Information Sharing Case Study—The 2010 Winter Olympics Model

by Mr. Doug Powell, CPP, PSP

Peer reviewed by Mr. Darren Nielsen, CPP, PCI, PSP; Mr. Scott Stephens, CPP; and Mr. Chris McColm, CPP

There are times in every security manager's career when crime-related issues require interface with law enforcement. In some sectors, regular interaction with police has led to cooperative programs that provide benefits to each participant organization. This is not true of intelligence and information sharing protocols as applied to critical infrastructure protection or national security, and certainly it is not applied equally across all CI sectors.

As this relates to critical infrastructure protection, especially since 9/11, the stakes have been raised by opportunity and necessity for information sharing to receive renewed focus. In some cases, federal and local agencies have purposefully committed budget and resources to working with industry partners to establish effective lines of communication. This has led to increased awareness about serious crime, terrorism and discreet information sharing in the forms of tips, shared intelligence and integrated briefings. This has been especially true where the public interest is best served through such cooperation as during an international event like an Olympic Games, a G8 or G20 world leaders' summit, and similar events.

As part of the ongoing battle against global terrorism it seems apparent that government and industry organizations are willing to reach out to one another for assistance and to work cooperatively over short periods of time. Over the long haul, however, this seems a more difficult proposition leading to program degradation and reduced sharing. This is a puzzle to many given what most would think is a win-win proposition for all stakeholders. Owner/operators with good information and intelligence can better target and prioritize protection planning. Federal agencies can benefit from a constant flow of industry incident reporting. The addition of industry reporting to intelligence community databases represents an enormous increase in "feet on the ground" as well as "eyes and ears" in every community looking for and reporting suspicious or criminal behavior. So why are such programs not sustainable?

This paper looks at a program that did work and a national protection program in Canada for the purpose of assessing such cooperation. This paper addresses cooperation in an environment where cooperation is necessary. With respect to sustaining information-sharing programs, perhaps necessity is understated in our daily operations, and common purpose requires greater emphasis as supported by more intentional funding efforts and membership support. Perhaps this will require greater incentive as offered by government. Whichever the case, the 2010 Winter Olympic Games provides a snapshot of a program that did work.

The Stakeholders

Key players in the 2010 Winter Olympic Games information sharing initiative included police from numerous jurisdictions as well as police support agencies; military; Emergency Management entities; industries representing the ten Canadian critical infrastructure sectors and foreign government agencies, as well as industry representatives from the U.S. and foreign protection details. During the Olympic Games period, only those organizations identified as primary contributors and infrastructure asset owner/operators were invited to confidential information-sharing sessions. The Integrated Security Unit, an RCMP-led security group made up of many different policing agencies, was the designated lead in the information-sharing initiative. Emergency Management British Columbia had lead in information gathering practices.

The Integrated Security Unit (ISU) for the 2010 Olympic Winter Games was in itself a complex group made up of many different agencies who needed to establish communication protocols, hierarchical relationships and confidentiality (need-to-know) restrictions. Public Safety Canada, a federal government ministry with accountability for national security and emergency management initiatives, was also operating under increased scrutiny following a 2009 report that made specific recommendations for improving Canada's national security posture.

All combined, interest was at its peak to see Canada's emergency management program advanced in light of the pending Olympic Games. New reporting and organizational structures were being planned and introduced as the Olympic Games preparations were carried out. Defaulting to a general belief that critical infrastructure owners/operators were capable of meeting protection standards for their own assets, the focus for the integrated security unit was to identify critical response issues in the event of a critical event. This was a reasonable assumption although it is safe to say that CI owners were not necessarily prepared to meet the elevated Olympic threat environment in every respect.

