Protecting Corporate Secrets

A Brief Primer on Contemporary Practices in *Information Security*

Michael W. Minieri, CPP, CCO

Certified Protection Professional

Certified Confidentiality Officer

PREFACE

This document is primarily intended to serve as a general primer on key issues related to the practice of protecting information in the modern corporate environment. It is important to note that this brief treatise is NOT – in any way – a guide to establishing a protective program. It is no substitute for a complete program developed by skilled and knowledgeable confidentiality professionals. While many of the aspects of corporate information protection have parallels in the defense industry, the focus herein is on the needs of those in the private sector that are not subject to requirements such as the National Industrial Security Program or similar.

In the computer age, the term information security has evolved nearly to the point where the protection of data networks from outside intrusion has overshadowed the attention needed for the security of information in the more classic sense. It can be said that information in an electronic form – in simple terms – is just the same information maintained in a different medium. While recognizing the importance of IT security, this paper focuses more on the information itself, and on the more traditional aspects of the confidentiality practice.

While the subject of protecting information has legal implications, there is no intent to provide legal advice herein. Competent legal counsel – from staff attorneys where available - is an essential member of any team developing a program for the protection of information.

INTRODUCTION

A company's information may well be its single most valuable asset. What a company – as a collective entity – knows may be at the heart of what gives that company its competitive edge. The continued success of the organization may hinge on its ability to keep certain information out of the hands of other parities, particularly its competitors. In an age when information is king, a company's very survival may hinge on its secrets.

Increasingly in the United States, domestic competitors are adopting some of the practices which have become nearly commonplace in many foreign countries. Foreign entities commonly employ competitive intelligence units to acquire information, sometimes legally, sometimes not. All too often, once such information is in their hands, it may be employed flagrantly and with little or no effort to disguise its origins. Some foreign governments themselves, have been guilty of industrial spying. As markets become more and more globalized and abuses are identified, companies find that many foreign governments have weak laws for the protection of business information, or none at all. Even where such laws exist, many regions are notorious for their lack of enforcement ability or support.

A mark of the legitimacy of legal information gathering is the existence of the Society of Competitive Intelligence Professionals (***http://www.scip.org/***). This organization supports the efforts of those who seek to gather information through legitimate sources. It would be naïve to think that less scrupulous practitioners – those that will employ illegal means, do not educate themselves with equal dedication. For our purposes here, suffice it to say that even if it is legal, a company does not have to make it easy for others to procure its secrets.

While laws and enforcement are important benefits for recourse after the loss of key information, at that point much of the damage is done. If damages can ever be recovered from the perpetrator – often they cannot – such restitution is many years away and near term financial performance can suffer substantially. Restitution is of little comfort to the executive that must get the company through the crisis in the meantime.

A company often finds that it spends many times more money on activities in response to the loss of information, then it would have spent on measures to prevent the loss in the first place. Worse yet, the investment in proactive protective measures usually follows the crisis, so the preventive money is ultimately spent in either case.

The need to protect certain information for competitive reasons is that which usually comes to mind first at the mention of the subject, and this is absolutely an important reason. But there are others as well. Today, organizations face a seemingly overwhelming array of additional reasons to protect information in their possession. In addition to regulatory mandates to protect some information – such as some personal data in an employee file – there is a growing need to implement measures in effort to avoid or mitigate civil litigation.

WHAT IS IT CALLED?

Obviously, much of the information a company has is actually intended for public disclosure. Information such as that contained within "marketing materials" is a clear example. Some information must be disclosed as a matter of law, as is the case with Securities and Exchange Commission (SEC) filings and for patents. Then there is the information that is easily understood to be sensitive with the iconic example being the secret formula for Coca Cola®.

Many labels are applied in effort to distinguish certain information that is to be protected in some way, as a sub-set of all the information a company may have. Common terms include "intellectual property", "trade secrets", "confidential information" and "proprietary information". In the legal profession, some of these labels create important distinctions as they may be specifically defined by laws and other regulations.

The laws – some State and some Federal – usually stipulate a multi-part criteria that can establish a legal "test" for determining if the subject information qualifies for protection under that law. For those outside the legal community, it is likely that these distinctions require less emphasis. Best Practices for confidentiality professionals would tend to include elements for ALL of a corporations protected information that would meet or exceed the criteria necessary to qualify the information for legal protection under its appropriate legal classification. The essential criteria that is of focus here is that a company must "take reasonable steps" to protect its secrecy. While a comprehensive information protection program will create sub-sets of categorization, with some variations on the protective treatment each sub-set receives, all sensitive information will be accorded the same general protective measures. As a result, we will refer to this master set of information simply as "protected information" henceforth in this writing.

