WHAT HAVE YOU GOT TO LOSE?

The case for Corporate Counterintelligence

By Chris West, Jerry Hoffmann and Udo Hohlfeld

A principal concern of corporate security is the protection of a company's physical assets from loss, damage and destruction. IT security looks after computer systems while patent attorneys and legal teams are responsible for protecting intellectual property and trade secrets. But who looks after a company's other knowledge assets that are no less responsible for performance and profitability? Usually no-one is assigned to this task and valuable assets are being pilfered by a long list of covert observers who do not necessarily need to act either illegally or unethically to get what they want. With OSINT, HUMINT and Social Engineering the damages caused are an existential threat.

Introduction to proprietary knowledge assets

Security is a function that all companies should take seriously. Some may be more serious about it than others, depending on the business they are in and the amount of damage that can be caused by security lapses, but the requirements of insurers alone will ensure that even the smallest companies install some form of security system.

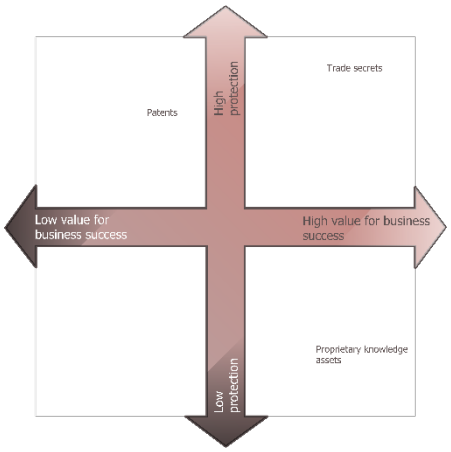
The question is not so much whether security exists but exactly what the security system is designed to protect, and this may be a major problem. Priority is always given to the protection of physical assets which if stolen or damaged will interrupt the flow of business and incur replacement costs. Security, IT, Intellectual Property and legal teams also protect staff, intellectual property and trade secrets from a range of threats but there is invariably a significant gap between the assets that are protected and the assets that need to be protected.

The security business quite rightly sets out to protect companies from "the bad guys"; those prepared to trespass, steal, damage, infringe, hack into, infect, abduct and extort. These are activities for which there is legal redress whether it is physical property, intellectual property or trade secrets that are being targeted. Unfortunately, although these events are serious when they occur, they are far from being the most common threats to a company's assets. They exclude the large number of organizations and individuals that are using perfectly legal and ethical methods to obtain information that may be regarded as sensitive but is by no means intellectual property or a trade secret. These are known as "proprietary knowledge assets".

Definition of Proprietary Knowledge Assets

Proprietary knowledge assets are the lubricants that make companies work. They are the bedrock that supports the structures for attaining company strategies. They are rarely acknowledged as assets in any formal sense and they have been acquired and modified over time as the company has grown and developed. They evolve as the company invests in new processes and procedures and in response to changes in conditions and the environments in which the company finds itself operating.

They may or may not be written down and although their value is seldom calculated and never included within the intangible assets shown on company balance sheets, the cost of acquiring them is usually substantial. Their value can be considerably more than the declared value of tangible and intangible assets. Individually they may not be unique but as a system they are proprietary to the company that has developed them.



Despite their importance proprietary knowledge assets are rarely protected.

What exactly are these assets? The following list is representative, but not exhaustive:

- **Indicators of progress, problems, changes, or new directions**; e.g. how well a product in development is doing, issues with a new product rollout, reorganizations in the sales force, new compensation schemes, etc.
- **Business processes**; aka "how things get done around here". This can include both current processes as well as contemplated or planned changes in process. Organization charts may be targeted, but additional "softer" information is also sought; such as who has the most influence (rank does not always equal power) or what informal reporting relationships exist that influence decision-making.
- **Deployments and locations**; i.e. where human and physical resources are located and what they do there. This can be as general as what is manufactured in a particular plant or as specific as the names and backgrounds of the senior leadership at a given research facility.
- **Recruitment**. This includes information about the jobs to be filled and the backgrounds of the people who have already been recruited. Information of this type is sought not only to identify remuneration and background requirements, but it is also frequently used as an indicator of a company's strategy, intentions, and future direction.
- **Contacts, contracts, relationships, and partnerships**. Competitors often seek information about a company's external relationships, including customers and other companies with a business relationship with the target company. These relationships are investigated not necessarily to identify new sales targets (in the case of identifying customers) or to interfere with these relationships in any other way. These relationships are identified to provide an informed – but external – source of information about the target company.
- **Supply sources.** Like other external relationships, supply sources are identified to provide information about the internal activities of the target company; in this case, usually to learn more about the target's value chain.
- **Manufacturing cost analysis.** Piecing together information on employment, local labor rates, rents, technology costs, raw material costs and several other key indicators to show the likely cost structure of a product or plant.
- **Differentiators that provide advantage** (for example, atypical partnering programs, non-traditional development methods and specialized workflow processes). These are processes and practices that can provide significant competitive advantage, and yet are not always identified or appreciated by company employees as such.

