Mergers & Acquisitions, The Dealmakers Journal

January 2004

A Field Day for Spies While a Deal Advances

By Guest Writer Richard Isaacs

Whenever we mention economic espionage or loss of critical information to anyone in m&a, we usually get either a blank look or a “Huh?” Not surprising, because few business folk, acquirers or otherwise, have ever worked with a company that had anyone specifically responsible for preventing or dealing with economic espionage and information loss. Perhaps some have read an article about this area. Fewer still have had any dealings with the small population of firms, such as LUBRINCO, that deal with combating corporate espionage.

Since the problem appears to be so rare that companies aren’t aware of it, and so rare that we have few competitors, why would you care?

Because it isn’t rare at all. It is merely below the radar of the typical company. According to the *2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, economic espionage and loss of critical information costs American companies more than $300 billion a year. The average cost per incident is $50 million for manufacturing companies and $500,000 per incident for non-manufacturing firms.

Short division tells us that if only manufacturing companies were hit, there would be 6,000 incidents a year, and if only non-manufacturing companies were hit there would be 600,000 incidents a year. The number for both combined is between the two, but large enough to safely assume that all participants in your acquisitions either have been, are, or at some point will be victims.

It should be no surprise that the risk of victimization increases during the m&a process, because m&a is widely recognized as a period of instability in a company’s lifecycle. This means two things:

- There is potential for loss because of the increased vulnerability inherent in the m&a process.
- It is only a matter of time before failure to recommend protective action will lead to a negligence suit against an investment bank or other consultant that knew — or should have known — of the increased risk.

Before leaping to its connection with m&a, we should address why, if economic espionage and loss of critical information is so costly and so prevalent, is it so seldom a business concern. The easy part of the answer is that after the Cold War ended most countries shifted their spies to economic espionage. Professional spies are, well, clandestine. If the spies are worth their salt, their work and your resulting losses should not be immediately obvious, and you shouldn't expect to be better than the government at spotting them!

As an example, we had a client trying to do business in France, a country that believes it has an obligation to support local industry. Our client assumed that the way his French competitors always fractionally underbidding him was a case of bad luck. Being less trusting, we had him hand-carry his next bid in a locked briefcase rigged to detect being opened. His proposal, a bogus one, was purloined and returned while he was at dinner, the detection system revealed. The next morning he went to his office, removed a diskette that was taped to his body, and printed out the real bid, which he then hand delivered. A competitor later told him, "I see you're learning."

The hard part of the answer is that while virtually no company has anyone dealing with espionage directed against it, virtually every company has a well-funded and highly successful competitive intelligence (CI) department. A good CI group should be able to get at least 80% of the information it wants from open sources, without resorting to espionage. This is because most companies never identify their most critical information, and therefore willingly disclose it to anyone who asks for it.

A widely publicized example of this chattiness was the **Procter &Gamble/Unilever** debacle, which the CEO of P&G discovered and voluntarily reported to Unilever.

Overzealous P&G subcontractors telephoned Unilever's hair care division, claiming they were students, and asked for sensitive information, which they were given. The impropriety was that they lied about being students.

Also, Unilever employees were in the habit of throwing out unshredded, sensitive documents. The P&G subcontractors took these sensitive documents from the dumpster while it was still on Unilever property, which is trespassing. Ironically, if they had waited until the dumpster was dragged to the street it would not have been trespassing, and removal of the papers would have been considered legitimate.

The bottom line is that, unlike a physical theft, you might never even be aware that your intellectual property was stolen, and incorrectly attribute problems triggered by espionage to a host of other plausible causes.

Damage that may be inflicted by loss of critical information:

- You may lose bids because a competitor knows your costs, your markups, and the terms of your proposal.
- Competitors may beat you to market because they have your marketing plans.
- Competitors can target your customers because they have your customer lists.
- Competitors can sell similar products at a lower price because your price has to cover your investment in R&D: They have by-passed those costs and can hit you with a double whammy, by diverting the funds that should have gone to R&D into more aggressive marketing.

