COMMON CORPORATE SECURITY VULNERABILITIES

Chris McSpadden, REI

Technological advances such as e-mail, computer networking, smart phones, fax machines, phone lines, video-conferencing, etc. allow us to overcome physical barriers to conducting business, no longer limiting the flow of information to the walls of the office building. While the exchange of information and business data has become more efficient, it has also become more vulnerable than ever.

Leverage espionage has become a multi billion dollar a year business, yet businesses and celebrities do little to protect their operational security. The biggest vulnerability to today's corporate security professional may very well be related to operational and information security. From the birth of a simple company directive or business plan, to its crumpled death in a trash can, the data and information will have passed effortlessly beyond locked doors and security checkpoints through fax machines, printers, copiers, filing cabinets, numerous employees, conferencing systems, and possibly hundreds of computer systems, not to mention discussed by employees in the company break room, at home, or other public locations. By identifying paths and potential vulnerabilities, the corporate security professional can quickly recognize a variety of information vulnerabilities:

Computer systems: Today's corporate security personnel must work closely with MIS/IT departments to ensure adequate security measures are in place (i.e. hard/strong password policies, network login procedures, remote e-mail/network access policies, physical controls, and proper network security applications, etc.).

Smart Cell phones: Today's Smart Cell Phone are vulnerable. Can someone listen in on my calls? Can it be done, yes. Is it likely, no. It is extremely hard, expensive and time-consuming to tap/bug your cell phone. In the corporate world Information Intercept Operators are a real threat and are highly paid for their nefarious and illegal activities. So, the easiest method to prevent your phone from being used as a listening device is to use a cell phone *Faraday cage pouch* when you absolutely don't want to be overheard. It's simpler to just place it in a case (Faraday cage pouch) and then in a drawer, than to shut it down, take the cover off and remove the battery. These pouches can be purchased on Ebay and over the Internet.

Copiers, fax machines, and photocopiers: Modern copiers, fax machines, and printers contain computer processors and storage devices, enabling them to store and/or recall data, making them an easy target that could be exploited to gain proprietary information. Not to mention the paper copies that usually set on these machines before the recipient actually retrieves the hard copy paper.

Removable storage devices: USB storage devices encourage the mentality of, "What I can't do at work I can finish at home." A full page of text requires about 20 kilobytes of disc storage and with a 1 Giga byte USB device I could go home with 50,000 pages of text at one time. Today's laptops and even some desktop systems come with memory card readers built right in that will read several types of common flash memory cards.

Wireless presentation microphones: These are probably the most common source of "self-bugging". These are extremely inexpensive, and common in conference rooms or other environments where presentations are given. Many modern multimedia conference rooms are already equipped with this type of equipment and can broadcast outside the building.

Computerized Telephone/Conferencing systems: Modern PBX and ACD systems pose a huge threat to our information security. Some systems even allow voice mail messages to be e-mailed to a users selected address as attached .wav files, potentially sending confidential voice mails throughout the world-wide-web.
Additionally, every office in a typical business building has at least one telephone, or likely a speakerphone, containing at least one microphone (speakerphones usually contain multiple microphones), that can easily be used to harvest intelligence or eavesdrop. Video Conference systems can also provide an open channel for an uninvited guest to "sit-in" on a private meeting from miles away. These systems need to be properly "secured" when not in use.

Trash: The simple act of throwing away a document may very well be handing the information to the competition. We have all read of cleaning personnel being paid to harvest the trash, or others helping themselves to dumpsters full of proprietary and confidential information. Once garbage is placed in a trash can or dumpster outside of a building, it is typically considered not illegal for someone to take it, in effect stealing corporate secrets. Proper disposal of company documents and document shredding is a must.

Business Travel/Trade Shows: Traveling employees and their laptop computers represent a treasure trove of competitive intelligence. Employees who travel or represent the company at trade shows or other events need to be aware of what information is appropriate to discuss, and what information should not be disclosed.

Sales Enquiries & Company Visitors: One of the most common competitive intelligence techniques is to pose as a potential customer, asking whatever information is desired. Prospective customers and/or company visitors should be qualified before any information is shared.

Employee Awareness: A regular security awareness briefing for all employees helps to not only raise awareness, but also the total level of security for the entire organization. The weakest link often lies with an organizations own people. Making sure that all employees recognize potential security threats increases the chance of preventing a breach of security. In today's business world, it is imperative to know what your competition is up to, and more importantly secure yourself from potential information theft/loss. Information security represents the biggest potential loss for a company, and can usually be easily avoided with some simple attention from the proactive corporate security professional.