Data Leakage Worldwide: The High Cost of Insider Threats

Executive Summary

The findings from a global security study on data leakage revealed that the data loss resulting from employee behavior poses a much more extensive threat than many IT professionals believe. Commissioned by Cisco and conducted by U.S.-based market research firm InsightExpress, the study polled more than 2000 employees and information technology professionals in 10 countries. Cisco selected the countries based on their diverse social and business cultures, with the goal of better understanding whether these factors affect data leakage.

In the hands of uninformed, careless, or disgruntled employees, every device that accesses the network or stores data is a potential risk to intellectual property or sensitive customer data. Magnifying this problem is a disconnect between the beliefs of IT professionals and the realities of the current security environment for countless businesses. The new findings show that “insider threats” have the potential to cause greater financial losses than attacks that originate outside the company.

- 33 percent of IT professionals were most concerned about data being lost or stolen through USB devices.
- 39 percent of IT professionals worldwide were more concerned about the threat from their own employees than the threat from outside hackers.
- 27 percent of IT professionals admitted that they did not know the trends of data loss incidents over the past few years.

Mitigating data leakage from insider threats is a difficult challenge. Businesses must take advantage of every opportunity to better understand how employee behavior and intent relates to security issues, and to make security a priority in every aspect of business operations.

Introduction

Although some hackers might still be planting viruses and worms to interrupt business operations, most are focusing on profit. Identity theft, selling your sensitive technical or financial information to competitors, abusing your customers’ confidential data, and misusing your corporate name or product brands are just some of the ways that hackers can profit from breaching your security and obtaining confidential content.

The threat of attack from outside the company is real, and warrants significant concern and action from IT professionals. But massive data loss also results from internal activities.

The insider threat is often characterized as an employee performing malicious behavior—through sabotage, stealing data or physical devices, or purposely leaking confidential information. However, organizations need to be aware that the insider threat is not just the rogue employee, but rather every employee and every device that stores information. Employees are insider threats if they speak loudly about confidential project plans while on the phone at the airport. A lost laptop containing company information can become an insider threat if it is recovered by an outsider with malicious intent.

The first two papers in this series focused on employee behavior that had the potential to jeopardize corporate data security. This paper looks more deeply into specific insider threats to data, through both negligent and malicious actions by employees. Mitigating the full gamut of threats from employees is an enormous challenge, with an unacceptably large cost of failure. IT professionals must be innovative and persistent in addressing security threats as we all move forward in the digital age. Understanding the insider threat is a critical part of that process.

The Insider Threat: Negligent Employees

The first two papers in this series, available on http://www.cisco.com/go/dlp, focused on how data security is comprised through the unintentional and unwise behavior of employees and IT professionals. The initial paper looked at data loss from an employee perspective. Data Leakage Worldwide: Common Risks and Mistakes Employees Make examined the relationships between employee behavior and data loss, as well as IT perceptions of those factors. The survey found that employees around the world are engaging in behaviors that put corporate and personal data at risk, that IT professionals are often unaware of those behaviors, and that preventing data leakage is a business-wide challenge.

The second paper looked at data loss from an IT perspective. Data Leakage Worldwide: The Effectiveness of Security Policies, offered insight into how security policy creation, communication, and compliance affect data leakage. The analysis showed that a lack of security policies and a lack of employee compliance with security policies were significant factors in data loss. And as in the first set of findings, the survey showed that IT professionals lacked important awareness—in this case about how many employees actually understand and comply with security policies. The paper concluded that companies must address the dual challenge of creating security policies and enforcing employee compliance.

Combined with the final set of results in this paper, these findings show that a lack of awareness, a lack of diligence, and defiance within company ranks pose a significant insider threat to data.

Lack of Awareness

Data leakage often results from risky behavior by employees who are unaware that their actions are unsafe. Some of this problem can be attributed to a lack of corporate policy or inadequate communication of corporate policies to employees. In other cases, IT professionals simply expect some degree of professionalism, security awareness, and common sense precautions on the part of employees—and don't get it.

