Viewpoint: The Risk of Information Compromise and Approaches to Prevention

M.M. Helmsa,*, L.P. Ettkinb, D.J. Morrisc

aSesquicentennial Endowed Chair of Business and Technology, Dalton State College, 213 North College Drive, Dalton, GA 30720-3797, USA
bThe University of Tennessee at Chattanooga, College of Business #6156, 615 McCallie Avenue, Chattanooga, TN 37403, USA
cGale Corporation, North Highlands, CA, USA

Accepted 22 September 2000

Abstract

With the growing popularity of competitive intelligence, few firms consider the opposite side of data collection — defensive intelligence (DI). This viewpoint article addresses the reasons for information compromise and lack of control measures in organizations. Specific sources of vulnerability to counter intelligence are outlined and ways to secure operations are presented. Finally strategies for employing proactive measures for DI are suggested as a way to ensure the long-term prosperity of an organization. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Information compromise; Competitive intelligence; Defensive intelligence

1. Introduction

The exponential growth of globalization and the prominence of information technologies (IT) have been catalysts to both legal and illegal information compromise. Competitive intelligence (CI) units are now deeply rooted in many US and international firms and serve one primary objective: the systematic thievery of your company’s competitive competencies. With the race to develop internal CI units, firms have made the costly mistake of neglecting the other side of data collection, counter or defensive intelligence (DI). When evaluating safeguarding information, consider this: bank robbers net about...
$85 per holdup and are caught 80% of the time. Information thefts average $800,000 in value and are caught 2% of the time (Kulczycki, 1997).

2. Why is information compromised?

With the information superhighway, modern decision-makers have a phenomenal amount of information at their disposal. Geometric advances in telecommunications and information sciences have heightened the competitive landscape of business with considerable pressure to formulate rapid-fire decisions before competitors. Arthur Anderson coined the term information for competitive advantage (IFCA) because information is the primary link to outpacing competition, enhancing market share, and generating revenues (Roukis et al., 1990). Good intelligence or CI results in the competition getting the product introduced before you, offering an improved version of your product at a lower cost or forcing you to abort the introduction of an obsolete product (Nolan, 1996).

In today’s era of intelligence dependency, companies that ignore or fail to protect their information commodities will have difficulty manipulating market standings and are doomed for failure. Several action plans result from this view of DI. One, it is to protect the knowledge which is the foundation of the business whether from external competition or from malicious internal personalities. Second, is to devise and implement a series of proactive countermeasures to actively neutralize hostile CI units.

3. Why are control measures not adopted?

Any student of organizational behavior appreciates the difficulties of developing and implementing a new procedure to address a problem. DI is certainly not immune from this and is overshadowed by other organizational goals. Perception is perhaps the chief stumbling block to adopting a DI system. The majority of corporations scoff at the idea that their business is a target of espionage. The common misperception is that information compromise is targeted at big business and more specifically, defense industries. This stance was certainly true during the Cold War; however, small business is now the favored choice of spies, due to the number of competitors, recent growth of entrants, and low security posture (Winkler, 1997).

Intangibility, complexity, costliness and bureaucratic friction all contribute to the absence of DI in the corporate sector. Instituting a DI program runs counter to the strengths most firms are built upon: the free flow of information. If knowledge is indeed the life-blood of the organization, control procedures, especially in up-and-coming, innovative, teamwork-driven IT firms, is not only ignored, but also viewed with contempt. Scott Gebhardt, CEO of PG&E Energy Services embodies the corporate philosophy of cumbersome DI practices by stating: “Every company I have worked for had issues with employees taking competitive information…but, to me, it’s unpalatable to put our associates in a cloak and dagger environment. We need to keep the free flow of information to keep innovation alive” (Radcliff, 1998).

Organizations feel it is impossible to secure all dimensions of a business and could even dilute the overall security. Intangible costs to the operation of a DI system can include
compartmentalization of information and inefficiency in the total work environment from duplication of effort, stifled project development, lack of information flow and communication, and even falsely generated paranoia. The most serious repercussion is the oppressive work environment a total security climate fosters. Loss of employees, hostile atmosphere and hindrance in the synergy of the creative processes are cataclysmic irrecoverable losses to the firm (Kulczycki, 1997).

