

***Blind Faith:
Executives Rely on Incomplete
Solutions, Organizations Vulnerable
to Private and Confidential
Information Leaks***

Information Security Study
US-based Organizations
May 2006

Study conducted by:

THE INSIGHT Advantage
2397 Hecate Court
San Jose, CA 95124 U.S.A.
Tel: 408-358-0700
Fax: 408-904-5062

Info@TheInsightAdvantage.com

SPONSORED BY:



Table of Contents

Table of Contents.....	2
Executive Overview.....	3
Detailed Findings	4
Importance of Protecting Information.....	4
Confidence Level & Concern	4
Awareness & Visibility.....	5
Enforcement Solutions.....	6
Conclusion	7
About The Insight Advantage	7
About Workshare	8

Executive Overview

Objective

The objective of the Information Security Study was to gather insight from potential and existing Workshare Protect Enterprise Suite customers regarding the challenges they face in protecting organizational information that is considered confidential, financial or private customer data.

Methodology

Over 37,000 email invitations to participate in a web-based survey were sent in early April to executives who have the following responsibilities in U.S.-based organizations with at least 1,000 employees: IT Security, Risk, Privacy, Compliance, and In-House Counsel. Out of the 575 executives who initiated the survey, 359 completed it, resulting in a 62% completion rate. Both qualitative and quantitative questions were asked in the study.

Key Findings

A number of key findings emerged from the study, including:

- 94% of respondents either believe email messages containing confidential or private information are leaving their organization each month or simply don't know if this is happening.
- 80% of participants reported having information leaks or admitted to no visibility into leaks that occurred within their organization last year. Of those, 17% were afraid to know how many leaks they had.
- Over 70% know that PDF conversion does not secure information. Alarming, 46% are still relying on PDF to enforce their information security policies.
- 68% stated personally identifiable customer data poses the greatest information risk and 56% said a leak of this type would result in their company losing customers.
- 57% don't have a specific method for enforcing data privacy and document security policies.
- While 100% of respondents consider it important to protect information within their organizations, 80% consider it "extremely important."

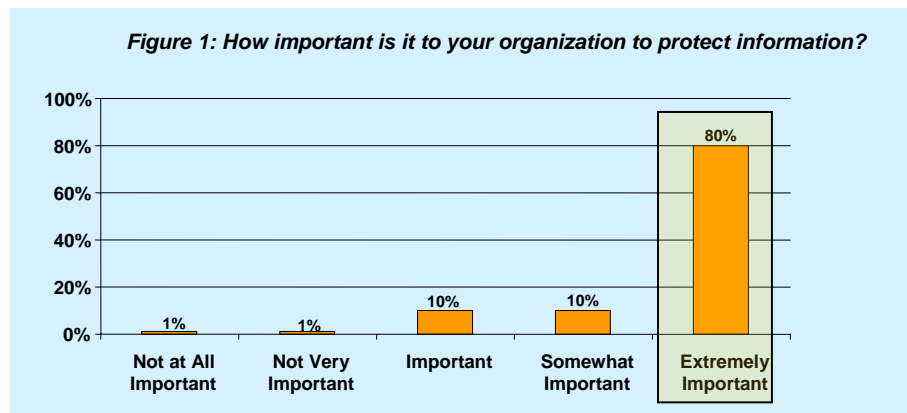
Conclusions

The study shows that the level of awareness about the risks and cost of information leaks is high. However, the study also confirms that the recent rash of publicized information leaks is only the tip of the iceberg; information is leaking out of organizations in large volumes. Moreover, executives responsible are running on blind faith that the incomplete solutions they have deployed are enough--despite their concern over and the existence of information leaks via electronic channels. This survey serves as a wake up call to develop and implement a comprehensive data leak prevention assessment and risk mitigation plan.