As the saying goes, "familiarity breeds contempt". These pieces of information are so taken for granted that they are seldom seen as valuable. Although they don't rise to the level of trade secrets, these are the assets that, individually and collectively, make every company tick and determine whether and how much profit is made.

So what is the threat?

If the information is so basic it is clearly relevant to ask what harm can come from a competitor obtaining it and why should it be defended. The answer is that competitive intelligence is only acquired if it can cause serious damage to the companies being studied and/or provide significant advantage to the company using the intelligence. Most major US corporations employ teams of staff devoted to collecting intelligence on their competitors and the estimated annual spend runs into several billions of dollars. A significant proportion of the expenditure is with specialist vendors who carry out investigations for clients using perfectly legal and ethical techniques. The level of expenditure suggests that the intelligence is not only highly prized but is also effective.

To understand the threat, it is essential to know what the intelligence is used for. Companies collect intelligence to understand the competition (or potential competition) that they are up against. They want to understand the competitors' strengths and their weaknesses; they want to know what they do and, more importantly, how they do it and at what cost. They key motives are:

- Emulation – copying what competitors do well to gain advantage or at least level the playing field
- Exploitation – using competitors' weaknesses as a tool to beat them
- Anticipation – foiling competitors' new initiatives such as product launches and new services

Companies are particularly interested in what competitors do well but also find it also worth knowing if there are elements of their activities that they perform badly. Weaknesses can be exploited in competitive battles and strengths can be emulated or bettered. Even more importantly, competitive intelligence collects myriads of relatively small and relatively innocuous pieces of information in order build big pictures that show strategic intent and the tactics by which that intent is to be achieved – things that no company would willingly make public.

So how does that work? Well, consider the following:

1. A company hires a new associate research director.
2. The same company quietly acquires a small technology startup.
3. A university scientist publishes an arcane piece of research in an obscure scientific journal.
4. The company applies for a permit to demolish an obsolete factory.

Is any of this important? Individually, no. Collectively, it alerts attentive company observers employed by the company's competitors that the company is probably embarking on a new strategy. Using well-honed skills in collection and analysis, they will soon learn that:

1. The new research executive has a background in a technology new to the industry.
2. The tech startup is one of the first to attempt to commercialize the same technology.
3. The university scientist's research is also related and was funded by the target company.
4. The demolition permit will soon be followed by a construction permit for a state-of-the-art factory to produce the new technology.

As a result, long before the target company announces its new product line, intelligence savvy competitors will have already taken action to diminish its value.

In fact, regardless of how sensitive they may appear to those inside the company, all proprietary knowledge assets have a value to a long and varied list of outsiders. The list includes many other observers whose attention is welcome, such as customers, distributors, business partners, suppliers and bankers who require information to help them decide whether and how to do business with the company. If these welcome observers, ask for information they will normally be told what they need to know. The others on the list are, to varying degrees, hostile observers who, if they require information, must collect it covertly. These can be classified into three groups:

- Those whose attention is unwelcome
- Those that can do moderate harm
- Those that can cause serious damage

An intelligence gathering campaign by any one of these observers will cause damage but what is usually overlooked is the multiplier effect that results from each group of observers using the others as information sources and adding their own observations on top.

THE OBSERVERS

- Unwelcome attention
  - Academics who seek information to support their studies and who may publish conclusions that are damaging to the company
  - Brokers looking for an inside track on information to support their profit projections, which may or may not agree with the company line
  - Commercial due diligence specialists assessing the value of a company on behalf of an unknown potential buyer
  - Private equity houses assessing the value in order to present the company to clients as a potential acquisition target
  - Trade Unions seeking information that is not provided to them through the regular communication channels to support negotiations
- Moderate damage
  - Competition authorities seeking evidence of anti-competitive practices
  - Consumer groups studying product problems and looking for poor manufacturing processes
  - Government departments, particularly the tax authorities looking for evidence of tax avoidance and evasion
  - Management consultants looking for information to support recommendations to clients
  - Regulators looking for information to indicate breaches of regulatory guidelines
  - The Press looking for any story – good or bad - about the company or information to support rumours or tip offs about the company
- Serious harm
  - Competitors looking for intelligence that will provide them with advance warning of

Can proprietary knowledge assets be defended?

The answer to this question is yes, but with difficulty and not by traditional security methods. The difficulty stems firstly and perhaps most significantly, from the fact that there is no group within the

company charged with the responsibility of defending proprietary knowledge assets. Secondly the information being sought is generally known to large numbers of staff (and ex-staff) and may also be known by third parties who have no strong allegiance to the company. The third problem lies in the fact that each individual piece of the information being sought can be made to seem non-threatening and whereas there are clear sanctions for giving away intellectual property or trade secrets there is nothing in place to defend knowledge assets of the type we have described. The fourth problem is that companies release far too much information that on its own may appear unthreatening but when pieced together by skillful analysts reveals a bigger picture that is extremely dangerous.

Finally, those who hold information can be approached by methods that by-pass all conventional defense methods. Virtually all staff with access to useful intelligence can be reached by telephone, e-mail or via social media with a modicum of effort to get around the simple defenses that are in place. Once in touch there is an armory of techniques that can persuade people to talk. Not every contact will do so but a skilled investigator knows how to play the numbers game and weave his or her way into the confidence of enough people in the know to get what they need.

