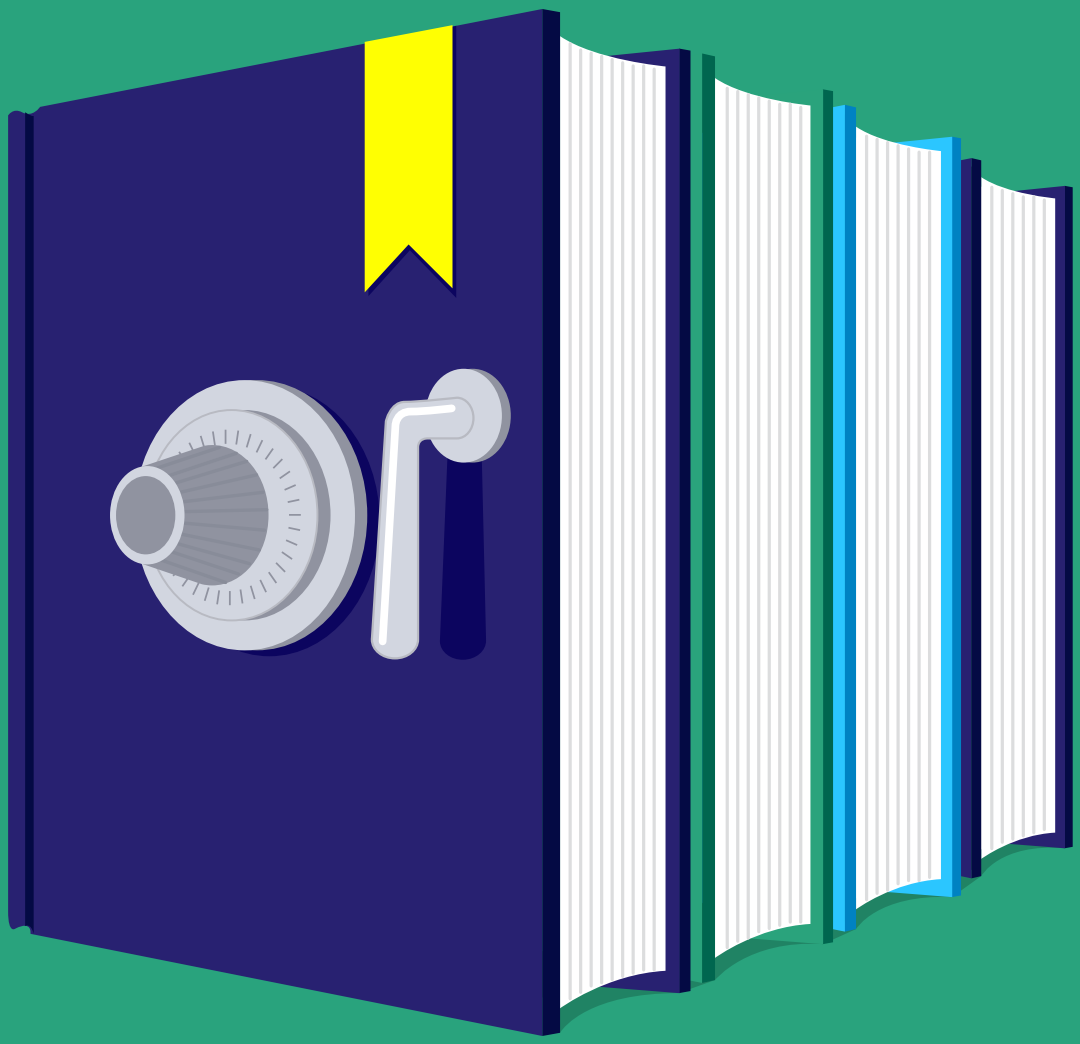
FTI JOURNAL September 2013

THE BIG STEAL

AVOIDING THE MENACE OF TRADE SECRET THEFT



Michael Pace
Global Practice Leader
Senior Managing Director
Global Risk & Investigations Practice
FTI Consulting

FTI CONSULTING™

In a recent White House speech, U.S. Attorney General Eric Holder quoted a security professional who quipped that "there are only two categories of companies affected by trade secret theft: those that know they've been compromised, and those that don't."

American Superconductor was a company that didn't know and nearly went under as a result. Technicians at the energy technology company were puzzled when a test version of their software control system didn't automatically shut down in a turbine made by China's Sinovel, the business' largest customer. To get to the root of the problem, the company thoroughly examined the software. The result confirmed its worst fears. The software had been pirated, and Sinovel now had another source for American Superconductor's proprietary code. That explained why Sinovel had ceased being a customer a month before. American Superconductor had to report to stockholders that it had lost a customer that accounted for two-thirds of the business. The stock price sank by 84 percent in just a few months.

Stories like these are all too common — and all too brazen. For example, a Chinese-born software engineer recently was convicted of stealing trade secrets from Motorola. A naturalized U.S. citizen and valued employee for nine years, she checked in for a flight to China with a one-way ticket and luggage stuffed to the brim with thousands of highly sensitive company documents. She was accused of intending to share the information with a Chinese telecom company for which she had been working clandestinely. And in 2009, 10 Starwood Hotels executives made the news after being accused of stealing copious documents that detailed the luxury hotel company's ideas and plans of previous employer Hilton.

