VOL 1 ISSUE 2 **November 2014**

IR3 Feature Articles

Editorial Corner

Angela Gendron

This second issue of IR3 once again focuses on information-sharing and co-operative partnerships as a means to improve crisis response and build resilience. Without information-sharing, no single organization has all the necessary resources or possesses all the relevant information and expertise to cope with every type of extreme event. Three of our contributors, **Raynald Lampron, Bill Isaacs and Myron Zukewich** review the topic from different perspectives: They identify barriers to information-sharing and collaboration and suggest best practice. Together they present a strong case for communicating, sharing and collaborating.

But there are perceived risks in doing so: In the last issue, I endeavoured to summarise research by Shore on the legal and moral obligations regarding information-sharing. In this issue, I am indebted to **André Brantz,** a former Competition Bureau of Canada attorney, for his efforts to clarify the position regarding information-sharing and competition law.

Trevor Hanson's article based on the simulation of a high-profile critical transport infrastructure disruption reminds us of the importance of learning lessons from the past in order to be prepared for disruptive events in the future. Support for his research from the New Brunswick Department of Public Safety is a good example of how valuable partnerships within and between the public and private sectors help in reducing the risks to society through anticipatory policies, prevention and preparation.

The literature corner in this issue tops up the comprehensive list published in Issue 1. Very few of us have subscriptions or library access to all these sources of information, so if you have found something to be of particular interest and value and would like to bring it to the attention of other IR3 readers, perhaps you would consider providing a review? A short review would merely provide the gist of an article or report so that others can decide if they want to access and read it in full; a longer review would set out the main points and provide an element of critical analysis.

The Next Issue

Issue 3 will focus on the 'Insider Threat'. If there is something you would like to say on this topic, insights or experiences you would be willing to share, or organizational lessons that might be relevant to others, please let me know. Draft articles (3 – 4000 words) would need to be with me by early October. IR3 positively solicits views from 'practitioners' – those of you who are responsible for the security of critical infrastructure, who develop and implement resilience programs or are otherwise involved in the functionality, dependability, security and resilience of critical assets and services.

You may not have much time or experience in writing 'academic' articles, but IR3's editorial board can provide guidance and help. The value to others is worth the effort and, as Raynald Lampron points out in his article, others may already have found the solutions which you seek or you may be able to share something which helps them.

Collaborative Communications

Raynald J. Lampron CD, MSM, RMC CPP*
Professional Security Practitioner
Associate, Infrastructure Resilience Research Group

E-mails, Facebook, LinkedIn, Twitter and PintoPin are only a few of the ways we communicate and stay in touch with one another in the modern world. The increasing speed with which information moves not only affects our personal interactions but also those of our business relationships as information flows within and beyond the workplace.

For any business to thrive in a fast-paced environment, it must operate and move forward with an analogous rhythm which can only be achieved through accurate and timely communication. Although control of the strategic process map rests with senior leadership, the operational delivery of the program falls upon every employee who must be empowered with a clear understanding of the envisioned end state if they are to achieve the mission. The first step in establishing a cohesive and productive work environment rests with the delivery of a clear message, supported by a framework that enables all those involved to discuss through collaborative communications.

Sadly, this is not the case in a culture where the majority of leaders control the flow of information as a means to advancement. The antidote to such destructive elitism is collaborative communication. Although this entails risks, the potential benefits can be the catalyst which changes a good department into a great one. Maximizing efficiencies is a noble aim but a cautious leader will remember to weigh the risks associated with potential losses against the management of the official message.

I. Collaboration as a Means to Advance the Mission of a Department or a Corporation

In a period of emphasized fiscal responsibility and resource management, everyone is asked to achieve more with less. While we have been faced with this reality for a number of years, a return to the "good old days" is not around the corner. Over the past few years, every employee has had to learn to innovate and change the way we manage the resources we are given in order to continue delivering the services for which we are responsible.

In order to meet these new and challenging times, various professions have looked for and secured a new approach to service delivery. Security professionals have moved toward technology, replacing human resources with new and innovative integrated security systems. Intelligent technology enables fewer security officers to monitor larger areas. Automated turnstiles provide access for employees and visitors to the work place. While technology has worked for security by performing some of the mundane tasks of a security officer at a front desk, for example, different solutions are needed for other functions in the work place. Faced with diminishing resources, meeting the needs of the customer means the service itself must be evaluated and recalibrated.