COMPARTMENTALIZATION

The fundamental rule for determination as to who should be granted access to protected information is the "NEED TO KNOW" concept. "Need" can generally and simply be described as "necessary in order to perform one's tasks and fulfill their assigned responsibilities" . There was a time when "authorized persons" – those granted access to protected information – were simply designated by their position on a vertical hierarchy, with regard to the level of sensitivity of the information they were permitted to see. In the defense industry parallel of the day, this would establish one's clearance level. Under this vertical structure, a person would have access to any information at their cleared level AND to all of the information at every lower level in the vertical hierarchy.

Today, it is understood that not everyone – even those holding higher positions in the hierarchy or in an organizational structure – really "need to know" all of the information that is being protected. To better integrate the concept, a contemporary practice known as "compartmentalization" is now utilized. Since 9/11, the media has given much coverage to terrorism and frequently uses the term "cells". In a terrorist cell (i.e.: group or unit), the members of that cell are only provided with a limited amount of knowledge about the activities of the overall terrorist organization of which that cell is a small part. In the event of their arrest or capture, even if the individual wanted to cooperate with authorities, that person does not have knowledge that would be particularly damaging to the overall organization. This is an example of the concept of "compartmentalization" in practice.

Compartmentalization is a Best Practice in the protection of information in the corporate environment. A simple example would be personnel information such as health records. Such records are a common sub-set within the overall category of protected information. The Vice President of Production may hold a very high position in the organizational structure, yet it is unlikely that this person would have a "need to know" about an employee's confidential health records, in order for him or her to fulfill their duties in the production division of the company. As a general rule in an information protection program, if the person does not have a valid need to know, the person would not be authorized to have access to that sub-set of protected information.

Likewise, a corporate security department would typically maintain their own files related to internal investigations and background screening it may conduct. In the event that an investigation should prove the need to terminate an employee for cause, the security department might report only the results of the investigation to the Human Resources department, rather than submitting the entire case file. In some cases, security might only communicate that the employee is to be discharged for misconduct or violation of company policy, without any

further detail. Of course, in the event of any resulting litigation, the security records must be sufficient to justify the action. Where pre-employment background screening is utilized, compartmentalization might suggest that the investigators report only that the subject has "passed" or has not, without further detail. This is only appropriate where a clear set of criteria has been established, and this criteria should undergo a legal review prior to implementation.

A more common example might be in a high-technology research and development department. Numerous individuals may be working to produce the Ultra-Widget, the companies next big competitive advantage product. It is commonplace to isolate Ultra-Widget information to the team working on this project. Increasingly, companies find it desirable or necessary to further compartmentalize information, even within the overall group of people working on this project. Sub-teams or even individuals themselves may be restricted to having only the limited information they need to know for their particular task or function within the overall project team. Each of these sub-groups would not know all of what the other sub-groups are doing, and may not have sufficient information about the end product to severely damage the project in the event they should disclose – intentionally or inadvertently – the information they know. It is common for R & D management to argue that such compartmentalization hinders the ability of the unit to reach its objective. This should be carefully evaluated as there is no necessity to withhold vital information from anyone that has a valid need to know.

CLASSIFYING INFORMATION

With respect to protected information within most corporations, the two most challenging hurdles in developing a comprehensive program are making the determinations as to "what is there to KNOW" and "who NEEDS to know it"? While a skilled confidentiality professional can facilitate this undertaking and greatly assist the client in this task by making the process proceed in a timely, efficient and thorough manner, this function is one that ultimately rests internally with the corporation. The scope of an engagement in this area of practice may focus more on establishing the program and educating client personnel on how to implement and maintain it, rather than the consultant having extensive access to the information itself.

Each information protection program development project must be specific to the particular nature of the client's business. Even common sub-category labels are subject to detailed refinement of their definitions when incorporated into the program for a specific entity. Corporations, non-profits and other entities will commonly find that they have need for at least 3 or 4 sub-classifications of their protected information, with some examples as follows;

PERSONNEL CONFIDENTIAL: These are the portions of employee records – of any kind - that are to be protected against general disclosure. This would include, but not be limited to, credit and health information. In some corporate environments, this label may use a term that is more encompassing such as "REGULATORY CONFIDENTIAL", which would include all of the other information that may be required by law to be protected from disclosure, in addition to personnel information.

BUSINESS CONFIDENTIAL: Generally, this would be information that is not subject to the Trade Secrets Act but that does have commercial value to competitors. Customer lists are often in this classification. In some cases, information that a competitor could legally assemble for themselves by expending time, effort and money, may still be subject to legal protection.

