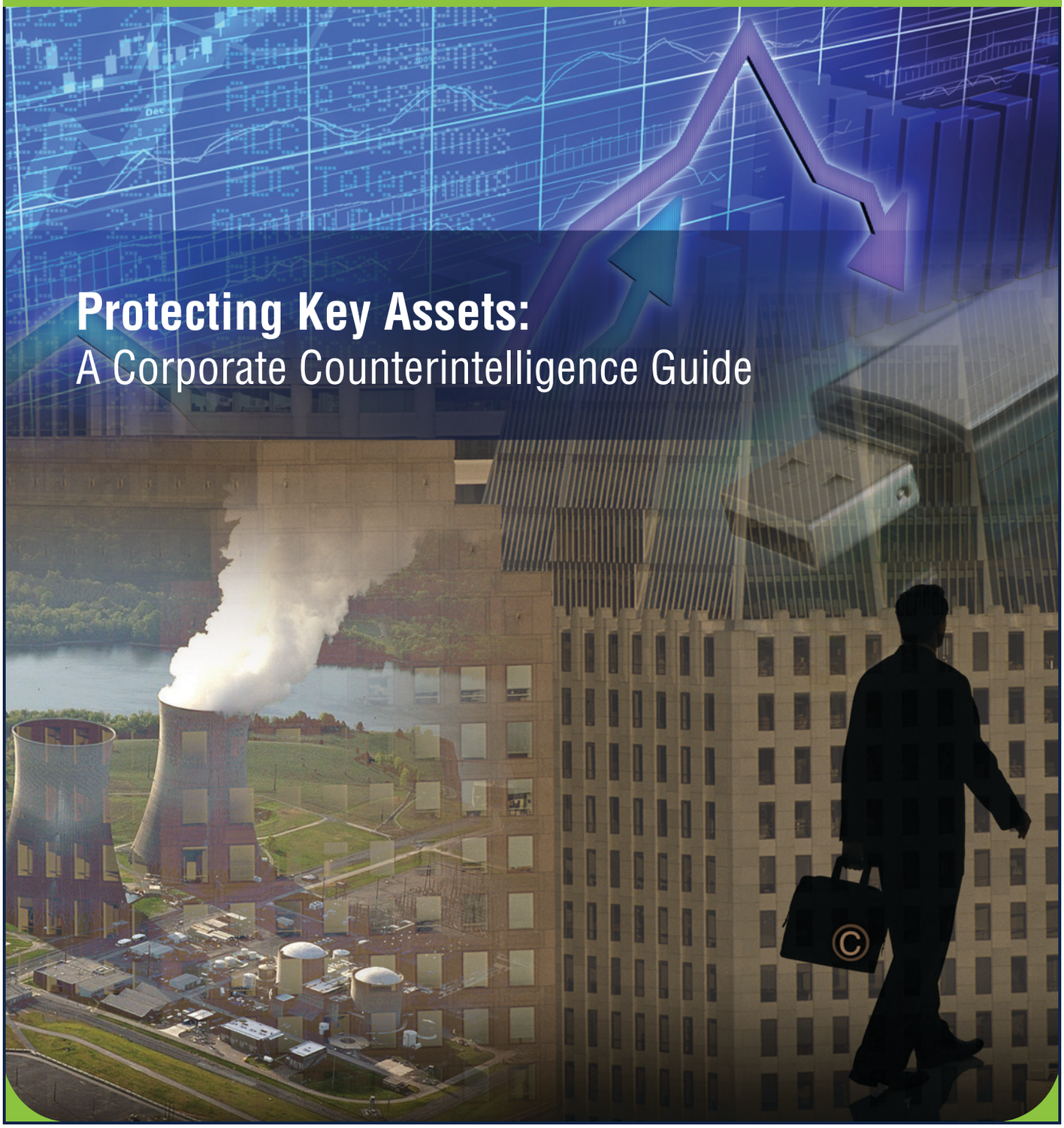
COUNTERINTELLIGENCE SECURITY

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Protecting Key Assets:
A Corporate Counterintelligence Guide



Counterintelligence for the Private Sector

Introduction

A disturbing trend has developed in which foreign intelligence services, non-state actors, and criminals are using intelligence collection techniques against American companies to steal valuable trade secrets and assets. This activity can bankrupt a company by compromising years of costly research and development, weaken the U.S. economy, and threaten national security. According to the FBI, the cost to U.S. industry is tens of billions of dollars each year.