Detailed Findings

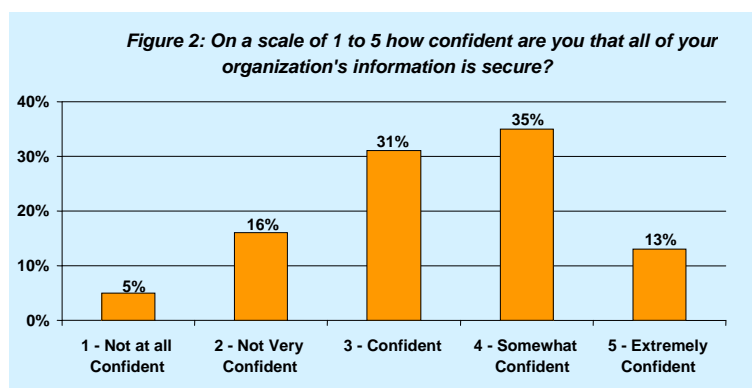
Importance of Protecting Information

As illustrated in *Figure 1*, 80% of participants consider it extremely important to protect information within their organizations, and nearly all consider it important.

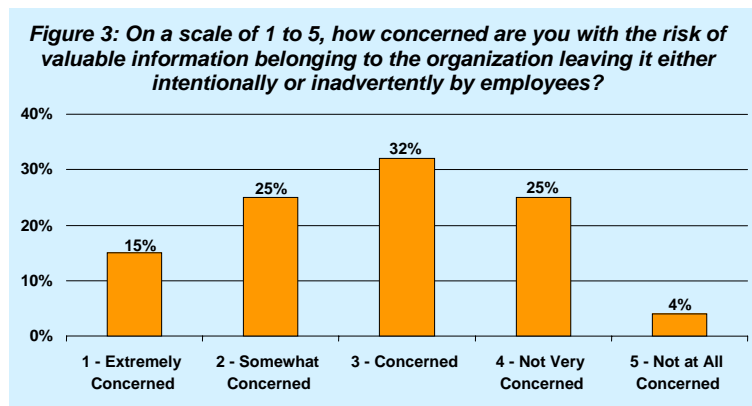


Confidence Level & Concern

As illustrated in *Figure 2*, those we surveyed, are only mildly confident that their organization's information is secure.

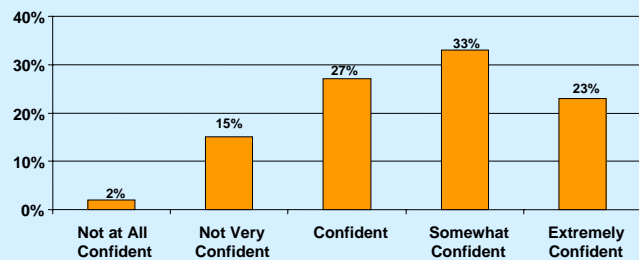


As *Figure 3* highlights, 96% of those we surveyed are concerned about the risk of employees distributing valuable information such as personally identifiable customer data, financial information or intellectual property belonging to the organization; only 4% were not concerned. In an ideal situation, the confidence level shown in *Figure 2* would align with the level of concern; however, it does not, and the disparity is significant and alarming.



Only 56%, as shown in *Figure 4*, of respondents have a relatively high level of confidence that employees understand the importance of maintaining confidential information.

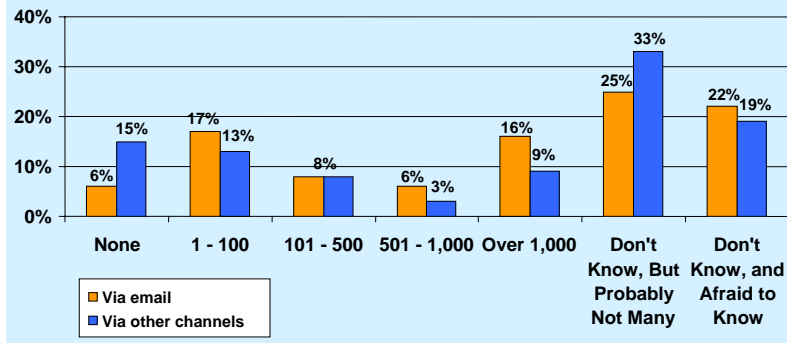
Figure 4: How confident are you that employees understand the importance/value of the organization's confidential information?