The review of core services, the manner by which they are delivered, and the resources required to complete the mission are key elements of any change management solution that addresses new challenges in the workplace. However, innovating in one area but not others will not prepare a Department or a Corporation to meet its needs but simply highlight failings in specific areas and continue taxing the entity as a whole. Change management cannot occur in a vacuum: To be successful, it has to be structured, coordinated and implemented with the buy-in of every person involved. Only through partnership and engagement can the leadership and employees come together to move their Department forward in a positive and constructive manner.

Whenever a change affects more than one person there will be a need for communication, whether between two individuals in a personal relationship or collectively at a corporate level concerning matters such as the delivery of programs and profitability. The first critical element to success will be effective and ongoing collaboration between all the moving parts which requires a common goal between the communicating parties. A second element is associated with professional capacity – the professional knowledge and resources available at a specific point in time. Finally, mutual communication requires an open approach and positive exchange between each of the parties involved.

Only by working collaboratively will departments or corporations be able to continue operating successfully in an era of austerity. An inward-looking approach which seeks to increase resources to meet challenges is simply not going to work in today's environment. As employees and leaders, we have an

obligation to communicate and exchange with others both within, and possibly outside, our own departments in order to continue delivering the services with which we are entrusted. Open and continued communication as well as ongoing collaboration is the only sustainable means to do this and meet modern challenges.

II. Understanding the Silo Culture

Silos are common occurrences in every corporation or department. Normally they are not created intentionally for nefarious purposes but to some degree may occur naturally. People are attracted to one another because they have common interests, a similar outlook or because they are part of the same mission. As people begin to identify with a specific team - Human Resources, Security, or Real Property, for example, they begin to exchange almost exclusively with their peers, seeing others as non-initiated and incapable of bringing added value to the conversation.

Silos are the product of the professionalization of the work environment: The creation of a specific lexicon to each trade as well as the fast pace of the modern environment, where leaders and employees are forced to make timely decisions in order to meet their various obligations. All of the aforementioned provide the foundation for an environment that may lead to the creation of sub-cultures which subsequently provide the building blocks of solid and long lasting silos in the workplace. Although everyone recognizes the benefits that can be gained from opening lines of communication, silos persist and communication is curbed because employees have chosen, sometimes sub-consciously, to see themselves as members of a sub-culture instead of the department itself.

In order to facilitate collaboration and communication within the whole organization, it is imperative that the leadership understand and acknowledge the existence of silos in their department. All too often key speeches promote open communication and collaboration at retreats and team rallies but they are followed by a complete lack of action. "Band aid" solutions are not only an impairment to solving problems but often compound the issues, diminish employee trust in leaders, and prompt the reinforcement of sub-culture leadership and silos from the inside.

Breaking the Silos

One of the most problematic aspects of the silo culture is at the design stage of a major project, people advance their own segment according to views which are shaped by exchanges in small specialized teams. The whole of the project falls victim to the technicality of each component. This polarization of each team's position further decreases the flow of communication until the only exchanges that occur are shaped by the biased language and hierarchy of memoranda and official meetings. Information is minimized for the benefit of self-protection.

Another challenge to collaborative communication is loyalty. Although an excellent quality, it can be a problem for leadership in a silo culture because loyalty is given to the immediate team instead of being directed toward the department or corporation. This means that employees begin to recognize the leadership of their sub-culture as the legitimate authority and seek to advance the cause of the team instead of working toward the mission of the department. In order to ensure employee loyalty is properly directed, the leadership's overarching message promoting collaboration between the various branches and divisions must reach everyone.

Corporate leadership has an obligation to inspire employees and to lead from the front by continually communicating with them on matters of interest as well as positively recognizing innovations and achievements. Initiating reciprocal communications between the leadership and employees and encouraging collaborative communications between employees themselves, will eventually break down silos and promote a single, shared identity. This may seem a Utopian aim but it is achievable through numerous small changes, continuous communications and encouragement of the 'whole team' concept.

III. What Looms Beyond the Silos

The benefits of a silo free environment pertain to employee identification with the overarching entity, the corporate mission, or the raison d'être of a department rather than a particular division or team. If the silo sub-culture mentality can be shifted towards an all-encompassing departmental 'appurtenance,' e.g. the identification of particular teams or sections with the actions and accomplishments of other parts of the entity, then this can lead to a greater overall sense of achievement as each appreciates that, by extension, the positive benefits reflect on everyone.