The lack of traceable benefits is yet another reason not to adopt a DI program. Accounting, marketing, finance and production typically view DI as an unnecessary and burdensome expense, providing no value-added or revenue generating qualities. Even if DI is effective, it often goes unreported beyond chief decision-makers because the discovery of an internal security breach can sink stock prices if a compromise is evident (Taylor, 1998). A survey of 1,600 IT companies performed by Price, Waterhouse & Coopers and InformationWeek indicated 73% of the companies experienced a breach or information compromise. Nearly half the compromised companies were unable to quantify losses attributed to the breaches (Friedman et al., 1997). With few empirical measures, it is difficult to express and illustrate the value of an effective DI program.

Traceable costs of implementing a DI program are significant barriers to justifying its adoption. Physical countermeasures incorporate the security dimension and include dogs, gates, encryption devices, safes, security guards, DI investigators, and video cameras. Ongoing maintenance requires additional work and/or personnel. Most DI practices are assigned to security departments as additional duties or are delegated to IT and IS departments (Winkler, 1997).

4. Organizations are vulnerable

4.1. Open source targets

Open source information is available to anyone and legal to acquire as long as the CI professional extracts the data through non-intrusive or legal means. The FBI estimates only 20% of all information compromised are accomplished through technical means (McCongale and Vella, 1996). The remaining 80% is through open source information including information the Internet, overheard conversations, company discarded trash, periodicals, books, interviews in trade periodicals, news stories in local and national publications, in-house publications, press releases, newsletters, speeches and technical publications.

Media is essential to promote, market and inform your customers of current and upcoming issues, services and products. However, too much information empowers the competition to formulate strategies against your intentions. The following media, although benign when separated, combined and properly analyzed, could provide a rival CI unit with a precious commodity known as ‘the whole picture.’ The following list attempts to provide the firm with simple and realistic remedies to counter rival CI media collection:

- limit strategically key in-house publications to employees only;
• post announcements deemed sensitive in secure or compartmentalized portions of the building;
• develop a classification system for vendors, contractors, sales force, officers and employees as to the sensitivity of the project or other form of media;
• require the press to send copies of all articles featuring personnel or the company to submit a complimentary copy to the firm prior to its public production;
• require employees taking surveys to know the company and individual surveying them and require the surveyor to furnish a copy of the final product;
• review all articles for publication prior to their release (McCongale and Vella, 1996).

4.1.1. Trade shows
Another favored method of information procurement is the special case of trade shows, conventions and conferences. These venues are viewed as accepted and legitimate venues to learn about the competition. Seasoned professionals in CI tend to strike it big at trade shows and conventions. Indeed, companies such as Compaq have fallen victim to the CI info-hounds from rival computer manufacturers. To date, Compaq will not attend the popular Comdex computer convention due to heavy information compromise from previous attendance. Compaq opined that “…it was giving more information to competitors than to potential customers (McCartney, 1994, pp. B1).”

4.1.2. Trash
A choice and legal method of procurement by spies is sifting through a company’s trash and converting it into a rival’s treasure. Your trash ultimately becomes public domain and can be legally absconded by rival CI units. Discarded phone records for instance, can aid CI units in pattern analysis. On the surface, old invoices and shipping manifests may appear useless bits of information. However, the trained CI professional can reconstruct your entire supply chain management system from this discarded waste. Below are some simple countermeasures to utilize in the safeguarding of documents:

• Establish Classification System. Establishing a classification system for all mediums, not strictly documents, to leave no doubt to the sensitivity of information contained therein.
• Establish Procedures for Discarding Classified. Ensure classified is shredded or burned and establish a log to track all classified material that has been destroyed.
• Establish a Copier and Faxing Protocol. Log or limit all copied and faxed classified documentation to provide a clear picture of tracking classified information.
• Off-site Business Centers. If possible, do not transmit classified faxes or copy classified documentation to or from external locations. This invites unintended consequences through human error and the possibility of CI professionals looking over projects in a public setting (Heffernan, 1997).
• Look at Your Office Set-Up. All printers, computers, and fax machines, which generate classified information, should not be located in high profile areas or common work areas (Shanley and Crabb, 1998).
• Destroy Carbons. Printers and faxes in particular use a film or carbon for output
purposes. The trained CI specialist can read this printed film. Thoroughly shred this legible medium prior to disposal (Kulczycki, 1997).