- 43 percent of IT professionals said they are not educating employees well enough.
- 19 percent of IT professionals said they have not communicated the security policy to employees well enough.

Lack of Diligence

Common examples of employee behaviors that demonstrate a lack of diligence with respect to safeguarding sensitive information include speaking loudly about confidential information in public places, failing to log off laptops, leaving passwords in sight or unprotected, and accessing unauthorized websites. A particularly large threat in this area comes from employees who lose corporate devices such as laptops, mobile phones, and portable hard drives, or have those devices

stolen because they are not properly safeguarded. Of these devices, the loss of portable hard drives was the top concern among IT professionals. New 64-GB removable devices that allow an entire hard drive to be copied onto a device the size of a pack of gum make it easier than ever to access, move, or lose intellectual property or customer data.

- Nine percent of employees reported that they have lost or had their corporate device stolen.
- Of those employees who reported loss or theft of a corporate device, 26 percent experienced more than one incident in the past year.
- The top concern among IT professionals regarding data leakage was the use of USB devices, with 33 percent sharing this concern globally. The number-two concern was email; 25 percent of global IT respondents shared this view.
- When asked why their employees are less diligent in safeguarding intellectual property, 48 percent of IT professionals responded that employees are dealing with more information than ever before, and 43 percent listed a growing apathy toward security stemming from the quickening pace of employees' jobs.

The Insider Threat: Disgruntled Employees

An employee who is disgruntled or seeks to gain financially through illicit actions that involve corporate resources can become an insider threat that adds a dangerous new dimension to the data loss prevention challenge.

The disgruntled insider threat defies a common perception that the most significant security threats originate outside the company. Employees with a spiteful agenda and a profit motive can use their insider status to engage in activities that cause even greater financial loss than external threats. Legitimate network access and stewardship of devices such as laptops and PDAs makes it simple for disloyal employees to leak corporate data.

Some employees simply fail to return company devices when they leave a job. This is an expensive and dangerous activity for businesses because it adds yet another avenue for data loss. Even if only 5 percent of exiting employees take a device, that adds up to 50 employees in a company of 1000, or 500 in an enterprise of 10,000 employees. For larger organizations, the financial and data loss risks are far more significant.

- A shocking 11 percent of employees reported that they or fellow employees accessed unauthorized information and sold it for profit, or stole computers (Table 1).
- Employee reasons for keeping their corporate devices when leaving a job included needing the device for personal use (60 percent), getting back at their companies, and a belief that their previous employers would not find out.
- 20 percent of IT professionals said disgruntled employees were their biggest concern in the insider threat arena.

Table 1. Theft or Illegal Access of Company Data and Other Resources

	End Users										
	Total (n=1009)	US (n=100)	BRA (n=101)	UK (n=104)	FRA (n=100)	DEU (n=101)	ITA (n=101)	CHN (n=100)	JPN (n=101)	IND (n=100)	AUS (n=101)
Known someone at work who has accessed someone else's computer to look for unauthorized personal or corporate information	**6%**	3%	7%	4%	14%	4%	3%	8%	0%	10%	6%
Accessed someone else's computer to look for unauthorized personal or corporate information	**5%**	1%	7%	3%	12%	2%	5%	11%	1%	4%	0%
Known someone at work who has stolen computers or other equipment containing corporate data from your company	**3%**	1%	3%	2%	4%	2%	8%	3%	0%	6%	0%
Known someone at work who has sold corporate data to another party for profit	**3%**	0%	5%	1%	3%	3%	1%	5%	3%	4%	1%
Stolen computers or other equipment containing corporate data from your company	**1%**	0%	0%	0%	1%	0%	2%	0%	0%	3%	0%
Sold corporate data to another party for profit	**1%**	0%	2%	0%	0%	2%	2%	0%	1%	2%	0%
None of the above	**89%**	96%	85%	93%	79%	93%	87%	82%	96%	84%	94%

Limited IT Awareness

Any insider threat is significant, but the potential impact of insider threats can be amplified when there is a disconnect between IT's perception of employee behavior and the reality of users' actions. Twenty-seven percent of IT professionals admitted that they did not know the trends of data loss incidents over the past few years.

