The Need for a REAL Defensive Information Operations Capability

Mark Ruchie

The Need for a REAL Defensive Information Operations Capability

Mark J. Ruchie

GIAC GSEC Certification Practical Assessment

April 22, 2002

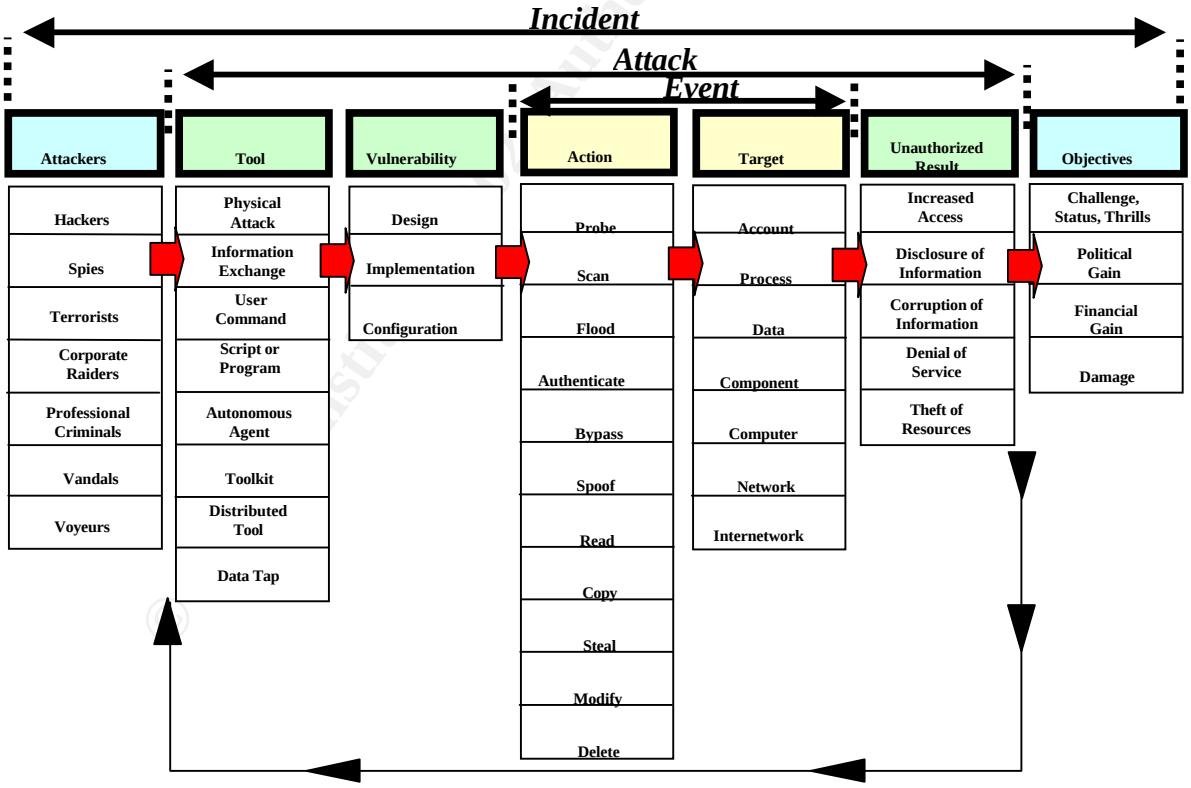
ABSTRACT

Corporate America's protection of information requires a new paradigm. All too often corporate America is concerned with the technical aspects of information protection. "Were we scanned today? How many user accounts haven't been active in the past three months? Are our web servers updated with the latest patch?" The result is a disjointed and sub optimal effort to protect corporate information. Someone needs to be concerned with the protection of the flow of information regardless of form. This can result in better efficiencies, magnify mass, shape priorities, and support business operations. Today corporate information security programs are in varying stages of development, but all focused towards a standard information security program such as those recommended by organizations like SANS, Gartner, or any of the leading consulting firms. Typically these include elements of strong corporate sponsorship, a formal security program, security policies, a monitoring program (with the requisite incident response program), with a defense-in-depth security architecture (also commonly referred to as a layered defense). However, even the models currently in place in leading enterprises are insufficient for the task at hand. Information is not only a commodity to protect, but it is a strategic asset to maximize. As a matter of fact *it is* the competitive edge regardless of business area. As America moves from a traditional manufacturing-based economy to an information-based economy (in many respects more fragile, complex, and interdependent than ever before) it does not fully recognize information as *the* true competitive edge requiring protection. The model I describe will predominantly apply to large enterprises; however, the lessons described will apply to any company wanting to do business in the information age. I will use a technical model for computer security incidents to help explain the need for an expanded concept of information protection. The technical model will illustrate the shortfalls in typical security programs. The federal government (Department of Defense in this example) has begun to address the need to protect information in a more holistic manner than corporate America. Corporate America has already borrowed concepts and terminology from the United States Government (e.g., "defense-in-depth, "DMZ", even most security incident programs) so it is only natural to examine the Government's maturing concept of Information Operations/Information Warfare. There are many references to the idea of "Information Warfare" in security circles, but most only refer to a slight change to a traditional information security construct (and some only refer to the idea of the war against hackers). In order to address this area a new paradigm is required. I propose the term Defensive Information Operations (DIO). The military includes both Offensive Information Operations and Defensive Information Operations; however, this paper is limited to discussions of the later. DIO in this paper is derived from the United States Department of Defense concept that includes those actions that protect our information, information systems, and information operations from potential adversaries. Areas examined include a traditional information security program, operations security, counterintelligence, counter-propaganda operations, electronic protection, and counter-deception. I will provide descriptions of each of these concepts and then show why they are important for implementation. I will then make the case for a synergistic DIO program with centralized control. Some models in use today include elements of this model while other organizations have implemented limited components. However, failure to

incorporate these in a synergistic model that is fully synchronized for optimum business enhancement will result in enterprises continuing to lose valuable corporate information.

A TAXONOMY NOT SUPPORTABLE WITH TODAYS DEFENSIVE PROGRAMS

