Safeguarding Corporate Secrets

After three insiders are accused of stealing its trade secrets, Coca-Cola vowed to better protect its data. Don't wait for a breach to ensure your company's valuable information assets are protected.

Nikki Swartz

When three employees stole confidential company documents and materials, the Coca-Cola Co. did not see it coming. But it probably wishes it had protected itself better.

According to the 2005 "Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security Survey," average financial losses from unauthorized access to data skyrocketed to $303,234 in 2004 – up from only $51,545 in 2003. Average losses from proprietary information theft rose to $355,552 from $168,529. Total losses for those two categories were about $62 million.

As headlines scream out stories of stolen laptops that contain Social Security numbers, lost hard drives full of credit card numbers, and company computers being hacked, organizations have spent millions to protect their computers and electronic data. But, in the process, many may be overlooking the need to protect their valuable information assets from insiders.

Trade Secrets for Sale

In July, three Coca-Cola employees – including an administrative assistant for a company executive – allegedly stole trade secrets from the company and tried to sell them to rival PepsiCo Inc. for $1.5 million.

Joya Williams, the executive secretary, was seen on surveillance video at her desk at Coca-Cola headquarters in Atlanta rifling through corporate files and stuffing documents and a sample of a new Coca-Cola product in her personal bag. She was fired and arrested along with two accomplices, Edmund Duhaney and Ibrahim Dimson.

Coca-Cola and Pepsi, usually bitter enemies, worked together to expose the alleged theft plot. According to prosecutors, on May 19, Pepsi provided Coca-Cola with a copy of a letter mailed to Pepsi in an official Coca-Cola business envelope. The letter, postmarked from the Bronx, New York, was from an individual who called himself "Dirk" and claimed to be employed at a high level with Coca-Cola. "Dirk," who was later identified as Dimson, the FBI says, offered Pepsi "very detailed and confidential information."

After being alerted to the plot by Pepsi, Coca-Cola immediately contact-

ed the FBI and an undercover FBI investigation began. According to prosecutors, Williams was the source of the information Dimson offered to sell to Pepsi. They say that "Dirk" provided an undercover FBI agent with 14 pages of Coca-Cola documents marked "classified-highly restricted" and "classified-confidential." The company confirmed that the documents were valid, highly confidential, and considered trade secrets. Prosecutors say "Dirk" requested $10,000 for the documents.

Later, "Dirk" produced additional documents that Coca-Cola confirmed were valid trade secrets of Coca-Cola. He also agreed to be paid $75,000 for the purchase of a highly confidential product sample from a new Coca-Cola project, prosecutors said. During a meeting at the Atlanta airport, an undercover agent later paid "Dirk" part of that money. "Dirk" handed over documents and the Coca-Cola product sample, an FBI affidavit states.

Then, on June 27, an undercover FBI agent offered to buy other trade secret items for $1.5 million from "Dirk." The same day, a bank account was opened under the names of Duhaney and Dimson, and the address used on the account was that of Duhaney's residence, prosecutors say.

According to *The Atlanta Business Chronicle*, the three were arrested and indicted by a federal grand jury on a charge of conspiracy to steal trade secrets. The charge carries a maximum prison sentence of 10 years and a fine of up to $250,000.

"Information is the Lifeblood"

Soon after the incident, Coca-Cola Chief Executive Officer Neville Isdell sent a memo to the company's employees worldwide. It stated, in part:

"While this breach of trust is difficult for all of us to accept, it underscores the responsibility we each have to be vigilant in protecting our trade secrets. Information is the lifeblood of the company. As the health of our enterprise continues to strengthen and the breadth of our innovation pipeline continues to grow, our ideas and our competitive data carry increasing interest to those outside our business. Accordingly, I have directed a thorough review of our information protection policies, procedures, and practices to ensure that we continue to rigorously safeguard our intellectual capital."

Isdell ended the memo by emphasizing employees' shared responsibility to protect the intellectual capital of Coca-Cola and encouraging them to continue working together to move the company forward.

Unfortunately, Coca-Cola is not alone in its recent information theft travails. According to the U.S. Department of Justice, insider theft is growing at a rate of 15 percent annually. A Department of Commerce study revealed that one-third of all employees steal from their employers.