Objectives

The primary objective applied to information-sharing for the 2010 Games was to advance the aim of police, Olympic committees, and industry in protecting infrastructure so as to provide a safe operating environment for the 2010 Games. This included assurances that those living outside the Olympic operating theatre would not be adversely affected by any security incident that targeted the Olympic Games. Best efforts were made to identify critical infrastructure within the theatre of operations, to determine infrastructure interdependencies, and apply appropriate protection and support to this infrastructure for the duration of the Games operating.

The focus was on emergency response using prevention as a key driver to minimize the potential for adverse impacts on infrastructure. This also created governance challenges both in relation to collecting information from infrastructure owners/operators and in facilitating the distribution of all that information and intelligence to local infrastructure owners. While the ISU did its best to present a comprehensive and coordinated process for the collection and control of information, there was some misalignment between ISU members related to information handling process. Furthermore, this initiative was new and untested in Canada and had some important hurdles to overcome. These included mutual trust levels between industry, government and police, as well as confidentiality agreements, which related to collection, use, collation and deletion of the information being collected to the satisfac-

tion of infrastructure owners that their information was well-managed and protected. These concerns were overcome leading to new understandings, new programs and new relationships between industry and government, and established a new basis for information-sharing for critical infrastructure stakeholders in Canada. While this process is still not perfect three years after the 2010 Winter Olympic Games, advances have been made in terms of building trust, which far exceeds similar programs in other countries.

The Information Gap

Prior to the coordinated planning effort for the Olympic Games in Vancouver, Natural Resources Canada (NRCan) had already initiated a model for sharing some classified information as generated by police and intelligence agencies. Under agreement with approved industry representatives from the energy and utilities sector in Canada, industry representatives are cleared to "Secret" level under the same provisions as government employees and invited to attend classified briefings in the headquarters building of the Canadian Security Intelligence Service (CSIS). These sessions are always "pens down" with many restrictions applied to participation.

Within this secure environment, sensitive information can be shared by government agencies with industry partners who in turn can discuss confidential company and industry issues in this setting. This enables both sides to have a meaningful dialogue on national and regional security issues and develop trust relationships. The collaboration between police, intelligence agencies and industry partners extends to the sharing of risk information, threat trends, adversary capabilities and protection profiles. It has led to the development of other intelligence products like threat assessments and incident reporting on a national scale.

Within the context of preparation for the 2010 Olympic Games, however, many more players were involved who were not security cleared but wanted classified and sensitive information for purposes other than communicating threats and facilitating protection. Still, developing an effective emergency response capability on a regional basis was very important to the success of the Games, and having some information about critical infrastructure assets across numerous sectors was central to a program for prioritizing responses.

Framing the Problem

The problem in divulging information from industry's perspective was the potential to have information about its most sensitive asset and operational plans in the hands of government agencies whose best interests were to share and cross-reference this information which, potentially, could be inadvertently or purposely released into the public domain. Loss of control over information concerning critical infrastructure vulnerabilities and asset placement, especially when collated and stored in one place, would be a gold mine to any protest or extremist group. In an environment like the Olympic Games where global issues are often played out for the media with the Games as a backdrop, the release of any sensitive data seemed contrary to effective protection. This posture put the interests of industry in direct opposition to the interests of the emergency management and policing groups who were seeking information.

The central issue in this was trust. There was an apparent lack of trust that government agencies in any form were capable of effectively managing industry's deepest security secrets. The focus of this mistrust related to the government's ability to protect and control information provided to them. These concerns included the security of government servers, data protection on agency servers, information-sharing practices and permissions with other government groups and access to information by international partners within the Olympics' integrated security domain. There was a concern that diligence around data protection could become more casual or careless over time.

While critical infrastructure owners were working diligently to remove sensitive data from public sources, like the Internet of Things, it became apparent that an abundance of open source information about industry assets was already widely available. Much infrastructure plotting would have been relatively easy to do without industry's help. Industry assets already existed in government databases and printed materials from years past. It is true, however, that insider knowledge about these assets was necessary to understand the criticality of any such assets. And without detailed information about particular assets, it would have been very difficult to determine the interdependencies of particular infrastructure.

