



In the previous newsletter, the article “Understanding Intelligence Management” introduced the reader to the essentials of the intelligence process. By formulating an intelligence plan, organizations can be pro active in terms of business development, company resiliency, and security management. Identified in the piece, were the four phases of an intelligence plan:

1. The Intelligence Requirement(s) (IR) – 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

Whereas the previous article focused more closely on the first two phases, this article will highlight the latter two phases.

Phase III: Analysis

After an organization receives intelligence from a network of sources, the raw data has to be analyzed to assess its criticality to a particular project or to the organization as a whole. The foundation for effective intelligence analysis should be dictated by the nature and scope of the initial Intelligence Requirements. The IRs focus on the “who, what, where, why, when, and how” of certain events and situations. If an intelligence requirement calls for a list on known organized criminal gangs operating in a specific area, the organization should then hire a subject matter expert who has the skills and experience to analyze the list and determine which gangs possess a bigger threat to the organization than others. The more data collected during the intelligence collection phase; the more subject matter experts, intelligence databases, and reporting tools will need to be utilized by the organization to direct the decisions of policymakers. Often during the course of analysis, a request for more intelligence data is needed requiring a new intelligence collection plan.

The scope of the analysis of intelligence itself is essential to the success of the entire intelligence plan. Too narrow an analytical review of collected intelligence can cause an organization to be further victimized, vulnerable, or worse; to act on information with out understanding the full picture. Using the example from above, if a security department enacts protective measures for an organization based on just having a list of local criminal gangs without assessing the capabilities of each gang, it is quite possible that valuable resources may be lost due to over committing security efforts in certain programs and under committing security initiatives in other areas. Conversely, too wide an analytical review of intelligence can lead to a waste of time, money, and resources. Just as many organizations that have fallen prey to under analyzing intelligence data, have also have over analyzed data to the point where the time for making a decision or an action has passed; the quintessential “paralysis by analysis”.

The scope of the analysis of intelligence itself is essential to the success of the entire intelligence plan. Too narrow an analytical review of collected intelligence can cause an organization to be further victimized, vulnerable, or worse; to act on information with out understanding the full picture. Using the example from above, if a security department enacts protective measures for an organization based on just having a list of local criminal gangs without assessing the capabilities of each gang, it is quite possible that valuable resources may be lost due to over committing security efforts in certain programs and under committing security initiatives in other areas. Conversely, too wide an analytical review of intelligence can lead to a waste of time,



money, and resources. Just as many organizations that have fallen prey to under analyzing intelligence data, have also have over analyzed data to the point where the time for making a decision or an action has passed; the quintessential “paralysis by analysis”.

Phase IV: Dissemination

Once the intelligence has been reviewed, assessed, and edited by the analysts, the finished product has to be delivered to the key stake holders within an appropriate time frame so they can make an informed decision or action. Critical in the success of disseminating the analysis is the level of security applied to the delivery of the information. If an intelligence report includes a vulnerability assessment of current organizational protective or emergency response measures, not everyone in the organization need to be aware of the report’s existence.

Tactical intelligence reports generally have a shorter incubation process than strategic intelligence assessments, but in either case, a key to successfully disseminating the information is to limit the number of authorized viewers of the report. Circulating a specific intelligence assessment to a broad number of people can lead to leaked information and inhibit needed decisions or actions by the specific stake holders.

“Protective Intelligence” is a term used to identify information or activities, which if exposed to the wrong people or even the right people at the wrong time, could cause harm to an organization’s physical tangible assets as well as its intangible assets such as growth potential and reputation. Some common sense protective actions to ensure safe delivery of the intelligence product via digital means are: high encryption programs, plus multi-layers of firewall protection for the organization’s computer networks, and a high discriminatory ID verification process for the sender and receiver of the intelligence report. Hard copy reports should also embed a high level of security when being delivered and stored. A basic tenet to live by regarding digital or hard copy intelligence reports or files, “Don’t give the file or report a name associated with its contents.”

In summary, the intelligence process should operate like a fine tuned machine. By clearly identifying the needed intelligence, means of collection, depth of analysis, and methods of dissemination, organizations will improve their chances for growth, be able to respond to dynamic events or circumstances locally and globally, and offer a safe and secure working environment.