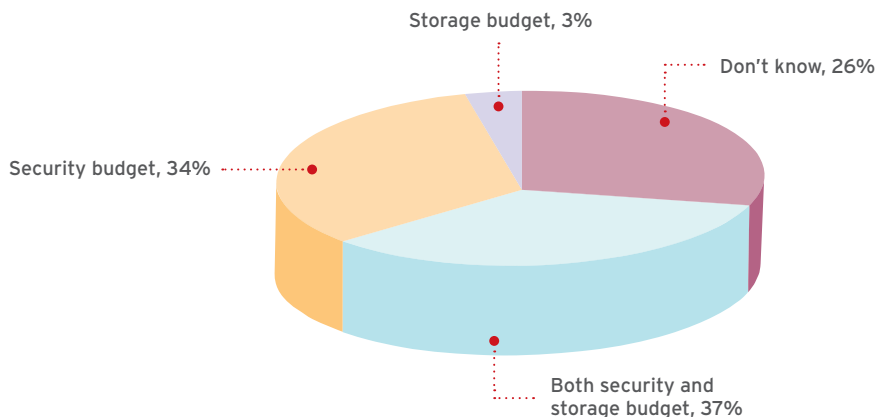


Data Protection Solutions at Midsize Organizations

SPENDING FOR DATA LEAKAGE PREVENTION

The average amount spent annually on data leakage prevention is \$144,980, representing an average of 8% of a company's total annual IT budget. The funds for data leakage protection solutions most frequently comes from either the security budget alone (34%) or from both the security and the storage budget (37%).

- Where does the money for data leak prevention at your company come from?



CONCLUSION

Data leakage will continue to be a problem area for businesses. As the workplace continues to mold and shift with the emergence of new technologies, companies will constantly be required to update their means of protecting the most critical data. Many organizations are already taking steps towards becoming more secure, including educating and training employees to handle sensitive materials, as well as making sure that their firewalls and anti-virus software are always up-to-date.

The good news is, while most of the data leaks experienced by respondents to this survey are internal, that also makes them the most preventable. With education of staff and closer monitoring of the internal and external networks, companies can feel confident that they are doing their part to reduce the threat of future security breaches.

While mobile devices continue to worry business executives, the technologies for securing remote access are also improving. As the global workforce increasingly becomes more mobile, companies need to continue to train users to be aware of possible threats, and also ensure that the security products and services they select to support mobile network users are able to keep pace with ever-changing security needs.

TREND MICRO INC.

10101 N. De Anza Blvd. Cupertino, CA 95014

• US toll free: 1+800-228-5651 • phone: 1+408-257-1500
• fax: 1+408-257-2003 • www.trendmicro.com

Research Conducted by:

IDG RESEARCH SERVICES

3 Speen Street, Framingham, MA 01701

