# Data Leakage Worldwide: Common Risks and Mistakes Employees Make

## Executive Summary

To understand the challenge that increasingly distributed and mobile businesses face in protecting sensitive information, Cisco commissioned third-party market research firm InsightExpress to conduct a study with employees and IT professionals around the world. As part of the study, surveys were conducted in 10 countries that Cisco selected because of the differences in their social and business cultures. In each country, 100 end users and 100 IT professionals were surveyed, producing a total of 2000 respondents. The research discovered that despite the security policies, procedures, and tools currently in place, employees around the world are engaging in risky behaviors that put corporate and personal data at risk. Employee behaviors included:

- **Unauthorized application use:** 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies' data loss incidents.
- **Misuse of corporate computers**: 44 percent of employees share work devices with others without supervision.
- **Unauthorized physical and network access:** 39 percent of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.
- **Remote worker security:** 46 percent of employees admitted to transferring files between work and personal computers when working from home.
- **Misuse of passwords:** 18 percent of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.

To reduce data leakage, businesses must integrate security into the corporate culture and consistently evaluate the risks of every interaction with networks, devices, applications, data, and of course, other users.

## Introduction

Employees around the globe are using business networks to communicate, collaborate, and access data. Businesses eager to increase productivity have embraced the growing integration of network communications and business operations, and have encouraged employees to take advantage of technology such as wireless devices and public hotspots. Productivity is booming, but network-based collaboration introduces corporate data into a broader environment that is more vulnerable and difficult to protect.

Data stored on the corporate network is also at risk because it is more accessible than ever. Organizations provide easy access to databases for information sharing, and storage and compression technology has allowed for more powerful (and risk-laden) endpoints. An 80-MB mobile device now holds 6000 Microsoft Word documents or 720,000 emails, and new 64-GB removable devices allow an entire hard drive to be copied onto a device the size of a pack of gum.

These devices make it easier for employees, partners, or data thieves to access, move, or lose intellectual property or customer data.

In addition to having more data at risk, businesses today suffer greater consequences if that data is lost or compromised. The loss of intellectual property, such as proprietary product blueprints, financial data, and merger and acquisition plans, can damage a company's reputation, undermine its brand, or jeopardize its competitive edge. Breaches of regulatory requirements for handling sensitive customer data can reduce customer confidence and lead to fines.

Savvy companies institute security policies and train employees about the risk of data loss, but the effectiveness of those actions is questionable. In the past two years, more than 250 million confidential records were reported lost or stolen.[1] And those losses do not always originate from external threats. Whether knowingly or unknowingly, innocently or maliciously, employees engage in behaviors that heighten the risk of data loss.

To reduce data leakage and protect corporate information, IT organizations need to understand how employee behavior increases risk and take steps to foster a security-conscious corporate culture in which employees adhere to policies and procedures.

### In-Depth Survey Exposes Risky Behavior

To better understand employee behaviors that put corporate assets at risk, Cisco commissioned third-party market research firm InsightExpress to conduct a study that spotlights common data leakage mistakes that employees make around the world. Two surveys were conducted in 10 countries: the United States, the United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil. Because the study's goal was to examine behavioral tendencies among employees worldwide, the 10 countries were selected based on their contrasting social and business cultures, as well as each workforce's relative tenure with the Internet and corporate IP-based networks. In each country, 100 employees and 100 IT professionals were surveyed, producing a total of 2000 respondents.

The survey results reveal a variety of risky behaviors and a widespread disregard for security policies. One of the most noteworthy findings is the varying prevalence of particular behaviors in different parts of the world. For example:

- China has such a high level of information technology abuse that IT decision makers audit computers for unauthorized content.
- In Japan, 65 percent of end users do not adhere to the corporate IT policy all of the time, and the research indicates that end-user abuse of information technology is increasing.
- End users in India tend to use email and instant messaging for personal use and change IT security settings on business computers so they can view unauthorized websites.
- Employees in Brazil use business computers for personal communications and for activities such as downloading music.
- End users in France have the lowest rate of IT policy compliance of all the countries surveyed, with only 16 percent of employees claiming that they adhere to security policies all the time.

The level of IT manager awareness concerning risky employee behavior also varies around the world. In China, IT managers confront employees directly for not adhering to security policies. IT

[1] http://www.privacyrights.org, 2008

professionals in India have a low awareness of the extent to which security is being compromised by employees, with less than half believing that end users are using non-IT programs and applications on their company computers. Brazil showed the greatest alignment between employee abuse of IT and IT decision-maker perceptions of employee behavior, with IT decision makers evaluating and updating corporate policies more frequently than any of the other countries surveyed.

