

## **Information Security PROTECTING YOUR PRIVACY**

Presented by  
Keith Flannigan, PhD, CFE

### **Protecting your company from Industrial Espionage!**

Most victims of espionage tell us "I can't believe it could have happened to me". That statement is the reason that it can happen. If you did not believe that someone could steal your car and you left it sitting with the keys in the ignition and did nothing to protect it, there is a high probability that we will see you at the car dealership looking for a new car. It is the same principal with any security subject, if you ignore it long enough it will eventually happen to you.

I.T. (Information Technology) Security is the same as any security program that you have ever managed. You have Premise Security of your complex or building, with IT you have the security of the entire computer system. You then go to access control; with your computer, you have password control. You then restrict employees or guests from sensitive areas of your building. In your computer we build "Firewalls" to restrict unwanted or unauthorized visitors.

The techniques are the same as you have used for many years. What we must do now is learn what new technology is available and how to utilize that technology in a way that is best for your company. With the current war and terrorism issues, it is more important than ever to insure that the communication and information systems in your facility are secure. Having a vulnerable communication system could lead to loss of critical information, compromising employees by making them accessible to physical attack and loss of revenue from Research and Development information and bid proposals being eavesdropped on by competitors. We also have to realize that there are people out there that will go to great lengths to disrupt your business as well as attempting to steal your proprietary information.

With any information-gathering program you have to look at three things, No Tech, Low Tech and High Tech. No tech is the competitor sending beautiful women to get information from one of your employee's. They could also sit next to your employee's at lunch and listen to their conversations or even have someone hired into your offices. This is still the number one method of intelligence gathering in business today. Fortunately, in most cases the intruder does not get the total picture and the financial loss is not catastrophic.

Low tech would be the employee placing a tape recorder in a conference room or on a phone or fax line. We now have intelligence information that the Al Qaeda has gone to great lengths to have sympathizers hired into key positions at important businesses known as "sleepers" waiting to be called upon to disrupt American Financial and Defense Industry business. They can also hire one of your employees that have the information that they wish to obtain. This is fairly common and the losses are a bit higher.

High Tech is more complicated; this deals with the monitoring of conversations by microwave or laser listening devices. Redirecting satellites to monitor conversations or photograph shipping or manufacturing facilities, tracking of vessels to determine customers and shipment destinations and the

International Dynamics Research Corp.

Campus Facility Management

"HACKING" into your computer system to obtain vast amounts of sensitive data. Unfortunately, when your competitors have these resources they will almost always be using them in conjunction with the above methods also.

The main thing that you need to look at when determining your vulnerability from a competitor is: Does he have: TIME, ACCESS or MONEY? If he has the money, he can get the other two.

If he has the time, he can have someone hired in to your business either as an employee or as a contractor or maintenance person. There are several other ways from cleaning staff to having the person hired into the local utility company so they can come in to work on your phone system with no questions asked. If one has enough time and a good imagination the possibilities are endless.

Once the competitor has access to your facility or information systems, they can devastate a company from underbidding you on contracts to changing data to cause you to make critical errors in your own calculations that can cause you to loose money. Having your production down is almost as good as stealing money from your company to an unscrupulous competitor.

The most devastating problem is when they just want to steal your product. They don't have to break in with a crow bar and a truck. All they have to do is access your computer system, have you deliver an order to them and then delete the invoice or proof of delivery. They can then have you send them another order for free. The possibilities are too many to name. The thing that we do know is that if you are going to stay in business, you must not let it happen to you.

There are many things that you can do when you are traveling to reduce your chances of having your proprietary information stolen.

The first thing you need to do is know where you're going and what the past record of incidents are at that location. You can obtain this information from your Director of Security. If he is not familiar with the location, he will have contacts that he can call to get current information on the trends and frequency of intelligence gathering at that location.

Once you have made the decision to travel, you must take responsibility for the sensitive information that you are carrying. Do not leave equipment or information unattended in hotel rooms or in hotel safes. I recommend that you save all critical data to a disk or use an external hard drive and not keep it on the hard drive of your notebook computer. I have seen several cases where the portable computers were forcibly stolen from executives when leaving hotels. This brings us to the point that you don't carry your data disk in the computer case. Remember, there are some excellent encryption programs available, use them.

You also need to limit any sensitive discussions in hotel rooms or public areas. If you do have to meet in a hotel room or area that is not controlled by your company, have an electronic technical counter-measure sweep (TSCM) conducted to better insure your privacy.

Do not use the computer or facsimile equipment in hotels or business centers for any sensitive matters. There have been cases reported where the hotel loaned shredders to business guests that had scanners

built into them so that everything that you shredded was copied and sent on to be reviewed.

You need to be cautious of anyone who attempts to engage you in conversation about business or personal matters. When flying, never check your personal computer. Always keep your computer and any important or sensitive documents with you as carry on baggage.

From your company's point of view, you must have an information safe environment. This means that it is the company's responsibility to the stockholders and the board members to take all prudent measures to insure that corporate information stays corporate information. You must also realize that in any organization pay increases and bonuses are directly related to profits. You don't see companies losing millions of dollars going back and giving employee bonuses. The more profitable the company is the better chance you will have of being given a raise in salary or a bonus. So it is important for everyone to work together to insure that the company is profitable.