This vision of appurtenance does not have to stop at the level of a corporation. A government, like a multinational company, has several departments with similar structures. Each may have a security team, an HR Division, financial planners and so forth. Embracing collaborative communications and pooling limited resources is more likely to achieve maximum

results for the employer (For example, bringing together the security professionals from across the various departments to work on policy). It is not unusual for a Department to invest significant resources to meet a particular challenge, develop policy or research a new tool only to find later that this work has already been done elsewhere. How many times must we be taught the same lesson to actually learn it?

IV. COLLABORATION WITH OTHER UNITS IN THE SAME DEPARTMENT

Before assessing the various lines of communication that exist *between* Departments, the way internal communications are managed and conducted must be examined: The genesis and dynamics of these *existing* communications and partnerships are critical to an understanding of the challenges and empowering tools within the organization.

Some partnerships are based on needs and reciprocity or are a spontaneous result of employee personality and camaraderie. Partnerships that come naturally are the most conducive to collaborative communication: the interlocutors speak a common language, aim toward similar goals and are mutually invested in similar end-states. Symbiotic relationships such as that between the emergency preparedness division and the business continuity planners exist in every corporation. In such a case, communication occurs continuously as both parties have a vested interest in working toward a similar goal and appreciate the benefits each can bring to the other.

In contrast to relationships that occur naturally and are mutually beneficial, there are others which are created to follow the lines of organizational structures. These relationships are likely imposed upon various divisions without consideration for their needs or the actual nature of the task each are called upon to perform. Such relationships may be created by the corporation in order to facilitate portfolio reporting and possibly reflect a power relationship in which one group has authority over the other. Consequently, there is an imbalance in communication which impedes the free flow of information and collaboration.

While employees recognize that not every team can report directly to the Head of a Department or Chief Executive Officer, the functionality of a multi-level hierarchical structure can be counterproductive. Leaders have an obligation to reduce these levels where appropriate by regrouping particular teams or sections to prevent the creation of silos and to gain synergy by bringing together those which should naturally communicate and collaborate.

Such groupings are not always obvious. Some departments have experimented with placing Security under the leadership of Real property, the rationale being that the budget for the latter is far superior to that of the former and both have an association with corporate services. Whilst not advocating this arrangement, collaboration between these two teams has its advantages. Retro-fitting a facility with new equipment is far more costly than installations that are done during the construction phase – yet several real property projects, if not most, are conceived without the input of the Security Section. Once the building has started, imposing security and legal considerations will be seen as a burden which causes additional expenditure and delays. Whenever lines of communication are limited, or whenever people do not look at the larger picture, mistakes will be made, opportunities lost and productivity reduced.

Leaders and employees are the stewards of resources which must be managed with care and attention. A collaborative and open approach will best assist the entity to achieve its mission efficiently, effectively and in a fiscally responsible manner.

Collaboration Between Departments to Achieve the Mission

Apart from legal and security requirements, there is no valid reason why collaborative communication should not go beyond the boundaries of a department and extend to others that work for the same employer. For example, collaboration should be possible between the Canadian Food Inspection Agency and Health Canada in areas such as Security, Human Resources and even some scientific projects. The purpose of such collaboration would be to develop better services and enhance productivity by changing the status quo and creating new and innovative partnerships.

There are currently a number of such initiatives within the Government of Canada that aim to maximize output and lower service delivery costs by encouraging exchanges and discussions. Success can be contagious and spread a culture of inclusion and partnership which benefits the Canadian public as a whole. Developing partnerships between entities which most resemble each other will reduce the initial shock and optimize the chances of success – especially when implemented by employees who believe in outreach and the benefits of exchange and collaboration.

Synergy and Clusters

A clear distinction must be made between silos, a concept already explored, and clusters which comprise a regrouping of various teams, sections or departments. While silos prioritize the team before all other groups, clusters draw synergy from bringing together people or teams that have one or more aspects in common and promote the advancement of all. They should be viewed as a place from which to begin and learn but ultimately they need not be limited to like-minded entities. Instead, they should encompass every group and organization. By breaking down barriers to productivity and service delivery, clusters help to deliver maximum efficiency.

Extending lines of communication is not without risks so in choosing this journey, decision-makers should start out fully informed of the costs as well as the benefits.

