Data Leakage Worldwide: The Effectiveness of Security Policies

Executive Summary

A second set of findings from a global security study on data leakage revealed that many companies do not have security policies—and that security policies that are in place are often ineffective. This analysis provides additional justification for the initial survey findings, which reported that employees around the world are putting corporate and personal data at risk.

The survey was commissioned by Cisco and conducted by InsightExpress, a U.S.-based market research firm. It included more than 2000 employees and information technology professionals in 10 countries that Cisco selected because of the differences in their social and business cultures. The new findings offer insight into how the use and effectiveness of security policies affect data leakage:

- 23 percent of IT professionals work for a company that does not have security policies.
- 47 percent of employees and 77 percent of IT professionals worldwide believe that their companies' security policies need improvement and updating.
- A 20 to 30 percent difference between the number of IT professionals and the number of employees who know that a security policy exists indicates that IT is not sufficiently educating and communicating security policies to employees, and that employees may not be paying attention.
- The majority of IT professionals believe that employees don't always adhere to policies because they don't understand the risks involved with their behavior, because security isn't a top-of-mind priority or issue, or because the employees just don't care.

As the lines blur between work and home, and as employees use an increasing number of interactive applications and devices, data loss has become one of the most prominent concerns for businesses around the world. Creating, communicating, and enforcing sensible security policies is critical to protecting corporate assets.

Introduction

Instant messaging. Video conferencing. Social media sites. Blogging. Wireless phones. PDAs. Humans have grown accustomed to a world were we can be electronically connected to networked information and to each other at home, at work, and almost anywhere in between. With these communications options and the expansion of the work environment to homes, automobiles, airports, and coffee shops, the line between work life and personal life has faded almost into oblivion. With that demise has come a dangerous side effect: Employees are sharing corporate information over insecure networks and failing to safeguard equipment, facilities, and sensitive data. We are a connected world, but we are an undisciplined security culture.

The consequences of inadequate security are significant. Loss of customer and sensitive corporate data, theft of capital equipment, business disruption, reduced productivity, and increased operational expenses are common results of security breaches. Despite this fallout and a continuing struggle by IT professionals to implement and enforce security policies, effective IT security remains elusive. Stumbling blocks include a failure to create security policies, ineffective education that leads to employees misunderstanding or bypassing security procedures, and impractical processes that employees feel they must ignore in order to accomplish goals and objectives. The prevalence of each type of security breach varies throughout the world, but the data leakage problem is global and measurable.[1]

IT professionals can and must overcome these problems in order to safeguard corporate assets in a manner that complies with external regulatory requirements and internal corporate governance specifications. The challenge is creating and upholding workable security policies while embracing different cultures and business practices, so employees with varying backgrounds can safely share information.

New Findings Target IT Policies

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

The survey analysis described in this paper focuses on the corporate use of security policies to shape the ways that employees treat sensitive information and corporate assets. Those findings start with the revelation that one out of four companies does not even have a security policy for the appropriate access and use of corporate information. In Japan, that percentage increases to two out of every five. For businesses with policies, the findings uncover a significant gap between the beliefs of IT professionals regarding employee compliance and the actual behavior of the employees. The results also revealed some of the reasons why employees knowingly ignore or bypass security policies and put personal and corporate data at risk.

These findings expand on the initial survey report, which examined data leakage from the perspective of employee behavior. Those results revealed a variety of risky behaviors and a widespread disregard for security policies. The prevalence of particular behaviors and the level of IT manager awareness concerning those behaviors varied throughout the world. The findings indicated that cultural differences can affect how employees and IT professionals address security issues and react to security directives. For more information, see the white paper **Data Leakage Worldwide: Top Risks and Mistakes Employees Make** on http://www.cisco.com/go/dlp.

Together, the two survey reports demonstrate the importance of a comprehensive security policy approach that includes education and accountability.