Several studies estimate that this theft and dishonesty costs U.S. businesses between $60 billion and $120 billion annually, not including the billions spent on theft protection. Former Attorney General John Ashcroft painted an even bleaker picture in October 2004 when he said intellectual property theft was costing U.S. companies $250 billion each year.

Consider these additional eye-opening business security statistics:

- Internal theft causes one-third of all businesses to fail, according to LPT Security Consulting.
- According to the FBI, authorized users account for 80 percent of asset misdirection and inappropriate disclosure of sensitive information.
- A 2005 Harris Interactive poll revealed that 68 percent of U.S. employees have sent or received e-mail via their work e-mail account that could put their company at risk.

According to the FBI, authorized users account for 80 percent of asset misdirection and inappropriate disclosure of sensitive information.

Mobile Devices Heighten Risk

Protecting corporate information is even more difficult with the proliferation of mobile devices and electronic data that can easily be deleted, altered, or transported by employees in mere seconds and with little or no trace.

According to Gartner, more than half the *Fortune* 2000 workforce will soon have mobile devices, which will collectively contain 40 percent of all corporate data as they accompany employees off company premises each day.

To highlight the pervasive threat of data theft, a U.S. security expert devised an application that can fill an Apple iPod with business-critical information in a matter of minutes. *CNET News* reported that Abe Usher, a 10-year security industry veteran, created an application that runs on an iPod and can search corporate networks for files likely to contain business-critical data. At a rate of about 100 megabytes (MB) every few minutes, it can scan and download the files onto the mobile storage devices.

The scenario is frightening because someone doing this would look like any other employee listening to their iPod at their desk, *CNET* said. Even worse, the person stealing data would not even need access to a keyboard; they could simply plug into a USB port on any active machine.

"In two minutes, it's possible to extract about 100MB of Word, Excel, PDF files – basically anything which might contain business data – and with a 60 gigabyte iPod, you could probably have every business document in a medium-size firm," Usher said.

Usher said most operating systems cannot manage this threat effectively without impairing other functions. Experts say Microsoft's forthcoming Vista for Windows might include some capability for better controlling USB devices, but it is two years away. Usher says companies cannot afford to wait that long.

"The cost of being proactive is less than the cost of reacting to an incident," he said.

Many Canadian companies are taking proactive steps and banning popular mobile devices in the workplace. (See Sidebar.)

Canadian Businesses Ban iPods

Canadian businesses are increasingly banning mobile devices from the workplace, according to two new surveys. Fear of data theft is prompting corporate Canada, as well as governments, to target small computing devices including MP3 players, personal digital assistants (PDAs), and even laptops, Yahoo! Canada reported.

According to a new survey of IT managers by market research firm Ipsos-Reid, almost one-third of mid-sized to large Canadian businesses are telling employees to leave their Apple iPods at home. Even fewer companies allow workers to bring in their personal laptop or thumb-sized USB storage devices.

The survey, commissioned by Sun Microsystems Canada Inc., found 30 percent also had banned MP3 players from the workplace.

"You could store even millions of data records in something the size of a cellphone or smaller," said Andy Canham, president of Sun Microsystems Canada.

Such devices can be used to transfer large files to take back to a home office or even download podcasts some companies now use to pass information to employees. But, according to Canham, instances of employee laptops that have been stolen or lost, sometimes compromising confidential company or customer records, have opened organizations' eyes to the importance of data security.

The survey indicated 28 percent of consumers would end their relationship with an organization that compromised their personal information.

However, businesses must strike a delicate balance between productivity and security. About 80 percent of the companies surveyed said workers with remote access to information were more productive. Most gave their employees cellphones and laptops to use for work, and one-fifth offered remote access to their networks.

But only 30 percent believed they had a full understanding of the risks associated with remote and wireless access.

Avoiding Insider Data Theft

Global competition, increased outsourcing, new technologies, and regulatory compliance have changed information security requirements significantly. Today, many experts say, companies must secure their information from the inside out.

According to *Business Communications Review*, about 80 percent of corporate security breaches begin inside the company by careless or corrupt employees. Today, companies spend enormous sums on technology to protect them from external breaches. But, in doing so, they often neglect the very real risk of attacks from the inside. Ernst & Young recently polled 1,233 organizations and found that IT departments that are vigilant about perimeter security often overlook critical internal risks.

