SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Programs & Operations > Counterintelligence >

Economic Espionage and the Growing Case for Corporate Counterintelligence

Created by John Slattery, SEC Emeritus Faculty, former Federal Bureau of Investigation Counterintelligence Deputy Assistant Director

In the 2016 movie "Snowden," former National Security Agency intelligence contractor Edward Snowden uncovers massive amounts of illegally obtained data assembled to track digital communications from foreign governments, terrorist groups and ordinary Americans. For many, the biographical political thriller was a wakeup call. For those in risk management and information security, it reaffirmed what we probably already knew or suspected — that many different entities around the globe know quite a bit about where we work and live and our daily habits.

For corporate businesses, information protection is critical and the risks and threats keep changing. Now, information and intelligence is increasingly gathered on U.S. companies from foreign entities that use the results for a variety of different types of what is now called economic espionage.

In a nationwide campaign launched by the FBI aimed at educating business and industry leaders about the growing threat — and mounting losses — of economic espionage, Andy Ubel, the chief intellectual property counsel of Valspar Corp., stated: "My company had firsthand experience dealing with an economic espionage case." Ubel was included in the campaign and corresponding video, The Company Man: Protecting America's Secrets. The video, created by the FBI in collaboration with the National

Counterintelligence and Security Center (NCSC), is based on an actual case involving the attempted theft of trade secrets from the U.S. company by a foreign competitor.

According to the Chicago Division of the FBI, a former chemist for Valspar's architectural coatings group pleaded guilty in 2010 to theft of trade secrets, admitting he stole formulas and other proprietary information valued at up to $20 million as he prepared to go to work for an overseas competitor. He confessed to using his access to Valspar's secure internal computer network to enter databases containing trade secrets and to download approximately 160 original batch tickets, or secret formulas, for paints and coatings, stated an FBI press release.

Trade Secret Theft and Competitive Resource Compromise

There have also been cases of trade secret theft, which included Dumpster diving for intellectual property such as discarded prototypes. In one case, the FBI said, Chinese nationals were caught digging in cornfields in Iowa in search of seeds developed by a U.S. company for pest and drought resistance. While the theft of corn seeds seems inconsequential on its surface, the company that developed them spent tens of millions of dollars on technology and research to come up with its formula.

Economic espionage and its players circumvent normal costly research and development by copying methods of production or other processes. In one example given by the FBI, spies targeted the manufacturers of sprinkler heads hoping to gain an edge in their market by stealing specific production data that led to greater economies of scale.

In 2015, the FBI's Counterintelligence Division said in a news report that there was a sharp spike in the number of espionage investigations by the agency, citing a 53% increase in caseloads and with state-sanctioned corporate theft by China at the core of the problem. It added that spies of Chinese origin were using dramatic tactics to steal critical information from U.S. companies. At the time, Beijing was cited as the most predominant threat facing the U.S.; an FBI survey of 165 U.S. companies found China was the perpetrator in 95 percent of economic-espionage cases.

Global Threats to U.S. Businesses Heighten

Although the exact dollar figure of the losses to U.S. businesses from economic espionage is difficult to document, the amounts are substantial. A 2013 report by the Blair Huntsman IP Commission, The Report of the Commission on the Theft of American Intellectual Property, estimated the total losses in the "hundreds of billions" each year. Those numbers did not take into consideration companies that do not detect, do not report, or under-report losses tied to economic espionage.

Those responsible for the theft are usually foreign competitors or governments looking for trade secrets, production methods, innovations and even insights into labor or trade disputes.

The Office of the Director of National Intelligence (ODNI) released the National Counterintelligence Strategy of the United States 2016 to address "the diverse threats and challenges which include not only foreign intelligence services and their surrogates but also terrorists, cyber intruders, malicious insiders, transnational criminal organizations and international industrial competitors with known or suspected ties to these entities."

The strategy was developed in accordance with the Counterintelligence Enhancement Act of 2002 (Pub. L. No. 107-306, 116 Stat. 2383 (as amended) codified at 50 U.S.C. sec. 3383(d)(2)). It sets forth how the U.S. Government will identify, detect, exploit, disrupt, and neutralize foreign intelligence entity threats. It provides guidance for the counterintelligence programs and activities of the U.S. Government intended to mitigate such threats.

According to NCSC, foreign intelligence entities, which may include foreign governments, corporations, and their proxies, are actively targeting information, assets and technologies vital to both U.S. national security and global competitiveness. Every business, corporation, and vertical market may be at risk from these new threats, and now, establishing in-house counterintelligence (CI) programs is considered a necessary proactive measure.

Late last year, during a Security Executive Council (SEC) Security State of the Industry briefing, the organization dug deep into the topic of emerging risks and threats to corporate business information today—and how to protect and provide CI effectively.

The online briefing for the SEC's Tier 1 Security Leaders featured leading industry experts who identified horizon and emerging issues and the process and value proposition for establishing an in-house CI team.

I was joined by presenters Dina Corsi, Deputy Assistant Director, Counterintelligence Division, FBI; and Brad Brekke, former Director, Office of Private Sector, FBI and former Vice President of Security, Target Corp. and led by moderator Bob Hayes, SEC Managing Director. The briefing focused on rising threats and significance of malicious acts to corporations, as well as the expanding profile of potential perpetrators.

"When you hear counterintelligence, many think about it in military terms. But corporations are now being targeted at such a high rate that it's creating an urgent responsibility for corporate security to address the issue," said Bob Hayes.