Corporate boards and executive officers must understand the true threat their companies face. It is one that has evolved beyond the stage where information security, as one example, can simply be delegated to the security office or CIO - it requires full executive engagement. With the tools available to economic spies, the American private sector is more vulnerable than ever.

Not too long ago, traditional corporate espionage was dangerous. It required the corporate spy to betray one's coworkers, clandestinely collect company documents, load and mark dead drops, and operate under the constant risk of exposure and arrest. Yet corporate espionage, like so many activities, has moved into the realm of cyberspace. In cyberspace, many American companies are left working in the modern equivalent of the Wild West, an unregulated frontier where the crown jewels of the corporation - trade secrets and intellectual property - are hijacked every day, often without the victim's knowledge. In turn, America often finds itself competing with the very developments and technologies our companies pioneered.

Companies must have aggressive security programs to protect their intellectual property, trade secrets, business processes, strategic goals, and the integrity of their brands. This guide outlines the steps involved in building a corporate counterintelligence (CI) program to complement your company's security program and respond to the intelligence collection techniques used by today's spies. An effective CI program will ensure that your company has identified its most vulnerable assets, understands the threats to those assets, has discovered the vulnerabilities that might make your company susceptible to exploitation, and has taken the appropriate steps to mitigate risks.

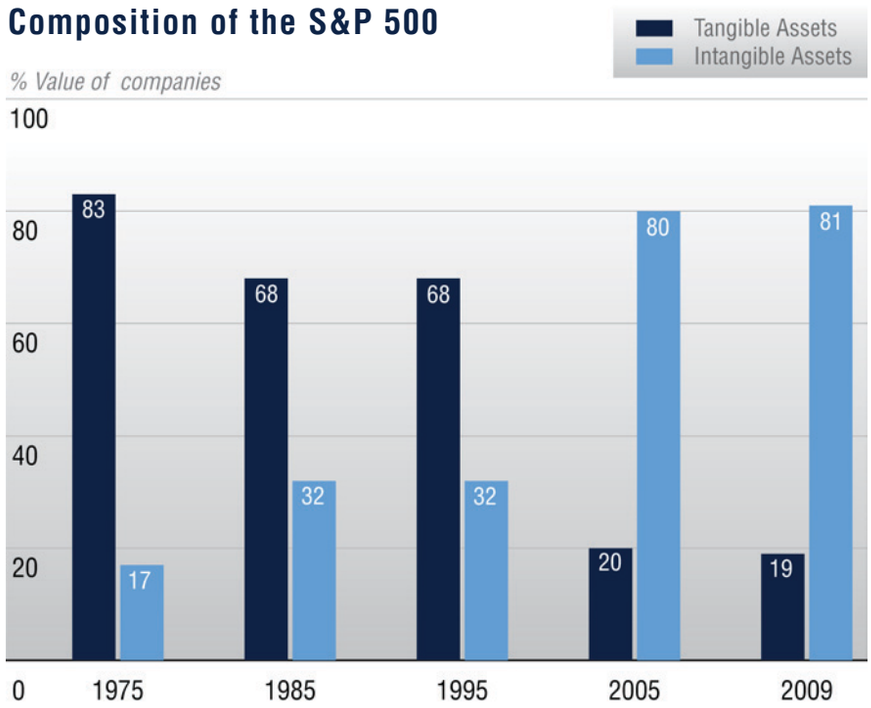
Unlike many of our most active competitors who engage in cyber espionage, the United States does not have a centralized industrial policy - nor should it. Our long-standing prosperity is a reflection of the free market. That places a large responsibility on the shoulders of American CEOs. The U.S. Government will share threat and warning information to the full extent of the law, but to protect our economy and our position on the global stage, much of our national security will have to move from the war room to the board room.