SPECIAL CONTROLS: A description for this class might include that it is of significant economic value to the holder and would include ideas that may be at a stage of development that is premature for submitting a patent application. All information that is subject to the Trades Secrets Act, is also assigned to this category.

SECURITY SENSITIVE: Information that could be used to compromise or circumvent security measures of the company needs particular care. This would include aspects of Executive Protection programs and some other information such as floor plans featuring the placement of security system devices.

CLASSIFICATION PROCESS GUIDANCE

Those charged with identifying and classifying information to be protected within an organization should strive not to be too inclusive. To do so tends to trivialize the importance of the information itself and the company commitment to the protective program. More importantly, it may be argued that your protective measures are not reasonable in that you have classified information that is arguably not worthy of special measures. As a rule, information that would not normally tend to be classified for protection would include that which IS generally known to one's competitors and any information that is obviously in the public domain.

Care should be exercised when considering information that could be viewed primarily and simply as embarrassing to the company if it were disclosed to the news media, for classification as "protected". There may be negative implications for the overall program if these cases would tend to evidence that the otherwise reasonable measures are regularly abused. An example for debate would be the questionable use of corporate aircraft. Executive travel may reasonably be considered as "security sensitive" information subject to protection within the policies and procedures. In the event that an executive should take his family on a mini-vacation aboard the plane – if in fact this is an abuse - the protection of that aspect of the trip might lead some to suspect that the information protection program is a tool for covering up corporate scandal.

There are many items of information that are subject to protection as a result of a legal agreement with an individual, other business entity or through a governmental relationship such as licensing. This would include information covered by "non-disclosure agreements" and similar contractual provisions. A particular sensitivity should be accorded information gathered during activities related to mergers and acquisitions. This focus should be magnified in cases where the transaction does not result in an integration of the two entities. It may be prudent to strictly limit much of the information gained exclusively to those involved in the negotiations, and this issue should be a part of the policies and procedures resulting from the process of developing a comprehensive information protection program.

ESTABLISHING A COMPREHENSIVE CONFIDENTIALITY PROGRAM

The end product of the process of developing an information protection program is primarily a document or set of documents that outline the company policies and procedures pertaining to the subject. Another important part of the program is to add "an emphasis on protecting information" to the corporate culture. While nearly every company has policies on this subject, and many also have procedures, it is extremely common that these documents are not sufficiently comprehensive and lack the necessary detail for them to be adequately implemented and executed. The following overview of the primary elements of a confidentiality professional's consulting engagement will serve several functions herein. The outline will convey many of the key elements that must be considered and addressed within a comprehensive program, and it will help convey the depth, breadth and scope that can sometimes be associated with any effort – internal or external – to produce the final documents.

ASSESSMENT: Nearly every project will rightly begin with a three-part assessment. The first part will focus on determining what existing policies and procedures are currently in place, and will include a preliminary analysis of their efficacy. This will involve a review of existing documentation as well as extensive interviews with numerous personnel. An element in considering efficacy is the matter of determining whether or not the existing program materials are adequate, and if they are generally found to be adequate, are they being strictly practiced and enforced. The second part of the assessment is the production of a general outline of the elements of the Best Practices in confidentiality that are appropriate for the specific environment of the organization under evaluation. Finally, the result of comparing what exists against what should exist, is a form of "Gap Analysis". The Gap Analysis becomes the foundation for outlining the tasks that need to be performed in order to complete the development project. An extensive assessment performed in greater depth and detail would be the fundamental scope of an audit engagement.

PROGRAM OF REQUIREMENTS (POR): The Gap Analysis is converted to an outline of the elements to be addressed in the final program document, and establishes the Program of Requirements for the balance of the project. Without an attempt here to be as specific as would be the case during an actual engagement, the following describes many – but certainly not all – of the matters to be addressed in the program (not in any particular order);

GENERAL TASKS AND PROVISIONS:

- Identify the types of information the organization holds that is to be protected
- Create classifications appropriate for the sub-sets of information so identified.
- Outline criteria for granting authorized access to each class of information
- Establish a marking and labeling scheme including serialization numbering
- Determine storage needs, methods, media and security measures for same.
- Procedures for accessing protected information and recording transactional activity
- Procedures for processing newly created information into the program
- Procedures for de-classifying information no longer in need of protection
- Procedures for the transmission, conveyance and transfer of protected information internally and externally, by any means and methods.
- Develop employee training and awareness program, including orientation presentations.
- Procedures for internal reporting of abuse or suspicions and follow-up response.
- Procedures and schedule for periodic reviews and audits of the program once in place.
- Employee non-disclosure agreements.
- Human Resources exit interview package
- Signage and posted notices.
- Vendor confidentiality agreements.
- Document shredding and prototype destruction.
- Work area / office precautions and after hours inspection program
- Trash and rubbish handling procedures
- Custodial and visiting vendor procedures.
- Visitor procedures for sensitive areas
- Contractor and sub-contract agreements and procedures
- Premises security issues: layout, systems, controls, monitoring and surveillance
- Technical Security Counter-Measures (TSCM) considerations (i.e. "bugging", etc.)
- Policy for copying and duplicating protected information
- Policy for internal review of articles, scientific papers and presentations
- Review of public website content
- Trade show, convention and conference practices.
- Parallel considerations for non-paper versions within Information Technology (IT)

