

A Service of Benson Records Management

September 2009

GUARDING AGAINST CORPORATE ESPIONAGE

Call it proprietary information, intellectual property, trade secrets, commercially valuable information or pursued data. By any name it is valuable material that is subject to being stolen. Studies have shown that insiders, employees, are responsible for 70% to 85% of data espionage crimes. But many instances of stolen data are not reported to the police because the owners do not want it publicly known that this has happened.

In the United States, Congress passed the Economic Espionage Act of 1996 which has two sections defining federal criminal offenses. 18 U. S. C. §1831 sets large dollar fines and a prison term for persons or organizations which steal or receive a trade secret that will benefit a foreign power. 18 U.S.C. §1832 covers theft of trade secrets to benefit anyone other than the legal owner, again with prison terms and large fines for the guilty person or organization.

In order to prosecute under the EEA, the plaintiff must be able to state the monetary value of the stolen data and the loss sustained.

Look beyond the firewalls to set up protection.

Some experts say that a "preoccupation with technical security" causes data to be vulnerable while non-technical methods are given little attention although they could make a great difference in an organization's defense mechanism. Given that insiders create most of the havoc, the topic of personnel security becomes important.

The first impulse is to make sure that background checks are performed on all persons who will have access to sensitive information. But that narrow focus on the "higher ups" overlooks the fact that persons doing clerical work, or serving as janitors or security guards, may have inadvertent access to information that should be protected. This premise is detailed by Ira S. Winkler of the National Computer Security Association in *Case Study of Industrial Espionage*



Through Social Engineering. He states "It is time for commercial information security professionals to realize that information security is more than computer security."

Cerulean Associates LLC is a company specializing in intellectual property (IP) security. As a beginning step, they offer a free self-assessment tool at (www.ceruleanlic.com) with 27 questions such as "Are intellectual property and trade secret security policies regularly audited?" or "Does your computer department take a 'snapshot' backup of the data and emails of any employee or contractor who will be leaving your company?" Cerulean also cautions U. S. companies that outsource work overseas to look at the Special 301 report produced by the Office of the U. S. Trade Representative (www.ustr.gov) which lists countries deemed to have poor controls for intellectual properties.

When does a "regular" employee become a dangerous insider?

The Compliance Training Group (www.compliancegroup.com) offers employers training sessions concerning the legal consequences and risks that can come from economic espionage. One of the first steps is learning to recognize behaviors in employees that may signal an effort toward espionage. Some changes or issues may be:

- A sudden shift to negative attitude about the organization;
 - Trying to gain access to information by coming in early, staying late or working through lunch;
 - Avoiding vacation which might bring long-term espionage to light while they are gone;
 - Being motivated by a need for money or revenge.
- Beyond employees, if your organization shares data with vendors or customers, there is a danger that these entities could put your intellectual property in harm's way.

Be careful with printed information as well as electronic data.

While the fluidity of electronic data may get it most of the security attention, some studies show that 75% of data theft is done by physical actions such as dumpster diving, taking papers off a desk, making a file folder disappear, etc. Thus, print protection is important to not only guard information but also to ensure originality and authenticity. AuthentiGuard company (www.authenticate-360.com) presents these and other techniques.

- Do not print sensitive personal information unless absolutely necessary.
- Use strong locks to keep intruders out of file cabinets and other storage units.
- Shred documents but do not leave them unprotected until shredding can be done.
- Use technology on copiers that will prevent sensitive data from being copied.

Is it corporate espionage or is it competitive intelligence-gathering?

Ira S. Winkler, cited earlier, uses the term industrial espionage in discussing ways in which corporate intelligence may be gathered so that one company gets an advantage over another. Some of these methods are legal and he describes them as they relate to U. S. technology.

A company may purchase another company, or certain products, as a method to gain critical technologies. A U. S. company wishing to do business in a certain foreign country may find itself pressured to train native workers in a sought-after technology in order to do business in that country. Faced with having to give up its secrets this way, it may decide the venture is not worth it. Another avenue is a joint venture with a second company, possibly a competitor. Again, a company will have to divulge its trade secrets to make this a "go."

OSI, or open source information, can include today's news, annual reports, court papers and more. Conversations at trade shows can be a rich source of information for industrial espionage specialists who act like potential customers.

For a tough-minded look at competitive intelligence (CI) and how it can be used to benefit the strategic efforts of an aggressive, forward-looking company, read

Corporate Espionage or "Intrapreneurship," CI Fortifies Decision Making by Ark R. Johnson, November 1, 2001, (www.kmworld.com).

Corporate espionage hits the headlines, big time.

