The Basics of Information Security

By Felipe Guillen

July 2003

INTRODUCTION. This tutorial discusses the basics of information security for small businesses and acquaints you with effective tips to help protect your company from current and evolving threats. This area is rarely thought of or prepared for in even the best business plans, even though it has the potential for destroying not just new start-up businesses, but even well established and profitable companies. In fact, victims of improper or absent information security programs are in the media, almost daily!

BACKGROUND. Every business has essential information and ideas which are critical to its success and which if violated or lost to a potential competitor – would not only damage the business but would also give the competitor a valuable boost to its own marketing success. This essential information may be in written, spoken, or electronic formats. Examples of information that needs to be properly protected and why includes:

Business plans (Delivery of such information to your competitors for example, would provide them with detailed operating contingencies that would not only be open to their own exploitation, but which would facilitate their efforts to delay or totally disable a competitor {YOU!}. Remember; If your idea can make YOU money, it can make SOMEONE ELSE money too!

Client contacts (This information would obviously facilitate the competitive marketing of similar services such as yours, to your own selected or targeted clientele base by others {THEM!}.

Key personnel (Professionals use this information in various ways including; for recruitment of key people to their own "side" or efforts {usually via bribery}, blackmail {when monetary coercion is not effective}, to identify personnel weaknesses which they may exploit further, etc.).

Trade secrets (This information may be put to use by competitors to improve their own competitive offering to your clients, and to eliminate any special or unique "edge" which may have otherwise made your firm the preferred or better choice for the client to retain).

Pending mergers and/or acquisitions (Smart competitors can use this information to improve their own positions by for example; "warning" your existing clients of your potential instabilities {to influence them into instead dealing with more solid firms such as theirs}, if the move would indeed improve your operations – to attempt to covertly block or sabotage negotiations for said mergers or acquisitions, or even to become a key player in any viable mergers/acquisitions!

Operating expenses (When this element is known by your competitors, it enables them to plan actions or marketing ploys which would bring your firm to operate in the loss or negative profitability range. They would then continue these efforts until you can either no longer even attempt to compete – or you go broke trying! Note: this is an old and very effective ploy.)

Electronic infrastructure (This information includes such elements as; the type of computer system and servers you are using {especially if they incorporate easily hacked wireless network communications}, the type of phone system in use, whether or not your firm is protected by any type of alarm and/or CCTV system, whether your offices and meeting rooms have any ceiling speakers {either for paging or background music}, do you have any conference rooms with teleconferencing or video conferencing features and equipment, etc. This information provides them with a very detailed and valuable map of your "Hazards in Place" which they can profitably and quickly exploit by assembling action plans to thoroughly make use of each unprotected vulnerability you have in place – such as using the ceiling speakers to electronically eavesdrop on all of your office conversations or remotely compromising your phone systems voice mail features for updated duplicates of all messages being left, as just two examples. Today's electronic systems and computers, are very much a 2-sided sword!).

As vital as this area of business operations is (especially to today's commercial undertakings), it is a subject that is almost always totally ignored and not even taught in even the finest of business schools! Why? Because even those who teach in business schools do not understand and are not aware of even the very elemental basics of this very specialized field. Ignoring the proper implementation of this very vital business element – is equivalent to going skydiving without a parachute!

IMPLICATIONS. When critical information is taken, it can endanger the survival of your business. While it is not within the scope of this tutorial to instruct you on every type of technical (electronic device based) and tactical (personnel based) security threat, it will at least make you much more aware of these hazardous and long-term threats. You will also be in a better position to seek out qualified professional assistance to aid you in "hardening" your business against such acts of business espionage.

EXAMPLE. First we will explore some of the avenues and tools used by Operatives (the people who would steal your proprietary information) for the discreet "acquisition" of the targeted information, after which we will review a few of the procedures and programs available to you to protect against such insidious affronts.

How is one victimized and by whom? To concisely illustrate how this occurs, let's take an example from a newly started company with high hopes for the future and which has a viable and otherwise good business plan. Let's call them the BAWT company (for **B**oy **A**re **W**e **T**oast!). The BAWT Company consists of its key executives; the President (who is also the CEO), a Vice President, the Treasurer or CFO, Corporate Secretary, and a manger in charge of Marketing and Sales. The line employees consist of various office personnel, a contracted janitorial crew, and a receptionist. BAWT provides secretarial services and part time or "temp" office personnel to other companies. Having established a good base or core of starter clients, they are doing quite well so far. Now it Starts.

Several problems exist within BAWT, which are completely unknown to its founder and senior staff. First, is an overly ambitious employee who will resort to any means to become successful in her own right, and second is a trusted employee who's making excellent "side" money by selling critical inside information to a competitor of BAWT. These two individuals take two different paths to the same end – the improvement of their own financial position, at the cost and ultimate demise of the BAWT company.