IT IS REALLY ABOUT PEOPLE

When confidentiality professionals discuss the subject of information protection with corporate executives, it is often clear that management tends to think first about the efforts of outsiders to acquire their secrets using methods worthy of the TV character Magiver. As with experts in any endeavor, security practitioners of all specialties study the tactics and techniques of their potential adversaries. In researching the practices of those who seek to obtain corporate secrets, most are surprised at how easy it is to elicit information from unsuspecting employees. The operative word here is "unsuspecting". What may seem to be an innocent and common conversation may – in reality – be a carefully crafted pretense to acquire protected information. Personnel in scientific fields tend to work in a culture where sharing research and other information is the norm. Once engaged in a conversation, such as at a tradeshow booth or job interview with a competitor, anyone might inadvertently let slip some tidbit that – added to data assembled from all available sources – makes the difference between who gets an innovative new product to market first.

As a result, the single most important element in developing, implementing and maintaining an ongoing confidentiality program is the education and training of ALL employees in the organization. Information Security must be an integral part of the orientation process, of the policy and procedure manual and of the employee handbook. Some excellent lessons in this regard can be taken from occupational health and safety professionals, and a glaring contrast becomes evident. When was the last time you saw posters on the wall reminding employees about protecting information?

CONCLUSION

It is highly likely that there is a tendency among the public to believe that the theft – or loss by other means – of a company's sensitive information is a rare occurrence. They think similarly of occurrences of kidnap and ransom and the reason for this thinking is the same in both cases: Most people tend to make such judgments based upon the contents of the news media such as television, newspapers and magazines. If they do not see an issue in the news frequently, "it must not be happening". Like kidnap and ransom events, the loss of sensitive information is an issue for which there is every reason to keep quiet, and few (if any) good reasons to make it public. None-the-less, if one searches for evidence of it, there is considerable and substantial justification for concluding that information disclosure is the largest single source of financial losses in corporate America. The U.S. Trade Commission has estimated these losses at $300 BILLION annually.

Like many skills, it would be understandable if many outside the confidentiality profession were to assume that any intelligent person – even a traditional security professional – can establish a program for the protection of sensitive information. Also as is typical of such thinking, it would be erroneous. Having a policy and having procedures is one thing…having an effective and comprehensive program is quite another.

Outside of national defense, the protection of corporate information of economic value may be the most important factor in the United States' global leadership in commerce. To the employees and shareholders of any company, there may be no fiduciary responsibility having a greater potential for negative impact on the company than that of securing company secrets, and therefore, none more important.

Every corporation seems to understand the need to have firewalls, passwords, locks and keys and there is no argument here against the absolute necessity for these and other protective measures. When it comes to traditional information security, the steps taken by most companies can amount to installing a vault door on a circus tent.

ABOUT KROLL

Kroll is the worlds foremost independent risk consulting company. For more than 30 years, Kroll has helped clients reduce their exposure to global threats, capitalize on business opportunities and protect employees and assets. Kroll has offices in more than 60 cities around the world and its services include;

Corporate Advisory and Restructuring
Forensic Accounting, Valuation and Litigation Consulting
Electronic Evidence and Data Recovery
Business Intelligence and Investigations
Background Screening
Security Services

ABOUT THE AUTHOR

Michael Minieri is a Senior Associate in Kroll's Reston Virginia office outside Washington D.C. He is a 30 year veteran of the security industry and law enforcement community. His qualifications are extensive and he holds 7 professional credentials including CPP (Certified Protection Professional) from the American Society of Industrial Security (ASIS) and CCO (Certified Confidentiality Officer) from the Business Espionage Controls and Countermeasures Association (BECCA). A leading security industry publication stated that "Michael Minieri is one of the most prominent people in the industry" in its introduction to a cover story and exclusive interview with him in 1998. Mr. Minieri provides security consulting and integrated protective systems engineering services to Kroll clients both domestically and internationally, for private sector and governmental entities. He can be contacted at mminieri@krollworldwide.com