In April 2009 a lawsuit was filed in U. S. District Court for the Southern District of New York brought by Starwood Hotels and Resorts Worldwide, Inc. against Hilton Hotels Corporation and senior Hilton executives Ross Klein and Amar Lalvani. Klein was the former president of Starwood Luxury Brands Group and Lalvani was former senior vice president of Starwood Luxury Brands Group. Both were recruited to Hilton in June 2008. They are accused of stealing more than 100,000 electronic files of proprietary and highly confidential Starwood information which was then used to Hilton's benefit to enter the lifestyle hotel market and reposition its luxury brands. The act was in violation of their contractual and fiduciary duties, according to the lawsuit. Starwood is seeking compensatory and punitive damages from Hilton, Klein and Lalvani. Starwood also asks that Hilton provide a detailed accounting of the revenues derived and expenses saved because it had use of Starwood's confidential information. From (www.eturbonews.com), April 18, 2009.

In 2004 Air Canada brought a \$220 million corporate espionage lawsuit against WestJet, accusing WestJet management of using the password of a former Air Canada employee to access an Air Canada website containing commercially sensitive information. The suit was settled in May 2006 when WestJet apologized to Air Canada and agreed to pay \$5.5 million to cover Air Canada's investigation and litigation costs. Additionally WestJet was to donate \$10 million to children's charities in the name of both airlines.

On a smaller scale, in August 2008 a study by Symantec brought new information about typosquatting, the underhanded practice of registering domain names that are similar to legitimate sites but with a typo in the name. Typosquatting usually catches web surfers who mistype a domain name. Instead of getting "page not found," they end up at the typosquatting site, usually full of ads. In studying typosquatting, Oliver Friedrichs found such a domain registered to someone in China. It had no web page but had an MX record that allowed it to receive e-mail. So did the person who registered the typosquatting domain want to collect e-mail that was meant for the real company? Could your domain be at risk? To check it out, input typosquatting variants of your name in this tool: <http://whois.domaintools.com> (From Erik Larkin, *PC World*, August 15, 2008.)

Corporate espionage need not be international or flashy. Prevent backyard espionage by talking with your storage contractor about how you can further safeguard the information that is the heart of your organization.

HHS Issues Rule Requiring Individuals Be Notified of Breaches of Their Health Information

New regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached were issued today by the U.S. Department of Health and Human Services (HHS).

These "breach notification" regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations, developed by the HHS Office for Civil Rights (OCR), require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

"This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information," said Robinsue Frohboese, acting director and principal deputy director of OCR.

The regulations were developed after considering public comment received in response to an April 2009 request for information and after close consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA.

To determine when information is "unsecured" and notification is required by the HHS and FTC rules, HHS is also issuing in the same document as the regulations an update to its guidance specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information. This guidance will be updated annually.

The HHS interim final regulations are effective 30 days after publication in the Federal Register and include a 60-day public comment period. For more information, visit the HHS Office for Civil Rights web site at <http://www.hhs.gov/ocr/privacy/>

FTC Delays 'Red Flag' Rule

The Federal Trade Commission (FTC) has delayed enforcement of the 'Red Flags' rule until November 1, 2009. Following is the FTC's announcement on July 29, 2009:

To assist small businesses and other entities, the Federal Trade Commission staff will redouble its efforts to educate them about compliance with the "Red Flags" Rule and ease compliance by providing additional resources and guidance to clarify whether businesses are covered by the Rule and what they must do to comply. To give creditors and financial institutions more time to review this guidance and develop and implement written Identity Theft Prevention Programs, the FTC will further delay enforcement of the Rule until November 1, 2009.

The Red Flags Rule is an anti-fraud regulation, requiring "creditors" and "financial institutions" with covered accounts to implement programs to identify, detect, and respond to the warning signs, or "red flags," that could indicate identity theft. The financial regulatory agencies, including the FTC, developed the Rule, which was mandated by the Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA's definition of "creditor" includes any entity that regularly extends or renews credit - or arranges for others to do so - and includes all entities that regularly permit deferred payments for goods or services. Accepting credit cards as a form of payment does not, by itself, make an entity a creditor. "Financial institutions" include entities that offer accounts that enable consumers to write checks or make payments to third parties through other means, such as other negotiable instruments or telephone transfers.

The FTC's Red Flags Web site, www.ftc.gov/redflagsrule, offers resources to help entities determine if they are covered and, if they are, how to comply with the Rule. It includes an online compliance template that enables companies to design their own Identity Theft Prevention Program through an easy-to-do form, as well as articles directed to specific businesses and industries, guidance manuals, and Frequently Asked Questions to help companies navigate the Rule.

Although many covered entities have already developed and implemented appropriate, risk-based programs, some - particularly small businesses and entities with a low risk of identity theft - remain uncertain about their obligations.