> *"Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries."*
>
> *- ONCIX Report to Congress on Foreign Economic Collection and Industrial Espionage*

Where the money is:
Transformation in Corporate Asset Values Creates Economic Vulnerability

The U.S. economy has changed over the past 20 years. Intellectual capital rather than physical assets now represent the bulk of a U.S. corporation's value. Research by Ocean Tomo Intellectual Capital Equity that is captured in the chart below shows the transition from an economy of tangible assets (real estate, hardware, vehicles) to one in which intangible assets (patented technology, trade secrets, proprietary data, business process and marketing plans) now represent 81 percent of the value associated with the S&P 500. This shift has made corporate assets far more susceptible to espionage.

Simon Hunt, Vice President and Chief Technology Officer of McAfee, said in a 2011 report titled "Underground Economies" that: "Criminals understand that there is much greater value in selling a company's proprietary information to competitors and foreign governments . . . the cyber underground economy has shifted its focus to the theft of corporate intellectual capital."



Source: Ocean Tomo Intellectual Capital Equity.

When Security is Not Enough

When companies become targets of competitors, foreign intelligence services, and criminal elements, even aggressive security programs may not be enough. A CI risk assessment (described later in this guide) can help determine the threat of espionage activity against your company and the size and scope of the CI program or capabilities that are needed to address this threat.

Counterintelligence and security are distinct but complementary disciplines, and it is important for organizations contemplating the establishment of a CI program to understand the difference.

- Every corporation in America needs an effective physical security capability that ensures employees, facilities, and information systems are protected. Security, at its root, is defensive.
- Counterintelligence is both defensive and proactive, and it incorporates unique analysis and investigation activities designed to anticipate, counter, and prevent an adversary's actions, protecting company resources and innovation.

Counterintelligence and security programs create a continuum of effective protection for your company.

Step One
Conducting a Counterintelligence Risk Assessment

The decision to create corporate CI programs and practices will be based on concerns that your company and its assets are a target of foreign intelligence services, criminals, economic competitors, and private spies-for-hire. Therefore, the first step in establishing a CI program is to conduct a risk assessment that evaluates the threat to your company by examining available threat information, assessing your organization's vulnerabilities, and gauging the consequences of losing critical assets. A senior executive or board member of your company should oversee the CI risk assessment process from start to finish, drawing on both in-house experts and outside expertise in CI analysis, operations, and investigations to complete the assessment. A risk assessment will help determine the capabilities and resources that will be required to run an effective CI program.

While companies will need to tailor CI risk assessments to their unique circumstances, all assessments require three important actions:

A. Identifying and Prioritizing Assets

Your company should identify and prioritize its most critical assets, to include people, groups, relationships, instruments, installations, processes, and supplies. The loss or compromise of these assets would be the most damaging to your organization, could result in substantial economic losses, or could harm U.S. national security.

Collaboration with industry partners and Federal agencies that have oversight or regulatory responsibilities in your business sector can provide a fuller picture that will assist your company with this prioritization process. Your company's management will have to make the final assessment of those assets most worthy of protection.

B. Determining Threats

Next, your company will need to assess the capabilities, intentions, and opportunity of potential adversaries to exploit or damage company assets or information. You also should determine if there are any gaps in an adversary's knowledge of the company or if your company is working on a particular technology or product that an adversary may be trying to acquire. Company executives should seek the assistance of counterintelligence professionals and establish relationships with Federal agencies to make use of existing threat reporting for this part of the assessment.

C. Assessing Vulnerabilities

Finally, your company will need to assess the inherent susceptibility of its procedures, facilities, information systems, equipment, or policies to an attack. You will need to determine how an adversary, including a malicious insider, would attempt to gain access to your critical assets. When assessing vulnerabilities, a company should consider the physical location of its assets and who has access to them, including both employees and outsiders.

