BEYOND TOP SECRET

How the

CIA, NSA and DIA protect sensitive information

And how the same techniques can protect a corporation

Hal Walter

Hwalter@email.uncc.edu

Phone: (704) 687-4660

ABSTRACT

Ten years ago, the idea that a company would need security equal to that of the Central Intelligence Agency, the National Security Agency or Defense Intelligence agencies might have seemed alarmist. However, in today's business environment, corporations often require an equivalent level of protection for critical and sensitive proprietary information. The goal of this guide is to enable a CEO, CIO, CISO, or business owner to understand the risks and apply some of the same tools, concepts and practices to safe guard information and communications above and beyond the norm. A business needs a place, be it a room, a building or an entire plant where extremely sensitive information may be discussed, managed, transmitted and stored without concern for interception, misuse or unauthorized dissemination. This guide shows how these highly secretive agencies protect their most sensitive information and how that same level of protection can be applied to the corporate environment.

IDENTIFYING THE NEED

This guide provides a step by step plan for developing, implementing and enforcing a comprehensive Information Security program for your organization. The guide is based upon criteria established by the U.S. military for the security of strategic and tactical intelligence, the Manual for Physical Security Standards for Sensitive Compartmented Information established by the Central Intelligence Agency of the United States of America and the National Security Agency's published standards for protecting the confidentiality, integrity and availability of Sensitive Compartmented Information.

While it is generally neither necessary nor cost effective to apply all the standards of Sensitive Compartmented Information Facility design and control to a business setting, nonetheless, some degree of information security may be obtained by careful and thoughtful application of the processes and practices used to protect the nation's most closely held secrets. Understanding that security starts and ends not with technology but with people, it becomes incumbent upon business leaders to design, establish, implement and enforce a well considered security capability to protect sensitive corporate secrets.

Information Security classifications within the federal government are generally of one of three well known types:

CONFIDENTIAL: Applied to information or material the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

SECRET: Applied to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.

TOP SECRET: Applied to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

Less well known within the Top Secret category is information so sensitive that even the extra protection measures applied to Top Secret information are not sufficient. This information is known as "**Sensitive Compartmented Information**" (SCI). A Sensitive Compartmented Information Facility (SCIF) is a specially created area, room or facility designed specifically for the handling, discussion, access, control and/or storage of Top Secret Sensitive Compartmented Information (TS/SCI) which requires extraordinary security safeguards.

"SCIF design must balance threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk." (2) Director of Central Intelligence Directive 1/21 Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), Effective 30 January 1994 Source: CIA Hardcopy, Freedom of Information Act

This applies to security in business also. Management must first identify and evaluate the risks before determining appropriate controls to reduce those risks to an acceptable level. Just as a company would be unlikely to leave financial records lying about or post personnel files in the local newspaper, so should no company leave those same records accessible electronically. Within a well designed and properly enforced facility, Information Security becomes both the

responsibility and in the best interests of all granted access. The corporate SCIF concept focuses on four specific areas: physical, personnel, communications and information security.

"A common mistake in contingency planning is an excessive focus on computer recovery when what is needs is a business recovery plan." (1)Jae K. Shim Anique A. Qureshi Joel G. Siegel, "The International Handbook of Computer Security", Glenlake Publishing Company, Ltd Chicago, 2000, page 192.

Creation of a SCIF for business begins with risk assessment. Determine what information is of utmost criticality to the continued operation of the organization and would create the most irreparable harm if compromised. For instance, financial records are obviously important and unauthorized release of customer credit information is of considerable consequence. However, terms of negotiation during union discussions, corporate acquisition plans, civil, legal or judicial preparation discussions may be more sensitive. Consider how records, files and electronic data are currently protected, how access is controlled, who has accountability and how the permanent log of systems users is maintained and full off-site backup available and protected from unauthorized access. The goal is to prevent or minimize release or unauthorized access to information considered sensitive and vital to an organization's business activities.

