CYBER-ESPIONAGE

BY ERIC KRELL

The proliferation of industrial and economic espionage incidents reported in the news media sound wickedly sophisticated and dizzyingly complex.

With increasing, nearly daily, frequency we read about crippling denial of service attacks, instances in which millions of customer records are swiped and estimates of billions of U.S. dollars lost to pilfered intellectual property (IP). It's easy to picture Lex Luthor-esque hackers hunkered over keyboards in their high-tech lairs. But many of these accounts, not to mention our imaginations, are misleading, according to the world's leading cybersecurity experts.

"Generally, these criminals take advantage of the most basic and simple vulnerabilities that exist in an organization," explains Ira Winkler, the president of Annapolis, Md.-based security firm Secure Mentem and a renowned security expert who has been called "A Modern Day James Bond" by CNN. "...These attacks rarely involve super-advanced techniques."

As the frequency of attacks on companies' trade secrets (i.e., "industrial espionage") and countries' IP (i.e., "economic espionage") mount, it is important for business managers and executives inside and outside the information technology (IT) and security functions to understand the true nature of these acts. The need for this understanding coupled with knowledge of the most effective security practices intensifies as more managers and executives, at companies of all sizes, travel internationally with greater frequency.

"It has become much, much easier for companies in many different countries to trade with each other," notes professor of Economics Steve Gardner. Gardner, who chairs the department of Economics and serves as director of the McBride Center for International Business in the Hankamer School of Business, describes this reality as the positive side of one of several "good news/bad news" dynamics defining global trade today. The bad news attached to the growing ease and volume of international travel, as well as ubiquitous Internet and communications connectivity (including smart phones and other mobile devices), is that more business travelers and more companies are exposed to greater cybersecurity and IP-theft risks.

This risk is no longer unique to large, multinational conglomerates. Given the increasingly global nature of competition, the need to keep sourcing costs extremely low and the need to recoup product investments quicker among other drivers, more small companies, notes Les Palich, who holds the W.A. Mays Professorship in Entrepreneurship, "have little choice but to go international, depending on their product or service offering."

Luke Benice, managing director of Security Management International (SMI) in Falls Church, Va., confirms that "a lot more smaller companies, even mom-and-pop-sized organizations are travelling globally more frequently – and more people are travelling with intellectual property." Benice, a former Raytheon Company security consultant who previously served on the U.S. Department of State's Foreign Emergency Support Team, also says professionals in smaller to mid-sized companies are less likely to receive the same level of cybersecurity and IP-theft training that their counterparts in Fortune 500 companies receive.

"It's easy to picture Lex Luthor-esque hackers hunkered over keyboards in their high-tech lairs. But many of these accounts, not to mention our imaginations, are misleading, according to the world's leading cybersecurity experts."

REWIRING

OUR CYBER THINKING AND PRACTICES

The misconceptions surrounding cyber-espionage center on the techniques and defenses, not the magnitude of the threat.

"The ongoing cyberthefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history," writes U.S. Army General Keith Alexander, who also serves as director of the National Security Agency, chief of the Central Security Service and commander of the United States Cyber Command.

Industrial espionage is also a major problem. Last year, Twitter suffered a cybersecurity breach that exposed usernames, email addresses and passwords of a quarter-million of its users; JP Morgan notified 465,000 prepaid cash card holders whose cards may have been hijacked, and cybercriminals swiped credit card data from more than 2 million customers of St. Louis-based food-store chain Schnucks. Not to mention the recent breach that exposed the credit card and debit card information of as many as 70 million Target customers who swiped between Nov. 27 and Dec. 15, 2013. Yet, these examples represent only a sliver of all cyber attacks: according to IBM, an average of 1.7 cybersecurity incidents – an attack that organizational security experts examine and then investigate further – occur each week within global companies.

Understanding individual human vulnerabilities represents a crucial step in fortifying an organization's cyberdefenses, Winkler and Benice agree. A prudent initial step involves recognizing several common misconceptions that often hamper organizational security capabilities; these include:

OVERESTIMATING the Adversary:

"The first misconception is that these criminals are geniuses," says Winkler. "Most of the criminals who are out there are kind of on the pathetic side. They really just get lucky because organizational protections are so poor."

NEGLECTING Effective Forms of Defense:

"The second misconception is that [cybersecurity] requires highly advanced methods and technology," Winkler notes. "Most organizations make themselves incredibly vulnerable." Examples of this vulnerability include leaving doors and building unlocked, failing to update computer operating systems and anti-virus software, and carelessly disposing valuable information in hard copy form (e.g., by tossing it in the trash).

IGNORING Brain Drain:

Oftentimes, the most valuable trade secrets stroll out the front door – unprotected by basic non-disclosure agreements (NDAs) – when employees leave the company for another organization or are fired.

Recognizing and correcting these judgment errors can help organizations focus more attention on the most effective ways to bolster their cyberdefenses:

1 Address the Basics First: Lock doors and buildings, ensure that employees who work with sensitive information and data sign NDAs, update operating systems and anti-virus applications (on all hardware, including smart phones and other mobile devices), and revisit knowledge management and transfer policies to ensure they address the protection of sensitive information.

2 Create and Sustain Awareness: Many cybersecurity and industrial espionage training sessions function more as check-the-box compliance activities, Winkler observes. The key to effective training, he adds, is sustained awareness. This awareness inspires business travelers to think twice before leaving a laptop in a hotel room, accessing a public Wi-Fi connection, or dashing off a work email in a far-flung internet café (where you should expect keystroke loggers to be lurking close by, says Benice).

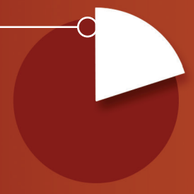
3 Address Technology, But Focus on Human Glitches: Technology plays a major role in cyberdefense, and some of these considerations – protecting professional and personal mobile devices or cloud-based data, for example – can be quite difficult. However, the most important defenses to shore up are more sentient: flattering, curious and chatty neighbors on international flights, for example.

"Everybody thinks that cybersecurity is number one when it comes to preventing industrial and economic espionage," Benice adds, "But the old-fashioned tricks more often result in losses compared to someone hacking your email account from a distance. The human factor is huge."

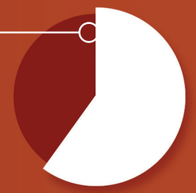
bbr.baylor.edu/cyber-espionage

CYBER CRIME Adds Up

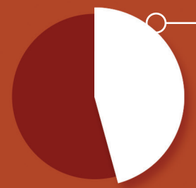
20% Portion of global businesses with procedures dedicated to protecting intellectual property (IP)



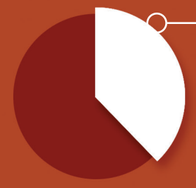
60% Portion of security budgets among Asia-Pacific companies expected to increase in 2014



46% Portion of security budgets among European companies expected to increase in 2014



38% Portion of security budgets among North American companies expected to increase in 2014



Note: First four figures from PricewaterhouseCoopers 2014 Global State of Information Security Survey; the fifth figure comes from 2013 IBM Cyber Security Intelligence Index; the final figure comes from software security Symantec.

Top 5 Most Cyber-Attacked Industries Globally 2013:

1 — Manufacturing
2 — Finance and Insurance
3 — Information and Communications
4 — Health and Social Services
5 — Retail and Wholesale

378 million adults globally experienced some form of cybercrime between October 2012 and October 2013; the total cost of these crimes reached $113 billion.