Information Security is *Information* Security[1]

Ira S. Winkler, CISSP
ira_winkler@compuserve.com
(410) 544-3435
(410) 544-1404 (fax)

Abstract

All too often Information Security professionals focus their efforts on technical security. They try to protect computers and networks from intrusions. They ensure that passwords are strong. They set access policies and develop the appropriate plans and procedures. Hopefully, they even review audit logs and check for unusual accesses. While this is good, it is severely lacking if this is the focus of an *Information* Security program. Information is Information in all of its forms. An *Information* Security professional cannot be happy when the information that they protect to their death on a computer is crumbled up and thrown on the trash after it is printed. The title, Information Security professional, should do more than make you appear to be more than a technical professional. If you are a Computer Security professional, then call yourself that; or else assume the responsibilities that the title infers. It is important to note that the name of this conference was purposefully changed from the *National Computer Security Conference* to the *National Information Systems Security Conference*. This paper serves as a reminder as to what are the common forms of information, and provides for further discussion. The associated presentation provides an overview of protecting all of the forms of information discussed.

Introduction

Disclosure of sensitive data, such as the fact that someone has AIDS, can ruin people's lives. The damage to corporations can be just as severe. In a 1995 lawsuit, Proctor & Gamble (P&G) and Bankers Trust sued *Business Week* magazine in an effort to prevent the publication from revealing the details of a lawsuit involving the two corporations and some questionable investments; P&G feared the embarrassment and loss of confidence that could have resulted from the disclosure of these details. A Supreme Court ruling was required to resolve the temporary restraining order against *Business Week*.

Information in the wrong hands can destroy a corporation, put people out of work, bankrupt local merchants, and devastate shareholder families.

It's all about *information* but not exclusively *computer* information. If your competitors want your company's strategic plans, they don't care whether they get them from your computers or your garbage. Information is information. The *form* it takes is irrelevant; it's the content that matters.

[1] Some material in this paper has been excerpted from the book, *Corporate Espionage*, by Ira Winkler (Prima,1997)

The means by which that information is acquired is equally unimportant. It can be obtained verbally, electronically, physically, or visually. It can be snatched from computers, certainly, but a well-placed bribe can be just as effective.

Forms of Information

When I use the word “information,” what exactly am I talking about? The classic definition describes information as “organized data,” but that’s not really very useful in our present context. In these pages, *information* refers to any piece of knowledge that could hurt your organization or help your competition if it were to fall into the wrong hands. That piece could be great or small. It could be a business plan or a phone number, a set of blueprints or a computer password, a high-tech prototype or a business card. The following sections describe the various and common forms in which information can be obtained. While it was previously stated that the form of information is irrelevant from a spy’s perspective, it is extremely relevant to knowing how to protect yourself.

Computer-Based Information

Almost every piece of information generated by a modern company or other organization eventually finds its way onto a computer somewhere. Information is either recorded on a computer to formalize it or actually created in a computer environment. Nowadays, most executives type their own messages and correspondence directly into computers; the dictation-taking secretary is an anachronism. Computers are used for spreadsheets, databases, project design, and tons and tons of e-mail.

E-mail is one of the most potentially vulnerable types of computer information, because most people don’t think much about how they’re using it. In modern corporate America, most organizations are swimming in e-mail. People use e-mail to convey virtually all types of corporate information, from the most banal interoffice memos to the most sensitive project details. The corporate e-mail “conversation” is dense with information about company problems, personnel issues, and project status. Stop and think about the e-mail you have sent and received during the last week. What would happen if it were intercepted by an unfriendly party?

Nearly everyone understands the importance and potential vulnerability of computer-based information. Most people do take steps to protect their most sensitive computer documents. But many do not realize how damaging their supposedly non-sensitive computer information can be. E-mail discussing travel plans can compromise potential mergers. Informal notes usually contain as much details as finished documents. Computer-based information has been, and will only continue to grow as an extremely fruitful source of information to would-be spies.

Formal Documents

Companies generate many kinds of formal documents for a variety of purposes. Strategic plans, contractual status reports, manufacturing specifications, production reports all must be printed out and kept as hard-copy documents. These reports contain critical information that could ruin a company if it were compromised.