These differences make it challenging for multinational companies that attempt to maintain a centralized security policy for distributed sites and IT departments. And as more employees join the global trend of working at home and while mobile, the lines between work life and personal life will continue to blur. Combining cultural behaviors with the use of mobile phones, laptops, Web 2.0 applications, video, and other social media at home, at work, and on the road creates an even more complex environment to safeguard. Global organizations must understand today's work environment and embrace cultural differences in behavior and its impact on risk to data, and localize education, policies, and technology decisions accordingly.

## Risky Behaviors Revealed

Employees revealed a stunning set of behaviors that put corporate data and assets at risk, despite corporate policies that define correct procedures. The following examples show how employees knowingly and unknowingly lose and leak data.

### Unauthorized Application Use

Using unauthorized applications on business networks can place sensitive corporate data and employees' personal information at risk. Personal email is the most commonly used unauthorized application, followed by online banking, online bill paying, online shopping, and instant messaging. These applications pose a high risk for data loss by an employee or data theft by a hacker because they are often unmonitored and do not use corporate security standards. Employees using these applications also risk infection from malicious sites.

- 78 percent of employees accessed personal email from business computers. This number is approximately double the level of authorized use.
- 63 percent of employees admit to using a work computer for personal use every day, and 83 percent admit to using a work computer for personal use at least sometimes.
- 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies' data loss incidents. This belief was most common in the United States (74 percent), Brazil (75 percent), and India (79 percent).

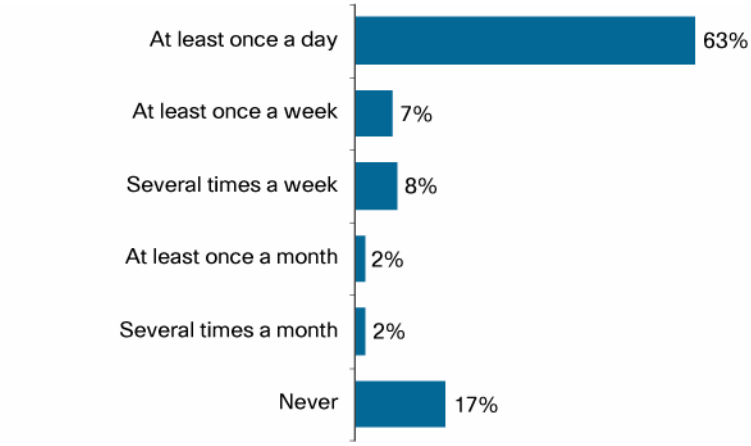
### Misuse of Corporate Computers

Many employees knowingly use corporate computers in ways that undermine IT security policies. Some examples include altering security settings and sharing work devices and sensitive information with non-employees. Employees bypassed IT settings to download music, shop online, pay bills, and in some cases, engage in online gambling and pornography. Approximately one fourth of the employees surveyed admitted sharing sensitive information with friends, family, or even strangers, and almost half of the employees surveyed share work devices with people outside the company without supervision. These behaviors can result in intellectual property leaking out of the company and reaching audiences that pose serious threats to corporate security and profitability.

- Bypass corporate policy and IT security settings
  - China: 42 percent
  - Brazil: 26 percent
  - India: 20 percent
- Share sensitive corporate information outside the company
  - Brazil: 47 percent
  - India: 27 percent
  - The United Kingdom: 26 percent
  - Italy: 22 percent
  - Germany: 24 percent
- Share work devices with non-employees without supervision
  - China: 43 percent
  - India: 28 percent
  - Overall: 44 percent (32 percent of respondents shared work devices with co-workers, and 19 percent shared work devices with non-employee family and friends)

Figure 1 shows the frequency with which corporate computers are used for personal use.

