WHITE PAPER:
HOW EMPLOYEES ARE PUTTING YOUR
INTELLECTUAL PROPERTY AT RISK

What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk

Who should read this paper

Anyone interested in understanding the growing problem of intellectual property theft in the workplace and the mindset of employees that result in the taking of corporate assets

Ponemon INSTITUTE

Confidence in a connected world. Symantec.

Content

Introduction

Companies today are losing valuable intellectual property (IP) on a regular basis. While many security initiatives focus on threats posed by cyber criminals and hackers, there is a less obvious player in the theft of corporate assets: employees. In most cases these trusted employees are moving, sharing, and exposing sensitive data in order to do their daily jobs. In other cases, they are deliberately taking confidential information to use at their next employer, some of them without realizing that it is wrong to do so. The three parties – the employee, the organization, and the new employer – are all putting themselves at risk, and there are no real winners in any of these situations. This whitepaper explores the mindset and motivation of employees involved in IP theft.

Key Findings

- Employees are moving IP outside the company in all directions
- When employees change jobs, sensitive business documents often travel with them
- Employees are not aware they are putting themselves and their companies at risk
- They attribute ownership of IP to the person who created it
- Organizations are failing to create a culture of security

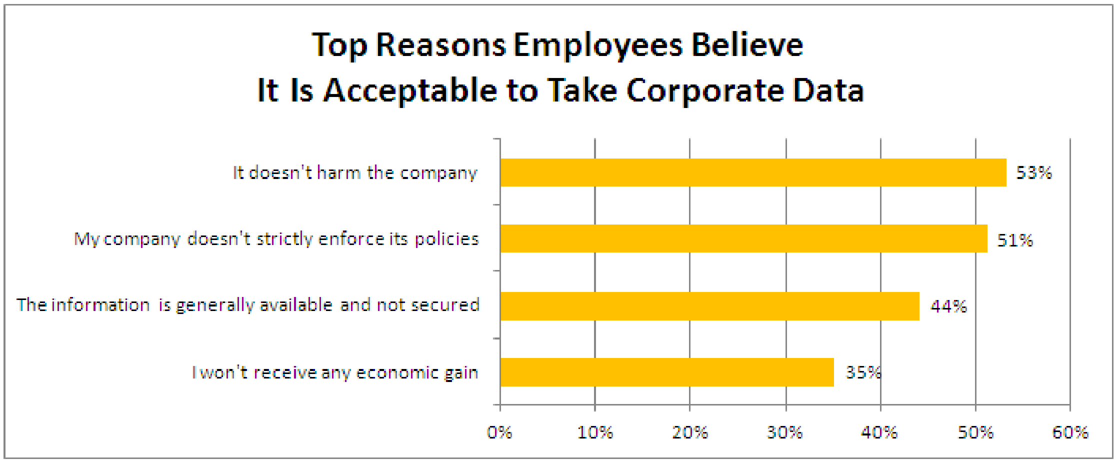
Impact on Organizations

According to Ponemon Institute, an independent data privacy research firm, **employees are moving IP outside the company in all directions**. Over half admit to emailing business documents from their workplace to their personal email accounts, and 41 percent say they do it at least once a week. Forty-one percent also say they download IP to their personally-owned tablets or smartphones – leaving confidential information even more vulnerable as it leaves corporate-owned devices. The data loss continues through employees sharing confidential information in the cloud: 37 percent use file-sharing apps (such as Dropbox^{TM} or Google Docs^{TM}) without permission from their employer. Worse, the sensitive data is rarely cleaned up; the majority of employees put these files at further risk because they don't take steps to delete the data after transferring it.

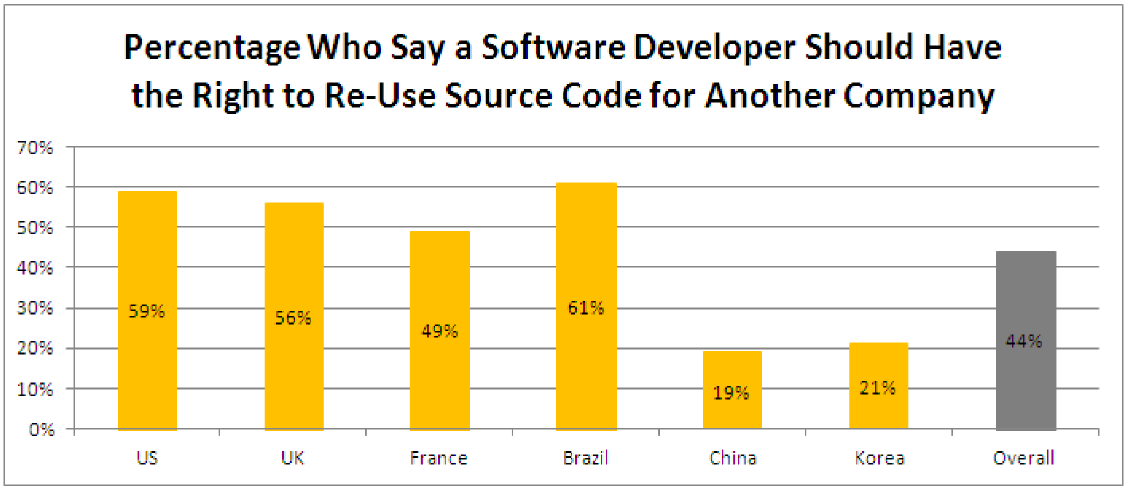
When employees change jobs, sensitive business documents often travel with them. In most cases, the employee is not a malicious insider, but merely negligent or careless about securing IP. However, the consequences remain. The IP theft occurs when an employee takes any confidential information from a former employer. Half of the survey respondents say they have taken information, and 40 percent say they will use it in their new jobs. This means precious intelligence is also falling into the hands of competitors, causing damage to the losing company and adding risk to the unwitting receiving company.