Establish a committee of decision makers within the organization to review, formulate, test and implement a corporation wide security plan. A committee made up of personnel from security, systems support, applications development and the user community will be tasked with creating a plan which covers human safety issues, business impact and recovery, in addition to

limiting legal liability, while insuring adaptability to changing threats and conditions. Earthquakes, floods, or hackers effect business operations in different ways and each requires a different response. The committee determines who is to be notified and in what order when a critical incident arises, who has access to the secured facility during an incident, where and which records are considered vital and what backup plans to initiate, when and by whom. Backup facilities, whether a hot site in that they may be used immediately or a cold site in that some time is required to re-establish business operations exist whereby a business may move operations off-site either temporarily or permanently. Cost and the results of a threat analysis will determine the level, scope and complexity of backup services selected. Backup also includes the need for storage of the day to day data used by the business. Again, several options exist. On-site storage is convenient but may prove less than satisfactory in case of fire or flood. Remote off-site storage reduces the potential for total loss, however it must be inspected periodically to insure storage is both adequate and effective. There have been cases in which storage tapes thought to contain vital information have in fact been completely blank as no one thought to actually check as they were "recorded".

The off-site storage of critical or sensitive information however, requires greater planning and more depth of security than normally required. It may be advisable to keep highly sensitive data contained within the SCIF regardless of the threat. If it then becomes untenable to maintain full SCI level protection, automatic destruction becomes necessary. Be advised, do not rely upon office type paper shredders or burn bags. Shredded documents can be restored to readability. Burned documents are also salvageable and an erased disk drive is still quite readable. Magnetic devices cannot, under current technology, be fully, completely and safely erased. Tools exist

which restore data thus compromising the SCIF concept and purpose. Plan for worse case and insure that all data contained within the SCIF is completely and utterly destroyed very quickly. For instance, first burning and then soaking paper documents tends to make them unreadable. Physically removing the magnetic substrate (the rust colored material) from a disk drive or tape by scraping or burning makes restoring the data unlikely. Simply smashing with a hammer will not suffice. Consider wiring the door to the SCIF with extremely powerful electro-magnets which are activated upon unauthorized entry. This applies best in a vault, where any intrusion would automatically destroy the contents. Again, the idea is to insure with as much confidence as possible that certain information remains under authorized corporate control at all times under the worst possible conditions.

PHYSICAL SECURITY

"The scope and level of physical security is determined by the conditions under which sensitive information is handled, be it closed storage, open storage, continuous operations, or within a secure working area." (2) Director of Central Intelligence Directive 1/21
Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), Effective 30 January 1994 Source: CIA Hardcopy, Freedom of Information Act. The standards for each are different, but at minimum, there should be one access point or door, no windows, a white noise generator, no personal radios and in fact no personal electronic devices whatsoever in the secured facility, solid not dropped ceilings, no ungrounded wires, solid but well insulated walls, an immediately accessible and highly secure vault storage area, all contained within a zoned secure area.

A white noise generator is a device which broadcasts a continuous low level multi-frequency audio sound which masks voices making eavesdropping difficult. Windows act as large speakers, vibrating in tune with voices and sounds within the room assessable at considerable distances by properly equipped individuals and with little chance of detection.

One door limits the potential for surreptitious entry while well insulated walls limit the usefulness of unauthorized listening devices. False ceilings provide numerous access points for unauthorized listening and video recording devices. Ungrounded wires retransmit electronic signals. The vault provides quick storage of material in case of fire or other interruptions. Finally, alarms alert security to violations of physical security standards. Security however, must be able to respond very quickly and have immediate access to a reserve response force for assistance if needed. Insure the walls, floor and roof are solidly constructed, non moveable and made in a manner that provides a visual indication of intrusion. Be especially mindful of sound suppression techniques. As noted above sound is easily retransmitted, electronically or through various open or solid objects. Insure doors and access points are hinged inside or that hinges are welded in such a way as to prevent removal and that doors are sufficiently framed to preclude gaps in door seals which provide eavesdropping access by outside listeners. An emergency exit door should have no external hardware, secured from inside the SCIF and should set off audible alarms when used.

