SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Intelligence & Analysis >

Intelligence Analysis in the Private Sector: Growth, Challenges, and Applications

At the SEC we’ve increasingly seen private-sector clients and Tier 1 leaders turning to intelligence analysis to help them manage risk. According to the Harvard Business Review’s 2022 article “How Corporate Intelligence Teams Help Businesses Manage Risk,” this trend has resulted in intelligence programs becoming ubiquitous; most major companies either have one or are building one.

From the C-suite’s perspective, it’s not hard to see why. Intelligence analysis promises the ability to see around corners, providing relevant and detailed insights that can allow a business to foresee and limit certain risks while leveraging others for new competitive advantage. Particularly for large companies navigating a global operating environment, this kind of knowledge can mean improved strategy, reduced loss, and increased profitability.

But despite companies’ embrace of intelligence analysis, misconceptions persist about what private-sector intelligence analysis is and how it can aid organizations.

What the Field Is

Private Sector Intelligence: applying intelligence techniques to external operating environments legally and transparently to facilitate strategic decision-making and mitigate geopolitical and security risks.

- Maria A. Robson Morrow, Program Coordinator of the Intelligence Project at the Harvard Kennedy School's Belfer Center [1]

The private sector intelligence field involves much more than information collection.

It involves carefully selecting sources of publicly available data, legally and transparently collecting and processing the data they offer, synthesizing it into relevant, meaningful insights, and presenting those insights clearly and concisely to the appropriate decision makers in the organization.

Private sector intelligence has multiple aims – facilitating strategic decision making, mitigating geopolitical risks, and mitigating security risks. This casts a wide net, taking in competitive intelligence, cyber intelligence, market intelligence, protective intelligence, business transactional intelligence, geopolitical intelligence, and reputational intelligence.

Each of these subcategories deals with diverse facets of risk that are commonly managed in different functions across the organization.

How It Evolved

For centuries, even millennia, intelligence gathering was viewed as an element of war and political affairs. It wasn't for businesses; it was for governments. Finding relevant information required man-hours, extensive training, travel, access, discretion, flexibility – in other words, a substantial investment of resources. For government organizations, this investment could reap benefits that justified the expense, but not so for most companies. What's more, companies generally don't have the same legal rights to intelligence gathering that governments have.

But the scope and reach of intelligence collection and analysis has evolved quickly with the progression of the Information Age.

Private-sector Intelligence collection spiked in the United States after September 11, 2001, relying in large part on the hiring of and partnership with public-sector intelligence community

[1] Morrow, "Private sector intelligence: on the long path of professionalization," *Intelligence and National Security,* Vol 37, Issue 3, 2022

professionals with government clearances.[2] These partnerships allowed businesses to leverage government intelligence resources with the goal of enhancing homeland security.

At that time, the World Wide Web was in its infancy. Now, however, it is a treasure trove of free, accessible information. The proliferation of publicly available information on the Internet – open-source intelligence (OSINT), including search engines, social media, public records, news sources, libraries, web sites, dark web, image searches - has contributed to a significant uptick in private sector intelligence capabilities. Government clearance is of course still necessary to access many types of intelligence, but OSINT can provide game-changing insights if gathered and analyzed by professionals with the right skills.