IT Policy Effectiveness Explored

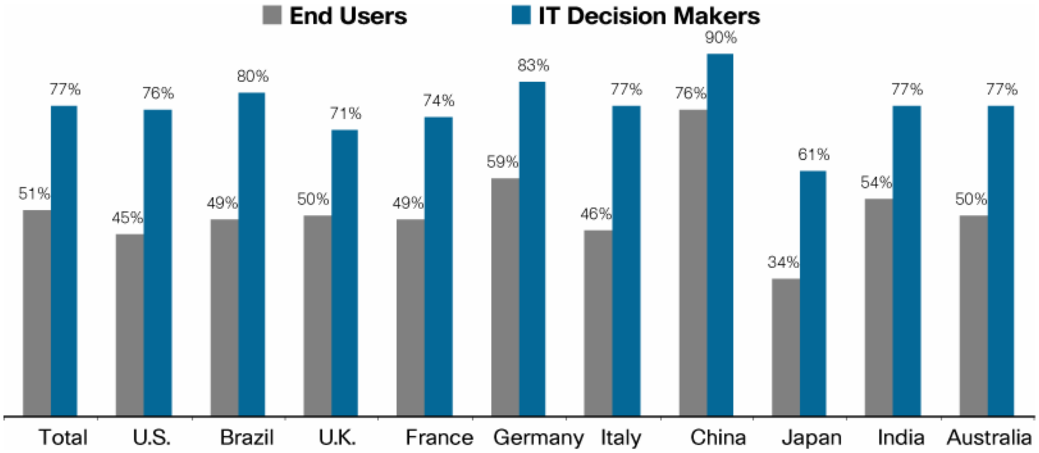
The survey results reveal that the methods used to communicate security policies to employees and the perceived fairness of the policies are critical to success. The following data shows how security policies impact data leakage.

[1] http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-499060.html

A Failure to Communicate

Three out of four companies surveyed have security policies. However, 40 percent of employees in the surveyed companies did not know that the security policies existed—and a surprising 20 percent of IT professionals were unaware of an existing security policy. Figure 1 shows the difference between the number of end users and the number of IT decision makers who are aware of a policy regarding acceptable use of company resources.

Figure 1. The Disconnect Between End User and IT Security Policy Awareness



Why is there such a disconnect between policy makers and the employees who must apply the policies every day to safeguard corporate data and assets? According to the survey results, one crucial reason is a lack of direct and consistent communication.

- 11 percent of employees say that security policies were never communicated to them or that they were never educated about the policy.
- Europe had the highest prevalence of this belief, where the United Kingdom (25 percent) and France (20 percent) far exceed the global average.
- Germany also has a high percentage of employees who claim that IT never communicates security policies to them (16 percent).

In many cases, the lack of communication regarding security policies begins with a missed opportunity when employees are first hired. Fifty-six percent of IT professionals report that security policies are communicated to new hires during orientation, yet only 32 percent of employees say they were educated. This statistic reveals a significant disconnect between the beliefs of IT professionals and newly hired employees regarding the communication of security policies.

Businesses in the United States, China, Australia, and Japan tend to communicate security policies to new hires more often. Two out of three IT professionals in these countries claim that security policies are communicated to new employees. Yet those nations still reflect a significant gap in understanding between the IT and general user communities.

- In Japan, 66 percent of IT professionals claim they communicate security policies to every new hire, but only 35 percent of employees say they received that information.
- The United States had an even larger gap (42 percent), with 70 percent of IT professionals claiming that security policies are communicated to new hires and only 28 percent of the American employees saying they received these briefings.

Email Limitations

Once employees are hired, new and updated security policies are often conveyed via email. Fifty-nine percent of employees and 68 percent of IT professionals say they receive or send emails on policy updates. But with so many email messages entering employee inboxes every day, the potential for an employee to ignore or accidentally delete an important communication from IT is high. And even when employees do read email regarding security policies, they might be less likely to retain the information or acknowledge the importance of the message than if the information was communicated in person.

Lack of Compliance

Creating security policies and communicating those policies to employees are important initial steps in safeguarding corporate assets. But these efforts have little value if employees don't understand or don't comply with the procedures. More than half of the employees surveyed admitted that they do not always abide by their companies' security policies. France featured the highest percentage (14 percent) of employees who admitted they adhere to policy sometimes, hardly at all, or never. India wasn't far behind, with 11 percent of employees admitting that they hardly ever or never abide by corporate policies.

Limited IT-Facing Policies

Employee-facing security policies are essential, but it's equally important for companies to address IT-facing security issues such as storing and destroying data. These issues are often transparent to employees. The survey results revealed that the majority of corporations have and enforce policies for managing confidential and stored data.

- 72 percent of IT professionals say their company has a policy and process for disposing of confidential documents. This number jumps to 85 percent in the United Kingdom. Brazil and France had the lowest number of IT policies in place to destroy confidential documents, with a little over half of IT respondents saying they had this policy in place.
- More than 80 percent of IT professionals say their company has a policy and process for the electronic storage of old company data. However, they are evenly divided on how rigorously it is enforced. A larger proportion of IT professionals in China say their company has a policy for electronic data storage and it is rigorously enforced (62 percent).
- More than half of IT professionals say their company does have procedures in place to destroy old company data after a certain period of time. Eight in 10 IT professionals in the United States say their company destroys old data in a timely manner.
- About 70 percent of IT professionals who work for companies that do not destroy old company data at all say they just like to keep all of their company records. About a quarter of respondents say this is for regulatory reasons.

