INTELLIGENCE

SETTING UP AN INTELLIGENCE HUB

Introduction

Intelligence in some form is in use today across a broad spectrum. No longer just the purview of Government entities, business intelligence is a common term and practice amongst corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic or person. The immense growth of social networking in the last few years has added to a rich information bank that is readily accessible to anyone with an internet connection. The challenge today is to sift through immense quantities of information to uncover and piece together the information you require into an intelligence picture that supports your operations. The value of your own information can increase exponentially when combined with open source research and other entities with whom you are willing to share some information.

Why Have an Intelligence Hub?

An intelligence hub is a central repository for intelligence gleaned from different entities. These entities can be different departments within one entity or they can be a co-operative venture between different entities. Before setting up an intelligence hub it is essential to ask the question why? The answer to this question will help determine the purpose of your intelligence hub. An intelligence hub without a clearly defined purpose will generate lots of activity and few results. An intelligence hub can be created to fill a singular need, such as sharing information about a single cross-jurisdictional investigation or to address a multitude of related issues such as sharing threat information and lessons learned about a country or region where co-operating entities are operating. Once you have determined the need and purpose it is important to follow a structured process to ensure your hub meets the purpose for which it was created.

Setting up an Intelligence Hub

Identify the Participants

Who are the participants that should be included? As an example, the borderless nature of crime and terrorism has seen many intelligence hubs or fusion centres created to allow law enforcement and intelligence agencies to share information in support of a common goal. There must be trust and common ground between the participants. Ideally, each participant will have information to contribute and something to gain through their participation.

Agree on Governance

A board of directors or steering committee from each participating organization should be formed to agree on how the hub will be governed and to strategically direct the activities of the intelligence hub. Crucial to success is determining what information will be shared and what will not be shared. Corporations in particular have valid concerns about proprietary information that must be protected. Determining up front what information will go into the hub and how it will be shared will make sure that expectations are clear from the start. Once the information is in the hub how will it be protected? What level of security do you need to meet all participants' risk tolerance level? Once the hub is up and running how will decisions on priority and activity be made and by whom? Ideally Directors should be committed enough to attend steering meetings and senior enough that they can make decisions on behalf of their organization.

Set Primary Intelligence Requirements

Once the participants are chosen and the governance has been set it is time to set the primary intelligence requirements. These are the main topics that the participants agree should be the focus of the intelligence hub's efforts. Primary intelligence requirements should be reviewed continually and updated regularly to ensure that they are still meeting the needs of the participants. Normally these topics will be areas where a gap exists in information required by the participants to enable their operations.

Create a Collection Plan

Once the requirements are defined a formal collection plan should be developed to determine sources of information available to meet the requirements and how to obtain information from these sources. There are many legitimate source of information that, combined with the information the participants already have, can provide valuable intelligence that can mitigate threats, improve operations keep employees safe. Potential sources include Government agencies, open source searches, and interviews of knowledgeable persons or partner companies. A formal collection plan will keep activity focused toward results that flow from the primary intelligence requirements. It will ensure time is not wasted on broad and general fishing expeditions and instead focused on what is vital to the participating organizations.

Create and Maintain an Analysis Capability

Get the tools and training required to analyze your intelligence. Depending on the volume and complexity of your intelligence needs this may range from rudimentary training and systems to complex training and technical tools. There are excellent tools to assist in analyzing vast quantities of information to produce focused intelligence. A common mistake; however, is to purchase tools such as intelligence software without establishing the framework for your

intelligence hub. Properly used tools are powerful enablers but without strategy they have nothing to enable. Your intelligence framework and products required will dictate the extent and complexity of the tools and training you will need.

Dissemination

Intelligence that is not distributed outside the Hub to people who will use it is of no value. What products are expected to meet the needs of the participating organizations? Products can range from simple briefings and written updates to complex reports with link analysis diagrams that show the reader important links amongst vast quantities of information. How often will they be distributed and who specifically will get them? Briefings on time sensitive information may be required immediately whereas monthly reports may be sufficient for longer term issues.

Feedback

Continued success of an intelligence hub requires a feedback system to make sure that the intelligence program is continually focused on the needs of participating organizations. Are the primary intelligence requirements up to date? Are the products useful and timely? Are changes required? In addition to these questions communicating success stories resulting from the intelligence hub's efforts reinforces the value of the hub and the efforts of those doing the analysis.

Intelligence, like any other activity provides best value within a strategically planned framework linked to the needs of the organizations it supports. The quantity of information available through open sources today requires a formal approach to sift through it and identify what is important. Linkages between pieces of information held by different entities can increase the value of one's own information immensely. An intelligence hub concept offers immense value to partners willing to share with each other and that take the time to build an agreement and intelligence strategy that will meet their needs.