The contrast between employee behavior and IT perception is highlighted further by projections for the future. Fifty-seven percent of IT professionals believe that data leakage incidents will not decrease in the next 12 months. That leaves a surprising 43 percent who believe that their data will be safer over the next year, despite the survey findings that employees commonly disregard security policies and engage in behaviors that put corporate data at risk.

The Bottom Line for Data Loss

When considering the cost of data loss, the easiest aspect to measure is the capital cost of replacing lost and stolen equipment. These costs vary with the sophistication of the equipment lost and the size of the company. For smaller companies, the cost of replacing a cell phone or a laptop is likely to be more significant than for a bigger company with a larger technology budget.

A more significant cost for any company is the operational expense associated with equipment theft. When a device is stolen, an IT professional must resolve the issue by ordering and configuring the new device, which drains valuable productivity that could have been used for other purposes. Operations costs increase even further when the lost or stolen data or device is used for malicious damage that the IT staff must spend valuable time correcting.

Capital and operating expenses are measurable indicators of the cost of data loss. Even though these costs are painful, they pale in relation to a facet of loss that cannot be measured in terms of a budget. That facet is the use of sensitive data to damage a corporate reputation, brand integrity, or customer confidence. These factors can change the competitive landscape.

It is difficult to put a monetary value on the loss of data that is used for malicious purposes. How much does it cost an organization to lose its competitive advantage because source code was stolen or merger and acquisition plans were leaked before they were public? How much is your brand worth? The loss of customer credit card information carries the dual impact of a regulatory fine and the loss of customer confidence. Data is a priceless resource that must be protected.

Best Practices for Combating Insider Threats

One the greatest challenges that IT professionals face is the omnipresence of insider threats. Employees leak data verbally, physically, and over the network. They engage in behaviors that risk corporate data for technical, cultural, monetary, job requirement, personal, and malicious reasons. This is a lot of ground to cover, and IT professionals can't do it alone.

Preventing data leakage is a business-wide challenge. IT professionals, executives, and employees at every level of responsibility must work together to protect critical data assets. This requires a comprehensive approach that embraces different cultures and business practices, and focuses on education and accountability.

- Foster a security-aware culture in which protecting data is a normal and natural part of every employee's job, and not an additional task that is perceived as a burden or contrary to other goals.
- Provide the tools and education that employees need to keep data secure, starting with new-hire training and continuing with verbal updates instead of email that might be ignored or lost.
- Evaluate employee behavior and the associated risks based on factors such as the locale and the threat landscape. Then sculpt threat education, security training, and business processes around that intelligence.
- Continuously analyze the risks of every interaction between users and networks, endpoints, applications, data, and of course, other users, to maintain an awareness of the threat environment.
- Create, communicate, and enforce sensible security policies. Simplify enforcement by creating a limited number of easily understandable security policies that are integrated with business processes and aligned with job requirements.
- Provide clear leadership through executive commitment and visibility, so employees understand that executives are engaged and accountable.
- Proactively set security expectations.

Plugging Data Leakage

Corporate cultures vary around the world, and there is no one right way to protect data. But the insider threat is a global problem with costly consequences. Insider threats must be addressed with the same energy as attacks from outside the company. Like outsider threats, addressing the insider threat demands a comprehensive approach that includes education, policy, and technology. Those companies that take the additional steps of addressing the nuances of their individual corporate cultures and communicating with employees on a personal level will be even better positioned to create and enforce sustainable security strategies.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-506224-00 11/08