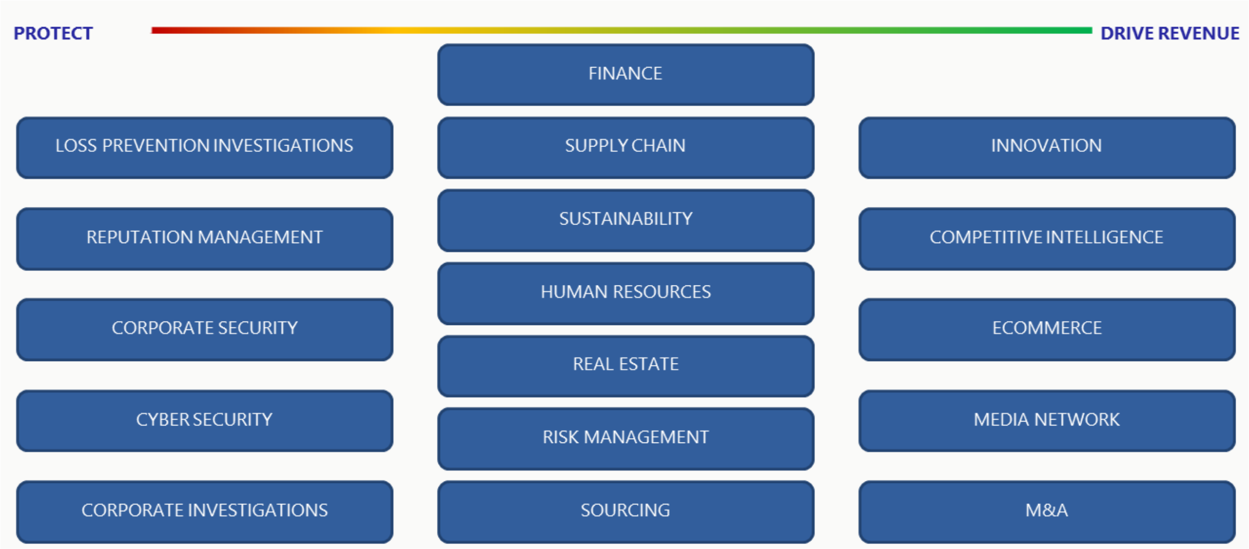
Applications for Private Sector Organizations

Businesses can use intelligence analysis in myriad ways. Here are just a few examples.

- To identify reputational risks (e.g., slander, activist action)
- To identify physical and protectional threats (e.g., pandemic, terrorism)
- To identify cyber threats (e.g., attack indicators and behaviors)
- To identify and safely exploit business opportunities in new geographic areas
- To protect and track assets through the supply chain
- To vet and validate third parties
- To understand the potential implications of business decisions
- To inform business strategy
- To understand competitors' strategies
- To recognize industry trends
- To conduct pre-transactional diligence in mergers and acquisitions or management changes
- To support the organization in legal disputes and investigations

The graphic below, created by Lindy Smart, Executive Director of Intelligence Studies at Mercyhurst University, shows how several common applications of intelligence range from protective to revenue-driving services.

[2] Daniela Baches-Torres, "Private Sector Intelligence: A Developing Professional Environment," APU Intelligence Blog, 4/30/2021, https://www.apu.apus.edu/area-of-study/intelligence/resources/private-sector-intelligence-a-developing-professional-environment/



PROTECT

DRIVE REVENUE

LOSS PREVENTION INVESTIGATIONS

REPUTATION MANAGEMENT

CORPORATE SECURITY

CYBER SECURITY

CORPORATE INVESTIGATIONS

FINANCE

SUPPLY CHAIN

SUSTAINABILITY

HUMAN RESOURCES

REAL ESTATE

RISK MANAGEMENT

SOURCING

INNOVATION

COMPETITIVE INTELLIGENCE

ECOMMERCE

MEDIA NETWORK

M&A

Lack of Uniformity

Because private sector intelligence is a relatively new field, it hasn't yet developed all the characteristics of a true profession, one of which is a shared identity with common terminology.[3] This presents some specific challenges.

For one, finding the right place to seat it in any given organization can be a trial.

In a survey of 94 private sector intelligence professionals, Maria Robson Morrow, Program Coordinator of the Intelligence Project at the Harvard Kennedy School's Belfer Center, asked where intelligence roles were situated in the corporate organizational chart.

Twenty-four percent were in Security or under the CSO, 18% in Legal, 16% under Operations, 10% in HR, 9% under the CIO or in Information Security, 5% in Finance, 2% each in Facilities, Supply Chain, Technical Services. A further 13% were in other business units not listed.[4]

Again, it's important to point back to the broad scope of private sector intelligence. Roles that focus primarily on one subcategory of intelligence will likely be situated accordingly. Those who manage primarily cyber intelligence may report through the CIO, while those who deal with market intelligence report through Legal or Finance, and protective intelligence analysts are seated in Corporate Security.