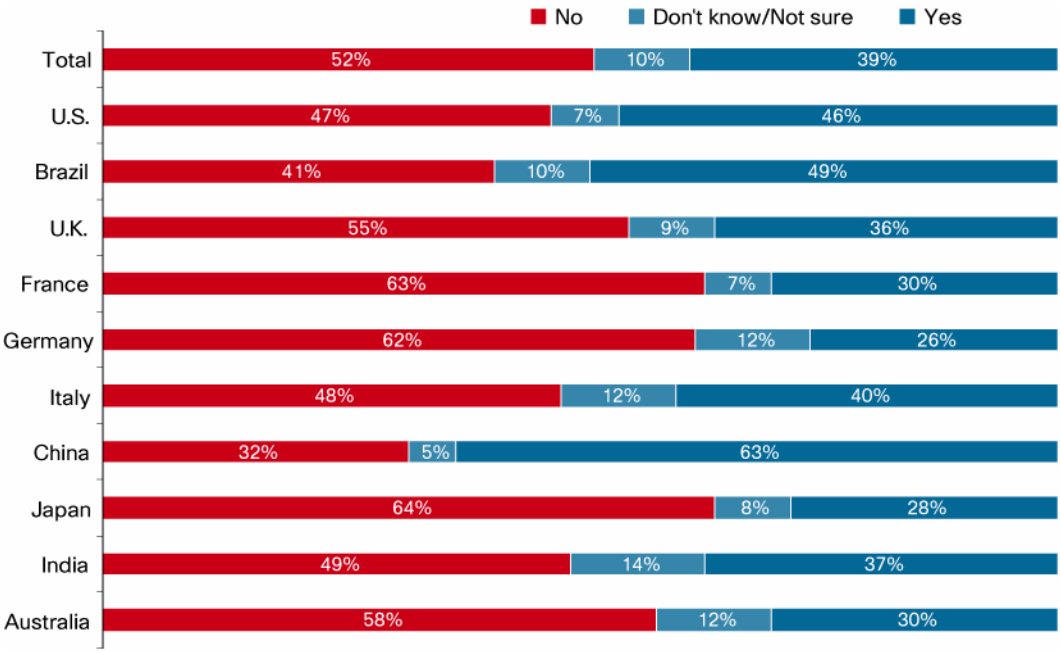
**Figure 1.** Frequency of Personal Use



### Unauthorized Physical and Network Access

Many workers let unknown individuals enter corporate facilities in a behavior known as “tailgating,” or give non-employees the freedom to move around corporate facilities without supervision. These actions give unauthorized individuals the chance to physically steal corporate resources or access sensitive information. Employees are sometimes guilty of accessing unauthorized parts of a corporate network or facility as well. Figure 2 shows the number of times IT have had to deal with an employee for accessing unauthorized networks or facilities:

**Figure 2.** IT Decision Makers Encounter Unauthorized Physical and Network Access




- 39 percent of IT professionals said they have dealt with an employee accessing unauthorized parts of a company’s network or facility, with almost half of IT professionals reporting this in Brazil (49 percent) and the United States (46 percent), and 63 percent in China. Although Japan (28 percent) and Germany (26 percent) featured the least incidents among IT professionals, every country showed at least one fourth of its IT professionals encountering these types of incidents.
- Unauthorized physical and network access was more prevalent among midsize and enterprise businesses (46 percent), but small businesses also have frequent incidents (32 percent).
- 22 percent of German employees allow non-employees to roam around offices unsupervised.

### Remote Worker Security

As businesses become increasingly distributed, mobile employees broaden the potential risk for data loss. Behaviors such as transferring files from a work device to a home computer that is not protected or maintained to IT’s standards, using personal communications that are not as safe as corporate communications, talking about sensitive company matters where others can hear the conversation, and failing to use a laptop privacy guard when working remotely in a public place all invite information theft. Employees also fail to safeguard equipment such as laptop computers and portable storage devices, which can be lost or stolen.

- 46 percent of employees admitted to transferring files between work and personal computers when working from home.
- More than 75 percent of employees do not use a privacy guard when working remotely in a public place. This number is much higher in Brazil, China, and India—countries that have the most reckless behavior.
- 68 percent of people do not think about speaking softly on the phone when they are in public places outside of the office.
- 13 percent of those who work from home admit that they cannot connect to their corporate networks, so they send business email to customers, partners, and co-workers via their personal email.

**Misuse of Passwords and Login/Logout Procedures**

Logging out of a computer and using a password are some of the oldest and simplest means of computer security. It's hard to imagine today's tech-savvy users bypassing these basic security features, but they do—and in surprising numbers. At least one in three employees said they leave their computers logged on and unlocked when away from their desk, such as when they go to lunch or go home for the evening. Another common practice is to leave a laptop on a desk overnight, sometimes without logging off. One in five employees store system login information and passwords on their computer or write them down and leave them on their desk, in unlocked cabinets, or pasted on their computers.

Any of these failures to observe security protocol provide dangerous opportunities for attackers. Taken together, they not only open the door to potential threats, but also invite the attacker inside. For example, an employee who leaves a system logged on, on a desk, and with a password attached is inviting an intruder to steal the computer now and sensitive data at their leisure. If the employee used that computer for personal use, that information is also now readily available to the attacker.

