THE FLYNT GROUP INC.

ACTIONABLE KNOWLEDGE ®

Random Ripples: Seeing Below the Waterline

Building a Corporate Intelligence Unit

THE FLYNT GROUP INC.
ACTIONABLE KNOWLEDGE®

PO BOX 20111
KANSAS CITY, MO USA 64195
877.FLYNTGP (359.6847)
INFO@FLYNTGROUP.COM
WWW.FLYNTGROUP.COM

Flynt Group White Paper
Building a Corporate Intelligence Unit

Corporations require timely, accurate information to maintain a competitive edge. Major firms have assessed their information processes for relevance in the 21st century, and consequently are adopting quasi-governmental approaches and advanced analytical technologies and techniques to gain advantage over competitors, protect their knowledge, and expand market share. Past corporate security models, while exercising capabilities that remain necessary and useful, are no longer sufficient to maintain pace. Traditional functions, such as loss prevention and investigations, have been radically changed and new functions like computer forensics and geo-political analysis of events impacting global supply chains are essential.

Globalization and the ascent of the virtual world in the competitive space are disruptive changes. They increasingly render obsolete traditional corporate security departments modeled as civilian versions of law enforcement, focused primarily on physical access and investigations. The leading corporate security departments of ultra-competitive global brands possess a highly sophisticated intelligence capability consistently apprising their senior executive team of developments impacting the firm's interests and bottom line across a spectrum of diplomatic, informational, military, economic, political and other dimensions.

Building a corporate intelligence unit to meet the challenge of competitors and a 21st century business environment requires three tracks: attracting suitable talent with the requisite knowledge and skills; training and resourcing the necessary technologies and techniques; and leading an initiative to integrate new functions and processes in the organization.

Flynt Group's mission is to equip our clients with *Actionable Knowledge*® to wisely manage their risk positions and achieve their goals across a broad spectrum of hazards and threats. Should we be able to provide any further information, please contact us at 816.243.0044, or via email at Info@FlyntGroup.com.

Sincerely,

Bill Flynt

Bill Flynt, Ph.D., LTC (R)
President
The Flynt Group, Inc.
"Actionable Knowledge"®

Introduction

Corporations require timely, accurate information to maintain a competitive edge. Firms are assessing the effectiveness of their information processes, and adopting quasi-governmental approaches and advanced technologies to gain advantage over competitors.

Intelligence analysis is essential to supporting enterprise objectives and protecting employees, assets, operations, and market share. An effective corporate intelligence unit reduces corporate risk, enhances the quality of executive decision, and can financially return on investment.

Global brands have a sophisticated intelligence function. This analytical cell conducting the corporate intelligence function benefits the entire enterprise, from equipping the Chief Security Officer (CSO) with *Actionable Knowledge*® to inform the CEO and Board of critical developments, to conducting due diligence and market research preceding a significant expansion into foreign markets or a large acquisition. Intelligence enables the identification of both opportunities and risks, and is an essential input to a credible Enterprise Risk Management (ERM) program.

Most mid-to-large corporations have an analytical capability in their corporate security function. However, Flynt Group has found that, in some cases, the department's functions are tasked with narrowly-scoped technical analysis (e.g., appropriate use monitoring of computer networks) or traditional, quasi law enforcement functions (e.g., access control analysis, investigations) with visibility at the lower management levels of the firm. Although these functions are necessary and useful, they are not a complete answer addressing the needs of a major corporate brand requiring strategic decisions at Internet speed—globally.

Executive decisions of strategic consequence require what Flynt Group titles *Actionable Knowledge;*® a comprehensively informed, full spectrum understanding of the context and variables surrounding a decision, and the explicit, ordered actions required to pragmatically achieve the corporation's objectives. Flynt Group's mission is to equip our clients with *Actionable Knowledge*® to wisely manage their risk positions and achieve their goals across a broad spectrum of hazards and threats.

Intelligence analysis is an essential, strategic business function of major corporations. Any significant course of action considered by a corporation's C-suite and Board should integrate intelligence analysis into the decision making process.

Mission, Goals, and Objectives

The mission of a corporate intelligence unit is to provide timely, accurate, and quality analyses informing executive decision and action in support of the firm's mission, goals, and objectives.

The role of a corporate intelligence unit is to reduce risk, increase the probability of success of initiatives, and to protect personnel, assets, operations, knowledge, and interests. Trained analysts equipped with appropriate technologies and techniques are critical to accomplishing the mission.

Based on the mission, goals should be established for the analysis unit. The goals may be communicated as statements, including:

- To support the investigative efforts of the corporate security department through the provision of analysis and products for cases;
- To support the intelligence needs of the firm through the analysis of data gathered, completion of assessments, provision of knowledge products, and other activities;
- To support the safe travel of our firm's employees, domestically and abroad, through the provision of detailed, accurate travel safety briefings and timely information regarding their destinations; and,
- To inform executive decision and action regarding corporate plans, initiatives, and interests.

Based on those goals, objectives should then be developed that state specific metrics (e.g., number and types of cases supported) or knowledge products (e.g., special executive research reports) to be published yearly by the unit. Performance criteria can include: number of knowledge products produced, timeliness of support, avoided costs, return on investment, internal client satisfaction with services and products, and other measures.

Delivering timely, quality analysis that executive decision makers find useful is the corporate intelligence unit's mission-critical task.

Executive Critical Intelligence Requirements (ECIR)

Information is not intelligence. Rather, intelligence is synthesized from information through analysis. Analysis adds value by deriving the meaning and significance of information and transforming it into intelligence.