This activity is a long way short of industrial espionage and defending against it requires an approach that responds directly to the significantly softer techniques used by intelligence collectors. We call this Corporate Counterintelligence.

Corporate Counterintelligence

Corporate Counterintelligence (CCI) is a process installed at a corporate, subsidiary, or divisional level that is designed to at least frustrate, if not completely neutralize, the efforts of covert investigators to access proprietary knowledge assets. It is a skill that brings together:

- Detailed insight into how investigators work and the techniques they use
- Knowledge of the pinch points in the intelligence gathering process and how these can be used to frustrate their activities
- Experience in setting up a human/technology-based solution
- Experience in using the output from counterintelligence to identify problems, calibrate the threat they represent and devise sanctions.

There is a misconception that the outflow of intelligence from staff members can be contained exclusively by training. Certainly, training is an important part of the process, but it is far from enough. To be effective the process needs to include all the stages that precede investigators talking to staff. In far too many cases, if conversations with staff members occur it is already too late, and intelligence will be lost

While a CCI program can be designed to work as a standalone process, it should be an integral part of an all-inclusive corporate security program.

Where does corporate security fit in?

Corporate Counterintelligence is the responsibility of every employee, but the effort to imbed it into the corporate culture is best led by a consortium of company functions with applicable expertise. The makeup of this consortium may vary somewhat across companies, but the involvement of certain groups is essential. They are (in no particular order):

- The company's own competitive intelligence professionals. They should be able to provide an understanding of the competitive intelligence process and the methods used to identify, contact and extract information from company employees and others who have access to the proprietary knowledge assets of the company.
- The legal department. Company lawyers provide guidance in the legal aspects of the remedies or actions that can be taken against identified intruders and the legal appropriateness of any organizational or personnel steps that the company might consider mitigating the intrusions.
- Corporate security. Last but by no means least, corporate security can make three important contributions to the organized defense of proprietary knowledge assets:
    1. *Professional leadership and expertise*. Corporate security has the overarching responsibility for protecting corporate assets. Although proprietary knowledge assets, as we define them, do not typically fall within its purview, the security team follows basic precepts of security and professional standards that are applicable in any security situation. Corporate security's recognition of the threat to proprietary knowledge assets, and its importance, is a key factor in getting the rest of the enterprise to act against it.
    2. *Implementation*. Regardless of the program that is ultimately designed to protect the company's proprietary knowledge assets, corporate security is often in the best position to make it work. Indeed, in many – if not most – companies that have an enterprise-wide security program, it is corporate security staff that is responsible for managing the program.
    3. *Integration*. Corporate security has existing tools, particularly tracking tools such as IRMS, to integrate corporate counterintelligence into the larger corporate security effort and thereby make the CCI program even more impactful.

In addition to the contributions above, corporate security can begin the process by taking a leadership role in closing the gap through which so much valuable private company information is currently flowing. Using its position as the single function totally devoted to securing company assets, corporate security can influence the decision to begin building an effective CCI process that is appropriate to the company's culture and needs.

Conclusion

Corporate security teams have a vital role to play in defending companies from the large numbers of predators that seek to obtain access to the substantial body of vital but generally unrecognized assets – the performance-creating knowledge that all companies acquire as they develop their business. The defense process is generally unfamiliar to conventional security teams but can be learned from experts who know how intelligence is collected and how to build it into existing security procedures. By championing the introduction of corporate counterintelligence into their company's security program, security professionals can plug this very significant – but largely ignored – gap in the protection of corporate knowledge assets.

Authors

Chris West spent 20 years plus running CIS, a London based vendor of competitive intelligence services, and has in-depth experience of primary and secondary intelligence collection. In 2001 he published "Competitive Intelligence" one of relatively few UK texts on the subject. On retirement from life as an active poacher he turned his hand to game-keeping and in 2009 he founded CounterAction together with Jerry Hoffmann. Chris is a founding member of Counter Force Group.

Jerry Hoffman was Director of Competitive Intelligence for Eli Lilly and Company and prior to that held a similar position at SBC (now AT&T). In addition to his competitive intelligence responsibilities at Lilly, he also developed and implemented a highly effective corporate counterintelligence program which was jointly administered with corporate security. Like Chris West, he has been a competitive intelligence professional for over 20 years. Jerry is a founding member of Counter Force Group.

Udo Hohlfeld founded INFO + DATEN to supply targeted intelligence helping clients succeed in their markets. He is a recognized intelligence specialist with experience since 1992 in the intelligence arena. Udo's unique portfolio of intelligence services supports clients' business activities in the key areas of security and strategy. His specialties are Offensive Intelligence aka Competitive Intelligence and Protective Intelligence aka Counterintelligence. Clients are assured of the highest possible quality of deliverables by Udo's extensive international network of intelligence experts and by his project experience in many industries. The network is the foundation for the Counter Force Group that Udo established in 2019. Fortune 1000 clients have benefited from hundreds of projects so far.