



“ Jet Liner Goes Down”

“ Labor Strike in France”

“Underground Explosion in San Francisco”

These headlines are examples of what we read, watch, or hear through open media sources. For some people and organizations, these incidents may directly impact their business process or livelihoods requiring them to act (intelligence), and for others these headlines are considered simple news items.

A common problem facing many senior security managers is the feeling of being overwhelmed with the constant influx of information via the Internet, broadcast media, the corporate intranet, and co-workers. There is also the unspoken added pressure the chief security officer puts on him or herself to be the guy or gal who is expected to know everything that is happening anywhere in the world at any given time. Unfortunately, some managers, fall into a trap of subscribing to every conceivable security oriented e-mail list possible, with the hope of finding something “actionable”. Casting a wide net in the hope of catching a single nugget of actionable intelligence will tax corporate or organizational resources, demand many hours of analysis, and clog up the security department’s communication infrastructure.

How does one actually assess what it is considered intelligence and what is non-essential news to that organization’s business continuity or security? How does one navigate through a plethora of information sources? The answers to these questions and other’s can be found by understanding how to manage the intelligence process. Valuable time, money and even reputations can be saved by knowing what the intelligence needs of an organization are first and then designing a plan to capture the intelligence.

The Intelligence Process

Intelligence like the security apparatus can be applied on the macro level (*strategic*) or on the micro level (*tactical*). Dependent on the situation on hand, a *strategic* intelligence plan has goals that will enable corporate or organizational decision makers to take appropriate action in order to grow the company, i.e. business intelligence and to ensure long term business continuity. Strategic intelligence as applied to business normally falls under the responsibility of the business development or sales and marketing divisions. The security department is often tasked with developing a *tactical* intelligence plan geared toward situations or scenarios where more immediate action is needed to protect the organization’s assets. In some global business circles a *tactical* intelligence plan is carried out to limit the advantage of a competitor or adversary.

To manage an intelligence plan, whether strategic or tactical, one should establish a consistent process to ensure that decision makers are getting the right information at the right time. There are certain innate phases of intelligence that when harnessed and used correctly help managers leverage corporate or organizational resources to either promote or protect the company or organization.

Phases of an Intelligence Plan:

1. Defining the Intelligence Requirement(s) – information needed to determine actions
2. The Collection Plan – how the intelligence will be gathered



3. Analysis – understanding what the intelligence means and its criticality to the organization
4. Dissemination – delivering the right intelligence to the right people at the right time

Phase I - Intelligence Requirements Defined

The first step in managing intelligence is to first identify what the Intelligence Requirement(s) (IR) that are needed so a decision or action can be executed by management. IRs can be strategic in nature or tactical but the intelligence process is the same. It is important to distinguish that IRs will differ from department to department even within the same organization. For example, in a corporation, the sales and marketing division will have Business Intelligence Requirements that will direct actions to help the organization grow and the security department will have IRs for the purpose of protecting the company. For our purposes we will focus on the latter.

The IRs are generally comprised of a number of questions as it applies to a given situation(s). The questions usually start with “*who, what, when, where, how, and why.*” A potential scenario that will spawn IRs:

A large commercial development company in South San Francisco has received menacing phone calls from anonymous callers; pamphlets calling for the developer to stop building have littered the jobsite, and corporate executives have had the tires of their cars slashed.

IRs: Who are on record of opposing this development project? What is their motive in disrupting company operations? When do threatening calls, graffiti, or other nuisance crimes occur? Where do groups with grievances against the company congregate? How does this person or group fund their operations? Why is this activity happening now?

The IRs give the security executive a game plan so he or she can dedicate the appropriate resources to acquire the needed intelligence.

Phase II: Collection Plan

Once the IRs have been generated and evaluated for criticality, the next step is designing a collection plan. The collection plan will identify the methods, means, and assets needed to acquire the desired intelligence. Possibly much intelligence can be gathered via open source intelligence OSINT (internet, print, and broadcast news sources) or through human sources (HUMINT). Examples of human sources could be local law enforcement, journalists, subject matter experts, or even a person that can infiltrate an organization and report real time intelligence developments back to his or her handler. Other intelligence may need to be collected through technical means. Video surveillance, a derivative of photo intelligence (PHOTINT) generally considered a tool for deterrence, has the ability of capturing images and giving descriptions of individuals or vehicles near or in a company’s property. Electronic Intelligence (ELINT), listening devices; has long been a valuable method to gain intelligence but legally is questionable. IT networks and databases can of course be targeted in order to find a treasure trove of intelligence, though this method isn’t advocated for legal reasons within the private sector.



Embedded into the collection plan are timelines for when the selected intelligence is needed by decision makers to act. Also of paramount importance is the need to define how the collected intelligence will be communicated back to the security or project manager. Some means of communication can be overt others may need to be covert to protect the source of the intelligence. A third necessity is creating due diligence procedures to ensure that the intelligence collected is accurate. Sources of intelligence must be vetted to ensure that the collector of the intelligence is not receiving misinformation or forwarding rumors onward to analysts.

By knowing how to develop and manage an intelligence plan, security and business executives will be empowered to control the flow of information and not have information control them.

Stay tuned for PART II in a future issue that will cover Analysis and Dissemination.