4.1.3. Happy employees

Few will argue that employees are a company’s most valuable asset, but the lack of employee awareness to security threats, coupled with the general indifference on the worth of information, can turn employees into unwilling accomplices for rival CI units. Seasoned CI experts can capitalize off this psychology and feed the insatiate ego for information without the subject being cognizant of the transaction. Former National Security Agency member and famed CI/DI advisor, Ira Winkler, affirmed that salespeople would invariably provide sensitive information (Winkler, 1997). Unknowingly, the client in turn may be an impostor collecting data for a rival firm. Winkler himself was able to gain total access to a bank's network via telephone conversations while posing as a human resources specialist. Numerous simple countermeasures can be instituted in this case to prevent compromise and below are just a sampling of suggestions:

- **Develop a Security Awareness Program.** The goal here is not to make all employees DI experts, but to make employees at all levels aware of the value of corporate information and the importance of information management.
- **Prioritize Data.** Inform employees that some data cannot be discussed in any circumstance outside the work environment (i.e. product development designs, pricing lists, R&D issues, hierarchical reporting structures and ensuing legal problems).
- **Badge System.** A color-coded badge identification system helps keep wandering eyes out of sensitive locations and can be designed to compartmentalize ‘need-to-know only domains’ of the building.
- **Employee Contracts and Nondisclosure Agreements.** Ensure all members of the organization do not divulge any sensitive information. Employers or prospective employers have a bad habit of attempting to extract information regarding a new employee’s previous place of work. Nondisclosure agreements and policies in company handbooks explicitly disallow such actions.
- **The Restaurant Method.** Restaurant marketing pros entice your appetite through colorful information tent cards. Organizations can place similar ‘information tents’ in conference rooms, cafeterias and next to photocopiers to remind the otherwise aloof of the importance of safeguarding your coveted secrets (Johnston, 1997).
- **Be Aware of Surroundings.** Participants are notorious for leaving sensitive data on notes, charts and blackboards in conference rooms. Teleconferencing equipment and speakerphones can theoretically broadcast to unintended listeners if not carefully examined (Kulczycki, 1997).

4.1.4. Disgruntled employees

Industrial espionage costs corporate America approximately $250 billion per year. Currently there are over 700 open industrial related espionage cases. Employee involvement is estimated between 60 and 70% of the instances. A series of safeguards need to be
enforced when an employee is dismissed or leaves the company. Exit briefings emphasizing confidentiality, immediate termination of access privileges and security audits of the individual, their contacts and their systems should be performed (Radcliff, 1998).

4.1.5. Supply chain partners

Another real and often overlooked threat to information integrity within the firm is seemingly friendly rapport with outside entities. Partnerships, alliances, joint ventures, temporary employees, contractors and suppliers all pose a valid threat to essential elements of information. Tactics below provide suggestions in preventing suppliers or other outside sources from access to your information:

- Know Thy Dance Partner. Examine how much business the supplier or partner conducts with other competitors. Address the degree of importance your partner has with other vendors or competitors and weigh the value of your proprietary assets against the relationship.
- Secure all data in the presence of your ‘guests’. Unless there is a definitive need to know, protect your information accordingly. Information that is unsecured or left in open viewing is classified as public domain and thus not protected by U.S. laws.
- Signed and Defined Agreements. Establish the appropriate legal boundaries in the administration and handling of information. Ensure all legal, ethical and past improprieties are explored. Address all need to know issues, confidentiality agreements and competitive covenants to define all legal ramifications and draw clear boundaries for the company and other party.
- Include Third Party Participants in Security Audits. Over time, vendors, suppliers or sub-contractors may develop stronger relationships with the competition. Examine these other parties in relation to you and your competition. This should be a quarterly practice (Royal, 1998).
- Define Distinctive Borders with Third Parties or Partners. Isolate the third party from other company matters. Attempt to minimize communication from other departments, which have no bearing on the relationship between your interests and the other actor involved in the partnership, joint venture or third party (Banham, 1999).

4.2. Open and closed source targets

4.2.1. The internet

The overwhelming flow of electronic data, the easy accessibility, heightened visibility and transferability of this media crosses the spectrum of both open source and closed source targets. The Internet (including local area networks (LANS), wide area networks (WAN) and all electronic platforms for communication) is the primary means of data communications in the information superhighway era. Ethical CI units search and acquire a great deal of open source data via approximately 6,150 databases available to legally access everything from press releases, company profiles, import/export records, patent information and financial reports (Economic espionage explosion, 1998). Hackers, on the other hand, use the net to penetrate computer systems to disrupt operations and/or steal
information. As a testimony to this, technical security services have risen by 25.8% annually from a $3.7 billion industry in 1997, to a projected $7.3 billion by the end of 2000 (Radcliff, 1998). Several countermeasures are discussed below to stifle hacker undertakings.