Awareness & Visibility

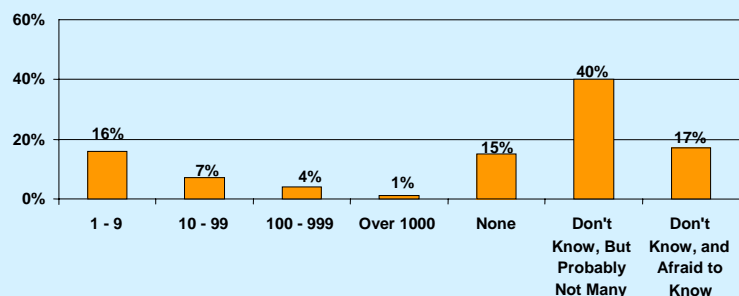
Figure 5 highlights that 94% of respondents either believe email messages containing confidential or private information are leaving their organization each month or simply don't know if this is happening. In addition, *Figure 5* indicates that information is leaking not only through email, but also through other channels such as HTTP, ftp, and instant messaging.

Figure 5: How many messages are leaving your company each Month containing confidential data?



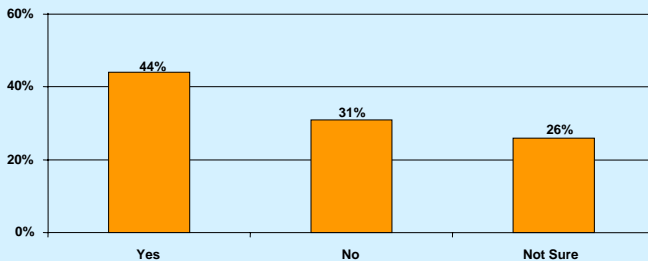
As *Figure 6* illustrates, 57% of those we surveyed have no visibility into the number of risky information leaks that occurred the previous year and only 15% reported zero information security breaches last year. Given the significance that these findings indicate, information is leaking out of organizations consistently and the protectors of an organization's lack visibility into what and how much is leaving.

Figure 6: Approximately how many leaks of dangerous or risky information occurred in your organization last year?



Enforcement Solutions

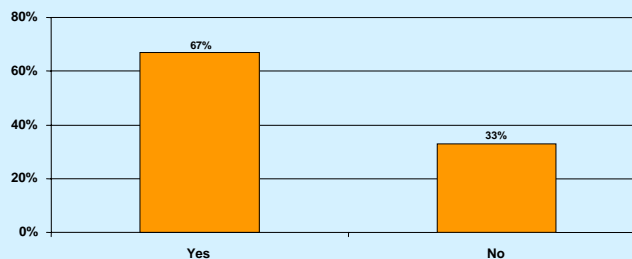
Figure 7: Does your organization have a method of automatically enforcing internal information privacy or document security policy compliance?



As shown in *Figure 7*, only 44% of participants reported having a “solution” for automatic enforcement. 57% either do not have such a method or are unsure whether they have such a method.

As illustrated in *Figure 8*, the majority of organizations we surveyed reported having “solutions” in place to secure information within the corporate perimeter. However, given the lack of visibility and prevalence of information leaks, most solutions employed today are ineffective.

Figure 8: Does your organization have solutions in place to secure information within the corporate perimeter?



As shown in *Figure 9*, the most commonly used point solutions for enforcing information security policies is document and email encryption. In addition, nearly a quarter of respondents still use PDF conversion as an enforcement technology.

Figure 9: What technologies are you currently using to enforce information policies?

