Corporate Espionage and Protecting Proprietary Information

Apr 27, 2016
Author: J.D. LeaSure, CCISM, President. ComSec LLc

- **On average, corporate espionage costs businesses more than $400 billion yearly.**
- **Certain precautions must be incorporated into the framework of an effective Data Security Program to protect valuable corporate information from espionage attempts.**
- **TSCM is an acronym that stands for *Technical Surveillance Countermeasures*.**
- **Personnel charged with maintaining your cybersecurity program are trained to detect network threats, and typically are not trained to detect eavesdropping devices.**
- **If your risk management program does not include Cyber TSCM™ , you have made the job of the corporate spy much easier.**

On average, corporate espionage costs businesses more than $400 billion yearly. Corporate information theft implements can range from cyber espionage attacks

in your enterprise to the use of bugging devices to capture data, audio or video. The individual or "spy" behind the attack may be anyone motivated to: damage the reputation of a business, access insider information to profit from making illicit trades, undermine relationships with business partners, gain a competitive advantage or access personal/sensitive data.

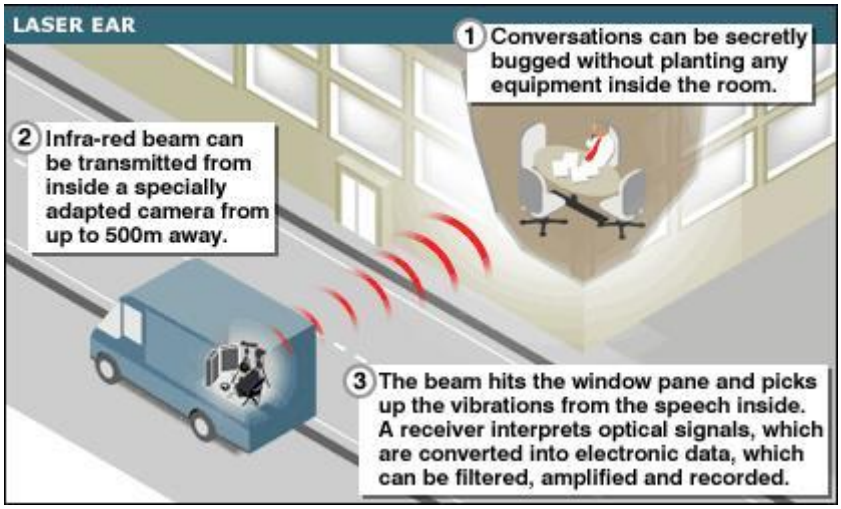
Preventing the success of corporate espionage attempts is challenging. Data Security and Compliance efforts require controls to limit and prevent unauthorized access, theft or disclosure of sensitive data. Executives must also ensure valuable corporate intellectual property is protected from theft and/or unintended disclosure. Misconceptions about information security can leave companies vulnerable. These vulnerabilities can go undetected for long periods of time and may result in significant corporate losses.

A recent Wall Street Journal article mentioned that a big part of that push is old-fashioned human intelligence, or 'humint' in military and intelligence parlance. These firms are using real people and traditional spycraft to foster interpersonal relationships and trust across a nebulous and often anonymous network of hackers, middlemen and those benefiting from purloined data.1

The reality is that internal audit programs cannot detect all threats. Most programs do not even address detecting electronic eavesdropping threats, including eavesdropping threats that use the cellular network to capture network data. To protect valuable corporate information from espionage attempts certain precautions must be incorporated into the framework of an effective Data Security Program. These precautions include preventive TSCM/Cyber TSCM™.

WHAT IS TSCM ?

TSCM is an acronym that stands for *Technical Surveillance Countermeasures*. The term refers to methods used to detect, negate and exploit penetration technologies. TSCM involves the methods and technologies used to detect illegal eavesdropping. Technical surveillance is one tactic that can be used by corporate spies to access and steal critical information that must be protected by your organization. In fact, corporate espionage has been conducted using electronic eavesdropping devices for decades. But, any belief that eavesdropping device technology is outdated is a misconception. Eavesdropping devices are now smaller, technologically advanced, can be remotely activated, can exploit connectivity vulnerabilities efficiently (e.g. 3G, 4G, Wi-Fi, apps, IoT devices, etc.) and do not require frequent battery replacement unlike their predecessors. Modern bugging devices are a credible threat to effective data and intellectual property protection.