- **Encryption:** the transformation of data into a form that cannot be recognizable or understood by anyone without access to the encryption formula. Encryption is merely an additional tool in hindering the perpetrators and not an end onto itself.
- **Analyze Log-Ins:** a careful analysis of daily log-ins, specifically failed system log-in attempts, provide key indicators to individuals attempting to illegally penetrate your system or network.
- **Separate Network and External Servers:** your network or LAN system should be dedicated to in-house operations. Dedicate a host terminal to serve external operations such as Internet and outside email correspondences. By separating networks, you can hedge against a great deal of external risk of virus, hacking or information compromise.
- **Firewalls:** not a means to an end, nonetheless essential in slowing down the potential exploitation of your systems. Establish a network of firewalls between your in-house users and Internet site (Friedman et al., 1997).
- **Prevent Insurance Policies:** insurance policies are electronic back doors created by current employees that are destined to be former employees. Essentially, they provide employees with hidden access into host terminals or there former terminals. Diagram the network to examine all connections and access points of entry into and out of the system and use system administrators to monitor traffic.
- **Software Packages:** several software packages exist to eliminate theft of intellectual property by entering proprietary or company-sensitive terminology into its customizable text search dictionary than pinpointing the exact location of the information. From this juncture, security or data managers can better safeguard system information against penetration. The *Disk Tracy Network* from WatchSoft Inc., specializes in 'counter-hacker,' software and also provides a tracking system that monitors all employee usage of the Internet (Disk Tracy takes aim at employee internet abuses, 1998).

### 4.3. Closed system targets

#### 4.3.1. Disks and files

The convenient and small mediums of floppy or zip disks make it easy for information to physically leave the company. A cataloged system can help reduce some theft, but it is extremely difficult to prevent this form of compromise. Hard drives, the major repositories of stored data, are considered to be the least secure part of the computer system. Seasoned hackers can extrapolate residual files that may have been deleted but are still accessible in the system. For instance, a Microsoft Word document automatically stores itself every fifteen minutes. Hackers can reconstruct entire sensitive documents from string or discarded auto save documents. The print queue, in relation to the hard drive, is another source of inadvertently stored documentation. A search through DOS directories, UNIX servers, Word files, temporary files or Windows Explorer can aid the perpetrator in
discovering coveted secrets. Another preferred method of hacking is the penetration of Internet caches through the hard drive. Thus, the hard drive is an endless well of information beyond what is currently perceived as stored on the system. Countermeasures exist to protect or delay systems from compromise or total data destruction and include:

- **Passwords.** A series of passwords will make the penetration of your coveted secrets a more time consuming endeavor. Naturally, the more intricate the password series, the more time it will take to penetrate your system.

- **Scrubbing the Disk.** Clearing up the floating documents, which pose an information security hazard, as well as a memory burden, requires regular defragmentation of the hard drive (Friedman et al., 1997). The advantages are twofold, one, it terminates any deleted data. Second, it frees up memory and capacity, thus helping your system runs at greater efficiency.

- **Clearing Out the Hard Drive.** This simply requires the user to delete any temporary, temporary Internet, Internet history, Internet cache or miscellaneous files that act as a default for standard deletions such as Word files. Not only is this a security measure, but also like the scrubbing process, it provides more free memory to your system and should be done once a week.

4.3.2. **Viruses**

The biggest threat to information in the electronic arena is not from rival CI units, but from hackers deliberately bent on the systematic destruction of computer systems by using viruses or a piece of computer code that attaches itself to other programs and proceeds to alter or destroy the data contained therein. Viruses originate from the vindictive employee looking for a means to exact vengeance upon his current or former employer or from the demented computer enthusiast whom arbitrarily devises a virus as a challenge, political message or thrill.

Newer and more lethal viruses like the retroviruses, or viruses contained within an anti-virus program, assault the hardware by causing disk drives to spin faster and ultimately wear out the system. Worm programs are like a cancer that chews away at all files stored on hard disk. Port scanner programs are designed to look for and exploit open Internet and fax/modem ports which are then flooded by Nuker programs that render systems useless. Ping programs are designed to shut down firewalls by overwhelming the firewall server with a bombardment of requests. IPspoofing is a technique to deceive machines that direct information traffic that the spoofing program is a ‘friendly’ machine. Finally, bombs can be entered into the system that devastate and totally renders all functions of the hard drive (Radcliff, 1998). Some inexpensive but effective methods to hinder the viral process:

- **Install Vaccine Programs.** A wide array of commercial vaccines programs exist which hunt and destroy viruses but most vaccine programs can only counter present and historical problems. Update your vaccine programs frequently via the Internet in order to prevent system losses due to recent and future viruses.