Most people recognize the value of formal documents and take appropriate steps to protect them.

Draft Documents

While people instinctively recognize the value of formal documents, they often treat the draft forms of those documents as worthless. They seem to assume that once a finished document is available, the drafts are outdated, inaccurate, and therefore unimportant. Although the draft document itself might be of little use once the final draft has been issued, the information it contains is hardly worthless. Much of it is very valuable indeed, and corporate spies know it. Typically, the draft documents contain the same hard facts as the final document; only the presentation changes significantly. As often as not, the first draft of a document is as valuable to a competitor as the thirty-fifth draft.

Working Papers

Much of the information contained in formal documents and their earlier drafts can be found in the working papers that are part of your day-to-day business routine. Project teams produce action lists, status reports, research summaries, business correspondence, and product specifications. Although the distribution of these documents is generally limited, they aren't usually thought of as sensitive in themselves, even though they can contain critical information about specific aspects of a project or organization. These working papers often are not controlled in the same way as formal documents, and people frequently lose track of them.

Scrap Paper

In the process of performing work, people inevitably record thoughts and notes on hundreds of bits of paper. We scribble on note cards, appointment calendars, and cocktail napkins anything from a grocery list to the invasion route for a military campaign. If the working papers are neglected, these bits of scrap paper are usually ignored. We don't give a second thought to that Post-it with our computer access code or the telephone message slip with the project supervisor's e-mail address. Yet, once again, these seemingly unimportant carriers of information can contain the same sensitive data as the formal documents that we tend to protect.

Other pieces of paper with potentially unnoticed valuable information include travel tickets, credit card receipts, invoices, and shipment manifests. They may not give a competitor the big picture, but they can help to fill in the pieces. They can give a spy a sense of where to direct his or her attack efforts. A purloined appointment calendar can show me that an important executive meets frequently with an individual from another company, which could indicate a possible merger or joint venture in the offing. That's extremely valuable information. With enough scraps like this, I can put together all I need to know to cause a lot of damage.

Internal Correspondence

Internal company correspondence contains an incredible amount of information. Companies produce their own newsletters, policy documents, and meeting minutes, for example, which are filled with project data, details about people, company status updates, and a variety of other information. Often, the people producing these documents have no idea they are generating sources of sensitive information. They don't anticipate the numbers of people who will eventually see the documents.

Unfortunately, I was personally involved in an incident involving an internal memo containing too much information. My work involves identifying vulnerabilities in many publicly known companies, so I use code names for my clients in most of my documentation. Only those people who need to know the client's real name actually know it. This is, or at least should be, a common practice in my business. But in a firm I used to work for, a purchasing officer put out a memo that put the code name together with the client's name. Although I was able to recover all copies of the memo, the information leak could have been disastrous.

Legal and Regulatory Filings

Government agencies and regulations require organizations to publish a variety of information. Companies produce annual reports, patent applications, FDA filings, and a wide range of other documents that are required by law. The content of these filings and releases is usually specified by the relevant government agencies, both foreign and domestic. However, many companies go beyond the scope of these requirements, releasing much more information than necessary.

This situation has spawned the growth of a new industry made up of legitimate businesses that provide a specialized checking service. For a fee, these services simply check new government filings on a daily basis, searching for useful information and passing it along to their sponsors. Of course, industrial spies check these records, too, if they don't use one of the commercial services themselves.

Other Records

Almost every action leaves a record somewhere, especially in the business world. When you travel, you generate records at hotels, airlines, and car rental companies. When you take out a library book, your selection and its due date appear in the library computer. When you place a telephone call or when you receive one, the action is recorded. When someone pages you, when you log on and off a computer system, and when you browse an Internet web page or look at Internet newsgroup messages, all of it *all* of it is recorded. Depending on the security capability of the computer system on which you work, each and every one of your actions may be recorded.

These types of records have been used to convict people of crimes, to provide leads to corporate secrets, and to compromise the most sensitive operations. In many cases, accessing these types of records is completely legal.