I will move from discussing concepts at a very broad level down to a specific taxonomy to support my argument that today's programs will not provide the enterprise with the needed information to do battle in the information age. In October of 1998, John D. Howard and Thomas Longstaff published "A Common Language for Computer Security Incidents."[1] A taxonomy is a principal of classification which enables the gathering, exchange and comparison of information. I chose this taxonomy because it represents a mature computer security incident model. At first look this is just another "incident" description. SANS is a prime example of an organization that provides a high-level taxonomy for security incidents describing an incident as "…an adverse event in an information system, and/or network, or the threat of the occurrence of such an event."[2] However, anyone with incident handling experience will quickly realize that most of these are only high-level descriptions that require additional granularity. Howard and Longstaff attempt to take the concept of a computer security incident to a higher level and state that they published this taxonomy to "…enable the exchange and comparison of computer security incident information."[3]



[1] Howard, John D. and Longstaff, Thomas A., "A Common Language for Computer Security Incidents," Sandia National Laboratories , October 1998, www.cert.org/research/papers.html
[2] SANS – SANS Security Essentials II: Network Security, page 4-5, 2002
[3] Howard, John D. and Longstaff, Thomas A, "A Common Language for Computer Security Incidents," Sandia National Laboratories , October 1998, www.cert.org/research/papers.html

Figure 1[4]

In their taxonomy they describe three interrelated components to a computer and network incident. They include an *event*, an *attack*, and an *incident* in a relationship with the next outer element including the entire previous item (i.e., an *incident* includes unique elements and all of an *attack* and *event*, and an *attack* includes unique elements separate from an *event* – see Figure 1). Typical security programs are geared to recognize components of the innermost item and all or part of the second ring, but rarely the third ring. An *event* is the centermost item. Two items comprise an *event*; an action (e.g., probe, scan, flood, read, etc) and a target (e.g., account, process, data, computer, etc). Even within this ring some incident programs only examine the action (e.g., "there was a probe"). The second component is the *attack*. It includes the tool and vulnerability that occurs before the *event* and adds the unauthorized result after the *event*. Again, most security programs are not able to utilize any of these components because either it is not performed by the enterprise or is so fragmented it cannot effectively address these items. For instance, how many programs even attempt to identify the tool (e.g., physical attack, data tap, information exchange) or analyze the unauthorized result (e.g., disclosure of information theft of resources)? If so, it is probably only because it is a very serious attack or involves a significant loss of resources. Finally, the outer most item is the defined *incident*. The attacker is identified as the initial element with the objective of the attacker being the final element in this taxonomy. Unless there is a significant investigation (including legal) and potential prosecution, the attacker and objectives will seldom be noted. Again, this illustrates the shortcomings and need to re-tool the entire concept of protecting corporate information. The attacker (e.g., hacker, spies, terrorist, corporate rater) and objectives (e.g., challenge, status, thrill, political thrill, financial gain, etc) are elements almost wholly outside any organizations abilities to identify. Again, for most enterprises it is probably luck if any of these are identified in an incident using this taxonomy. While this model is intended for computer security incidents it illustrates the need to create a more synergistic model that will protect corporate information in any state. The point if that nobody intrudes on computers just for the heck of it. This concept must be placed in a larger context.