In sum, your firm may lose market share, lay off employees, close facilities, and eventually go out of business without your ever knowing how you have been picked clean.

M&A and Economic Espionage

Although a business is vulnerable to espionage at any time, the time surrounding a merger or acquisition is really a spy's delight. In fact, it is pretty much impossible to run an m&a process without loss of critical information. Reducing the loss requires that two issues be addressed, and one considered.

- The amount of information voluntarily revealed.
- The state of chaos as the deal unfolds.
- Has either or both companies been victimized before.

Opening the Kimono

The first issue to consider is that a lot of critical information is revealed willingly in the m&a process. When Donaldson Lufkin Jenrette, ultimately acquired by Credit Suisse First Boston, was on the block, potential buyers got to see the production figures for the individual members of the sales staff. This guaranteed that the best producers would be lured away very quickly, to the detriment of the acquiring firm. While information

deliberately revealed is not espionage, this illustrates the liability associated with loss of critical information.

This willingness to reveal critical information can be fatal for smaller companies. It is perfectly legal for the big players to listen when smaller players say they have potential competing technologies and identify specific employees that can make this competition real. Once the key players are known, the larger company can acquire the competitors or hire-away their top employees. This eliminates some competitors through acquisition, and eviscerates the rest through brain drain. For a large company — or a small company with venture capital behind it — acting on critical information is more cost-effective than espionage, and legal.

Whether stolen or given away, loss of critical information is costly, and the first issue a company involved in m&a should resolve is which pieces of its critical information should be revealed to whom during this tense and often-prolonged process.

The game changes dramatically with globalization. Foreign companies have a very different standard of what is proper, and sometimes use m&a talks as an information-gathering tool. The objective is to steal information from a potential partner or to develop contacts for future espionage. There may appear to be a good-faith intent to merge, but when the deal falls through, the foreign company may be able to walk off with a good deal of useful information.

In some overseas environments, technology is always stolen, and it is better to be aware of this before you commit, rather than after. An American company doing business in China should realize up front that shared technology will soon begin mysteriously appearing in the hands of competitors. The bad news is that you can’t control theft of intellectual property in China at this point in time, nor can you stop the use of counterfeit products within China. The good news is that you may be able to prevent its export.

Much of the critical information that needs protection is not trade secret, nor is it necessarily “intellectual property.” Critical information is any information that, if known, would give your adversaries and competitors an advantage. If a company sends senior scientists to a series of specialized conferences, we can make a good guess as to their future development plans. If we see cartons of raw materials on your loading dock, we can make a good guess as to the ingredients in your products, and their relative proportions. We see critical information exploited with the success of competitive intelligence, and in larger companies killing off smaller competitors.

So how do you protect critical information? OPSEC, i.e., Operations Security. This is the discipline devoted to the identification and protection of critical information. OPSEC was developed by and is pervasively used within the government, and is virtually unknown in the private sector. Prevention is better than dealing with victimization during or after the fact, and OPSEC can help assure that m&a negotiations are not giving away the store needlessly while sharing information necessary to cement a deal.

Chaos, the Spy Magnet

The second issue is that there is a state of chaos as the merger unfolds. With managers and employees distracted, both companies are prime targets for espionage. This means you should anticipate increased vulnerability, and take care to deal with increased threats.

Trusted insiders, who are trusted merely as a consequence of their jobs, carry out most economic espionage on behalf of the spies. They may include accountants, attorneys, business partners, consultants, contractors, employees (including managers and executives), government officials, OEM manufacturers, security guards, suppliers, temporary staff, vendors, and even visitors. In effect, everyone you trust or let into your facility, plus their families, friends, associates, is a potential threat.