Why Employees Don't Follow Security Procedures

Why do employees fail to follow security procedures that they admit have been communicated to them? Are policies being communicated without education or explanation? Are employees apathetic? Or worse, are they "insider threats" who purposely bypass security policies for personal gain? Table 1 shows some of the reasons that employees violate corporate IT policies.

Table 1. Reasons for Violating Corporate IT Policy

	IT Decision Makers										
	Total (n=776)	US (n=76)	BRA (n=85)	UKV (n=71)	FRA (n=75)	DEU (n=83)	ITA (n=77)	CHN (n=92)	JPN (n=61)	IND (n=77)	AUS (n=79)
They do not think there is enough risk to be concerned	**47%**	51%	44%	44%	41%	52%	38%	59%	49%	51%	39%
They think IT is there to protect them if something goes wrong	**41%**	39%	36%	39%	33%	41%	38%	47%	38%	52%	44%
Security is just not top-of-mind for them	**39%**	34%	29%	45%	31%	33%	31%	77%	25%	38%	39%
They do not care	**38%**	38%	21%	34%	57%	37%	31%	34%	49%	39%	41%
They do not know about or understand the policy	**34%**	30%	35%	31%	43%	29%	25%	45%	41%	35%	29%
They do not know that security is a concern for IT	**33%**	28%	22%	23%	24%	41%	29%	59%	30%	36%	35%
They are in a hurry	**25%**	29%	24%	24%	27%	40%	12%	17%	13%	38%	23%
We need to create or improve our employee education and training programs	**22%**	21%	27%	11%	5%	14%	12%	40%	30%	44%	14%
Other	**2%**	1%	0%	8%	1%	1%	1%	1%	2%	0%	4%
Don’t know/not sure	**2%**	4%	1%	3%	3%	1%	6%	0%	0%	0%	3%

According to survey results, only 22 percent of IT professionals believe that security education needs to be improved. A greater number of IT professionals believe that employees are wayward because they don’t understand the risks of their behavior, because security is not a top-of-mind priority, or because they simply don’t care. The data validates these beliefs. When asked why they altered security settings on computers to view unauthorized sites, for example, 52 percent simply replied that they wanted to view the site—regardless of its conflict with corporate policy.

IT’s perception of employee apathy is highest in France (57 percent), which parallels the French employee acknowledgment that they often ignore company policies. In China, 77 percent of IT professionals said security is not a top-of-mind concern for employees. Many IT professionals (41 percent) believe that employees are willing to engage in these risky behaviors because they think that IT will solve any problems that arise as a result, or that no one will know.

The most common reason why employees do not adhere to corporate security policies is a lack of alignment between job activities that are perceived as necessary and policy constraints. Forty-two percent of employees worldwide knowingly disregard security policies because they believe that the policies limit their ability to perform their work effectively. China (62 percent) and the United Kingdom (55 percent) featured the highest percentages of employees expressing this frustration.

In some cases, employees blatantly circumvent security policies for personal gain. 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 the fact that employees often violate security policies, IT professionals do not confront employees very often. About three out of four respondents say they deal with employees who violate their company’s IT policy a few times a year or less frequently. In Australia, only 10 percent of IT respondents say they confront employees once a month or more often.

Consequences of Corporate IT Policy Violations

The consequences of violating corporate IT security policies are extensive and expensive. According to IT, virus containment is the leading consequence resulting from employees breaking security policies. In the United States, violations of security policies lead to extensive wireless network abuse, with almost half of respondents sharing this belief. IT respondents also believe that violating corporate policies leads to insider abuse, theft of devices such as laptop computers and mobile phones, and customer data loss or theft.

Create Security Policies that Work

The survey results show that the biggest risk to data loss is the lack of employee awareness of and compliance with existing security policies. IT professionals must look beyond the technical aspects of creating security policies to the human elements of awareness and compliance. That requires clear, pointed, and personal communication. In addition, IT must educate employees about the importance of observing security policies so they are willing to make compliance a priority every day. The following guidelines can help you create and enforce successful security policies.