WHY IS TSCM IMPORTANT IN PREVENTING THE SUCCES OF CORPORATE ESPIONAGE ATTACKS?

Methods for storage and protection of intellectual property and enterprise data can differ. Intellectual property is often intentionally not stored on corporate networks to protect this information from cyber attacks. If the information is not stored on your network, cybersecurity measures do not protect it. A “spy” may use audio recording devices, video recorders, key loggers or other electronic eavesdropping devices to steal corporate intellectual property that is not stored on your network.

Corporate information stored on the network requires other considerations. A strong cybersecurity program is vitally important. But, spies typically choose the path of least resistance. As corporate cybersecurity programs become more effective, use of electronic eavesdropping tends to increase. Striking the proper corporate balance between cybersecurity controls and electronic eavesdropping detection can strengthen your information protection program.

Preventive TSCM /Cyber TSCM™ that addresses new risks is the most effective approach. All organizations are unique and will have certain compliance challenges and goals. But, developing a strategy to detect data breaches and attempts to steal intellectual property that considers: the evolution of new and emerging threats, changes in your organization and corporate goals and objectives, will better protect your brand, corporate reputation and ensure your data and information are secure.

A thorough TSCM survey should include a physical and electronic inspection designed to detect audio and optical threats. The detection of telephone taps, wireless transmitters, wire and microphone taps is another critical component of an effective sweep. A detailed post-operation report should be provided. This report should provide details regarding any findings and recommendations to mitigate future risk of recurrence.

Cyber TSCM™

Personnel charged with maintaining your cybersecurity program are trained to detect network threats. Typically, they are not trained to detect eavesdropping devices that may exploit the cellular network. They also cannot detect hybrid devices (e.g. are they trained to detect a data cable with an embedded eavesdropping device used to listen to conversations in the C-Suite?) Regretfully, our goal can no longer be purely prevention – we must proactively search out and hunt down all potential threats. The obvious problem is that you may have unwanted guests and it is difficult to locate and defend against a threat you can't see.

Cyber TSCM™ services are designed to effectively detect electronic eavesdropping devices that use cellular networks (e.g. 3G, 4G, Wi-Fi, etc.) These devices may capture audio, video or data remotely. They may also capture sensitive data on your network using a cellular eavesdropping device that is physically located at your site. These devices enable cyber intruders access to your data from anywhere in the world via mobile phone signals. For more information about this threat, read the IMSI catcher case study.

Corporate information stored on your networks may be at risk if you are just relying on your cybersecurity controls alone to protect it. If your risk management program doesn't include Cyber TSCM™, you have made the job of the corporate spy much easier. Protecting corporate information from corporate espionage cyber threats is a critically important function.

How to Reduce Your Risk of Exposure

Certain industries are at an elevated risk for cyber espionage. Companies that handle or store significant amounts of personal private information (PPI) are also at an elevated risk. Changes in your corporate environment can also place your company at an elevated risk for espionage attacks. Developing a customized approach to reducing your risk of corporate espionage by addressing the operational complexities of your organization is the goal. An effective data and intellectual property protection program must “detect, prevent and mitigate” corporate espionage efforts.

Is your company at an elevated risk of illegal eavesdropping?

- ***You operate in a high-risk industry, such as critical infrastructure, defense, banking, healthcare, green energy, government contracting, etc.***
- ***You handle or store significant amounts of PPI.***
- ***You suspect a data leak, but have not been able to identify the source using cybersecurity controls.***
- ***Your Intellectual property is novel or extremely valuable to the homeland or a foreign entity.***

If you can answer “Yes” to any of these questions, you are operating at an elevated risk of electronic eavesdropping. Many times companies put extensive controls in place to protect against unauthorized access to network data. But, if the network data controls do not consider protection of data or intellectual property by means of electronic eavesdropping, the controls may not accomplish the goal. By incorporating TSCM / Cyber TSCMTM, data and intellectual property protection can be improved. By hiring experienced, properly trained, well equipped and vetted TSCM / Cyber TSCMTM service providers, you can ensure the success of your efforts.