Duct work opening within the SCIF must also be secured. Limit duct size as much as feasible and place sturdy grill work over all openings both within and beyond the SCIF. Be aware that duct work is an excellent carrier of sound and therefore must be adequately insulated, baffled and protected. Additionally, where duct work goes through walls, it may provide access to overhead

spaces not regularly patrolled by security. Therefore bars, grills and baffles are necessary. Remember to install inspection plates but only within the SCIF. Small openings accessible by angled mirrors and flashlight work insure access for inspection purposes.

Electronic devices generate electrical frequencies which replicate the actions within the device. In other words, when you view a computer screen, the electrons being transmitted by the screen do not stop at the glass. They continue to travel, uninterrupted for considerable distance until absorbed by materials or atmosphere. (4) CYBERSHOCK, Surviving Hackers, Phreakers, Identity Thieves Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, Thunder's Mouth Press, copyright 2000, page 435-436. This is known as TEMPEST in military language and is of considerable concern to security managers. Consequently, the SCIF design insures that computer screens are angled down, duct work is electrically insulated from radio frequency energy, computers and magnetic storage devices are contained within shielded and well grounded housings.

This gives a basic overview of SCIF physical security concepts and problems. Additional considerations include sensors, which detect body heat or air movement or changes in carbon dioxide, thermal scanners, audio listening devices and various alarm devices. The above presumes a SCIF built within a secure area, as a room within a building. However, the security plan must take in to consideration surrounding facilities, the grounds and access points beyond the physical confines of the SCIF. Walk through your plant area with a screw driver and a 9/16 inch wrench and you will find numerous places where entry can be gained while leaving no trace. Consider replacing chain link fencing with closely spaced vertical rails and remove all vegetation from three feet on either side of the fence to better see footprints or tire tracks.

Review outside lighting for coverage, consider landscaping with thorny brush to preclude concealment and insure security guards patrol in a random fashion to reduce intrusion options.

COMMUNICATIONS SECURITY

"No telephone conversation is free from the risk of interception: The telephone system is widely accessible by many people, such as maintenance technicians or switchboard operators, in the course of their normal duties. Authorized and unauthorized monitoring of telephones is possible at junctions and distribution points throughout the system." (5) Security in the Government Sector www.security.govt.nz http://www.security.govt.nz/sigs/html/chapter8.html

The telephone is both ubiquitous and an often overlooked threat vulnerability. Telephones are quite capable of retransmitting voice to an outside listening device properly tuned to the correct frequency. Therefore, phone conversations within a SCIF become problematic. Encryption reduces the risk of exposure but only if both sender and receiver are correctly configured. Similar concerns affect Fax machines as they also use unsecured, open and easily intercepted communication lines. Do not use the same fax to send or receive both sensitive and non sensitive data. All telephone cables and wires should go through a single hole in the SCIF wall and be attached in such a way that every wire strand is accounted for and identified. In other words, there can be no loose wires. All telephones must have a positive disconnect, such as the ability to remove the phone jack from the wall plate. There are special telephones available designed for high security areas which use line filters, better grounding and meet strict security compliance standards. See (6) Physical Security Requirements for NSA/CSS Sensitive Compartmented Information Facilities, April 2000 for more detailed information.

Another area in which the telephone may become a threat is by social engineering whereby considerable information about a business may be obtained from secretaries, service people, helpful employees and others. It is incumbent upon management to reinforce telephone security to all systems users including vendors, customers and temporary employees.

Within the SCIF, telephone usage is limited to encrypted, cable connected secure voice systems. While not common, equipment is available that will pick up signals retransmitted from telephones, even when not in use or unconnected to a land line. These unintentional electronic signals are referred to as compromising emanations. Cell phones and satellite phones are not allowed within a SCIF. Cell phones are an obvious danger, due to their ease of concealment, photographic and voice retransmission capabilities. This applies to both analog and digital cell phones. Radios, stereo equipment, tape recorders and other similar electronic devices often taken for granted cannot be allowed within the SCIF. All are capable of retransmitting signals due to the high quality of their internal microphones, even when not in operation. Signals thus transmitted can be intercepted up to 50 feet away. To anyone who has ever used a baby monitor, the ability to pick up cordless phone conversations requires no explanation. Obviously no cordless or unencrypted wireless devices would be allowed within the SCIF.