Any period of corporate stress makes insiders uneasy because they quite reasonably expect to be made redundant. They certainly know that a quarter to a third of their merged confrères might be let go. No matter what kind of propaganda the two companies put out, trusted insiders have no particular reason to assume that they will be among those allowed to stay, or permitted to continue to provide the services that allow them to support their families. They are at their most vulnerable, and, therefore, are prime candidates for being approached by well-prepared spies.

An offshoot of low staff morale and high staff vulnerability is relative indifference to protecting the assets of the merged entity that they expect will be putting them on the street. As the m&a process moves forward, we always see a definite increase in carelessness and indifference to procedure, which can be taken advantage of by the unscrupulous. This is a good time for serious bad guys to try to gain access to information by all sorts of means. Besides suborning a trusted insider to steal, we have seen cases in which men and women met and fell in love with some person who stole information that was innocently, albeit imprudently, brought home from

work. In some cases the theft was accomplished by accessing computer systems from the trusted employee's home.

Finally, operational vulnerability is much higher during a merger or acquisition. All systems in both companies are in a state of flux, and are easy targets for exploitation. A lot of security procedures are by necessity bypassed until systems can be consolidated. Strangers are given access to places that had been well guarded and information is shared with reckless abandon.

A spy may be able to simply walk in off the street, sit down at a computer (and it is unlikely that anyone has changed the default systems passwords), and download whatever information they want. If systems passwords have been changed from the default, merely asking for access will often get the spy what he or she needs.

It is prudent to ensure that the unavoidable chaos caused by m&a does not become the causal factor in loss of critical information to third parties by spies drawn by staff fears and possible laxity in the protection of information.

Which Ship is Leakier?

Although not directly related to m&a, the third issue to consider is whether either company is an ongoing victim. If neither company has anyone assigned to prevent or deal with espionage, there may be no knowledge of the victimization(s).

A case in point. A major corporation called us in recently because there were signs it might be the victim of espionage. Based on what we were told, we believed it had been victimized. Before we had a chance to help them deal with the attack, the firm's stock price coincidently dropped, and management cancelled all outside contracts to demonstrate that they were "controlling expenses." In subsequent conversations it was clear that the theft was proceeding apace, with a consensus that the company would soon be tens of millions of dollars poorer.

In the m&a process, the side most concerned about hidden liabilities will likely be the acquirer, which wants to know a number of things, including what intellectual assets the target has. Since 70% of a company's assets may lie in its intellectual property, many buyers disconcertingly find on first pass that, other than trade secrets, there has never been an audit and evaluation of IP. From the OPSEC perspective, the natural corollary to this is that there is no policy or person in place to protect these unidentified assets, and no awareness of victimization.

Discovery of ongoing espionage is not necessarily a disqualifier, because any adverse effect is already reflected in the numbers. If espionage is discovered and eliminated, and the damage not fatal, the numbers would hopefully get better. Either way, the buyer would be prudent to find out how vulnerable the company might be to espionage, and if it is being victimized. Yet, espionage victimization is not a standard part of m&a due diligence.

What to do?

Dealmaking is about the marriage of organizations, not about catching spies or preventing information loss. Nonetheless, the chaos introduced by m&a is a magnet for spies, and espionage issues should be dealt with. If m&a includes exercise of due diligence on the target, a logical part of this due diligence should be identifying and dealing with significant vulnerabilities to loss of critical information — at least with regard to vulnerabilities introduced by the m&a process itself. The small incremental costs for an OPSEC system to prevent loss of critical information during m&a, including implementing any recommended countermeasures, are a minimal and legitimate part of the deal process.

Prevention

How Does OPSEC work? Risk is calculated as:

Risk = probability × impact

Where:

Probability = threat × vulnerability

So that risk decomposes to:

Risk = threat × vulnerability × impact

Threat — Threat comes from specific competitors or adversaries. If there is no threat, there is no risk. But the numbers tell us that there is a real threat — that a specific individual or organization has the desire, the skill, and the intent to acquire your critical information.