V. General Considerations Associated With Collaborative Communication

Managing the Threats Associated with Free-Flowing Information

Opening the lines of communication at every level creates a number of risks which must be managed**.** Although this article advocates collaborative communications, it does not do so at all costs or without an approved framework. Moving forward with an open communication platform, without rules or limitations, would promote a laisser faire approach which could have two (or more) probable outcomes: The first being that nothing happens. No communications are generated and before long, any desire to collaborate will have been extinguished. The second probability is that information which flows without format or direction will lose its meaning. While it is always possible the message will be conveyed in a way intended by its originator, it is more likely that desires and wants will interfere and the final outcome will no longer be in line with the initial intent.

Assessing the risks associated with communication requires a structured process analogous to a standard threat risk assessment, especially where sensitive information is involved. The asset, in this case information, must be given a value, then an evaluation made of threats posed to the information that is to be exchanged and the intentions and capabilities of possible threat actors. Finally, a value is given to the safeguards in place to manage the risks to the exchange of information which can only properly be evaluated by a balanced approach which compares the potential risks against the expected gains.

Prohibitions Associated with Communicating Sensitive Information

In communicating sensitive information there are rules that must be followed in accordance with policy (information management for government) or legislation (trade secrets for corporations) in order to preserve confidentiality. Some rules prohibit the sharing of certain information beyond a very small group of people. Trade secret legislation prohibits any communication of commercially sensitive information beyond those with a 'need to know.' In the case of government Classified or Protected Information, only those persons who have a 'need to know' as part of their official duties, and a right to access (as confirmed by an appropriate security clearance) can take part in the conversation. The exchange of information must respect appropriate protocols. For example, where this takes place over electronic media, a set of pre-established rules should be followed.

Risks Associated with Instant Communication

While instant communications are a wonderful way to maintain both personal and professional contact with support networks, there are risks attached to speed: Sober second thought often gives way to unwise, spur –of-the-moment declarations which are repented at leisure. A medium such as Twitter enables others to 'Re-Tweet' the message leaving the originator with absolutely no control over information that might then go viral. Apart from being aware of the risks when discussing work-related matters we should also be cognizant of our corporate obligations and the security restrictions that might apply to the information being exchanged.

Management as a Leader in Communications

Management's role is to provide guidelines and leadership when it comes to collaborative communications. Although the best approach to innovation and collaboration is to allow employees at all levels to exchange information, this should not result in a loss of control over the mission or the message itself. Employees should be empowered to communicate with independence in their sphere of competence. However, *opinions* regarding the mission, peers or leaders have no place in an open forum. Employees not only have a duty of loyalty to leaders but also a duty to protect company resources, including information, with which they have been provided in order to complete their tasks.

Leaders must be present in discussions, provide clear guidelines, and support collaborative initiatives between employees. Anything short of that will either result in the loss of the message, an absence of collaboration, or an exchange of information and constructive ideas.

VI. THE WAYFORWARD

Notwithstanding the potential risks associated with collaborative communications, openness offers considerable opportunities for those with the audacity and vision to seek partnerships and open up to 'the big picture.' Only by unlocking the power of communication can employees reveal their true potential and surpass management expectations. Collaborative communications have the potential to yield positive results that far outweigh the potential risks. When leadership is engaged to guide and inspire employees, the result will be a happier and more productive workforce in which everyone will feel themselves to be an integral part of the achievements and successes realized by the department or corporate entity.

*Raynald J. Lampron is a member of the Federal Public Service Executive's Team at the Director level in Ottawa. Previously, he was Chief of Security and Emergency Operations, Natural Resources Canada with primary responsibilities for physical security, policies and governance, health and safety, facility emergency response. He spent over 27 years in the Canadian Armed Forces as team leader, Sensitive Investigations Unit, Human Intelligence Operations, and Force Protection both within Canada and Foreign theater of operations; with United Nations, NATO and Department of Foreign Affairs.

His final military duty was Wing Provost Marshal, 19 Wing, Comox, British Columbia.

He continues his military journey as a reservist, Brockville Rifles, Canadian Armed Forces, as Officer Commanding Administration, and legal and disciplinary Advisor to the Commanding Officer.

Mr. Lampron holds a Bachelor of Arts, Psychology and Political Science from the Royal Military College of Canada and a Masters in Security Managements (Hons.) from the American Military University. He is also a long standing member of the American Society of Industrial Security (ASIS International) and holds the prestigious ASIS *Certified Security Professional Certification*.

Security Belief and Influence

Myron Zukewich, Security Advisor*
mpzukewich@yahoo.ca

This paper is based on three organizing ideas: Security program failures can sometimes be attributed to complacency and disregard for security's role; security practitioners need influence skills to build constituent belief in security programs; and existing criminological theories can be applied as an influence lever to attaining a comprehensive security program.