Personal Electronic Devices are another potential security risk. These act as voice re-transmitters and may conceal cameras or recording devices or may be capable of infrared data transmissions. Wireless devices, such as laptops or palm computers are similarly capable. Pager signals are easily intercepted as they are radio frequency transmitters and therefore should not be used to send sensitive unencrypted business data.

INFORMATION SECURITY

The goal is to keep sensitive corporate information secure. Discussions, conferences, meetings and memos need to remain within the facility, between known individuals and unavailable to any outsider. Most companies have firewalls in place, preferably several placed strategically to impede hackers and some companies have learned the value of encryption-though often not very well implemented. Encrypting data only after it is transmitted over the Internet is far too late. Data should be encrypted at the desktop, as it is generated. Even then, keystroke monitoring software placed surreptitiously on the desktop can decode enciphered passwords. Encrypted passwords may be intercepted and used, in their encrypted form, by unauthorized individuals. It is strongly suggested that desktop machines not be equipped with floppy disk drive units as this is still the primary means by which viruses and Trojan horses are introduced to corporate networks. Additionally, floppies are ideal for the non-technical individual to copy and steal corporate information with little chance of detection. More tech savvy individuals have much faster and more efficient methods. An excellent source of information on the range of possible methods used to break into networks and databases is found in (4) CYBERSHOCK, Surviving Hackers, Phreakers, Identity Thieves Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, Thunder's Mouth Press, copyright 2000.

Within the SCIF, information security takes on a more consequential edge. It is within the confines of the SCIF that information requires a much tighter control and protection. As stated previously, network connections must be kept to a minimum, wireless devices are prohibited and encryption is vital. Also, consider using Virtual Private Networks (VPN) for data transmissions

outside the SCIF. A VPN creates a private "tunnel" through the Internet, allowing more secure connectivity.

General information security is concerned with physically limiting access to data with passwords, encryption or firewalls. However, at the upper levels of information security, the data is far more critical and the means to intercept it far more advanced. The act of transmitting a message creates electrical impulses which can be intercepted and decoded. This form of signal interception does not require physical contact, does not leave evidence of interception and cannot be prevented without considerable care.

An antenna is a conductor attached to a changing voltage. A receiver is a conductor and amplifier of changing voltages. Therefore, any time a signal is passed down a wire-or a plumbing pipe or the fire suppression water sprinkler system or anything else that conducts electricity it will create a signal just like an antenna. This is the basic concept behind TEMPEST (possibly an acronym for **T**ransient **E**lectromagnetic **P**ulse **E**manation **S**tandard or depending on the source **T**elecommunications **E**lectronics Material **P**rotected from **E**manating **S**purious **T**ransmissions but actually it is simply a U.S. government code word which has no particular meaning). TEMPEST describes both the equipment and the techniques used to control or limit unintended electronic or electrical signal transmission. Other terms you may encounter include compromising emanations, electromagnetic interference, or Sigint (Signals Intelligence). The goal of SCIF design is to limit unintended signals leaving the confines of the secured area. This is accomplished with shielding, filters, grounding, RF emissions limiting devices, screens and various other methods. For example, a wire connects a keyboard to a computer. Every key

stroke generates an electrical pulse which, with proper equipment, may be picked up, amplified and reproduced. Note that the act of encryption does not occur until AFTER the keystroke is received within the computer, therefore the generated signal is both unencrypted and subject to interception beyond the walls of an office and therefore a potential risk of information compromise.

What are the chances that someone is monitoring the electrical impulses generated by your organization? Not much probably, however there is no data, no criminal records and no surveys to provide a picture of the threat. After all, TEMPEST signal interception leaves no trace. It has been shown through testing that off the shelf hardware is available and fully capable of capturing electronic data signals at some distance. An example of the technology behind this is the Television Detector trucks which drive down streets identifying which homes and even in which rooms an unauthorized or unlicensed television set is operating. These are effective up to about 200 feet distance. The unlicensed television viewer is unaware until notified by authorities.