The overly ambitious employee we'll call Grace. The employee selling company information to BAWT's competitor we'll call Joe. Though they know each other, they are not affiliated in their illicit endeavors, and they do not know of the others similar acts of business espionage. Two worms in the same apple! (Interesting Note: Many apples, have multiple worms!)

Grace seeing the excellent money being made by BAWT, decides to start her own similar agency but in her distant cousin's name, thus no affiliation to Grace can be easily made by any interested parties (like her current employer!). Grace structures her own firms operations after the successful business plan of BAWT. In order to assure herself of a successful core of clients, she supplies her cousin with a list of BAWT's own clients and a detailing of the services being provided to each – and the pricing structures. Grace can thus present competitive sales or bid contracts to these clients, at just under BAWT's fees. Needless to say, BAWT soon suffers serious business losses by Grace's hand. Grace however, steadily increases her profits at a handsome rate. Grace is one very happy person, especially since no one at BAWT ever discovered or even suspected her deception.

Now enter Joe. **Joe is; [1] an opportunist and, [2] an aficionado of electronic gadgetry.**
For instance, Joe has always been fascinated with the many "spy" types of shops that sell various kinds of electronic devices such as eavesdropping transmitters. In addition, Joe now also finds an extensive additional outlet for his much regarded bugging devices – via the Internet. Joe thus has quite a broad amount of bugging devices to pick from, and an equally extensive number of places to purchase them from. Now, Joe has combined his two personality traits into one profitable side line – the purchase and placement of "bugging" devices in select office areas and phones of his employer, for profit!

In short order, Joe has collected volumes of valuable office and phone conversations which discuss critical BAWT business, including the fact that BAWT will be bidding on a new, very lucrative contract. The potential client firm is about to start accepting bids for a contract which promises to be a major and very profitable account for the lucky agency that wins the bidding process. BAWT has an excellent chance of being awarded the contract – that is until Joe entered the picture. Joe has been providing a competitor of BAWT's with regular critical inside information, for cash "side money"! Now Joe brings them this valuable information on the new contract bid – including BAWT's bid! Bad for BAWT - Good for Joe.

As in Grace's case, the executives at BAWT were unaware of the serious internal assault they were under. They were also glaringly unprepared to defend themselves from these "invisible" but deadly threats. How could the executives at BAWT have acquired this vital knowledge and specialized assistance to have prevented these fatal business information losses? The answer is both simple and complex. Simple because by simply having retained the services of an intelligence security agency, their problems could have been handled effectively - while at the same time establishing permanent protective countermeasures for long term protection from future similar acts of business espionage. Complex because true intelligence security agencies are hard to come by. While directories are full of agencies which can provide such services as guards, alarms, investigators, consultants, etc., intelligence security agencies are few and far between. This type of business security is a specialized field.

Special Note: The field of electronic eavesdropping devices deserves special mention. The rapid and continuous advances in todays technology has not been overlooked the field of eavesdropping devices. In fact thanks to todays advances, eavesdropping devices of the class formerly only available to **professional operatives** – have now found their way into the hands of the **general public!** The threat caused by these advanced devices is significant. Not only are they now readily available and at costs which even school kids can afford – but the features they tout make them a true threat to be reckoned with. Let's review just a **few** of the more prominent and threatening features of these popular devices (Remember – the following covert devices are **already** in the hands of the "general public"!);

a. **Extreme** miniaturization of both eavesdropping transmitters and recorders. Example; A spy recorder with dimensions of approx. one inch wide, by two inches long and one eighth inch thick – but capable of recording over 300 hours of crystal clear voice. P.S.: This same device may also be used to instead covertly and quickly - steal computer data!

b. An easily concealed (including concealed as wearable jewelry) micro camera that can continuously take discreet – clear digital photos (at for example 5 seconds intervals) for over 24 hours before running out of recording capacity. The photos can then be downloaded to your computer for printing, E-mailing, etc., with recorded sound as an option!

c. Extensive forms of computer spyware (both in software AND hardware versions) that permit the total and complete, long-term duplication of all activity (including passwords) that was transacted on the targeted computer(s) – and which can then be transmitted to the awaiting spy. In addition, the easily placed hardware versions are not detectable by any anti-spyware or similar detection/protective programs.

d. Easily concealed micro-cameras that will broadcast their images to the spy's Listening Post, anyplace on the globe served via the Internet! Yes, sound is also available.

e. Tracking AND Eavesdropping devices that can be quickly placed in vehicles that will not only transmit in continuous **Real Time** the conversations from within said vehicle, but also its speed, current location, direction of travel, etc. The information is then relayed to the spy who is monitoring the signals from the comfort of his/her Listening Post – anywhere on the globe!

f. Sensitive "Contact Mic" systems that permit the total overhear of all room conversation from any common wall, ceiling or floor. Thus permitting the eavesdropping on desired rooms, from any adjacent room whether it be next door, above or below the targeted room/office – and without requiring any actual access or entry into the targeted rooms or offices.