I. THE CONSEQUENCES OF IGNORING SECURITY WARNINGS

Nortel Networks, the Canadian Company established in 1895, filed for creditor protection in 2009. The multinational telecommunications and data networking company, once on track for exponential growth, is now in free fall due to a decade of persistent cyber-attacks. Media sources, citing Nortel's own internal investigation, referred to hackers "having access to everything." The theft of technical papers, critical research and development documents, emails and internal discussion documents represented a loss of proprietary and intellectual information that ultimately contributed to the company's demise.

It seems that Nortel was well aware that it was under cyber-attack but chose to focus on building the brand. Alarms raised by internal security and even the Canadian Security and Intelligence Service (CSIS) went unheeded. Michel Juneau-Katsuya, a former CSIS analyst, speaking unofficially, said "that as early as the

mid-1990s it had become apparent that there was quite a lot of activity around Nortel but (CSIS) attempts to approach Nortel were brushed off[1]." As Nortel's fortunes declined, a parallel Chinese company entered the market producing exact replicas of Nortel networking equipment, manuals and systems.

The 2013 terrorist attack on the In Amenas Algerian Joint Venture gas facility resulted in the deaths of some 40 people by an al-Qaeda affiliated brigade. The Norwegian company StatOil published an unflinchingly candid analysis of the incident which included the circumstances leading up to the attack and recommendations to address detected security lapses. StatOil's report described a comprehensive security program replete with a span of controls, security audits, emergency response plans and intelligence updates - a program enviable by any standard. However, the report goes on to highlight several failures including an intractable difficulty in understanding and actioning intelligence, an over-reliance on military support to such a level that it squelched imaginative and creative internal security solutions, and a security program that lacked sufficient influence in comparison to the disproportionate and all-encompassing focus on safety. The conclusion drawn in the report is "… security is generally not well understood within Statoil's leadership ranks and has not been prioritized, resourced or managed properly." A UK news item[2] further commented that a retired soldier acting as the security liaison had raised concerns over terrorist threats and had told others he could "no longer guarantee their safety."

Common to both events are security professionals who lacked sufficient influence, and key decision-makers who failed to value and support the security program. A focus on business output excluded and marginalized necessary security expenditures. As security officers are generally aware, it is often the case that a deficit in security has much to do with belief as budget. The belief or perception that the threat is not real or imminent or that it is unlikely to have significant consequences are just two of the common excuses for failing to prioritize security issues. When security practitioners fail to engage business leaders, it is likely due to a lack of confidence in the credibility of threat assessments; misplaced priorities or trust, complacency, or a perception that the costs or procedures associated with proposed security measures will outweigh the benefits and subsequently impact negatively on business profitability.

[1] Marlow, I. Nortel turned to RCMP about cyber hacking in 2004, ex-employee says. The Globe and Mail. 2012 Sept 5.

[2] Gatton, A, Olden, M., "Death in the desert - did a security man see it coming?:, The Independent[UK], 2013 Sept 12

Is the problem rooted in organizational culture? Organizational structures, hierarchies and bureaucratic procedures can stifle initiatives which seek to anticipate or reach beyond the known. Or perhaps the problem is innate to individuals who may be reluctant to contemplate or accept new costly mitigation measures – the outcome of which is uncertain. Either way, if security professionals are to wield influence and be regarded as trusted advisors, they must demonstrate competence and have knowledge of security threats; be creative in devising pragmatic responses, and have a thorough understanding of the likely impact of both threats and mitigation measures on the core business functions. Just as important, they must be able and willing to back their security assessments and recommendations – even when encountering opposition from the business line.

The protection of critical infrastructure, of people and the company's reputation, should be a partnership in which corporate executives, employees and the security advisor actively engage and share information. Partners should pursue a rigorous, pro-active security plan together which takes account of all perceived risks to individuals and to the systems and assets of the company. It is possible to draw an analogy with business unions which, unlike the adversarial trade unions of former days, see themselves as acting in partnership with modern management to further mutual interests.

II. THE PARADOX OF PROTEC TION

Dave Grossman[3] does an admirable job in explaining a paradox in the protection of people:

> "Violence is still remarkably rare. This is because most citizens are kind, decent people who are not capable of hurting each other, except by accident or under extreme provocation… they are the sheep. Then there are the wolves… and the wolves feed on the sheep… evil men capable of evil deeds. The moment you forget that or pretend it is not so, you become a sheep. There is no safety in denial. Then there are sheepdogs to protect the flock and confront the wolf."