Companies should identify any systemic or institutional vulnerabilities. Situations in which employees are dispersed geographically—including at overseas locations—or have access to or are involved in sensitive systems or projects deserve extra scrutiny.

Step Two
Laying the Groundwork for a Corporate CI Program

The risk assessment will provide a better understanding of the scope and nature of the threats to your company's most important assets. At this point, a number of initial activities should be considered that will lay the groundwork for building an effective CI program. To prepare for implementation, your company should:

- Assign or hire a program manager who is dedicated to the CI program and has direct access to the CEO or senior partners so that CI and security issues can be addressed expeditiously, discreetly, and with appropriate authority.
- Establish that the CI program will have a centralized management structure but will support the entire corporation, regardless of location.
- Take steps to begin or continue strengthening strong relationships among the company's security, information assurance (IA), general counsel, and human resources (HR) departments; these relationships are critical to effective CI.
- Develop liaison relationships with relevant U.S. Government law enforcement and Intelligence Community agencies to ensure effective two-way communication on CI issues of concern to both the corporation and the U.S. Government.
- Ask the company's legal counsel to provide clear guidance on the new program's potential activities.

Step Three
Identifying the Capabilities Needed

As progress continues on laying the groundwork, your company should begin identifying the CI capabilities needed for an effective CI program that is focused on protecting your company's assets, brand, and intellectual property. The risk assessment will be an important guide during this step. The Office of the National Counterintelligence Executive (ONCIX) recommends a layered approach to acquiring CI capabilities. CI capabilities are essential to identifying and countering insider and cyber threats, which represent the two most challenging threats to U.S. corporate assets.

The following are six primary capabilities that should be considered when determining the size and scope of the CI program your company requires:

Corporate CI Program Capabilities

1. Threat Awareness & Training

New employee orientations and continual refresher training can equip the workforce with the skills needed to understand who your company's adversaries are, identify threats, and follow reporting procedures for suspicious activities. A highly trained and aware workforce is key to the early detection of potential threats. Companies should utilize a CI-specific non-disclosure agreement before divulging their threat and vulnerabilities.

2. Analysis, Reporting & Response

An analysis, reporting, and response capability can integrate resources and information from across relevant corporate elements (CI, security, IA, HR, general counsel) and provide assessments and warning on data that may be indicative of a threat. Mature CI programs will also want to incorporate risk assessments related to sensitive acquisitions into this analytic and reporting process.

3. Suspicious Activity Reporting

Defining, training the workforce, and developing company reporting policies on suspicious activities that are deemed inappropriate or potentially threatening could provide an effective "early warning system" of potential threats to your employees or company.

4. CI Audit

A CI audit capability would enable your company to monitor user activity on corporate IT systems. This would help to identify anomalous behavior, deter the theft or unauthorized use of company information, and protect the company from network intrusions.

5. CI Investigations

Companies with more advanced corporate CI programs may wish to augment their ability to conduct security investigations with a capability to perform preliminary CI investigations that are consistent with the law.

6. Liaison

Companies should consider establishing or continue strengthening liaison relationships with US Government law enforcement and Intelligence Community agencies, to facilitate the flow of intelligence reporting, investigations, referrals, and training opportunities.

Step Four
Implementing a Corporate CI Program

Once the risk is assessed, the groundwork has been laid, and the CI capabilities required are identified, your company can begin implementation of a CI program. Although the investment needed to build an effective program will use company resources that might otherwise be dedicated to product development, marketing, and other priorities, it is important to remember that a properly designed program that is tailored to your company's unique security needs and that protects your critical corporate assets can more than justify the costs.

Program Management

The following describes three management frameworks that are recommended based on the level of capability your company requires. The functions are cumulative and build toward what ONCIX considers to be the framework for a full scope CI program.