- 28 percent of employees in China store login and password information for personal financial accounts on their work devices.
- 18 percent of employees share passwords with co-workers, and that rate jumps to 25 percent in China, India, and Italy.
- 10 percent of employees in India, the United Kingdom, and Italy keep written notes of login information and passwords on their desk at work, leaving sensitive data accessible if the machine is stolen even if the computer is logged off.
- 5 percent of employees in the United Kingdom and France leave passwords to personal and financial accounts printed on their desks at work, so their information can be stolen with any other computer even if their work computer is safeguarded.

## Why Employees Put Data at Risk

Developing statistics that show how many employees are executing behaviors that reduce data security is a worthwhile exercise, but the real value comes in understanding how to change those behaviors and increase data security. To do that, businesses need to understand how employees view security and why they ignore or bypass corporate procedures.

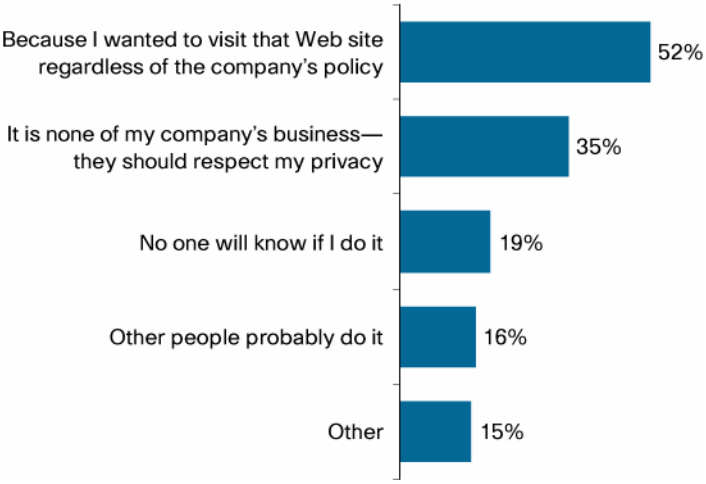
The InsightExpress survey looked beyond the statistics and asked employees why they behaved in a manner that put data at risk. The survey then presented these findings in the context of large and small businesses, different cultures, and the perspectives of employees and IT professionals.

As the survey results revealed throughout, employee noncompliance often outweighs the importance of security policy compliance. When the survey asked why employees share sensitive corporate information, for example, 44 percent replied that they needed to “bounce ideas off of people.” Other popular reasons included “I needed to vent,” (30 percent) and “I didn’t see anything wrong with it,” (29 percent).

When asked why they altered security settings on computers in a clear defiance of corporate security measures, the answer was more acerbic, as 35 percent felt that it was “no one’s business.” And those employees included the IT staff in this belief. Fifty-two percent simply replied that they wanted to view the unauthorized site, regardless of its conflict with corporate policy. Thirty-five percent felt they could get away with it because no one would know.

Figure 3 shows in graphical form **the reasons employees gave for altering security settings on their computers**.

**Figure 3.** Reasons for Altering Security Settings




Sometimes the reason for putting data at risk was monetary. It is simply cheaper to use the computer supplied by an employer for a family or household. This is a very compelling reason in cultures where extended families live together, but it increases the potential for non-employees to access corporate information.

Of course, in some cases, the problem is not that the employee ignores the threat, but that the employee is the threat. If employees are unhappy with their jobs, disgruntled with their manager, or feeling vindictive for any reason, they can become an “insider threat” who deliberately damages or leaks data.

Despite an IT department’s best efforts, it is possible that some employees do not understand the security procedures in place in their work environment. Employee use of communication services compared to what their IT department has approved reveals some interesting differences. Most evidently, a significantly larger proportion of end users use personal email at work (49%) compared to the proportion that say it is approved at their company (40%). In China and Japan, the gap between those who use personal email at work and those who say it is approved by IT is even larger.

The survey numbers indicate that although many companies have attempted to prevent employees from leaking data, their efforts are not achieving the desired results.

## Prevent Data Leakage

Threats to data security are continuing to evolve. Hacking is increasingly a criminal profession and adversarial collaboration is a for-profit venture. Much of the danger comes through the Internet, which is a vital component of today's business infrastructure. And in this perilous environment, employees around the world are leaking data despite the best efforts of IT professionals to staunch the flow.

With ignorance, defiance, and a simple lack of caring playing primary roles in employee data leakage, there is clearly no magic solution to securing corporate data—especially as businesses and their data become more mobile and operate with virtual instead of physical boundaries. The most effective way to prevent data leakage is to support an ongoing process with an all-out approach that is holistic and strategic.