Grossman talks of an inherent conflict: "The sheep generally do not like the sheepdog because he looks like a wolf; he has fangs and the capacity for violence, and disturbs the sheep in his constant reminder that there are wolves in the land. Until the wolf shows up, then the entire flock tries desperately to hide behind one lonely sheepdog".

Grossman's anecdote, corrected for being somewhat self-aggrandizing, might be deemed applicable to the security professional's dilemma when negotiating security measures and expenditures with those who do not assign a high order value to security. Latent threats are low priority and high threats are improbable. Security warnings are like the sheepdog's constant worrying of the flock – an unwelcome reminder to those who are in denial about the risks or who actively wish to remain oblivious. When an 'incident' occurs, security professionals receive attention and feel valued (or, alternatively, feel blamed for having failed to identify or sufficiently articulate the threat).

III. THE STRATEGIC SHEEPDOG

Achieving appropriate levels of security requires a strategic sheepdog, not just a tactical one. The strategic objective must be to achieve a secure environment in which the core business functions can flourish, or as one security professional stated, "Where we are not seen as the 'no-team'". This entails plans to instill an awareness of the company's vulnerabilities, convincing others that real threats exist, and articulating to corporate executives how these threats have the potential to impact company safety, profitability and reputation.

Too often the security function is not seen as part of the core business and the security advisor is not accorded the status of a partner in the strategic enterprise but rather a manager of security plans and tactical measures. A failure to wield sufficient influence and move the security function to the forefront is likely to result in a repeat of past failures and tragic consequences. This is not just a matter of high impact/low frequency events such as espionage and terrorism but also low impact/high frequency events such as petty theft and vandalism. The headlines are less dramatic, but the consequences for the company's bottom-line, reputation and staff morale can be just as significant.

The 'added value' of professional security with respect to particular tasks is readily apparent. Executive protection, for example, benefits the organization by fulfilling the primary goal of protecting the executive while at the same time creating a safer working environment for everyone in

[3] Grossman, D., On Killing: The Psychological Cost of Learning to Kill in War and Society, Little, Brown and Co, 1995

the vicinity.[4] Protection allows the executive to function undistracted by personal security concerns thus creating a productivity boost and minimal downtime. Similarly, where corporate security providers have found a role in disrupting "internal crime, corruption and integrity problems", they can do so in a way that is compatible with internal interests and needs. Frankly, initiatives of this type fill a gap often left by police forces that may show disinterest in investigating within the private sphere.[5]

IV. The Security Advisor as an Agent of Influence

The security function leverages multiple tasks across different aspects of the business:

- As a non-technical risk manager,
- As a business enabler,
- To increase compliance and avoid lawsuits,
- To add to (and protect) competitive advantage,
- To aid and confirm decision-making through analysis and intelligence.

Skolnick[6] described the police as having morphed from crime fighters into a composite of soldier, school teacher, and industrial worker within a matrix of authority, danger, and public expectation. The same might be applied to the traditional "guards, gates and guns" approach to forming a security team that is evolving to meet the demands of modern security. Staff are becoming a composite of analysts, educators, negotiators, strategic advisors and managers of expectations as the security function has become:

- A leadership activity based on trust, strategy and relationships. The nature of the relationship is often political and negotiated;
- An influence activity to transmit and provide awareness and intelligence to the constituency;
- A risk -management activity that is critical to contingency planning, business resilience and operational readiness;
- A tactical management activity that reactively and proactively mitigates non-technical risks.

Effective security should be valued equally with safety, environment and health. When used in concert, these portfolios become a force multiplier for achieving the organization's mission.

V. It's Not About Winning, It's About Not Losing

Crime prevention has developed over the years into a scholarly discipline. Security management, however, is bereft of the rigorous, academic analysis associated with criminal justice and criminology. The validity of criminological theories over the years has been verified by sociological studies and empirical testing and is now being applied to many aspects of social control. To some extent, these theories provide an influence model for security professionals to follow in order to gain a strategic and tactical foothold. The goal is not to offer theories as a learning tool, but to raise awareness. Proven theories can offer a framework for practical pathways towards solutions.