Increase Awareness

A security policy is only successful if employees understand and regularly observe the procedures. Those in charge of corporate security must understand the level of employee awareness in order to determine whether security policies are effective. Conducting a survey can help you determine this level and take steps to raise awareness, if necessary. Some of the questions such a survey might include are:

- Do employees know that there are security policies?
- Do they know where to find them?
- Are the policies easily accessible?
- Have all the employees read the policies?
- Do the employees understand the policies?

Communicate Effectively

Whether you are explaining security policies to new hires or sharing updates with employees, clear communication through established channels is critical. Look at how your company uses Web 2.0 and collaborative tools, and try to communicate your policies using those tools. Making sure that employees understand why they are being asked to comply with security policies is also an important aspect of communication. Additional communications guidelines include:

- Target communications for various user communities.
- Provide a list of policy updates in your annual training.
- Supplement primary communications vehicles with website and newsletter articles.

Simplify Enforcement

Once you’ve determined that employees are aware of security policies and that you are effectively communicating new policies and updates, the next challenge is convincing employees to comply with every policy, every day. Enforcement is a challenging proposition, but you can ease the enforcement burden and generate a higher level of compliance by creating realistic, workable policies.

- **Create a manageable number of policies**—Keep the number of policies manageable (preferably less than 12), so your users can more easily find the policy that they need.
- **Make policies understandable for all audiences**—Use language that is suited for an international audience to ease translation, with examples to illustrate how the user can comply with the policy.
- **Make it easy to comply**—If you make it difficult for users to comply with your policy, they won't. Consider including random employees in your policy review process to get some sense of the ease of compliance.
- **Integrate security with business processes**—Integrate security policy compliance into business processes, so employees won't need to bypass security procedures in the process of doing their jobs.
- **Align policies with job requirements**—Even well-intentioned policies can get in the way of job requirements. Faced with the choice of doing a superb job or complying with security policies, employees will most often choose to do a better job. Try to avoid this situation by creating practical policies that target only the most significant threats.

Integrate Security with the Corporate Culture

Integrating security into the corporate culture is an excellent way to convince busy employees and harried executives that security is central to business success. This approach can foster a feeling of community and encourage everyone to feel that their support of security policies is important.

- **Make employees a partner in the security challenge**—Employees will be more likely to support security initiatives if they feel that the security team is there to help them instead of to police them. Establish good relationships and use the awareness program to encourage business leaders to drive security within their organizations.
- **Make security policy part of a larger compliance initiative**—Work with your human resources, legal, and other compliance teams so that there is importance, credibility, and urgency attached to any policy training or communication.
- **Tie security policies to your company's code of business conduct**—Educate your employees to understand that their compliance with security initiatives is integral to overall appropriate behavior and critical to business success.

Provide Clear Leadership

Senior executives set the tone for an organization's culture. Garnering the commitment of these leaders and maintaining a security focus with ongoing communication will encourage executives to advocate and champion the importance of security policies. Cisco executives recognize the importance of maintaining a strong security policy posture across all aspects of the business. They visibly support security policy efforts and participate in communications that show the rest of the organization that they are engaged and accountable, and that they expect the same of all employees.

Use a Good Security Policy Creation Process

Good security policies often align with an industry standard, such as NIST or ISO. Understand that creating comprehensive, workable security policies takes time. Set appropriate expectations that it can take months to work through a full policy development cycle. Document your process and your policies using a hierarchy of materials that includes standards, procedures, practices, and guidelines. The high-level documents might list organizational objectives, while specifications explain exactly how to comply with policies. Guidelines for creating good security policies include:

- Create a repeatable governance process.
- Understand what should trigger a policy change (elapsed time, technology changes, regulatory requirements, client requests).
- Establish consistent taxonomy and definitions, such as:
  - Policy—A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area.
  - Standard—A mandatory action or rule designed to support and conform to a policy to make it meaningful and effective.
  - Guideline—General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.
- Write policies that are realistic and enforceable.
- Monitor your policy exceptions so you understand why they are granted; trending exceptions might trigger a policy change if a policy is too restrictive for the current business environment and makes compliance difficult.

Promote Success with Creativity

Every corporate culture is different, and there is no one right way to create and enforce security policies. But each company must find a way to make its security policy strategy effective, or risk losing immeasurable value in sensitive information and expensive resources. Survey employees, consult with executives, or talk with others in the industry. Encourage executive commitment and employee acceptance through any means at your disposal. If you proactively set expectations for security responsibility and policy compliance and follow through with practical policies and good communications, your security policies can successfully help prevent data leakage.

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 C11-503131-00 10/08