This threat is ameliorated by the fact that monitoring generally requires the equipment to be placed close to the transmitting device and the equipment usually requires a technically sophisticated individual conducting the unauthorized monitoring for an extended period of time. That is why securing an entire facility is usually not justified. However, if the consequences of information compromise are sufficiently high to an organization, securing very specific information within a SCIF could well be worthwhile. Due to the high costs and technical expertise required to install, maintain and test for TEMPEST, it is advisable to limit the physical size of the SCIF to a room or small complex if possible. It will be within this secure

environment that extremely sensitive organizational data is stored, handled, discussed and used. All wires, cables and connections between computers and peripherals are shielded, power supplies are very well grounded (changes in power supply line voltage may be intercepted and indicate data transfers), monitors are screened (LCD and Laptop machines are not immune to TEMPEST signal interception) and all virus software is up to date (certain types of viruses serve to enhance illicit signal interception). This limits the signal interception capabilities of potential attackers and improves secure data transmissions within the SCIF. Note that computers must be isolated from power lines with specifically designed filters. Unfiltered machines will retransmit detectable signals back through an electrical outlet. Obviously a corporate SCIF is not the place for a dial up connection as telephone lines are completely unprotected. Also-cables and wires must be kept physically separate to prevent signals from one being coupled to another in close proximity. Every cable leaving any monitor, computer, mouse, keyboard or other computer peripheral must be shielded or grounded. Shielding the walls of the SCIF with foil, copper mesh and other conductive materials will aid in grounding out internally generated electrical and electronic signals. The National Security Agency lists equipment which meets U.S. Government TEMPEST standards. This may be helpful in selecting equipment for specific organizational requirements. The U.S. Navy's Automated Information Systems Security Guidelines manual contains a very well formatted security checklist. (7) Chapter 16 of the Navy's Automated Information Systems Security Guidelines, unofficial version http://www.elastic.org/~fche/mirrors/www.jya.com/navch16.htm

PERSONNEL SECURITY

"The purpose of a security plan is to assign accountability." (1)Jae K. Shim Anique A. Qureshi Joel G. Siegel, "The International Handbook of Computer Security", Glenlake Publishing Company, Ltd Chicago, 2000, page 167. A guiding principle for personnel security is accountability-who has access, responsibility and accountability. Within an organization, each facet of information security must have an identified person assigned responsibility. Under the SCIF concept, due to the extreme sensitivity and criticality of the information, it is therefore advisable to sharply limit access and to tightly control who knows what. This is the Compartmented piece of the Sensitive Compartmented Information concept.

Consider that there are two ways in which employees, vendors, contractors, partners or others may harm a business: deliberately or accidentally. Deliberate harm implies criminality and there are three factors to a criminal act: intent, motivation and opportunity. Controlling or mitigating any one of these will substantially reduce the risk to sensitive information through an unlawful act.

Intent may appear difficult to predict or control however there is considerable scientific and well documented evidence that proper use of both pre and post employment personality assessments tend to identify potentially dishonest traits and tendencies. Often employers have the misconception that such testing violates privacy laws or leaves them vulnerable to litigation for discriminatory hiring practices, yet quite the reverse is true. As listed in an internationally

recognized employee assessment company web site: Profiles International, Inc. **http://www.profilesinternational.com/products/sos.asp** shows the following;

- 56% of working people admit they have lied to their supervisors
- 41% say they have falsified records
- 64% admit using the Internet for personal reasons during working hours
- 35% have stolen from their employers, by their own admission
- 31% abuse drugs or alcohol

The point here is that the lack of knowledge about one's employees is risky but this lack of knowledge of one possessing access to sensitive company information would be catastrophic. By assessing an individual's concept of integrity, a corporation can gain valuable insight to an applicant or employee's potential for deceit. Obviously not completely infallible; however personality assessments provide additional information not available with background checks, reference checks or resumes.