VI. Dark Figure of Crime

Crime and threat analysis benefits from valid and verifiable data. It is well-known that numerous crimes go unreported, whether to avoid embarrassment, for reasons of inconvenience or otherwise, and therefore, crime figures can be misleading. In terms of protecting a company, it is important to acknowledge that latent or potential threats exist even while remaining hidden. For example, a competitor's loss may not be made public just as within one's own company, loss from fraud may not be detected or publicized. The persistence of state-sponsored cyber-attacks which seek to compromise a network, or the ubiquitous and unending criminal attacks, such as advance fee frauds which are directed at employees and others, are just two of an array of potential threats. Because they may not currently be manifest, some company employees and executives may be lulled into a false sense of security.

Being aware of "the dark figure of crime" can be useful in terms of communicating the risks and reminding decision-makers that significant threats are being addressed by security vigilance. By raising security awareness within the company staff can be forewarned and forearmed.

VII. Bystander Effect

The greater the number of people present at an incident scene, the less likely it is that someone will intervene or support a person in distress. This effect was first noted in the Kitty Genovese murder in New

[4] Oatman, R. 2006. Executive protection; new solutions for a new era. Noble House. Baltimore. p. 15.
[5] Meerts, C and N. Dorn. 2009. Corporate Security and Private Justice: Danger Signs? in European Journal of Crime, Criminal Law and Criminal Justice 17 (2009) 97–111, p 98-9.
[6] Skolnick, J. (1977). Justice without trial: Law enforcement in democratic society. New York: Wiley and Sons.

York, 1964, when she was stabbed in her apartment entrance. While accounts vary, it is widely agreed that that at least 12 people heard her distress calls. Yet 20 minutes elapsed before someone called the police. Recent experiments attribute this to a diffusion of responsibility. Conversely, onlookers are more likely to intervene if there are few or no other witnesses.
Another observed 'effect' was how an influential actor or actors play a vital role in signaling how others will behave when addressing a particular problem. Surprisingly, one experiment showed people willing to stay seated in a smoke-filled room because an influence agent swayed them into behaving as if the fire was benign.

Applied to security, all staff members need to understand that they are empowered and expected to take the initiative in security observations. This message should be reinforced by security-conscious leadership figures who demonstrate their willingness to challenge and report suspicious individuals or incidents. Finally, the security manager has the opportunity to promote security champions by finding and recognizing those with a pro-security mindset.

VIII. Broken Windows Theory

This theory suggests that a neighborhood of broken windows and other evidence of disorder may symbolize a lack of accountability which in turn provides an open invitation to some to break more windows. While the theory can be abused for political gain, (clamping down on disorder to enforce any manner of expected 'good behaviors,') the basic principle underpinning this theory is that an orderly site deters crime. A vandalized fence or parking lot is likely to become a target area for petty theft, just as the opposite is true when graffiti is removed and parking lots are protected.

Such physical measures to secure property and assets have additional spin-offs beyond crime deterrence. High profile guard forces and access controls can also deter other threats (terrorism/espionage) because these measures clearly portray a site where security is taken seriously.

This theory can be linked to the "hard target" philosophy of Crime Prevention through Environmental Design. Appropriate signage, lighting, gates, and surveillance cameras all contribute to communicating a security posture that deters the criminal element. Diversity and variation in security activities and duties enhances the general deterrence effect of moving criminals and other threat entities away from the facility. A security guard force designated to detect poor safety conditions (e.g. slips, trips and falls), can also improve environmental compliance (e.g. early detection of leaks) and other sorts of value-added activities thereby adding to the overall security of the company's mission. These derivative benefits to other areas of the business improve the security image of the company.

IX. Defensible Space Theory

This theory fuses psychological, environmental criminological, and architecture/planning to the idea that people will become more protective of environments where they are the key defence actors. This requires the site's layout, site plan and other physical characteristics be such that occupants feel a sense of ownership and responsibility for their immediate workspace. In articulating the idea of 'Defensible Space,' Oscar Newman[7] argued that four factors are needed for people to engage in the security of their shared space:

- Territoriality similar to the notion of a person's home being his castle;
- Natural surveillance capabilities where people have the ability to be able to see what's going on around them;
- Image or delineation of the physical attributes of a site such that any encroachment is obvious and thus made defendable;
- Milieu (surroundings) – making the most of a development's location in preventing crime.

Slogans like "see something, say something" and "security is everybody's business"' run through site, aviation and national security. However, defensible space theory suggests that there are several conditions that must be met before employees truly take on the security aspect of the business: Equally important to cultural expectation are: Site design, clear delineation, thoughtful selection of surroundings, and the creation of a 'controlled' territoriality where staff feel empowered.