About the Author

Stephen MOORE

Stephen Moore is a police, security and emergency management professional with over thirty years of experience. He has worked with all levels of Government and with police and security agencies both domestically and internationally. Highlights of his career include leadership of the security program for the Department of National Defence and service as the Canadian Forces Provost Marshal (Chief of the Military Police) leading an organization of 2000 members delivering policing, security and criminal intelligence services both in Canada and abroad. Stephen is currently the President of Presidia Security Consulting.

Additional Articles from Presidia Security[1]

Ask the Question – What is Your Security Strategy?

Security is often thought of as a tactical issue that should remain at the "gates and guards" level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company's "C Suite" and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

Assessing and Tracking Threats - Protecting Your Employees and Your Company

Recent incidents of violence in the workplace in Canada tragically illustrate what happens when threats materialize into actions; they serve as a stark reminder to businesses across the country of their responsibility to protect their employees in the spirit of "due diligence" and "due care and attention." Rarely, if ever, do these violent situations manifest themselves without some sort of prior indicators. This underscores the importance of having proper procedures in place to track and assess threats to your employees. Take the time to review the following recommendations to determine whether your company is prepared to address threats to employees.

Executive Protection Considerations

In today's fiscally challenged business environment it may be difficult to justify providing an Executive Protection Program for an organization's key executives. However, in making this important decision one also has to consider what the cost would be to the organization's bottom line and, perhaps more importantly, to its reputation should a key member of the senior leadership team be the target of an act aimed at harming or embarrassing the individual and the organization.

Due Diligence Investigations

If asked, many companies would say that they have "due diligence investigation" processes in place; however, these processes are often designed to review the financial and operational affairs of a particular company and fail to closely inspect the background of the main principals or executives of the company. In addition, many companies do nothing more than cursory checks on individuals they are about to hire. The lack of a robust background investigation can result in wasted time and can cause legal and financial problems. There is an abundance of legal findings across Canada, as well as internationally, that clearly articulate the liability facing companies who do not carry out appropriate due diligence investigations. In order to inspect this issue closer one must first begin with a definition and understanding of what "due diligence" consists of.

[1] Available online at our website: www.presidiasecurity.com/library.html

Take a Moment to Celebrate Success

Take a moment today to think about the successes you have had and the team that got you there. It is well worth it.

A Solid Foundation for Administrative Investigations

"Is it time for the implementation of standards, including proper training and oversight, as it pertains to the conduct of "administrative investigations"? It could be argued that administrative investigations are purely "administrative" in nature and as such there is no requirement for an enhanced capability. However, it can also just as easily be argued that these types of investigations can have a very negative impact on the lives of those being investigated, including the potential loss of their livelihood. They also bring with them a large degree of "personal and institutional liability" on the part of those individuals conducting the investigations and the" "organizations for which they are employed."

Marine Port Security - Published in FrontLine Magazine

"Since 9/11, marine port security has been the subject of increased scrutiny as it is clear that contraband flows - undetected and uninterrupted - through access and egress points of both Canada and the United States. Numerous reviews initiated by the United States Government Accountability Office (GAO) and the Canadian Standing Senate Committee on National Security and Defence have clearly articulated that ports are a haven for criminal activity and organized crime, as well as targets for potential terrorist activity. Both these reviews demand an increase in the level of intelligence sharing among partner agencies focused on policing and security of marine port operations."

Security Policy

"Policy writing: next to cleaning the coffee break area, doing personnel assessments or wrestling a hungry grizzly bear, it is probably one of the least desirable tasks in any organization. Its mere mention can send employees scrambling over desks and seeking cover in the hopes of being spared the mind---numbing drudgery of documenting the company's rules, procedures and practices. There is a good reason for this: writing is hard work – and writing clearly, concisely and meaningfully is even harder still. When it comes to communicating an effective security policy, capturing that policy on paper (or, in today's digital environment, electronically) is only the first – albeit most critical – step. Disseminating the policy and ensuring compliance are close second and third priorities, followed by periodic reviews to ensure the aforementioned policy continues to meet your organization's requirements. "

Travel Security

"Media reports continue to include stories about company executives, oil field workers and regular travelers who have been the victims of kidnappings, armed robberies and murder while visiting foreign countries. Recent events have seen a Canadian woman kidnapped in northern Nigeria and her captors demanding $136,000 for her release. This woman was a financial advisor who was in Nigeria with other Canadians as part of an exchange program and she was kidnapped as she was entering a house after attending a social event. There are also ongoing reports of oil workers being kidnapped by rebels in South

America and Africa; it would appear that these types of incidents are increasing rather becoming a thing of the past. "

Duty of Care

"The dynamic threat environment that persists in today's business climate demand constant vigilance and discipline. Under the Canadian Criminal Code, companies owe a duty of care to their employees. This means businesses must take "reasonable steps" to protect workers, whether they are in Canada or working internationally. If companies do not meet this duty of care, they can be found criminally and financially liable under the Criminal Code. In the most extreme cases, the company can face hefty fines and the executives can be prosecuted and potentially jailed. In addition to the criminal prosecution, individuals can also face personal civil litigation. "