Applying protection to specific critical infrastructure was necessary to prevent the possibility of a more profound impact across multiple assets. For example, transportation of emergency personnel could become impossible if one particular bridge was removed. If that bridge was also carrying a main communications cable over water, it would have an impact on regional telephone systems. Once these asset nexus points were better understood, they were prioritized in terms of their importance for the Games' protection. Seeking industry's input was therefore vital.

The Solution

A three tiered sharing model was designed and implemented allowing industry stakeholders a choice as to how much information they wished to share about their assets. The three available options included:

1. Sharing limited information in a protected manner. In this option no assets were named but criticality (for asset "y", for example) and their relative special placement were provided.
2. A moderate disclosure option under which assets could be named and location provided but more sensitive vulnerabilities and criticality issues left off the record.
3. Full disclosure in which the entire record of the company was delivered and nothing held back.

In the first case, where assets were identified but not named, they were given a criticality ranking. An emergency response protocol existed which required that, following a major event the industry partner would be consulted to provide more information about an impacted asset so that coordinated decision-making would be possible with emergency personnel.

Before industry partners submitted their criticality rankings, a non-disclosure agreement (NDA) between the RCMP (lead organization of the Integrated Security Unit) and the industry entity was prepared and signed by each. Within the context of the NDA, the industry partner had the right to request removal of and deletion of all of their data, as supplied in the information transfer once the Games had concluded. This was done in a prioritized fashion. The ISU was required to delete and destroy all such data at the conclusion of the Olympic and Paralympic Games. The RCMP was then permitted to retain the data for approximately one year longer before it, too, was required to delete it. Ultimately, the industry information provided for Olympic Games emergency management and protection planning could not be retained by any government body or agency beyond the use of the span of the Olympic Games unless there was specific permission given by the industry partner who submitted it. This restriction included the retention of industry data in any derivative format using industry supplied data.

In 2009, industry partners began evaluating their infrastructure using an asset rating system supplied by Emergency Management BC to identify criticality rankings. That survey information was submitted to the RCMP for protected use. Accountability for all information supplied rested with the RCMP as lead. This information was not provided to any other agency without the permission of the industry entity who supplied it. A well-defined governance model was implemented to ensure full trust and full accountability. In addition, security clearances initiated by the ISU addressed personal reliability of participants. Nevertheless, note-taking and document distribution was at a bare minimum during meetings. Mandatory participant introductions at each subsequent meeting ensured full disclosure about who was in the room. Attendance became part of an official recordkeeping process.

Through this information-sharing model, some excellent collaborative work resulted. Asset mapping and nexus plotting not only served to inform the integrated security unit about critical infrastructure, but for the first time in British Columbia (perhaps Canada) asset owners began to understand and plot their own interdependencies and protection requirements. This is not true of all critical infrastructure owners, but it was certainly true of many if not most. In retrospect, this Olympic exercise moved emergency management and critical infrastructure protection years ahead. Were this model sustained, and many efforts have been made to emulate it, Canada would stand out as a world class example for emergency planning and national security.

Additional Spin-offs

The model described was comprehensive and very important to pre-Olympic planning efforts, but other information-sharing practices also seemed to spring forward, building on this process that demonstrated not only refined and intentional collaboration but served as an example as to what is possible in the right operating environment. As time passed and the ISU took shape and key personnel were identified, industry partners (especially those controlling the most critical infrastructure in the Olympic theatre) began to share information in one-to-one meetings and through defined work processes. This included providing police resources close up inspection of protected industry assets, the sharing of engineering documents and knowledge about industry protection plans.

In return, industry requested information from police and intelligence agencies to allow owner/operators plan protection based on accurate threat information. Industry partners also integrated police response and intelligence resources for security problems arising during the Olympic Games. The immediate handling and application of resources allocated to protecting industry assets resulted in an effective response plan that benefited the Olympic Games and the CI entity. Furthermore, all Olympic security reporting and briefs that were generated served to informed critical infrastructure owners across Canada about such threats and the threat agents, themselves.