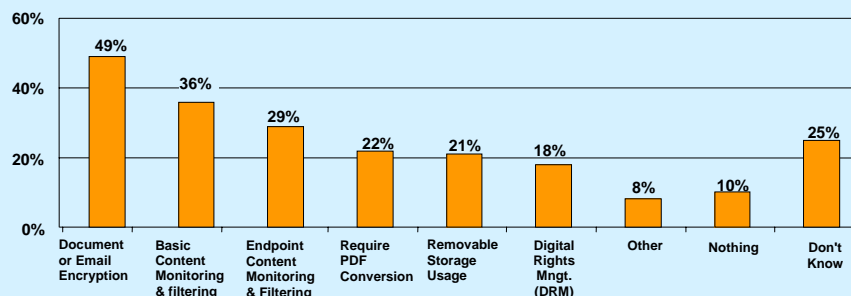
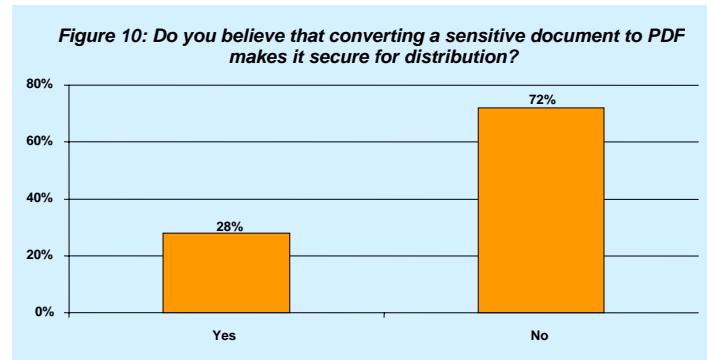


Figure 10 illustrates that 72% of those we surveyed know that that converting to PDF does not secure documents--yet it still remains as an enforcement solution.



Conclusion

Over 37,000 email invitations to participate in a web-based survey were sent in early April 2006 to executives who have the following responsibilities in U.S.-based organizations with at least 1,000 employees: IT Security, Risk, Privacy, Compliance, and In-House Counsel. Executives who participated in the study represented a broad spectrum of industries, including financial services, government, manufacturing, technology, insurance, and healthcare. Results gathered from the 359 executives who participated in the study showed an overwhelming awareness of information security enforcement challenges and the fact that attempts to solve them through point solutions like PDF conversion, encryption and other inadequate technologies are simply not effective. Executives are most concerned about customer data leaking and the subsequent impact, especially negative perception of the organization's brand and loss of customers. Alarming, the current solutions used, regardless of industry, fail to solve the problem of information leaking or alleviate executive concerns.

The study shows that the level of awareness about the risks and cost of information leaks is high. However, the study also confirms that the recent rash of publicized information leaks is only the tip of the iceberg; information is leaking out of organizations in large volumes. Moreover, executives responsible are running on blind faith that the incomplete solutions they have deployed are enough--despite their concern over and the existence of information leaks via electronic channels. This survey serves as a wake up call to develop and implement a comprehensive data leak prevention assessment and risk mitigation plan.

About The Insight Advantage

The Insight Advantage has worked with many different organizations across industries, helping to integrate customer insight into critical business decisions. The Insight Advantage has a strong commitment to helping organizations realize the link between increased profits and a commitment to making key business decisions with customers' current and emerging needs in mind. Customers in the technology sector include WebEx, Cisco Systems, Synaptics, Handspring, Pinnacle Systems, and Yahoo!. For more information, visit www.TheInsightAdvantage.com.

About Workshare

Workshare, an Information Security company, delivers Secure Content Compliance solutions to over 5500 organizations worldwide. Workshare solutions uniquely combine policy enforcement, management control and user education to ensure safe information exchange without business disruption. Its products include Workshare Protect Enterprise Suite, Workshare Professional, DeltaView and TRACE!.

Workshare's customer base spans small to large organizations in every industry segment with more than 62 percent of the Fortune 1000 and 85 percent of the ProServices 250. Over 900,000 professionals in 65 countries use Workshare software. The company has offices in San Francisco, New York, Chicago, Atlanta, Dallas, Washington DC, London, Frankfurt, Paris and Sydney. Workshare is the sponsor of www.metadatarisk.org, the definitive source for content security. For more information, visit www.workshare.com.

Workshare Technology, Inc.
208 Utah Street, Suite 350
San Francisco, CA 94103
(415) 975-3855