A. Basic CI Program (Essential)

1. A CI program manager is assigned responsibility for development and implementation of the program. It is often beneficial to have one program manager who is responsible for both CI and Security.
2. The program manager serves as the focal point for a centralized CI program and has insight and access to information from all corporate elements (security, IA, HR, general counsel) relevant to CI.
3. The program manager is responsible for liaison activities with U.S. Government law enforcement and Intelligence Community agencies to gather threat information, report information to the appropriate U.S. Government agency, and follow up on CI issues of concern.
4. Component security officers should report threat information to the corporate CI program manager and should also consider reporting to their local law enforcement contacts.
5. The program manager provides CI guidance and information to the workforce through existing corporate training programs.

CI Program Management Frameworks

Basic CI Program

- PM develops and implements CI program
- PM oversees a centralized CI Program office
- PM maintains insight into all corporate elements
- PM is responsible for liaison with US Government
- Security officers responsible for tactical CI
- PM provides CI guidance through training programs

Expanded Program

- PM has received professional CI training
- PM manages a broad analysis, reporting, and response function
- Employee records are centralized to enable PM access

Full Scope Program

- PM oversees branch employees responsible for CI
- CI manager oversees dedicated CI training programs

B. Expanded CI Program

1. The CI program manager has received professional training in counterintelligence.
2. The program manager manages a dedicated CI analysis, reporting, and response function that is responsible for assessing information from all the corporate components relevant to CI (security, IA, HR, general counsel).
3. Employee records are managed centrally to facilitate access by the program manager and to support CI investigations.

C. Full Scope CI Program

1. The CI program manager oversees employees in the company's subcomponents or major programs who are dedicated to CI responsibilities and have received professional CI training.

Staffing

Your company also will need to make staffing decisions when the size and scope of the CI program is decided. Most companies will begin by implementing a program that is centralized at headquarters and will designate points of contact at non-headquarters locations. Ideally, these points of contact will be dedicated full-time to the CI program, respond to headquarters direction, and understand the specific CI responsibilities assigned to company entities at non-headquarters locations.

A fully functional headquarters program should, at a minimum, be staffed with the following personnel:

- **CI Program Manager:** An individual responsible for managing the organization's counterintelligence program, who ideally has security or CI expertise and is given direct access to the company's senior management. If necessary, companies might consider hiring a former counterintelligence or law enforcement professional to acquire this expertise.
- **Program Officers:** The employees who will perform the CI program functions. The number of program officers will depend on the size and composition of the company, the company assets needing protection, and other factors identified in the risk assessment.
- **Security Analyst(s):** At least one individual with analytic training, appropriate understanding of the organization, and full access to relevant information technology systems who will maintain an appropriate awareness of threats to the company as a whole and to specific company assets. This person may attend analytic forums of interest on behalf of the organization.
- **Program Support Officer:** At least one individual to assist the program manager and senior company officials by performing basic program management functions, such as strategy, policy, budget, and program evaluation.
- **Liaison Officer:** An individual assigned to conduct extensive liaison with industry partners and with relevant U.S. Government agencies to ensure strong information sharing programs and processes.

Maintaining an Effective Corporate CI Program

Once your CI program is established, ONCIX recommends a number of follow-on activities designed to ensure that the program remains effective. We encourage companies with an active CI program to:

- Establish a process to share security and CI "best practices" across the company's CI, security, HR, and IA elements and ensure that these practices are applied consistently throughout the organization.
- As new technologies emerge, continuously update technical CI capabilities focused on countering insider and cyber threats. These measures range from employing the latest electronic security measures such as firewalls, auditing tools, and secure passwords to robust security and reporting practices.
- Build processes to screen sensitive company acquisitions for potential negative Foreign Ownership Control and Influence concerns and to reduce the risk of an adversary introducing new threats to your organization by exploiting your company's supply chain.
- Assess the effectiveness of your CI program and capabilities periodically to ensure that they remain focused on the highest priority threats to your company and are providing a valuable return on your company's investment.

To Report Counterintelligence Issues

To report criminal activity within your organization, contact the Federal Bureau of Investigation at (202) 324-3000.

For Defense and Industrial Contractors with concerns related to national security, contact the Defense Security Service at 1 (888) 282-7628.