Identify, Engage, Protect

CI is often misunderstood, and the world has changed, with new and ever-hostile adversaries emerging. Now, CI threats can come from a broad range of determined collectors, including employees and other trusted insiders, hackers, subcontractors, strategic business partners and even those in academics. And it's no longer simply about classified material; it is increasingly about technology-related proprietary data and intellectual property. As a result, the SEC stated that the CI threat is more significant than ever and is no longer 'spy versus spy.'

The best CI plan will identify assets most valuable to the company, engage and integrate internal physical and information security elements, and then engage and enlist the help of external elements like the FBI, law enforcement and industry security partners to enhance the protection of those assets.

Brad Brekke said the theory of CI should address cybersecurity as well as global and company business processes that may be susceptible to threats, and it must develop a value proposition based on theory but which maps out a planned approach. "This is an existential threat, of a magnitude that hasn't been clearly defined yet. Effective CI doesn't just raise a flag – it provides a plan to address the issues," Brekke added.

Corporate security executives need to define and discuss the risks with executive leadership, determine relevance and pertinent assets and develop a strong CI value proposition. At Target Corp., Brekke said the most important asset was data analytics on guests. "Target had acquired a lot of analytics based on guest data and the web, and at the time the trend was to outsource those analytics. We enlisted the support of the federal government to bring a different perspective to senior leadership on why they needed to establish an in-house CI team. Ultimately, what we were able to offer, at its core, was a small intelligence team that developed information working with service providers and agencies. We provided information and intelligence on determining potential threats. Initially, senior management thought cyber threats only affected certain companies. It was a challenge to inform senior leaders of the wide range of threats."

He added that three "E's" are the starting point for any CI discussion with management: **evaluate** and classify the risk assessment and potential threats; **engage** with the local FBI field office and other industry experts; and **educate** stakeholders by assessing risk from the C Suite to the bottom up and consider everything, including hiring practices."

Proactive Planning Can Lessen Potential Attacks

It's clear that getting out in front of issues and being proactive is critical. If an organization has a proprietary crown jewel or intellectual property that constitutes its lifeblood, a traditional security program alone might not be enough to adequately protect those assets from theft or compromise. CI 'thinking' expands the standard

security protective aperture by considering a broader scope of potential collectors who might be targeting those valuable items, as well as the techniques they use to accomplish that collection, which can be sophisticated and persistent.

In many corporate security organizations, CI is the cornerstone enabler of insider threat programs, especially for companies who support the U.S. National Security Industrial Base. CI can provide another set of eyes and ears along with a potentially more globally oriented mindset so that threats will be better understood and risk can be more fully defined. There has been an uptick in the deliberate targeting of U.S. trade secrets, intellectual property and next-generation technologies that are still evolving. CI, when implemented properly, can help level the playing field – because today, many other countries don't always play by the rules. Despite many recent examples of foreign government-sponsored (or condoned) thefts and compromises of trade secrets, U.S. private sector organizations sometimes still fail to consider the security risks that globally interconnected commerce brings.

A CI program can and should act as a force multiplier for other corporate security initiatives. CI integration with information assurance and cyber security assets is especially important. Many cybersecurity programs feature tremendous technical tools but fail to incorporate CI considerations into their threat analyses. This can create blind spots and an incomplete threat picture, especially with respect to the origin and attribution of specific threats. Many security programs are also increasingly being forced to deal with things like the 'off-campus' employee, where activity on the organization's networks is minimal and the majority of the activity is being conducted on someone else's systems and networks. Safeguarding sensitive information on multiple domains in multiple locations is always a challenge, but adopting a robust CI posture typically encourages security programs to consider additional threat vectors like these in the overall mitigation strategy.

Due diligence associated with mergers and acquisitions also benefit from a 'CI look', especially when there is a known foreign component involved. Assisting corporate investigations, fostering direct relationships with government agencies and networking with industry partners for training and threat intelligence sharing are additional examples of how CI resources bring additional insights and add value.

Because the concept of counterintelligence sometimes remains misunderstood in the corporate realm, some socialization and education are needed. The CSO must be able to comprehend the concept fully and know how to explain it to others in the organization so expectations are understood from the top down and everyone's role can be defined. They must own the program, right out of the gate, and that will help with its successful implementation. They must construct a transparent governance plan and be prepared to deal with possible cultural resistance.

Resources and Information on CI

Many organizations seeking to drive a successful CI program start by bringing in professionals trained in the CI discipline. These assets are easier to find than one might think. In addition to former federal CI practitioners (FBI, CIA, Department of Defense, etc.), organizations are turning to intelligence community analysts with CI expertise as well as former state and local law enforcement personnel, many of whom bring other knowledge, skills and abilities with them like investigations and interviewing.

There are also many great programs in intelligence analysis and exploitation at the college and university level, educating and training the future workforce on CI and threat analytics. The right person can help drive a program, but they need to be integrated with the proper tools, enabling partners and resources.

Corporate CI will never catch on in an organization that adopts a "sky is falling" philosophy. However, once you determine that a CI program might be right for your organization, take a measured and balanced approach. Clearly articulate a transparent policy and expectations, reinforce it through education and awareness training, and then roll it out in an iterative fashion. Hold the program owner accountable, ensure that governance and oversight are prevalent, and then manage it with discretion and employee privacy in mind.

Visit the Security Executive Council website for other resources in the Security Strategy & Operations > Counterintelligence series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/