Vulnerability — Some targets are more vulnerable than others, generally thorough neglect because the entire espionage issue has been overlooked. If vulnerability is lowered, risk will be lowered as well.

Impact of the theft — How damaging is the loss of “smart” assets? If the impact is low, you don’t care. If it is high, there is cause to worry.

To gauge the interaction among threat, vulnerability, and risk, look at theft of pens. The threat is high, because everyone walks off with pens. The vulnerability is high because nobody monitors pens. Since the impact is low (pens are cheap), there is little risk, so it is more cost effective to order another box of pens than to track them or to try to prevent their theft.

How do you assess risk to your critical information? Unless you have intelligence, counter-intelligence, or OPSEC professionals on your staff, you can't do it in-house. Espionage and OPSEC are similar to tax law. It doesn't pay to develop the expertise and experience in-house because there are specialist firms that can handle the assessment.

Identifying and protecting critical information through the use of OPSEC have five key iterative parts. Keep in mind that OPSEC is a process, not a set of steps to be followed sequentially, and the parts have no necessary order. They are:

- **Analyze the threat.** Which adversaries demonstrate both the intent and capability to be a threat to your mission, operation, or activity?
- **Identify critical information.** Critical information is developed from analyzing both friendly and adversary strategies to achieve their objectives. What is critical to them may not seem critical to you.
- **Analyze vulnerabilities.** Vulnerability exists when critical information is susceptible to capture by an adversary. Vulnerabilities are wide ranging and may include lack of training, use of non-secure communications, publishing VIP itineraries, publicizing attendance at specialized conferences, revealing marketing material, and poor system design.
- **Assess risk.** Risk is the likelihood that an adversary will gather and exploit your critical information (threat × vulnerability), and the resulting level of impact from the loss. Risk assessment is a decision-making step, because you decide if a countermeasure needs to be assigned to a vulnerability or threat based on the level of risk this vulnerability and threat combination poses.
- **Apply countermeasures.** A countermeasure is anything that effectively reduces an adversary's ability to exploit vulnerabilities. Countermeasures don't need to be exotic or expensive; they can simply be smarter ways of to do a particular task. The development of a countermeasure focuses directly on the vulnerability it is designed to protect, and the entity from which you need to protect it. After a

cost/benefit analysis, countermeasures are implemented to address the vulnerabilities that represent the most significant risk.

The process starts with questions to be answered before we arrive on site, and is followed by on-site analyses, inspections, interviews, research, and examinations to identify what critical information needs to be protected from whom. Different adversaries want different information. Once we know what needs to be protected from whom, we can determine the vulnerabilities and get management's assessment of impact of losing critical information. Finally, we can assign numbers to the threats, vulnerabilities, and impacts, and come up with a quantified risk for each item under consideration. This allows us to decide which vulnerabilities to ignore and with which to deal.

Countermeasures are designed to reduce risk, transfer it, or, at minimum, make it tolerable. Installing and maintaining countermeasures may have to be done by the company, or in conjunction with the company's consulting firm. It may be necessary, for example, to have the company do an audit and evaluation of intellectual property. Or it may be necessary for the company to implement a document control system for certain categories of information, or to have the IT department subcontract monitoring and active response to network intrusions. Implementation of these systems and processes require the specialized consulting assistance of lawyers, accountants, IT experts, and other specialists, rather than intelligence professionals.

From the m&a perspective, the goal of OPSEC is not to make either of the parties immune to espionage and loss of critical information, nor is it to stop ongoing victimization. It is, rather, the more appropriate goal of preventing m&a from turning the deal itself into a source of loss. By implementing OPSEC while the deal moves forward, partner companies can proactively and cost effectively discover and deal with vulnerabilities directly associated with m&a.

Richard Isaacs *is SVP of The LUBRINCO Group, an international vulnerability management firm that specializes in protection of trade secrets, intellectual assets, and other critical information.*