TRADITIONAL INFORMATION SECURITY PROGRAM

A traditional information security program is a key cornerstone of an effective DIO program. All too often information security programs are viewed from the technical perspective only. As information technology workers we are part of the problem. Of course technology is our middle name, but if it were simply just about installing a new tool we would not be value added as a career field. We are valuable to management because we analyze management's business objectives and determine ways to utilize technology to meet those business objectives. The first step for any information security program is executive support. An effective information security program requires executive commitment. Without an executive sponsor your program will be significantly degraded. Next is a formal information security program. This should include a charter

[4] IBID

and position descriptions. A long-term security strategy could also be included with the program. In order to execute the program there should be appropriate policies, procedures, and guidelines. These documents should be reasonable (e.g., having a password policy of 16 characters that must contain an alpha numeric character, capital letter, lower-case letter, a non-alphanumeric character, and a non-standard ASCII character is not reasonable) and they should be enforceable. A security-monitoring program is considered essential to anyone with a security program. This should include the tools to monitor, someone to monitor, and an incident response program. A forensics program is sometimes part of the incident response program, or it may be a separate program. If the forensics program is attached to the incident response program there should be a clear distinction between the formal incident response program and the forensics program. An incident response program is concerned with identifying anomalous activity as a formal incident (or as an event not requiring further investigation), followed by containment/eradication/recovery, and follow-up. Forensics is concerned with determining what happened and holding someone responsible (may involve legal action). The last component of a mature information security program is the underlying security technology. This is listed last because, without the previous items, resources spent on technology will be wasted. A good security program should also have an enterprise-wide security architecture that defines the program. This is all I will discuss because I want to concentrate on areas that are not adequately addressed in this field. This does not imply that most organizations have implemented mature information security programs, only that this concept is addressed in many other forums and any further analysis would only be duplicative.

OPERATIONS SECURITY

"No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution." (Niccolo Michiavelli) Operations security is a term that prevents competitors from gaining information about your operations. Some people may be familiar with the concept of operations security and think it doesn't apply to corporate America. After all, when one thinks of operations security one thinks of the military trying to hide a major operation. For instance, if the military is deploying a large number of troops to a specific country in the Middle East it may tell it's soldiers, sailors, and airmen not to tell their spouses which country they are deploying to, they may also move at night, or use any means to limit the visibility of its move. However, operations security involves much more than just this limited example. It involves identifying those actions that can be observable by any potential competitor. There are many "competitive intelligence" firms in the field today that may be "observing" your operations. As a matter of fact there is even a professional association for "competitive intelligence" professionals.[5] Many companies probably don't believe this is too big of a threat. However, according to Mr. John Nolan of Phoenix Consulting Group "…85 percent of people will share sensitive information about themselves and their companies with perfect strangers…"[6] In order to prevent this from happening enterprises should first identify those actions that can be observed. The next step involves determining

[5] www.scip.org

[6] The Huntsville Times, "Your online buddy could be a corporate espionage agent", April 30, 2000, www.al.com/news/huntsville/Apr2000/30-e27547.html

indicators of company operations that competitors might gather that may be interpreted or provides a clue that may be useful. Finally, companies should determine ways to eliminate or reduce the vulnerabilities of those actions to competitors involved in corporate espionage/competitive intelligence. This could be something very involved, or it could be something simple as Nolan states "Companies should train all executive and workers to avoid discussing their business with strangers, and should let everyone know how losing secrets can cost profits and salaries."[7]

COUNTERINTELLIGENCE (COMPETITIVE ASSURANCE)

