SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations >
Counterintelligence

The Emerging Role of Information Protection and Counterintelligence in Corporate Security

How corporate security can address current risks and develop proactive measures

Digging deep into emerging risks and threats to corporate business information today, the Security Executive Council (SEC) on September 12, 2017 presented a Security State of the Industry briefing on information protection and counterintelligence (CI).

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.

Presenters included moderator Bob Hayes, SEC Managing Director; Dina Corsi, Deputy Assistant Director, Counterintelligence Division, FBI; Brad Brekke, former Director, Office of Private Sector, FBI and former Vice President of Security, Target Corp.; and John Slattery, SEC Emeritus Faculty and former FBI CI Deputy Assistant Director. Each speaker had significant global knowledge on the issue—with the topic focusing on rising threats and significance of malicious acts to corporations, as well as the expanding profile of potential perpetrators. Dina Corsi covered the changing face of the counterintelligence

threat. (Editor's note: By request of the FBI we are limited in our ability to provide specific details about her presentation).

"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. "The goal of today's presentation is to demystify the CI topic, determine if CI is a relevant fit for organizations, and examine programs from leading corporations and organizations."

Identify, Engage, Protect

According to the speakers, CI is misunderstood, and because the world has changed, new hostile adversaries have emerged. Now, CI threats can come from a broad range of adversaries, including employees and insiders, hackers, subcontractors, business people and even those in academics. And it's no longer simply about classified property; it is increasingly technology related. 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 and engage and enlist the help of the FBI, law enforcement and others in partnership to make those assets easier to protect.

Brad Brekke said the theory of CI should address cyber security as well as global and company business processes which may be susceptible to threats—and 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 its 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."

John Slattery said getting out in front of issues and being proactive is critical, and CI is the cornerstone enabler of insider threat programs. "CI can provide another set of eyes and ears so a globally focused risk mindset can be more fully defined. There is deliberate targeting of U.S. trade secrets and next-generation issues that are still evolving. CI, when implemented properly, can help level the playing field—because today, other companies don't play by the rules." He added that a CI program is a force multiplier for other security initiatives and should integrate with cyber security.

"The CI resource also brings additional insights that can be used for special initiatives, liaison with agencies, networking with training partners—adding value to the business case for deploying a program."

The overarching theme of the event was that CI is no longer the sole responsibility of the cyber security team, commented Bob Hayes. "It's a whole, cross-functional team that has to work together and define individual roles. Partnership between all stakeholders has to be there."

Resources and Information on CI

Slattery said many organizations and groups can assist with finding the best information and resources to drive a successful CI program. "The greatest value of a CI program comes from bringing in law enforcement at the local level. Organizations like DHS and FBI have analytics and deep security analyses on the topic. There are also many great programs in intelligence analysis and exploitation at the college and university level. The right person can help drive a program, but they need to be integrated with the proper tools and resources."

Brekke added that the FBI has local agency members who focus on the issue and now engage and partner more fully with the corporate world. "There is a bit of urgency now because this issue is moving much faster over the last year. CSOs and CIOs need to understand the scale and scope of the threat and strategize a measured approach," he said.

A few of the resources noted during the briefing included:

Economic Espionage: Protecting America's Trade Secrets

A Corporate Counterintelligence Guide - dni.gov

Insider Threat is a Challenging Organizational Problem

Visit the Security Executive Council website for other resources in the Security Program 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/