Without executive guidance to focus corporate intelligence efforts, analysis and the corresponding intelligence produced may not be relevant. The standard is for analysis to be relevant to executive decision and action. Simply providing executives with information is not acceptable, and only adds to the flood of information they must process daily. The standard that corporate executives require be met is that intelligence equips them with *Actionable Knowledge.*®

An essential tool for corporate intelligence analysts is the ECIR list. This is a current list of the C-suite's and Board's knowledge requirements, general or specific, to make decisions and take actions furthering the firm's interests. Their knowledge requirements drive the corporate intelligence effort.

Based on ECIR, the intelligence staff develops a collection plan to answer more specific questions they develop, known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the C-suite and Board).

Without a direct support relationship and clear communications between the executives and the intelligence staff, producing intelligence that is relevant and benefits the firm is problematic. Therefore, the CSO provides the essential interface between the executives and the intelligence staff.

Staffing

A major corporation "typically" has a mid-level manager leading the intelligence unit, as a direct report to the CSO, and supervising from three to 12 analysts. Ideally, the unit manager should be an experienced analyst. The intelligence unit personnel should comprise a mix of experience, including military service, intelligence agency service, federal law enforcement, and technical / trade specialists (e.g., cyber security analysts, statisticians, researchers, journalists). Ideally, all intelligence personnel should be college graduates (four-year degrees), and a significant number should have professional credentials and advanced degrees.

Key skills and traits for analysts include: excellent research and writing skills; advanced computer and application literacy; creativity; ability to work independently; logical thought processes; persistence; attention to detail; willingness to make judgments; and, visualization skills.

Analysts need to have a disciplined work ethic and able to work a task through completion without repeated guidance. They must be able to craft a sophisticated research plan / line of investigative inquiry, and identify and obtain information resources that will assist the investigation or study.

The analysts may be specialists in knowledge domains due to their past experience or training. Some may focus on financial, criminal, or technical protective analysis (e.g., executive travel support). Alternatively, their focus may be geographically defined (e.g., Colombia), industry defined (e.g., international shipping), or target a specific group (e.g., foreign competitors stealing Intellectual Property).

The analytic unit should have adequate administrative support. One of the most time-consuming tasks within the analysis function is obtaining and manipulating data. Where appropriate, administrative support enables a more efficient use of intelligence analysts.

A corporate intelligence unit may also benefit from the judicious use of select interns recruited from universities. This is a cost-effective approach to obtaining hard science skills (e.g., computer security, statistical analysis) while assessing for future recruitment an acceptable pool of potential team members.

During the analyst recruitment process, Flynt Group strongly advises an evaluation process that corroborates capabilities, skills, and performance. CSOs should consider subjecting candidates for an intelligence analyst position to a reading test that ranks their speed, comprehension, and proficiency level; a writing test that entails addressing a complex issue and providing detailed recommendations for resolution; personality tests to assess an individual's organizational fit; logical reasoning tests; and, extensive background investigations.

Diversity in analytical expertise and focus should be a conscious recruiting goal in the unit. This broadening of the analysts' skills inventory can also be enhanced through training and assigning analysts special research projects that develop their domain knowledge.

Procedures

The unit should operate according to a formal, defined methodology of information collection, collation, evaluation, storage, analysis and dissemination. The business processes supporting the intelligence unit's work flow should follow the classic intelligence cycle of: Planning and Direction, Collection, Processing, Analysis and Production, and Dissemination.

Figure 1: Intelligence Cycle

Written procedures should be developed to guide operations, and vetted with intelligence professionals. The rigor and explicit detail of the processes should be clarified through comprehensive mapped process diagrams, which include inputs, work flows, production outputs, timelines, and metrics. For operational security, authorized distribution lists for sensitive knowledge products must be explicit and unequivocal.

For information collection, clear standards should refer to the need for legal acquisition of data and the evaluation of data as to its reliability and validity. For example, data must be collected in accordance with applicable state and federal laws and regulations. This is not a trivial point, and entails collaboration with General Counsel for vetting and approval of the collection and storage processes.

Training

Analysts should have as broad a range of training as possible. Ideally, this should include training in the intelligence function, internal procedures, corporate business processes and operations (e.g., supply chain, production, shipping, competitors, etc.), software applications used, and multiple intelligence disciplines.

Initial training requirements can be reduced by selective recruitment of military, government, or federal law enforcement analysts. Training must be a regular element of maintaining analysts' skills, additional professional development, and expansion of the intelligence unit's capabilities. Also, analysts should receive basic investigative training including collection methods, evidence handling procedures, corporate investigative protocols, interview methods, and court preparation. To enhance the effectiveness of the unit's training program, each junior analyst should be paired with a senior analyst to establish a Mentor-Protégé training relationship.

Training should be provided to everyone in the intelligence unit, including its senior management levels. This will instruct the investigators and managers to request and interpret analytic projects, as well as to evaluate them knowledgeably. Some orientation level of training should also be given to the managers of other departments to enhance their understanding of the unit's capabilities and provide an opportunity for customer feedback. Finally, the C-suite and Board should be briefed on the unit's capabilities to clearly demonstrate the intelligence unit's contributions to the corporation.

Conclusion

This White Paper has addressed select aspects of building a corporate intelligence and analytic capability. The task, of course, is not trivial and involves time and resources. However, the path forward is clear. The CSO must: attract suitable talent with the requisite knowledge and skills; train and resource the necessary technologies and techniques; and, lead a change management initiative to integrate the new operational functions and processes into the organization.

While the staffing and training tracks addressed above are the most straightforward to accomplish; the change management required to integrate the new functions and processes can be challenging in a large enterprise, and will demand focus and hard work from the entire corporate security team. However, as the CSO shepherds this initiative, the rewards of a solid corporate intelligence program will become evident throughout the enterprise as the newly-founded intelligence team contributes to reducing risk, increasing the probability of success of initiatives, and informs the protection of personnel, assets, operations, knowledge, and interests.