Counterintelligence is the next component of an effective DIO program. Counterintelligence is probably too strong a term for most corporate appetites, but the concept is sound. According to one leading expert in this field they can't use the term "counterintelligence" because of the negative connotations with this term so they use the term "Competitive Assurance."[8] However, I will continue to use the term "counterintelligence" because I believe it is more descriptive. Counterintelligence should protect everything involved in information flow (e.g., operations, information systems, technology, facilities, personnel) from corporate espionage. Corporate espionage could also include foreign sources, both from countries seeking gain for its industries and from seeking to do damage. As the dominant force in the world today there are a number of threats against American business. Stealing or attacking American industry is an asymmetric form of warfare that the smaller, less able adversary is sure to use. There are plenty of failures that provide adequate examples of non-existent programs. For instance, in 1997 Schwan's Sales Enterprise was developing a rising crust pizza and wanted to get information on rival Kraft's pizza development. Schwan's hired a "competitive intelligent agent" who was able to collect the information desired by Schwan's in less than two days.[9] If Kraft had an adequate counterintelligence program (not to mention Operations Security program) perhaps they may have discovered the action earlier. However, it is apparent that this is a common practice and this phenomenon is industry independent. It is not just coincidence that there are so many "copy cats" that arrive in the marketplace at the same time in every market segment. There is typically some sort of security function existing in corporate America that performs some component of this action; however, it is rarely adequate. It is also typically separated from the other DIO disciplines. A good counterintelligence program should attempt to identify threats from corporate espionage and then conduct an assessment of those threats through analysis. Finally it should work to neutralize those threats through investigations and operations.

COUNTER-PROPAGANDA OPERATIONS

Counter-propaganda operations are the next piece of the DIO program. The concept of a company being engaged in counter-propaganda operations may look foreign. However, if examined it is apparent American businesses need to be actively engaged in this arena.

---

[7] IBID

[8] Bass, Alison, "Now that the cold war is history, intelligence pros are turning their black-bag wizard targets—maybe even the likes of you," Darwin Magazine, June 2001, www.darwinmag.com/read/060101/defense_content.html

[9] Mokhiber, Russell and Weissman, Robert, "Corporate Spooks," Common Dreams News Center, March 6, 2001, www.commondreams.org/views01/0306-03.htm

The definition of counter-propaganda operations is when an enterprise identifies psychological operations occurring against them and they take actions to try to counter that image/influence friendly populations. Companies are constantly engaged in this process. Even Larry Ellison, Chairman of Oracle, one of leaders of the information age industry has engaged in psychological operations. He attempted to negatively influence rival Microsoft by obtaining negative information on Bill Gates. It is interesting that during this period he was consistently portrayed as an innocent player/underdog, when in fact he was not. While running a psychological operation against Microsoft he may have in fact been running his own psychological operation against the general public. According to the Toronto Star "Even Oracle Corp.'s hiring of detectives to dig up information on archrival Microsoft Corp., didn't shock executives in Silicon Valley, where "security" companies hired by many of those firms say it is standard procedure to get down in the dirt to muddy the image of competitors or profit off their work."[10] It appears that Microsoft realized only too late the need for a counter-propaganda operation in the Government lawsuits. If they had a coherent operation to influence the American public to counter the image created by the US government and, apparently, Oracle, rather than appearing as arrogant business people they might have fared much better. Again, I am referring to a program that focuses on countering negative images regardless of the transport medium. It is important to have a capability to counter negative or false information on the web, but it is just important to counter it if is in some other form.

COUNTER-DECEPTION

Approximately 2,500 years ago in his classic thesis on military strategy the military strategist Sun Tzu stated "All warfare is based on deception." This truism is valid for American business as much as it is for militaries. Counter-deception is an effort to gain advantage from or negate the effects of a competitors deception operation. This functional area probably has the least direct application to the business community, but I believe it has merit for inclusion in this model. Corporate America does not like to let it be known that they engage in deception operations, but it is becoming a known practice. Deception operations could be something very strategic like releasing information on a new product designed to throw off potential competitors or it could involve countering another organizations deception campaign to obtain information on your new product. According to Marc Barry, founder of a Competitive Intelligence firm in New York "But when it comes to things like profiling competitor's R%D—like finding out Pfizer's formula for a drug it's developing for arthritis—you're not going to get that without deception or trickery."[11] A nice example of a counter-deception campaign was one executed by Gene Roddenberry during the planning for Star Trek The Motion Picture. The motion picture makers were not releasing plans to use a different cast than the original series. Gene Roddenberry simply "leaked" the plans to use different actors causing the makers to end plans to use a different cast. While it is out the scope of this paper a case can be made that Daimler-Benz executed one of the most sophisticated