Understanding Employee Attitudes about IP Theft

The attitudes that emerged from the survey suggest that **employees are not aware that they are putting themselves and their employers at risk** when they freely share information across multiple media. Most employees do not believe that transferring corporate data to their personal computers, tablets, smartphones, and cloud file-sharing apps is wrong. A third say it is OK as long as the employee does not personally receive economic gain, and about half justified their actions by saying it does not harm the company. Others blamed the companies for not strictly enforcing policies and for not proactively securing the information. These findings suggest that employees do not recognize or acknowledge their role in securing confidential company data.



To shed further insight, over half do not believe that using competitive data taken from a previous employer is a crime. **Employees attribute ownership of IP to the person who created it**. When given the scenario of a software developer who re-uses source code that he or she created for another company, 42 percent do not believe it is wrong and that the a person should have ownership stake in his or her work and inventions. They believe that the developer has the right to re-use the code even when that developer does not have permission from the company. These findings portray today's knowledge workers as unaware that intellectual property belongs to the organization.



Recommendations

Given these findings, what can companies do to minimize risk? We suggest that companies take a multi-pronged approach:

- **Educate employees**. Organizations need to let their employees know that taking confidential information is wrong. Employee training and awareness is critical – companies should take steps to ensure that IP theft awareness is a regular and integral part of security awareness training. Create and enforce policies that provide the do's and don'ts of information use in the workplace and when working remotely. Help employees understand that sensitive information should remain on corporate-owned devices and databases. Make it clear that new employees are not to bring IP from a former employee to your company.
- **Enforce non-disclosure agreements (NDAs)**. Review existing employment agreements to ensure that it uses strong and specific language regarding company IP. Conduct focused conversations during exit interviews with departing employees and have them review

the original IP agreement. Include and describe, in checklist form, an overt description of information that may and may not transfer with a departing employee.[1] Make sure all employees are aware that any policy violations will be strictly managed and will affect their jobs. Employment agreements should contain specific language about the employee's responsibility to safeguard sensitive and confidential information.

- **Implement monitoring technology**. Support education and policy initiatives by using monitoring technology to gain insight into where IP is going and how it's leaving. Deploy data loss prevention software to notify managers and employees in real-time when sensitive information is inappropriately sent, copied, or otherwise inappropriately exposed. Implement a data protection policy that monitors inappropriate access/use of IP and notifies employees of violations, which increases security awareness and deters theft. Leverage technology to learn what IP is leaving your organization and how to prevent it from escaping your network.

Survey Methodology

The survey was conducted by The Ponemon Institute to examine the problem of IP theft or abuse by employees in the workplace. The results are based on responses from 3,317 individuals in six countries: United States, United Kingdom, France, Brazil, China and Korea.

Our research methods utilized a survey instrument and web-based channel to field results within all six countries. In addition to a set of background and demographic questions, the instrument contained five scenarios to determine respondents' attitudes and beliefs about information abuse, misuse and/or theft within their organizations. Respondents were pre-screened on three criteria: (1) present employment status, (2) access to business sensitive or confidential information as a job requirement and (3) normal use of mobile data-bearing devices in the workplace (such as laptops, smart phones and tablets).

Most respondents held full-time positions. The average headcount of respondents' organizations is approximately 7,000 and the median age of respondents is 35 years (with approximate half female/male split). All survey responses were fielded between in October and November 2012.

[1]. Shaw, E.D. and Stock, H.V. (2011) “Behavioral Risk Indicators of Malicious Insider Theft of IP: Misreading the Writing on the Wall,” Incident Management Group, December.

About Symantec

Symantec protects the world’s information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices
and contact numbers, please
visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com