Unfortunately for Coca-Cola, its sensitive documents and new product

sample were accessible to a secretary. But fortunately for other corporations, the beverage giant's incident has spurred chief information officers (CIOs) everywhere to re-evaluate their own policies and procedures for securing confidential corporate data.

Companies of all sizes can take the following steps today to begin better protecting their valuable information assets and making their entire organization less vulnerable to data theft:

1. Screen employees at all levels. Experts say thorough employee background screening at every level, from senior executives to mailroom clerks, is critical. A recent Michigan State University study subjected 1,037 actual identity theft cases to forensic analysis and found that as many as 70 percent began with an employee stealing data from work.

Insider theft is especially onerous because, unlike a hacker who breaches the enterprise from outside, the trusted employee knows where to find the most valuable information and is familiar with the security system. So while companies should be really careful when hiring a chief financial executive, it should also be cautious when hiring support personnel who will have access to sensitive corporate records.

2. Train employees on the value of information. Experts say information is grossly undervalued by the typical employee. But if companies do not train them on the importance of information as well as how to control, manage, and preserve it, they cannot expect employees to know which e-mails to save or which documents to classify as "confidential." Each employee has to know what information is confidential and understand all the corporate governance and compliance rules and follow them – no matter how inconvenient that might be. According to The Ponemon Institute, the most common source of security breaches is the well-intentioned employee who simply didn't handle sensitive information with sufficient care.

3. Protect confidential documents and records. In most workplaces, the reality is that employees can copy data files easily, leaving absolutely no trail or hint of the theft until it becomes public. To prevent such incidents, today companies must employ simple as well as sophisticated methods of protecting information.

For example, after Coca-Cola's recent theft, the organization's general counsel, Geoff Kelly, sent a memo to employees reminding them of company policy, which states that any materials classified as "confidential" must be secured in locked offices and drawers when not in use. He said materials marked "restricted" must be encrypted for electronic transmission, including e-mail, and hard copies must be secured when not in use. Kelly also urged employees to come forward if they see someone doing something inappropriate.

But organizations should constantly remind employees and vendors – via newsletters, meetings, and training, for example – that intellectual property must be protected.

On the technology side, *CIO Today* suggests turning off the USB drive feature in all corporate computers to prevent theft via mobile devices. CIOs also can set user privileges to prevent employees from exporting data from network storage to portable devices. Because IT departments cannot possibly safeguard everything, CIOs should prioritize data-security efforts to protect the most important information.

Few employees need access to sensitive corporate records, and so access to such information should be strictly limited to those that need it.

High-tech companies that maintain confidential information used by employees often put that data on a highly secure computer network that is password-protected to limit access. Employees also should password-protect e-mail accounts and files. Simply locking file cabinets and office doors works, too.

4. Control access to sensitive corporate data. *CIO Today* says companies should encrypt all user files and set rules for each user's access level. In addition, limiting, monitoring, and controlling access can also help protect sensitive data.

Controlling access to trade secrets and other confidential information is critical. Few employees need access to sensitive corporate records, and so access to such information should be strictly limited to those that need it.

But because some sensitive information cannot be locked down, companies should concentrate on managing who is handling the information, says *CIO Today*. It advises CIOs to either block access to certain data or monitor what is happening with it. Blocking access isn't always practical, however, because without access to certain company information, employees may not be able to do their jobs efficiently, if at all.

5. Don't let departing employees take information with them. Some proactive companies require employees to sign confidentiality agreements promising not to divulge trade secrets, even after they leave their jobs.

This is a wise move, considering insider data theft statistics. For example, *Business Communications Review* cites a recent United Kingdom study, in which more than two-thirds of respondents admitted to taking corporate secrets – e-mail address books, sales proposals/presentations, customer databases, and contact lists – when they left their previous jobs.

But a signed contract will not deter all thieves. *CIO Today* says the best way to discourage data theft from inside a corporation is to make an example of an employee who violates best-practice standards and is perceived as a risk. "The sudden firing and prompt removal from the premises of a questionable employee could prevent surreptitious data loss, as opposed to when a worker unexpectedly quits the company," according to *CIO Today*.

