ASSESSING & TRACKING THREATS

PROTECTING YOUR EMPLOYEES AND YOUR COMPANY

Introduction

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.

Define "threat"

A threat should trigger some form of action – whether it is simply documenting the incident in a security log or informing law enforcement authorities. Before getting there it is important to make sure that everyone understands what a "threat" is from the company perspective. While some threats - such as threats of death or serious bodily harm – are obvious to most people, others may be less apparent. Threats can be directed at disrupting business, individual employees, or different company departments (i.e., Human Resources), and can be verbal or written. Because everyone has a different tolerance level as to what constitutes a threat, it is important that the company makes it clear to all employees. Employees should be encouraged to err on the side of caution and to follow the airport security adage: "If you see [or hear] something, say something."

Define what is considered a "threat" from the company perspective to ensure that all employees understand when follow-on action must occur, regardless of whether or not they feel threatened.

Stipulate Employee Actions Following Receipt of a Threat

Once a threat that meets the company threshold is received the appropriate follow-on actions must be defined. In the face of an immediate and serious threat calling police is an obvious first step; however, it is important that all threats – whether they result in police being called or not – are also reported to the company management. Depending on the size of the company, this information would flow through the company security officer or the individual looking after contracted security. Details on reporting procedures should be clearly stipulated, including how

to file a report, the timeframe within which to report it and actions to be taken if a threat is received during non-business hours, to mention a few considerations.

Clearly stipulate to your employees those actions to be taken following receipt of a threat, including to whom, how, and when reports are be made.

Define Threat Assessment Procedures

Once a threat is reported and immediate actions (such as calling the police) have been taken, management must decide what additional actions, if any, are warranted. These might include enhancing the security posture, sending an advisory to all employees, or simply ensuring the threat is properly recorded using the 5 Ws (Who, What, When, Where, and How).

Following immediate actions required to safeguard your employees from imminent threats, management should review the threat to determine what, if any, further action is required.

Track Threats

All threats received by a company or its employees should be recorded and tracked. This will ensure that multiple threats that are received by different people or in different formats are not misinterpreted as a single event. It can also provide a record over time to assist law enforcement and/or company legal advisors in taking additional action, as required. A threat tracking system does not have to be complex or expensive. It should, however, be as detailed as possible and, at a minimum, should include the following information:

- Who received the threat
- When and where the threat was received
- The details of the threat – as accurately as possible describe what was said or how the information was received
- Details of the person or persons that initiated the threat
- All follow-on actions taken

All threats should be recorded and tracked as accurately as possible (use the 5Ws) to assist in follow on investigation and/or actions.

Review and Analyze Threats

Someone within the company should be assigned to review and analyze threats on a regular basis. All threats that are tracked and recorded as per above should be collated and reviewed to look for patterns, trends and or indications of escalation and, where concerns exist, law enforcement authorities should be consulted and company management informed. This responsibility will likely fall to the company security officer or security staff; however, accountability for ensuring this information is collated and acted upon, where appropriate, remains with management at all levels. Good communications will lead to good threat mitigation strategies and situational awareness throughout your company.

Threat information should be collated and analyzed and, where concerns exist, law enforcement authorities should be consulted and company management informed.

Conclusion

Assessing and tracking threats does not have to be an expensive and complicated endeavour. Of course, larger companies will necessarily require more resources to record, track and follow up on threats; however, with a good communications and intelligence plan, it is not overly difficult to put an effective threat assessment and tracking program in place. The recommendations provided above will help you make informed decisions protecting your employees and your business.

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.

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.

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.

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

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."

Setting up an Intelligence Hub - Published in FrontLine Magazine

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 among corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic, organization or person. The immense growth of social networking in recent 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 vast 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 information from other entities with whom you are willing to share.

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 travellers 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. "