Motivation is inherent in the type and criticality of the data being protected. Sensitive information by definition is of inestimable value and can be expected to provide sufficient motivation for misuse or misdirection to someone. Motivation is tied to the perception of discovery, punishment and/or risk of exposure. Therefore it is imperative that the physical manifestation of extreme security be apparent and that "incidents" are promptly identified and publicized. Holding violators of SCIF policies and procedures accountable and making it known that all breeches are quickly identified and dealt with tends to deter all but the highly motivated

attacker. Sharply limiting awareness of the existence of protected information to a few individuals also limits the motive for access.

Opportunity can be controlled by understanding, applying and enforcing the standards related to SCIF design, implementation and access. An excellent source of information concerning control of access to secure sites is found in (3) Access Control and Personal Identification Systems, Dan Bowers, copyright 1988, Butterworth Publishers.

The United States Navy assigns Communications Security (ComSec) Material System (CMS) custodians to insure strict accountability for every sensitive document, piece of equipment or item deemed critical to mission. This concept can be incorporated in a business setting. Select and assign two employees responsibility for inventory of documents, data and information contained within the SCIF. Each item is coded and both employees simultaneously physically sight and record each sensitive business document, computer, communications or other item as necessary. There have been too many instances of data not only lost but with no means of knowing how long it has been missing. Properly trained custodians assigned to inventory sensitive information, full accountability for each item, within a properly constructed and managed SCIF, under a program of limited access reduces the opportunity for loss of sensitive information and quickly identifies any loss or misplacement.

An excellent source of information for best practices can be found in the U.S. Navy's training plan for Communications Security: http://www.tpub.com/content/istts/14222/css/14222_77.htm

CONCLUSION

Security breeches are not generally caused by failure of mechanical, electrical or electronic devices. "The more common weakness is in the failure of management to understand the strengths and weaknesses of the automated system and to consider the function to be performed as a total system entity: a total system which includes mechanisms, people and the process which is being automated." (3) Access Control and Personal Identification Systems, Dan Bowers, copyright 1988, Butterworth Publishers, page 1.

Competition for supremacy on the battlefield of business requires an appreciation of the value of information. The establishment of a highly secure area within a corporate setting is both feasible and prudent. SCIF design concepts and practices are used by the federal government throughout the world wherever extreme security risks dictate extreme protective measures. As corporations become more global they encounter the same type of problems historically faced by governments and encounter the same need to protect extremely sensitive information, sources and resources. The SCIF concept allows the most sensitive and critical business information to be controlled through application of physical, communications, information and personnel security practices.

Hal Walter

E-mail: Hwalter@email.uncc.edu

Phone: (704) 687-4660

BIBLIOGRAPHY

(1) Jae K. Shim Anique A. Qureshi Joel G. Siegel, "The International Handbook of Computer Security", Glenlake Publishing Company, Ltd Chicago, 2000, page 104

(2) Director of Central Intelligence Directive 1/21
Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), Effective 30 January 1994 Source: CIA Hardcopy, Freedom of Information Act

(3) Access Control and Personal Identification Systems, Dan M. Bowers, copyright 1988 by Butterworth Publishers, a division of Reed publishing (USA0 Inc.
QA76.9 A25B68 1988 005.8 87-34220
ISBN 0-409-90083-4

(4) CYBERSHOCK, Surviving Hackers, Phreakers, Identity Thieves Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, Thunder's Mouth Press, copyright 2000, QA76.9.A25 S3537 2000 005.8 21-dc21 ISBN 1-56025-246-4

(5) Security in the Government Sector Protect - Detect - React www.security.govt.nz http://www.security.govt.nz/sigs/html/chapter8.html Last Updated: 22-Jul-2002 04:34:13 p.m.

(6) Physical Security Requirements for NSA/CSS Sensitive Compartmented Information Facilities, April 2000

(7) http://www.elastic.org/~fche/mirrors/www.jya.com/navch16.htm
Chapter 16 of the Navy's AUTOMATED INFORMATION SYSTEMS SECURITY GUIDELINES manual, unofficial version