TEN TIPS FOR SMALL BUSINESSES. Here are ten basic tips to incorporate in your most elemental security considerations;

1. Always do **thorough and detailed** background checks and pre-screen any and all job applicants before you bring them into your firm, especially if they are to have access to critical files, R&D data, and related sensitive internal information.
2. Where possible, opt for offices where you are the only tenant and can thus control access to your offices and building, especially after hours. The difficulty of securing your offices from Operatives (especially the Professional), is greatly compounded when you are just another tenant in a typical office building. Here you have greatly reduced say on who may enter the building, and when. This weakness is well known and fully exploited by the Pro's.
3. Provide some form of effective 24-hour executive office access control. Examples include card access systems which require both a card swipe and a personal identification code, before a door will open (and keeps a log of openings). Executive offices must be isolated from the remainder of the office and production areas. While this alone will not deter the professional operative, it will impact many of the amateurs which exist in many firms today.
4. **Never** assume your offices and telephones are secure unless they have been properly Swept and checked by a qualified and experienced intelligence security agency. **Discuss confidential matters at your own risk.**
5. Remember – homes and vehicles are also fair game (and favorites) for electronic eavesdropping devices.
6. Always secure sensitive documents in safes when offices are unattended. Leaving sensitive documents on top of desks or unlocked drawers is a well proven way to lose key information. The easy avenues are used first!
7. For long term Intelligence level security, retain the services of professionals to design and deploy customized - threat-specific intelligence countermeasures for your firm. There is no such thing as a "one size fits all" in intelligence security applications. Safeguards must be tailored to each situation and business hazard(s).
8. With confidential/critical company information, share it ONLY with trusted personnel with a "need to know."
9. Avoid using both e-mail and voicemail for communicating confidential/critical information. They are not at all secure!
10. Re-appraise your intelligence security requirements at least twice yearly. Your needs or new technical assaults may indicate the need for important program updating or modifications (these will always be in flux), to address changes in your business operations or newly introduced security hazards. Your protection must keep up with the hazards.

SUMMARY. Electronic information violations are rapidly becoming even more of a threat. Small, minority- and women-owned businesses need to incorporate information security into their business processes and technology plans. As our example illustrated, intelligence threats are not new and are used against both the large corporation – and family owned business alike. No one is immune from this form of assault. As new firms enter the world of commerce, whether they know it or not and whether they are prepared or not – they too will be exposed to these serious threats to their firms survival. Threats which informed companies have learned to control for some time (their survival is a testament to their awareness). Note: Babe's in the woods don't live long.

The costs for properly securing companies against intelligence losses vary with such client specific parameters as; how extensive is the current exposure of critical information to potential loss, how much of this information requires enhanced protection, what is the current level of risk exposure to your firm (the greater number of competitors for example, increases your risk potentials), what is the current design and effectiveness of your existing operations security, how many people currently have access to critical company information and to sensitive executive offices and areas, are all of your offices in one location and floor – or are they distributed, etc. A comprehensive, threat specific analysis must be first performed before solutions can be formulated and deployed. Depending on your current level of exposure, changes may involve basic – to very in-depth, detailed security programs compartmentalized to address specific threats that may exist for individual business elements and their directors or personnel.

The cost for NOT securing your firm against these unique forms of theft, may range from serious financial losses – to a total business failure. Operating without appropriate intelligence security safeguards, is equal to having offices without any door locks - or doors! The difference being that with intelligence based affronts – you cannot readily see the invitation to ruin (as you could with the missing doors example). Intelligence compromises are almost always successful because most firms are not even remotely acquainted with these invisible threats, and thus have made no attempt or allowances to provide any degree of protection from such advanced and very effective, proven forms of compromise. If you have a weakness – someone will find it!

The bottom line for today's business executives whether new or seasoned veterans – is to become aware of business intelligence threats, and prepare yourselves via education and technical experts (in-house, or hired consultants) to confront and defend yourselves and your firm from these insidious and growing forms of compromise. Your choice is either to become aware and protected – or wait until you become the next statistic. Learn form the mistakes of others – and don't join them in their misery!

FOR ADDITIONAL INFORMATION. Please contact the author below at:

Mr. Felipe (Phil) Guillen, President
OMEGA
Box - 964
Tinley Park, IL 60477-0964
(708) 429-1563