[10] rense.com, "Corporate Spying and Espionage Costs Billions – The Toronto Star Business", July 3, 2000, www.rense.com/general/corp.htm

[11] Bass, Alison, "Now that the cold war is history, intelligence pros are turning their black-bag wizard targets—maybe even the likes of you," Darwin Magazine, June 2001, www.darwinmag.com/read/060101/defense_content.html

deception campaigns during its takeover of Chrysler. It is well known now, but during the initial merging process the idea was a merger of co-equals. However, as we all know the German firm quickly seized control of Chrysler and incorporated it as another business entity. Whether Chrysler executives were involved may never be known, but the end result was the end of Chrysler as an independent carmaker. A counter-deception program may have alerted Chrysler management to the possibility of Daimler-Benz's deception campaign and the end game may have had a different conclusion. What would management do if they determined there was a deception campaign? They could ignore the campaign, expose the campaign (like Gene Roddenberry did), exploit the campaign, or eliminate the competitor's deception campaign. As in any risk management decision each would involve assuming a level of risk. Eliminating a competitor's deception program could involve lengthy legal action costing significant resources. However, risk management is a responsibility of the business world and if the business community cannot quantify counter-deception as a risk proposition then they may already be too late. Being able to counter a competitors deception program is of strategic advantage to enterprises regardless of size.

ELECTRONIC PROTECTION

Electronic protection is the final element that should be resident in an effective DIO program. It is old news that many security consultants perform wireless assessments by "walking" or "driving" around and locating wireless access points. It is also no surprise that many of those access points are not well protected. While, at first analysis it appears that there is little applicability for this in corporate America, however, when you consider the vulnerabilities associated with wireless and that it is one of the hottest trends in information technology, it should be apparent of the significance of electronic protection. According to META Group Inc. wireless and mobile transactions will account for approximately 20% of business-to-business (B to B) and 25% of business-to-consumer (B to C) transactions by 2003.[12] The growing presence and importance of wireless networks and PDA devices require adequate electronic protection to ensure information availability. Electronic protection components should include frequency hopping, frequency deconfliction, or even shielding of sensitive corporate systems. During a SANS class I attended, Eric Cole of SANS told they story of how 802.11b wireless LANs and microwave ovens both operate at 2.4GHz and how you could remove the coil from the microwave, insert it into a wok and you have a wireless jammer. Militaries have been engaged in jamming communications since the invention of communications, but it is not something thought of in the business community. While to date there are not any significant stories of one company jamming another's communications links, this simple story illustrates how vulnerable wireless networks are to potential jamming. It doesn't even have to be intentional jamming. If you do not deconflict other networks/frequencies you may inadvertently jam your own communications. The explosion of PDAs and eventual introduction/expansion of personal agents will only increase the potential vulnerabilities and subsequent need for electronic protection.

[12] "META Group Survey Finds 20% of Business-to-Business Transactions Will Be Wireless by 2003," Wireless Developer Network, September 12, 2001, http://www.wirelessdevnet.com/news/2001/254/news3.html

DIO AS A SINGLE PROGRAM

To be effective, all initiatives to protect corporate information must be understood and supported by every business unit. Today, even traditional information security programs are fractured and poorly supported across the enterprise. This model dictates some centralization of all information protection elements under a DIO program. The best way to protect information and ensure its use to expand business is to have a single program that proactively protects information regardless of form. An integrated model will help foster a synergistic program that will greatly expand the ability of enterprises to protect information. This will not be possible until businesses start to recognize information as a strategic asset that is "the" competitive advantage they have in the marketplace. Creating a single DIO program does not mean that businesses should move every discipline described in this paper to a single person/organization. A matrixed organization can be created that is every bit effective as if they all worked for a single person. However, there should be a single individual responsible for the protection of information that covers each function listed in this paper. If there isn't a single effort then enterprises will not realize the benefits of a single focused program. It will remain fragmented and may have dire consequences.