FOREIGN GOVERNMENTS IN THE MIX

Lone individuals aren't the only culprits — foreign governments also have been implicated. Two years ago, the Federal Bureau of Investigation (FBI) rolled up a network of 10 allegedly deep-cover Russian spies. Several of them had attended Ivy League schools in America and had developed high-level connections.

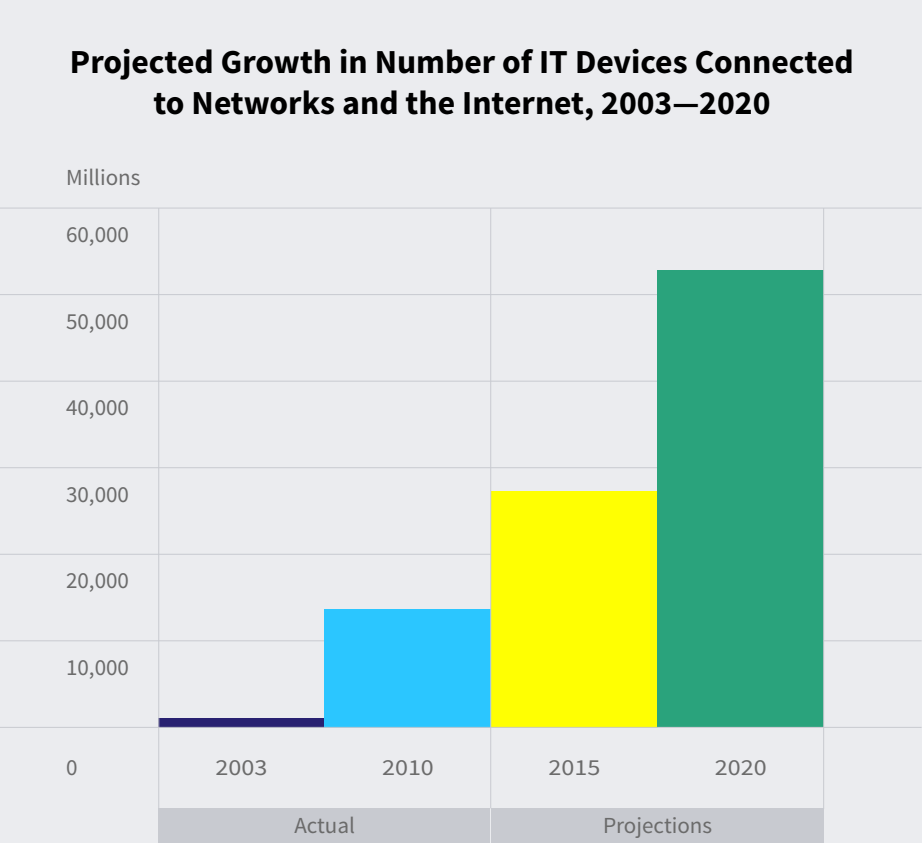
In 2011, the U.S. government uncovered a number of Chinese groups and individuals that actively were engaged in cyber spying. During the past decade, the networks of 760 companies, research universities, Internet service providers and government agencies were hit by groups of cyber spies in or from China. The list of victims includes some of the largest U.S. companies . Recently, the U.S. House Intelligence Committee declared that Chinese telecom giants Huawei and ZTE can't be trusted to install telephone and data networks in the United States. The committee argued that the potential influence exerted on the companies by the Chinese government poses a peril to national security.

Despite the threats emerging from within and from without, the majority of companies lack sufficient control of their data and trade secrets to avoid a major theft. Equally concerning, many companies don't turn to government or law enforcement for help when they suspect that important, sensitive information has been pilfered. In this article, we look at the advantages of working with government and law enforcement agencies, as well as the measures companies should be taking on their own.

COMPANIES AREN'T PREPARED

The scale and frequency of trade secret theft are rising quickly. In recent years, theft has drained more than $13 billion from U.S. company coffers. In 2010, cyber theft alone cost the U.S. economy more than $100 billion and the United Kingdom some $44 billion. The numbers keep growing as companies remain significantly unprepared. In our experience, we have found that a significant majority of IT and information security professionals don't know what data leaves their enterprise or where it goes. Most employees are saving work to external devices and email systems are often porous, leaving data exposed.

Although cyber attacks by third parties (and even foreign governments) are a growing threat, Daniel Rubinstein, a partner with the law firm Winston & Strawn, points out that most trade secret theft is committed by company insiders either working alone or collaborating with a small group of co-conspirators. The growing consumerization of technology is aiding their efforts. In the past, the theft of sensitive company information meant photocopying documents and unobtrusively removing them from an office. Today, those same documents can leave a company's control in seconds. Between 2010 and 2020, the number of devices that connect to the Internet is expected to soar nearly fivefold (see figure at right) . The enablers of trade secret theft are growing more rapidly than the implementation of measures to prevent such theft.