The titles of private sector intelligence roles also vary vastly between organizations and within industries.

[3] Morrow, "Private sector intelligence: on the long path of professionalization"

[4] Kolbe and Morrow, "How Corporate Intelligence Teams Help Businesses Manage Risk," Harvard Business Review, 01/04/2022

This is exemplified in another survey by Dr. Maria Robson Morrow, this one from 2019. It began by asking the job titles of the respondents, all of whom worked in private sector intelligence. There were 99 different answers across 126 responses. Sixty-four percent of the reported titles included the word "intelligence," but beyond that, there was little uniformity.[5]

The inconsistency in titling poses a challenge for organizations looking to hire analysts – since candidates won't always know which titles to apply for or where they may sit in a hierarchy - and for those looking to benchmark their existing programs – since it will be difficult to find adequate comparisons by title.

Despite the lack of uniformity in the profession, there are commonalities when it comes to the jobs themselves. Private-sector intelligence professionals are expected to have a fairly standard set of competencies to perform certain accepted responsibilities.

The SEC gathered job postings for titles across the spectrum of private sector intelligence analysis titles and looked for commonalities in responsibilities and required skills.

Risk Intelligence Job Titles

The Association of International Risk Intelligence Professionals lists the following examples of member job titles:

Director, Intelligence/Threat Intelligence/Intelligence & Analysis

Global Security Intelligence Analyst/ Manager

Program Manager - Protective Intelligence

Senior Manager, Risk Intelligence

Intelligence & Threat Analysis Manager

Intelligence Analyst/Lead Intelligence Analyst

Strategic Security Advisor

Common Required Skills

- Proficiency in OSINT tools (eg, Brandwatch, Liferaft, Skopenow, Flashpoint, CLEAR, LexisNexis)
- Knowledge of statistical programming languages (eg, R, Python, Scala, Java, C++) and database query languages (eg, SQL, Hive, Pig)
- Experience with data visualization/business intelligence tools (eg, matplotlib, ggplot, d3.js, Tableau, Power BI)
- Knowledge of the intelligence cycle, including analytic methodologies and techniques
- Research and intelligence gathering skills
- Strong algebraic and statistical skills

[5] Ibid.

- Project management skills
- Expertise in predictive analysis and threat assessments
- Ability to quickly and effectively synthesize and summarize large amounts of information from multiple sources into concise, analytic assessments
- Excellent oral communication
- Excellent written communication
- Excellent presentation skills
- Ability to prepare graphs, charts, tables, maps, and other illustrative devices from collected data
- Critical thinking
- Problem-solving aptitude
- Consistent track record of working with cross-functional teams

Common Responsibilities

- Identify information and intelligence needs
- Conduct research
- Develop methodologies for tracking, assessing, and scoring country-level risk conditions
- Compile and evaluate intelligence products from local, national, and international sources
- Identify subject matter experts and develop relationships for intelligence sharing
- Maintain and update databases
- Process, cleanse, and validate the integrity of data
- Analyze multi-faceted data to show processes, trends, and patterns
- Develop and deliver high-quality written products and oral intelligence briefings
- Present information using data visualization techniques
- Protect and maintain sensitive and confidential information

What the SEC is Doing

The Security Executive Council is working to help security leaders leverage the many security and business benefits of private-sector intelligence while helping to build up the community of intelligence professionals who will serve them.

As part of the internship program started with Mercyhurst University's Ridge College of Intelligence Studies and Applied Sciences in 2021, the SEC has placed more than 120 Mercyhurst interns with security leader clients to provide data analysis and intelligence as well as research and other projects.

In addition, this month will mark the grand opening of the Business Information & Innovation Lab at Mercyhurst University. This joint project will create intelligence research and products for corporate security leaders to use to inform their mitigation decisions and to advise their senior executives.

Contact us for information.

Visit the Security Executive Council web site to view more resources in the Program Best Practices : Intelligence & Analysis series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com