CONCLUSION

This paper has examined the need to significantly overhaul the concept of protection of information in American business. America has transformed itself from a manufacturing-based economy into an information-based economy. Information is the lifeblood of our economy. In the 1990s, the information-based economy spearheaded one of the largest expansions of the United States economy. However, along with the benefits come some pitfalls. The information-based economy is more fragile, complex, and more interdependent than ever before. Enterprises need to protect information, provide it in a timely manner, and be able to shape it in a positive image. There is a need to protect information and the flow of information regardless of information medium. This paper used a computer incident taxonomy to illustrate shortcomings with current security programs. The taxonomy was created to classify and understand computer security incident information. However, it will be very difficult to fully realize the benefits of this model without a significant restructuring of the concept of information protection. The military model is referred as Defensive Information Operations (DIO). DIO includes those actions that protect our information, information systems, and information operations from potential adversaries. Areas examined include a traditional information security program, operations security, counterintelligence, counter-propaganda operations, counter-deception, and electronic protection. Almost every American enterprise is in the process of implementing a traditional information security program. However, this is just the first phase of a truly effective information protection program. Most business people will share confidential company information with total strangers. A good operations security program will enable enterprises to identify critical items, lower the profile of those items, and train workers not to share corporate information without a valid need-to-know. A good counterintelligence (competitive assurance) program is required to protect corporate information from espionage activities. Counter-propaganda operations are needed to positively influence business operations. Even "good guy" industry leaders like Oracle's Larry Ellison are engaging in psychological

operations; therefore, enterprises need to be proactive in countering any possible situation. Counter-deception operations are particularly important as businesses seek to understand their competitors. If they can identify deception operations then they can react by ignoring, exposing, or eliminating the deception. With the increasing presence of wireless for B to B and B to C transactions there will be an increasing need for adequate electronic protection. These six functions need to be combined in a single effort if enterprises are to realize the benefits of protecting their valuable information. This paper examined each area and provided examples of why they need to be included in a formal program. If addressed as an entire program corporate America will be able to fully realize the true impact of the information-based economy.

REFERENCES

rense.com, "Corporate Spying and Espionage Costs Billions – The Toronto Star Business", July 3, 2000, www.rense.com/general/corp.htm

The Huntsville Times, "Your online buddy could be a corporate espionage agent", April 30, 2000, www.al.com/news/huntsville/Apr2000/30-e27547.html

Howard, John D. and Longstaff, Thomas A., "A Common Language for Computer Security Incidents," Sandia National Laboratories, October 1998, www.cert.org/research/papers.html

Air Force Doctrine Document 2-5, Information Operations, 5 August 1998

Vijayan, Jaikumar, "Employee Data Exposed on Web," Computerworld, February 11, 2002, www.computerworld.com/storyba/0,4125,NAV_STO68168,00.html

Vijayan, Jaikumar, "Former Global Crossing worker arrested in threat case," Computerworld, March 29, 2002, www.computerworld.com/storyba/0,4125,NAV47_STO69684,00.html

Tom, Pamela, "Perils of E-Mail - How E-Mail Evidence Led to Convictions of Corporate Spying," ABCNews.com, March 27, 2002, abcnews.go.com/sections/business/TechTV/techtv_emailespionage020327.html

Hamilton, Bruce, "Corporate spying in N. Fla. higher than national average," The Business Journal, May 24 2001, Jacksonville.bizjournals.com/Jacksonville/stores/2001/05/21/daily25.html

Mellon, Derek, "The art of corporate spying – To go without "competitive intelligence" would be like going into battle without a weapon," Ottawa Business Journal, November 30, 1998, www.go-global.net/media-981130.html

"META Group Survey Finds 20% of Business-to-Business Transactions Will Be Wireless by 2003," Wireless Developer Network, September 12, 2001, http://www.wirelessdevnet.com/news/2001/254/news3.html

McCullagh, Declan, "MS Espionage: Cash for Trash," Wired News, June 15, 2000, www.wired.com/news/politics/0,1283,37022,00.html

Johnston, Margret, "Business spy threat is real, former CIA chief says," IDG News Service, 10/17/00, www.nwfusion.com/news/2000/1017spythreat.html

Benesh, Peter, "Corporate Espionage Taking Over Where Cold War Spying Left Off," Investors Business Daily, October 12, 2000, www.infowar.com/class2_101200a_j.shtml

Bass, Alison, “Now that the cold war is history, intelligence pros are turning their black-bag wizard targets—maybe even the likes of you,” Darwin Magazine, June 2001, www.darwinmag.com/read/060101/defense_content.html

Mokhiber, Russell and Weissman, Robert, “Corporate Spooks,” Common Dreams News Center, March 6, 2001, www.commondreams.org/views01/0306-03.htm