In today's increasingly technological business world, it is critical that IT departments and CIOs continue to work together to minimize the risk of information theft, especially from the inside. When an employee can simply plug in a mobile device and walk away with the entire business in minutes – or simply stash a confidential document in her purse – the entire organization should start taking the threat much more seriously. Just ask Coca-Cola.

Nikki Swartz *is a freelance writer based in Kansas City, Missouri, and former Associate Editor of* The Information Management Journal. *She may be reached at* nikkiswartz@hotmail.com.

References

"Coke CEO's memo to employees on theft of trade secrets." *The Atlanta Journal-Constitution.* 6 July 2006. Available at *www.ajc.com/business/content/business/coke/stories/0706bizwebcokememo.html* (accessed 1 August 2006).

"Court Case Highlights Need to Lock up Corporate Secrets." *The Canadian Press.* 20 July 2006, Vol. 6, No. 15. Available at *www.businessedge.ca/printArticle.cfm/newsID/13091.cfm* (accessed 1 August 2006).

Germain, Jack M. "Protecting Your Most Vulnerable Corporate Data." *CIO Today.* 6 March 2006. Available at *www.cio-today.com/story.xhtml?story_id=41887* (accessed 1 August 2006).

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. "CSI/FBI Computer Crime and Security Survey," 2005. Computer Security Institute Publications. Available at *www.cpppe.umd.edu/Bookstore/ Documents/ 2005CSISurvey.pdf* (accessed 1 August 2006).

Hirschman, Dave and Scott Leith. "How UPS, BellSouth handle secrets." *The Atlanta Journal-Constitution.* 11 July 2006. Available at *www.ajc.com/business/content/business/stories/0711bizrecords.html* (accessed 14 July 2006).

Howard, Matthew. "Perimeter Security Leaves The Crown Jewels At Risk." 15 June 2005. *Business Communications Review.* Available at *www.bcr.com/opinion/imho/perimeter_security_leaves_risk_2005061524.htm* (accessed 1 August 2006).

"Indictment Handed Down in Coca-Cola Trade Secret Case." *Atlanta Business Chronicle.* 12 July 2006. Available at *http://phoenix.bizjournals.com/atlanta/stories/2006/07/10/daily23.html?t=printable* (accessed 1 August 2006).

Joyner, Tammy. "Corporate Treason Makes Companies Cautious." *The New York Times.* 15 July 2006. Available at *www.financialexpress.com/fe_full_story.php?content_id=134022* (accessed 1 August 2006).

Mertl, Steve. "'Leave iPods at Home,' More Security-Conscious Managers Telling Employees." Yahoo Canada. 17 July 2006. Available at *http://ca.news.yahoo.com/s/17072006/2/business-leave-ipods-home-security-conscious-managers-telling-employees.html&printer=1* (accessed 1 August 2006).

"Safety in Numbers." *CSO Online.com.* 9 August 2005. Available at *www.csoonline.com/metrics/viewmetric.cfm?id=834* (accessed 1 August 2006).

"Security Facts for Small Businesses." Essential Security Software. Available at *www.essentialsecurity.com/educationalfacts.htm* (accessed 1 August 2006).

"Stolen-Coke-Secrets Case Could Spur Review of Security Policies." Fox News. 8 July 2006. Available at *www.foxnews.com/printer_friendly_story/0,3566,202657,00.html* (accessed 1 August 2006).

Sturgeon, Will. "Beware the 'Pod Slurping' Employee." *CNET News.com.* 15 February 2006. Available at *http://news.com.com/Beware+the+pod+slurping+employee/2100-1029_3-6039926.html* (accessed 1 August 2006).

Weber, Harry R. "Coca-Cola Caper Puts Spotlight on Protecting Secrets." *Seattle Post-Intelligencer.* 10 July 2006. Available at *http://seattlepi.nwsource.com/business/276968_coke10.html* (accessed 1 August 2006).

Weber, Harry R. "Coca-Cola Trade Secrets Theft Case Likened to 'Something out of a Spy Novel.'" Associated Press. 7 July 2006. Available at *www.heraldtribune.com/apps/pbcs.dll/article? Date=20060707&Category=BUSINESS&ArtNo=607070579&SectionCat=COMMUNITY&Template=printart* (accessed 1 August 2006).