The E-INSET Initiative

Of particular note, in the months leading up to the 2010 Olympic Winter Games was the outreach and work of the RCMP's E-INSET division (RCMP E-Division, Integrated National Security Enforcement Team). Specializing in outreach as a core function, E-INSET served the Olympic Games preparations in part by raising awareness around terrorist event planning. E-INSET developed training and awareness programs for first responders that increased the ability of first responders to identify and report suspicious activities that could be precursors to terrorist activity. This placed hundreds more eyes in the public domain that knew their local environment and trained in identifying abnormal behavior.

In addition, E-INSET partnered with British Columbia's primary electricity utility to prepare a training video that raised awareness about terrorism. The utility provided the video and associated awareness training to its front line employees who were operating within the Olympic theatre or who had a role in the delivery of electricity along critical pathways. Through the E-INSET produced video, employees gained perspective on the precursors to terrorist acts.

Developing this type of training for industry established another trust-level relationship. The training is applicable to everyone who works on the front line, and could easily have been made a part of the utility's standard awareness program for employees throughout the company. The E-INSET product provided the basis for training materials to be made available to other utilities and other industries everywhere in Canada. E-INSET served to create a new model of private-public cooperation as it is applied to policing and asset protection. It demonstrated that this level of cooperation not only assists both sides of the protection and response equation, but is essential in combating terrorism and serious crime. E-INSET, along with the other cooperation established within the Olympic operations environment, raised the bar for critical infrastructure protection.

Future Hurdles and Lessons Learned

Lessons learned from the Olympic Games protection program seem self-evident. The ability of disparate organizations to come together and build cooperative environments produced desired benefits. One would have expected the Olympic program to be a framework for information-sharing on a national basis going forward. Certainly, there were numerous security and emergency management professionals involved in the planning who spoke positively about the experience. Events like the Olympic Games, however, often have a life of their own, grown out of the excitement and energy (and funding) applied to events of this type. Lessons learned will not necessarily be applied more broadly as industry standards.

With respect to the energy sector in Canada, it is clear that Natural Resources Canada and the RCMP Critical Infrastructure Intelligence Team, Federal Policing Criminal Operations (and others) have come together to continue building on information sharing practices, intelligence products for industry, classified briefings, a national security incident reporting database and other essential protection programs. The recent introduction of a National Energy Infrastructure Test Centre (NEITC)—an Industrial Control Systems (ICS/SCADA) research laboratory and industry training facility—is one such initiative that will serve critical infrastructure protection objectives. However, without industry support, funding for any program like these will be placed in jeopardy. Funding of such programs is a two-sided (industry and government) or three-sided (add vendors) proposition.

National programs like the ones sponsored by NRCan and the RCMP may not be widely appreciated within by company executives, risk managers and others who make policy decisions regarding industry program support. Or, those who participate in such activities as classified briefings and other training and information products, may not appreciate how they contribute to a national protection plan. In fact, it may be that a regional stakeholder in any industry may see their role as isolated from the national picture and are unable to draw a direct, relevant connection between government initiative and local stakeholder protection requirements. Industry players do not necessarily perceive terrorism as a serious threat to their local operations. Whatever the case, there is an obvious gap.

All of this serves to make information-sharing and other forms of cooperation difficult to sustain. Federally sponsored initiatives require demonstrated

industry support. Low levels of stakeholder support may indicate the need for a strategic change to federal programs. Still, any program related to national security will require collaboration and information sharing between stakeholders, as well as some form of disclosure in a trusted environment. Over time, industry participation always seems to waver irrespective of program type, program initiator or program sponsor. Perhaps the main questions should be how to make programs self-sustaining and how to keep them "fresh" or relevant.