If a company wants to remain strong in today's electronic world, they must have a strong security department. It is important for them to have guards and fences, but they also must be strong in the Information Security Department. Many companies are now hiring managers that are responsible for only the IT security. It is very important that the Physical Security and Information Security directors work together and understand the total security picture to better use the security budget so as not to waste money on duplication. If your company is not ready to hire an IT manager, you may want to hire an experienced consultant to look at your current security program and help you decide when it is time to make that investment. I also recommend that the IT Manager answer directly to the CEO or president so that their recommendations are not lost along the way with people that don't understand the importance of IT Security or may be in budget competition with them.

It is important that the employees know that you are serious about information security. If you as management don't take Security serious, they won't. It has been found that the best way to protect your company information is to establish a written Proprietary Information Security Program. This will be a hands-on counter-measure program as well as an informational program to include sending out memos on situations and incidents that have happened to other companies.

One of the largest current threats today is with the wide spread use of Wi-Fi Connections. A recent study determined that only 36 % of companies using wireless were using encryption and of those 53% were not using the proper level of encryption.

One of the first steps in establishing a Proprietary Information Security Program is to have a comprehensive threat analysis completed by someone who has knowledge of Information Technology and Physical Security. Once your facility is secure and you have determined that reasonable care has been taken to restrict unauthorized access, you can move on to checking for existing compromises to your communication security. This is determined by having a complete Technical Surveillance Counter Measure Sweep completed by a competent and reputable TSCM firm. This will insure that the company is free from listening devices when you begin your program.

After determining that your facility is secure and that you do not have a known compromise to your Information Security Program, you then need to establish a long-term education and maintenance

International Dynamics Research Corp.

Campus Facility Management

information security program. It is recommended that your sensitive areas be swept on a monthly or quarterly basis, depending on the risk to your facility. You should also provide your employees with memo's or newsletters that detail Information Security issues as well as using posters and warning labels around the work area on telephones, facsimile and computers systems reminding the user of the risk of eavesdropping and or "Hacking".

You should establish guidelines for your employees using "Online" systems as for what type of passwords should be used so they are not easily compromised and how often they should be changed. They should also be instructed to memorize their password and not write it down where it could be found. Be sure that they do not use easily guessed passwords like their children name or their date of birth. You also need to contact your online service and determine what type of security program that they have in place. What is your online providers written security and privacy policy and determine if they sell information to marketing companies.

Make your employees aware that it is possible to track your online browsing patterns. If your company is thinking of expanding to the Los Angeles area and you start doing research on the INTERNET for that area and someone monitors that activity, it could compromise your exposure there. It can also disclose your company or personal shopping habits again making you vulnerable to someone trying to infiltrate your company. One old intelligence trick is to find out what type of computer or modem a company is using and send the company a letter stating that your company is now handling the Technical Support for that product with a phone number for them to call if they have a problem. The person attempting to get information on your company just sits back and waits for one of your employees to call with a problem and then ask them "What is your log on and password". At that point your employee has compromised all of the security that you have worked to establish. That is why it is so important to have an educational program along with your normal security program. By knowing your shopping patterns, it would enable the person trying to gain information on your company to call you with a free sample modem or computer that is all ready wired for their ability to intercept your information.

Your staff also needs to understand that online communications are not private and that deleted messages can be retrieved. Most important be sure to use privacy protections tools such as encryption. This will scramble the data that is being sent by E-mail and help to protect your confidential information from unauthorized reading. Encryption is not 100 % safe, but a good encryption program can make your information virtually unreadable to most of the people in the world. You do need to keep in mind that the encryption program needs to be upgraded as technology changes and as your employees change.

When having a Counter measure sweep completed, you should ask the company the following questions:

### **Choosing a Counter-Measure Team**

To insure you are getting a professional Technical Surveillance Counter Measures service when interviewing the prospective team you should:

- Ask to see their Insurance Certificate that specifies TSCM.

- See proof of experience for the *Personnel* who will be conducting your sweep.
- See Technical Data sheets on the equipment they will use to conduct the sweep.
- Insure that their equipment will pick up Microwave transmitters (at least 20 GHz).
- Insure that you can have a printout, visual, and audio record (videotape) of any activity noted.
- Insure they have the capabilities to breakout data from a Burst Transmitter.
- Insure they are conducting a complete phone line analyzation, not just checking the voltage (the new electronics cannot be picked up by voltage).
- Insure they have the ability to conduct "Real Time" analyzation.
- Insure they can conduct "Non-Alerting" analyzation.
- Do they have credible references (who else do they work for)?
- Request a copy of a "Sanitized" report so you can see how professional they are.
- Request an overview of what inspections will be conducted.
- Determine if they are licensed to perform TSCM Sweeps (States require licenses).
- Determine if they have the personnel available to conduct a proper sweep (this is not a one-man job; a thorough sweep will take a team several hours).

A professional TSCM team will have at least \$50,000 invested in their equipment. Most will have well over \$400,000 worth of electronics. A professional team will have current up-to-date equipment and training to keep up with the most current industrial espionage threats. They should have at a minimum a Spectrum Analyzer, with the capability to read a minimum of 20 GHz, a Wideband Receiver, an Electro Magnetic Field Detector, an Analyzer capable of receiving micro wave transmittances, a Telephone Analyzer that can analyze break percentages and recognize blue streak taps, and equipment to recognize Laser transmittances.

The above should be determined prior to any services being completed. If they are not conducting a thorough sweep, they should not be there at all.

If you have any additional questions or if you would like a checklist that may help you justify an Information Security Program to your management, I may be reached at [IDRC@att.net](mailto:IDRC@att.net) or [www.goIDRC.com](http://www.goIDRC.com) and by phone at 877-650-7190 or my cell at 678-887-4933.