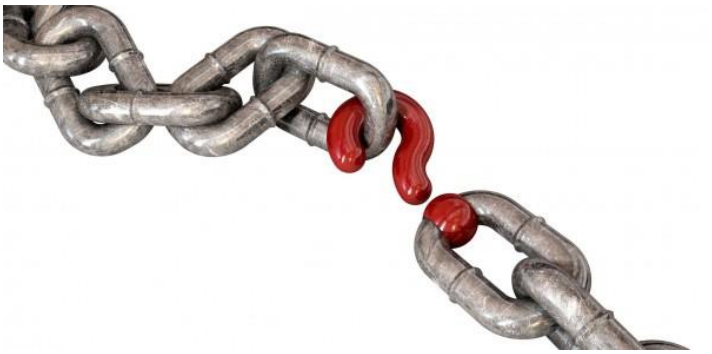
Supply Chain Risk Management

San Diego ISAC Counterintelligence Sub-Committee - September 2016



Supply Chain Risk Management
So what exactly is Supply Chain Risk Management? Well, here is a definition: Supply Chain Risk Management (SCRM) is a discipline that addresses the threats and vulnerabilities of commercially-acquired information and communications technologies within, and used by, any given company. At its most basic, any company has the goal to ensure the integrity of the equipment being used to process competition sensitive, company proprietary and higher categorizations of information and materials. Through SCRM, Information Technology or Information Assurance Systems Engineers can minimize the risks to systems and their components obtained from sources that are not identifiable or trusted. Additionally, Buyers and Global Supply Chain personnel can limit inferior material or parts and ensure business continuity.

Why Should the Facility Security Officer Care?
The preceding paragraph mentioned numerous disciplines outside of Industrial Security, which leads to the old adage of staying in proper swim lanes….right? Wrong. It is important for the Facility Security Officer (FSO) to become an integrated member of Site Leadership, as only then will the FSO be able to fully administer the requirements properly identified in the National Industrial Security Program Operating Manual and supplemental Industrial Security Letters. Counterintelligence within cleared defense contractor activities has the following citation at its core:

> NISPOM 1-302b. Suspicious Contacts. "Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported."

The FSO is encouraged to think beyond the standard viewpoint of the threat being a foreign visitor or unknown solicitor external to the organization. Imagine if you will that you are in charge of a large program and are tasked with setting up the information systems network which will process sensitive information. You order 50 desktops, 5 routers, 5 printers, and all the additional peripheral devices fulfilling the identified needs of the program. When the shipment comes in, Information Technology or the Information Systems Security Manager registers the routers and discovers 3 of the 5 have already been registered for service warranty. How is this possible for newly furnished equipment which was purchased from a reputable vendor? Often, what seems on the surface to be a glitch in the registration of the equipment is in-fact an indicator of counterfeit or tampered-with parts or software. In the worst case scenarios, this glitch could have the backdoor capability to transmit to a foreign country. No doubt this type of activity falls within the counterintelligence category of suspicious contact. While the indicators exist, it is believed many companies fail to register hardware and software as part of information security governance, leaving those companies susceptible to compromise of information and materials without notice.

The Threat Recognized

The supply chain threat is now recognized as a major cyber threat affecting development and operation of computer systems. National Security Presidential Directive (NSPD) 54, Homeland Security Presidential Directive (HSPD) 23, and National Defense Authorization Act 254 have made SCRM a national priority. The Center for Development of Security Excellence (CDSE) is also a valuable resource for the FSO detailing SCRM.

The Justice Department recently revealed that Federal Authorities over the past five years have seized more than $143 MILLION worth of counterfeit computing hardware, software, and labels in a coordinated operation that has netted more than 700 seizures and 30 felony convictions. In addition to costing world-recognized computing companies and other U.S. businesses millions of dollars, scams like these could threaten national security by infusing critical networks with hardware and software that is unreliable or worse, riddled with backdoors, spyware, or malware.

What Can the FSO Do?

Awareness of topic of SCRM is beneficial; however, the FSO needs to become engaged with internal company elements to help combat the fraudulent activity. Learn the processes your company follows for procuring equipment; build relationships with those individuals and disciplines which are involved in the integrity and daily usage of equipment. These individuals are best suited to identify any anomalies, which can be reported to the FSO. The FSO can then in-turn report to the applicable Defense Security Service (DSS) Counterintelligence Agent as well as the respective customer counterintelligence entity, whether that is Air Force Office of Special Investigations (AF OSI), Department of Homeland Security (DHS), Naval Criminal Investigative Service (NCIS), or any other applicable organization. Reports can be investigated and validated, or better yet disproved. Not only will the FSO be recognized as a team player adding value to the company, but the reporting will also strengthen the overall defense network protecting our nation's best interests.