SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Solution Snapshot: Protecting Intellectual Property

Mark A. Levett , Vincent Volpi, Chris Cox, Mary M. Forman

Originally Published in SecurityInfoWatch.com

November 2009

Solutions Snapshot: Protecting intellectual property

How can I best protect my organization's intellectual property?




How can I best protect my organization's intellectual property?

Mark A. Levett, Unit Chief, Counterintelligence Div, FBI Headquarters

Foreign espionage accounts for annual losses in the United States exceeding $250 billion. The first step in protecting intellectual property (IP) is to clearly identify what unique company assets are considered critical to your business continuity. Precise identification of IP is critical when allocating scarce security resources to a Counterintelligence (CI) protection plan.

The next step in risk management is to determine the threat to your IP. The FBI can assist in identifying the foreign espionage threat and the specific tradecraft utilized to steal IP.

Tradecraft includes the recruitment of a trusted insider, cyber intrusions and covert measures cloaked as overt business transactions. The FBI's Counterintelligence Division has a headquarters section and 56 field offices with Strategic Partnership Coordinators (SPCs) dedicated to assisting the private sector in identifying the threat to IP posed by foreign espionage. SPCs are able to provide CI Awareness briefings and CI Vulnerability Assessments to ensure companies have strong CI programs.

Vincent Volpi, Chairman and CEO, PICA Corporation

The first level of protection of intellectual property has to do with the creator. If the creator isn't under a solid contract and doesn't understand the importance of confidentiality and basic security precautions, all can be lost. Most creators are inventors, scientists or artists, not lawyers or security professionals.

Maintaining "four-wall" security and information security (including "need-to-know" criteria), are other common basics. Otherwise, to commercialize IP requires that you share it with others. This includes people involved in legal, sourcing, marketing and sales. Legal should be at the forefront, controlling everyone's use of IP by contracts that are strong, venue-specific and enforceable. Contracts also need to contain audit, compliance and penalty provisions.

Finally, you need a brand protection program designed around your budget and primary consuming and producing markets. You can't protect the world, so you have to protect the most important parts of it.

Chris Cox, President, Operations Security Professional's Association

There are many things to consider when protecting your intellectual property. Of course, you'll need to copyright your work, when applicable, and physically protect your facilities using safes, surveillance and whatever else would be cost efficient and effective. However, it's the human element that's all-too-often overlooked. There's a saying within the operations security community: "If you don't know what you're trying to protect, how will you protect it?" In other words, if your employees don't know what information is critical to your organization, they can't be expected to know what they should protect, or how to do so.

Also, employees need to be trained to recognize and react to social engineering attempts, which are low-tech attempts to steal information by exploiting human nature. Once they can identify the critical information and understand the threats, all employees become part of your security team.

Marcy M. Forman, Director, National Intellectual Property Rights Coordination Center

Take part in the fight to protect your rights. The National Intellectual Property Rights Coordination Center (IPR Center), hosted by U.S. Immigration and Customs Enforcement, is the government's leader for information related to potential criminal IPR violations. The IPR Center employs a true task-force model to optimize the roles and enforcement efforts of member agencies, while enhancing government-industry partnerships to support ongoing IPR enforcement initiatives. The center employs a three-pronged strategy, involving investigation to track down counterfeit goods, interdiction to stop them, and training and outreach to industry stakeholders and the public.

Leads received from industry are analyzed and vetted by agency partners, and reviewed for criminal investigation or interdiction activity, as appropriate.

Start by visiting our Website at **www.ice.gov**. There you will find contact information, and links for reporting an alleged IPR violation and to the IPR Center Report, a newsletter with information on enforcement activities and industry trends.

Next Month's Question: How can I make a good business case for a proactive security project

*Solutions Snapshot is presented by the Security Executive Council; visit the **SEC website** for more information about the organization.*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com