- **Carefully Examine Noncommercial Programs.** Programs downloaded from unfamiliar
sources, bulletin boards or shareware should be treated with extreme care. Immediately run a virus scan against such downloads.

- Store All Downloads on Floppy. Do not store unknown downloads on hard drive. This is inviting viruses to destroy ALL of your files. Storing on a floppy sets a buffer between the hard drive and storage device that renders the virus ineffective.
- Trust No Software or Files. Do not assume software given to you from another person is safe. Even if they claim they do not have a virus, it does not mean it may not be able to impact your system. Viruses can lie dormant for an extended period.
- Make Frequent Backups. Back up all software, documents and other works in several storage devices. Floppy, zip, jazz and hard drive devices can all fall prey to failure and or viruses.
- Utilize a Security Manager. An MIS or systems specialist should be designated with the duties of monitoring all viruses and updating all software to counter viruses (Roukis et al., 1990).

5. A long-term view of countermeasure techniques

5.1. The defensive view

The long-term strategic approach of DI and is crucial. Decision makers must become involved in DI and legitimize information security practices. Operational security (OPSEC), is a countermeasure tactic that examines how competitors could theoretically procure sensitive information. OPSEC was created as a response to the continued success the North Vietnamese army (NVA) enjoyed evading U.S. Air Force (USAF) strikes. USAF intelligence initially assumed NVA’s cognitive- like ability to move forces and equipment from targeted sites was attributed to an inside USAF source. USAF intelligence eventually realized the NVA did not have any inside sources but were able to effectively determine all USAF operations through observation of material, equipment and personnel patterns. A summarized list of the OPSEC analytical process includes:

- **Identification of Critical Information.** Not merely identifying key elements, but also sub-elements that can assist the competition in gaining a competitive advantage like pricing lists, vendors/client lists, formulas, financials, etc.
- **Analysis of the Threat.** Examine the capabilities of the rival CI unit against your vulnerabilities. It addresses targets and to what degree rival CI unit will dedicate resources to obtaining information. For instance, does the competition have a successful history of undercutting our price bids with contractors? Do they have a dedicated and effective CI unit?
- **Vulnerability Analysis.** Examines what areas are exposed to information compromise. For instance, do employees in the pricing department understand the fundamental importance of discretion when discussing bids with clients or suppliers?
- **Risk Assessment.** Uses simulation to address the ‘what if’s,’ of information compromise. How much market share could be lost or how far ahead does this put the competition?
- **Implementing Countermeasures.** Implementation of countermeasures requires a change
in corporate culture and the total work environment. It is this step that puts information at the forefront of the firm above executives and tangible assets (Kahaner, 1996).

5.2. The offensive view

The offensive weapon of DI involves the deployment of incomplete or inaccurate information designed to mislead others about your intentions or abilities. Johnson Controls discovered Honeywell was attempting to collect information pertaining to Johnson’s new building control system, LOBA. Honeywell was misinformed of the project and collected information on a project dubbed LOBO, an upgrade of a previous project and held no real competitive value. Approximately a year later, LOBA was launched onto the market as Metasys and enjoyed unbridled market dominance, partially thanks to deception of the competition (Nolan, 1995).

6. Conclusions

This article has taken the viewpoint that DI has merit and should be practiced by companies. Multiple internal and immediate motives exist for stealing classified information. Less likely, but equally as detrimental, are foreign governments and multinational actors targeting your business. A host of other vulnerabilities and hostile threats also exist. The first step to incorporating a DI program is to sell leadership on the effects of not adopting a DI plan. In the era of information, who can ignore the darker topics of information loss? It is not a pleasant topic but unfortunately needs to be addressed by ALL employees at all levels and not just coordinated with the security personnel and system administrators. Perform a ‘red-team’ test of your security system to show the level of vital information that can be obtained about your company. Develop a broad-based program that is balanced and customized with the nature and style of your industry and does not just focusing on the automated or technical vulnerabilities of the business like computers and telephones. Examine rival DI programs and see how the competition safeguards its data. Beyond securing your operation, employing proactive measures could prove to be an invaluable weapon for the long-term prosperity of your firm.

References

Kulczycki, G., 1997. Information security: it’s not just what you know, it’s also how well you keep it to yourself. Management Accounting 79 (6), 19.
Royal, W., 1998. Too much trust: are trade secrets safe with suppliers?. Industry Week 247 (20), 27.