Many businesses err by putting too much faith in technology alone, or by starting a security program with a technology blitz. The best security technology in the world won't produce a good return on investment without the foundation of security processes, policies, and education. Instead, businesses should start by evaluating employee behavior and the associated risks based on factors such as the locale and the threat landscape. Then threat education, security training, and business processes can be sculpted around that intelligence. At that point, appropriate investments in security technology can be applied.

This comprehensive approach is the best way to achieve sustainable security. It creates a foundation for evaluating the risks of every interaction between users and networks, endpoints, applications, data, and of course, other users. Most important, it makes security as integral to the business culture as it is to the IT infrastructure.

Following are some tangible steps you can take to prevent data leakage.

**Know your data and manage it well**—Since the intent of collaboration is to be open and share information, protecting your data begins with understanding how people interact with it every day. You'll want to:

- Establish tools and processes that track your data's movement so you know where it is stored, how it is accessed, and who is using it.
- Identify the types of data that require a unique protection regime within and beyond your company's walls.
- Consider new security approaches for next-generation tools and capabilities.

**Guard corporate data as if it is your most important possession**—Teach employees that corporate data is essentially money: Losing or leaking corporate data is like throwing money away and letting the people who pose the biggest threat to you pick it up and use it against you. And the data will likely be used to hurt your company's brand, revenue, stock price, and trust in the marketplace. Employees should understand and implement basic security procedures:

- Protect systems by using only authorized application and access methods, maintaining security software such as antivirus applications, respecting and maintaining security settings, understanding the consequences of agreeing to or negating Cisco® Security Agent pop-up actions, and preparing for spamming, malware, phishing, and other attack methods.
- Protect portable devices by keeping them in your possession or locked up at all times, not sharing your work devices or using them for personal activities, not forwarding confidential

information from work systems to personal devices, and not accessing inappropriate sites or downloading inappropriate information.

- Prevent unauthorized data access by logging off or locking systems when you walk away for a few moments or leave for the evening, using sound password creation techniques and not sharing passwords, and storing passwords securely.
- Prevent data theft while traveling by speaking softly when you have to discuss confidential information in public, using privacy filters to prevent over-the-shoulder viewing, using a VPN, and never using a business printer unless you are there to pick up the paper.

**Institutionalize standard codes for secure conduct in your business**—Information security policies are integral to a company's code of business conduct and need to be read, understood, and followed. IT professionals should think globally and act locally by setting global policy objectives and creating localized education that is tailored to a country's culture and threat landscape. Employees must understand that they play a critical role in maintaining corporate security and accept responsibility and accountability for protecting the enterprise. Sacrificing quality and security assurance for expediency is a mistake that the business cannot afford. Each employee should:

- Conduct daily business activities according to the company's code of business conduct—particularly those pertaining to information security.
- Be constantly aware of their surroundings and conscientious about security in every action they take in the office, at home, and on the road.
- Learn how to handle the different levels of confidentiality for their company's documentation. This includes understanding the differences between "public," "confidential," "highly confidential," and "restricted."

**Foster a culture and environment of openness and trust**—Employees must feel comfortable with the corporate security landscape in order to implement security directives. They should know the appropriate security organization for reporting suspicious behavior, recognizable attacks, or security incidents (even if they were the cause), and feel comfortable initiating that contact. IT professionals should teach employees:

- How to avoid security mistakes by spotlighting areas of high vulnerability.
- Proper practices to protect systems and data.
- What a computer security incident is and how to report it.

**Establish a security awareness and education practice in your business**—Creating an awareness of security issues is vital to obtaining employee support. Employees who believe that security programs are important are more likely to follow specific procedures. An education practice should:

- Educate and train employees about company expectations for protecting data.
- Include security awareness and practices in new-hire orientation events.
- Train employees about security considerations when answering the phone and connecting to Web 2.0, social networking, and collaboration sites.
- Train employees about physical security concerns, such as allowing only employees with badges to enter buildings.

## A Secure Future

Preventing data leakage is a businesswide challenge. The more people who understand that challenge, from IT professionals to executives to employees at every level of responsibility, the more successful a company will be in protecting its critical assets. The ultimate goal is for everyone, at every level, to believe that corporate security is critical, understand the policies and procedures for achieving a secure environment, and implement the necessary activities every day. That cultural shift is a process—and according to the InsightExpress survey, it is a process in which companies around the world need to dedicate more resources. With sufficient desire and investments, businesses can reduce data leakage. The reward will be well worth the effort.

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 C11-499060-00 09/08