The additional compliance guidance that the Commission will make available shortly is designed to help them. Among other things, Commission staff will create a special link for small and low-risk entities on the Red Flags Rule Web site with materials that provide guidance and direction regarding the Rule. The Commission has already posted FAQs that address how the FTC intends to enforce the Rule and other topics - www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm. The enforcement FAQ states that Commission staff would be unlikely to recommend bringing a law enforcement action if entities know their customers or clients individually, or if they perform services in or around their customers' homes, or if they operate in sectors where identity theft is rare and they have not themselves been the target of identity theft.

The three-month extension, coupled with this new guidance, should enable businesses to gain a better understanding of the Rule and any obligations that they may have under it. These steps are consistent with the House Appropriations Committee's recent request that the Commission defer enforcement in conjunction with additional efforts to minimize the burdens of the Rule on health care providers and small businesses with a low risk of identity theft problems. Today's announcement that the Commission will delay enforcement of the Rule until November 1, 2009, does not affect other federal agencies' enforcement of the original November 1, 2008, compliance deadline for institutions subject to their oversight.

ARMA International and ILTA Present the Legal Information Technology Conference

October 15-16, 2009- Orlando World Center Marriott

ARMA International and the International Legal Technology Association (ILTA) announce the first annual Information Technology Conference (LIT-Con) 2009: "Managing Risk Through Information Management: Current Challenges in the Legal Environment." This two-day event is designed to prepare you for today's risk management challenges.

Ethical, legal, and regulatory compliance, evolving technologies, lawyer mobility, and the current "challenging" economic environment are just a few of the issues organizations face in assessing and mitigating risk at your firm or legal department. Managing secure, compliant, and accessible organizational and client data is a responsibility that falls to everyone in the firm or legal department. This groundbreaking conference offers the comprehensive set of tools needed to collaborate in an efficient and effective way to create integrated risk management programs.

LIT-Con is designed for legal IT, conflicts professionals, records managers, litigation support, legal administrators, and anyone else whose role includes mitigating risk in the firm or legal department. It is being held concurrently with ARMA International's 54th Annual Conference & Expo in Orlando. LIT-Con attendees will have access to an Expo floor packed with more than 150 exhibiting companies, education, activities, and unmatched networking opportunities!

For more information on LIT-Con, visit www.arma.org/lit-con. LIT-Con is made possible by the support of our association partners the Association of Legal Administrators (ALA) and the Association of Litigation Support Professionals (ALSP).

About ARMA International

ARMA International (www.arma.org) is a not-for-profit professional association and the authority on managing records and information. It is known worldwide for setting standards and best practices, and for providing comprehensive education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession www.arma.org with a current international membership of more than 11,000. It also publishes the Information Management magazine.

About ILTA

For over three decades, ILTA (International Legal Technology Association) has provided peer-networking and information resources to those who support technology in law firms and law departments worldwide. The non-profit user group is truly peer-powered. For information about ILTA, or to obtain a membership application, visit www.iltanet.org.

What Happened to Customer Service?

Remember when customer service was personal? People knew your name and were familiar with your needs. You were promptly asked if you needed assistance, and the slogan "The Customer is Always Right" really meant something.

Unfortunately, in many cases there is no longer anything personal about customer service. Almost everything is now self-service, from simple purchases to pumping your own gas. Finding help while shopping in the "big box stores" always seems to be a challenge.

Increasingly companies force you to call an 800 number for service, only to be greeted by an automated phone system you need to figure out. If you do reach someone, they are in a call center in another state, or even a different country. And invariably, you get transferred from one person to the next, explaining your situation over and over again.

In short, customer service has become a frustrating experience. It seems like too many companies are more worried about the bottom line than their customers.

That is one thing that we never take for granted here at Benson Records. Being a locally owned and operated company, we put our reputation and pride on the line every day. We understand that it is our customers that drive our business, so we do everything we can to make sure their experience is a great one. It is personal and meaningful for our customers and us.

We are asked all the time what separates us from our competition, and the answer is always the same – it is our service. We have a friendly and knowledgeable staff that gets to know our customers and their needs. Valerie, Kim and Sandi show these qualities every day. They have over 18 years combined experience helping our customers with their needs.



Valerie VanderVeen
Customer Service Manager



Kim Donner
Administrative Assistant



Sandi Gonzalez
Administrative Assistant

Here is what Margie Rice, Records Manager with Fraser Stryker Law Firm, a long standing client of Benson Records, says about us: *"With more and more companies providing less and less help to their customers, it is always refreshing to deal with Benson. We talk to actual people and those people go above and beyond to help us with our every need!"*

No matter what your records and information needs might be, experience the difference that personal customer service at Benson Records can make for you and your company.