WORKING WITH THE AUTHORITIES

In the speech by Holder referenced above, he detailed the government's sizable enforcement resources. These include 230 specially trained prosecutors at U.S. Attorneys' offices around the country; some 240 FBI field agents; officials from U.S. Immigration and Customs Enforcement; and 20 additional international, federal and state law enforcement agencies. As Holder said: "We're fighting back more aggressively, and collaboratively, than ever before."

Strong Laws

Two strict laws add teeth to the fight: the Economic Espionage Act (EEA) and the Computer Fraud and Abuse Act (CFAA). These laws are broad in scope and define trade secrets as 1) any information that is not generally known, 2) where the value of the information lies in its secrecy and 3) the company has made reasonable efforts to protect the information.

The EEA imposes severe penalties on anyone who is convicted of knowingly stealing or duplicating information or receiving stolen information with the intent of using it for the economic benefit of anyone other than the owner. The penalties include imprisonment for up to 10 years, forfeiture and restitution. The fines can be especially stiff: $250,000 or twice the financial gain of the defendant or loss to the victim, whichever is greater.

Like the EEA, the CFAA protects confidential information. This act, however, focuses specifically on computer access and prohibits seven types, including accessing a computer with intent to defraud and trafficking in passwords. The penalties are equally potent and include prison terms of up to 10 years and fines as high as $200,000.

Powerful Enforcement

Despite the government's law enforcement and investigative resources, many companies refrain from turning to authorities often out of fear that such engagement could lead to embarrassing publicity or end up making proprietary information part of the public record. However, the U.S. Department of Justice (DOJ) and the FBI frequently are able to manage the risks and sensitivities.

Both the EEA and the CFAA, for example, allow the courts to enter protective orders to restrict access to confidential trade secrets. In addition, the Freedom of Information Act exempts disclosure of all confidential trade secrets and commercial information. Moreover, if a theft includes multiple levels of proprietary information, the DOJ can bring charges on less sensitive information in order to reduce the risk of compromising a company's trade secrets. Finally, the DOJ has the option to walk away from a prosecution if the court cannot protect important proprietary information.

Law enforcement agencies also offer unique advantages that internal investigators can't provide. The broad toolkit that authorities can utilize includes search warrants, undercover probes, grand jury subpoenas, geolocation technology and wiretaps. If law enforcement is brought in early, stolen data may be recovered, minimizing the impact on the company.

Turning to law enforcement can help prevent future thefts. Its mere presence at a company sends a strong message that the organization takes threats to its proprietary information seriously. Law enforcers can help a company understand how a theft occurred and determine what preventative measures it needs to put in place.

BEING AT THE READY

Rubinstein suggests that, in order to move swiftly and effectively after a theft is discovered, companies should have a standing cross-functional response team ready. The team should include members from legal, IT, human resources (HR), public relations (PR) and corporate security, with protocols and processes in place. Legal, for example, should examine which laws have been violated and assess what legal avenues can be pursued, including the use of law enforcement agencies. The IT department can ascertain what electronic evidence exists and where it is located. HR can provide pertinent employee background information, and PR can evaluate if and how to report the incident. Corporate security brings the effort full circle by implementing new measures based on what occurred.

We also recommend that companies take these preventative measures:

- Develop clear policies that limit access to proprietary information only to those who need it.
- Limit the amount of data that can be electronically copied, possibly even disabling USB and DVD ports and prohibiting the use of cloud storage sites.
- Conduct detailed employee background checks at the time of hire and follow up with periodic credit checks on employees in sensitive roles. Obtain permission for these checks in advance as part of routine onboarding processes.
- Use website banners, employee confidentiality agreements, training and other communications to leave no doubt that certain company information is proprietary and may not be disclosed. These measures help demonstrate to the courts that the company has made efforts to protect its trade secrets.
- Understand what data the company has and where that information is stored.
- Monitor and audit networks and maintain thorough records of who is accessing servers, as well as modifying, copying, deleting or downloading files.
- Make use of multifactor authentication measures such as biometrics, personal identification numbers and passwords, combined with knowledge-based questions, to assure that only legitimate users have access to proprietary information.
- Secure agreements from employees that detail what expectation of privacy they have on company-owned devices.
- Use e-mail journaling software that records enterprise e-mail messages and provides copies even if users attempt to delete written communications permanently.
- Be on the lookout for potential indicators such as an employee's change of mood, financial distress, office presence at odd hours and reports of lost or damaged computer equipment.
- Establish social media policies that minimize data loss from online social networking.

Trade secret theft is a growing risk for every company. It is being perpetrated by both individuals and wealthy foreign governments. The U.S. government and its law enforcement arms are ready and willing to help companies when an incident occurs. That support, along with proper preventative measures, can help businesses avoid the menace of trade secret theft and its significant financial consequences. ■

References

1. Bloomberg News, Market Intelligence Data
2. Source: Cisco Systems

Michael Pace
Global Practice Leader
Senior Managing Director
Global Risk & Investigations Practice
michael.pace@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.