The Press and Other Open Source Information

People don't always have to engage in illegal activity to begin to compromise an organization's information. The data they need to get started can often be found in newspapers and trade magazines. There are also many publically available databases that have a tremendous amount of information, most of which is available to anyone with Internet or library access. Anything that is publically available is typically referred to as

Open Source Information by the Intelligence Community. These resources search for or contain important industry news. They report who wins major contracts, which executives are moving to which projects, and a wealth of information that is quite useful in the initial stages of an attack. Every little piece of information helps give a spy a bigger picture. In some cases, spies are able to secure everything they need from open sources without ever having to resort to aggressive activities.

Corporate public relations and marketing departments play a key role in the dissemination of this kind of information. They quite naturally want to give out as much news as possible about their companies to help increase sales and profitability. That's their job. Unfortunately, they tend to go overboard, putting out too much information that makes its way into a variety of public and private databases, which are widely available to anyone with a computer account. Databases, such as EDGAR, contain complete Security Exchange Commission filings. There are special interest Internet newsgroups where people interested in specific companies or market sectors, post anything that they come across dealing with their "interests".

Formal Meetings

Most organizations hold some kind of formal meeting in which its members discuss a variety of corporate and project issues. The information discussed at these meetings is frequently very sensitive, whether the participants are senior officers or line supervisors. Typically, someone prepares a meeting agenda and materials. Someone else prepares the minutes of the meeting that summarizes everything that went on during the meeting. All of these things contain information that is of great value to corporate spies. This does not even address what could happen if someone actually bugs the meeting room.

Informal Meetings

Any time employees get together and talk about work, either in person or over the telephone, that gathering could be considered a meeting. The sensitivity of the information discussed at these informal meetings varies greatly. Telephone conversations in particular contain a great deal of very sensitive information. There's something about the device that causes people to relax and let their guards down. Many industrial spies make it a point to tap telephone conversations so they can pick up useful bits of conversation.

Casual Conversations

Perhaps the most overlooked source of valuable information is the casual conversations that take place both inside and outside the office every day. People can't help talking about their work. Sometimes they're just getting together with coworkers for a few beers, and work is the natural topic of conversation; sometimes they're trying to impress others by talking about sensitive company matters.

The smoking areas outside major office buildings are great places to pick up information through casual conversations. I've heard of spies taking up smoking specifically to exploit this vulnerability.

While consulting for a major New York investment bank, I took their employee shuttle from the Financial Center to an uptown office. I couldn’t help overhearing two employees sitting nearby discussing a major merger between two large firms that was in the works. If anyone else overheard them and used that information, the bank could have been accused of insider trading.

A secretary I know was having dinner with her husband after work in a restaurant, where she overheard a couple of sales executives from her company talking at the next table. She heard them laying out the details of the sales plan for a new product. This was very sensitive information that was surely overhead by possibly forty people.

In an incident of foreign espionage, a South Korean businessman set up a social club, to which he invited some of the most powerful people in Washington, D.C. to join. Of course, he had the club building thoroughly bugged. The conversations he taped were considered to be some of the most valuable intelligence South Korea ever collected.

These kinds of incidents go on all the time, and good, patient spies know how to exploit them over time. Over the long term, they can get everything they need just by being good listeners.

Conclusion

The form your information takes is utterly irrelevant to the people who want to compromise it. It is the content of the information that their customers, bosses, or spy masters want. Industrial spies don’t want your computers; they want the information you keep on them or the services that they provide. They’re perfectly happy to get information from the easiest and most overlooked sources including the trash or a vulnerable telephone. As a matter of fact, these sources are even preferable, because they involve less risk to the operative. A good spy always looks for the path of least resistance before trying anything fancy or high-tech.

Once you understand the forms of information that you should protect, you can start to implement the proper countermeasures. This is less straight forward than Computer Security, and it does get into areas that the typical Information Security professional is unfamiliar with. However, it is very intentional that the Intelligence Community addresses all of the described forms of information in their security programs. Unfortunately, most Information Security professionals from a technical background do not appreciate this, especially in the commercial sector. The related presentation does touch upon the relevant countermeasures using actual cases of espionage as a reference. However other and future papers should address these countermeasures in more detail.

###