In the United States, we can look to programs like National Fusion Centers[1] and InfraGard[2] as key examples of government initiatives that serve as industry stakeholder and national security initiative related to information exchange. In fact, the view of this paper is not that significant effort and intentions have not been applied in the area of cooperation and information-sharing. Moreover, the view is to highlight a requirement that is still not part of the day-to-day operations of most industry partners and which is still clearly lacking in terms of the quality and consistency of information and intelligence shared by both sides. There are many organizations and associations established for the common good of participants across every critical infrastructure sector. There is simply a lack of traction and support for something more cohesive and comprehensive across all sectors (as was demonstrated in the 2010 Olympic Games model) especially as it relates to the provision of secret level clearances or something similar for the sharing of classified materials to industry. But equally important is the need for intentional, ongoing dissemination of incident information by industry to a national database.

The Olympic Games demonstrated that, despite awkward beginnings, an environment of collaboration and cooperation can be created when there is a sense of need and urgency. Translating this into an ongoing, national program will be difficult without the necessary commitment from industry and government partners.

Summary

Without a doubt, national security and emergency planning efforts on a national scale require a program of trusted information-sharing between government agencies and industry. The justification for such information-sharing may be ongoing, but without it, national security will be reduced to a model of industry-based standards for protection and response. Local emergency responders will be standing outside waiting until they are called in when disaster strikes. Understanding the various threats to infrastructure, as well as the motivations and capabilities of threat actors, assists protection planning. Working alone, industry can only achieve so much. In time, industry might look to the police and intelligence agencies for assistance to advanced threats, but some pieces to the puzzle will be missing.

It is difficult to rally all industry partners to participate and contribute to national programs. Despite the continuing threat from terrorism and other forms of extremist behaviors, owners/operators often have a localized vision of responsibility that fails to recognize interdependencies needed to support and contribute to a national response for the common good. During the 2010 Olympic Games preparations and operations, it was well understood that industry, police, intelligence and support agencies were working towards a common goal and a common outcome.

Emergency planning and national security initiatives are producing excellent collaboration and cooperation between lead government agencies, industry associations and other critical infrastructure stakeholders. Information-sharing is developing in some sectors and across some stakeholders although in many respects government is taking the lead in such initiatives. Although various levels of government continue to fund these efforts, it is at a basic level and industry is not filling the gap to the extent many would wish. Collaboration and cooperation is, therefore, not wide-spread. This is true despite the numerous times industry and police have worked together to thwart attacks or respond to emergent situations. The message doesn't seem to be reaching many stakeholders that support for these programs is essential to national critical infrastructure protection planning.

This white paper is a derivative of, and companion to an original article on this subject written by the same author as published in the Carlton University, Infrastructure Resiliency Research Group peer journal, Infrastructure Resilience Risk Reporter, *January 2014 edition. The objective of the IRRG is to advise and promote interdisciplinary knowledge-building initiatives regarding risks and vulnerabilities pertaining to national critical infrastructure in an all-hazards environment, including threat assessments, managerial precepts and risk management solutions.*

---

1 http://www.dhs.gov/national-network-fusion-centers-fact-sheet

2 https://www.infragard.org/

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street, Alexandria, VA 22314-2818 USA
Phone: +1.703.519.6200 | Fax: +1.703.519.6299 | *www.asisonline.org*

About the Author

Mr. Powell manages Security, Privacy and Safety risk for smart metering at BC Hydro. Doug has 30 years' experience managing security, showing leadership internationally by working on committees like the ASIS Utilities Security Council, ASIS Critical Infrastructure Working Group, and Canada's Advisory Board in the U.S. In 2014, Doug begins his service as CVP for ASIS International.

Doug won the 2012 Security Seven Award by Information Security Magazine. *He was named 2010 CSO of the Year and his team won the 2011 Security Program of the Year, both from* SC Magazine. *Doug is a speaker of high-profile and has authored numerous topical papers and articles.*