X. Bad Man Theory

Bad-man theory is a jurisprudential doctrine that suggests while a good person follows the law out of deference and morals, a bad person sees the law as a barrier or challenge to by-pass, connive or calculate against. The person who seeks to work around the law is also a person mostly concerned with the degree of

[7] Newman, O, 1996. "Creating defensible space". Rutgers University Center for urban policy research. Accessed: http://www.huduser.org/publications/pdf/def.pdf

punishment incurred if they are caught. The Bad Man theory exposes the limits and weakness in that law.

Drawing upon this doctrine, the security manager must take account of the 'bad man's likely reaction to a requirement to follow company policies and procedures. Building policies and rules aimed at furthering the safety, security and profitability of the company must account for those persons who, whether 'bad' or merely thoughtless, always find ways to circumvent the rules.

Thinking like a "Bad Man" is equally useful to risk assessment methodologies in which scenario-based events and mitigation measures are developed to give decision-makers and project-owners a qualitative assessment of risk and demonstrate how the reduction in the risk to an acceptable level can be achieved.

XI. CONCLUSION

These theoretical models which inform behavioral analysis and organizational psychology offer a potential tool to security managers for articulating known threats. They can help decision-makers understand the threats and potential impacts, and caution against unintended consequences. While corporate executives may not be aware of, or interested in behavioral theories, they may pay heed to action research data from associated studies which support the security advisor's recommendations. The irony of modern life is that in dealing with complex and intractable problems, solutions chosen instrumentally rather than rationally more often than not deliver unwanted outcomes.[8] By combining theory with practical experience, a more holistic analysis may limit these sorts of errors and provide the opportunity for creative security responses.

The primary concern must be to ensure that all potential critical infrastructure failures[9] are considered and a robust security response plan developed and activated. Beyond proven security practices and the communication of realistic threats and risks, the security team will be required to act as influence agents in seeking partnerships, attaining resources and winning the constituency's support. This paper has suggested how criminal justice theories can be used as one tool among many to help security managers to gain the influence necessary to deliver critical infrastructure protection.

[8] Heath, J.2000. *Ideology, irrationality and collectively self-defeating behaviour*, in Constellations, v. 7, n. 3. p. 365.

[9] Graham,A. Critical infrastructure; when is safe enough safe enough. National Security of Canada Series. MacDonald Laurier Institute. p. 21.

REFERENCES

[1] Marlow, I. Nortel turned to RCMP about cyber hacking in 2004, ex-employee says. The Globe and Mail. 2012 Sept 5.

[2] I Gatton, A, Olden, M., "Death in the desert - did a security man see it coming?:, The Independent[UK], 2013 Sept 12.

[3] Grossman, D., On Killing: The Psychological Cost of Learning to Kill in War and Society, Little, Brown and Co, 1995.

[4] Oatman, R. 2006. Executive protection; new solutions for a new era. Noble House. Baltimore. p. 15.

[5] Meerts, C and N. Dorn. 2009. Corporate Security and Private Justice: Danger Signs? in European Journal of Crime, Criminal Law and Criminal Justice 17 (2009) 97–111, p 98-9.

[6] Skolnick, J. (1977). Justice without trial: Law enforcement in democratic society. New York: Wiley and Sons.

[7] Newman, O, 1996. "Creating defensible space". Rutgers University Center for urban policy research. Accessed: http://www.huduser.org/publications/pdf/def.pdf .

[8] Heath, J.2000. *Ideology, irrationality and collectively self-defeating behaviour*, in Constellations, v. 7, n. 3. p. 365.

[9] Graham,A. Critical infrastructure; when is safe enough safe enough. National Security of Canada Series. MacDonald Laurier Institute. p. 21.

*Myron Zukewich has worked in corrections, law enforcement and advanced police training for more than 25 years. He currently services as the Security Advisor for a major energy company with duties throughout Canada. He holds a Master of Arts Degree in Leadership and Training, and a Master of Science in Criminal Justice.

Times of Crisis

Bill Isaacs, President*
Crisis Leadership Ltd.
crisisleadership@gmail.com

I. INTRODUCTION

During a crisis it is imperative that the two distinct tasks, Crisis Management and Crisis Leadership, are performed well if there is any hope of coming out of the incident intact. There is an important difference between the two:

Dancing With The Tiger: The Art of Business Crisis Leadership[1] the author defines the difference as:

> "Emergency Managers must patch holes in the fence—fix the problems. Their plans and actions must focus on getting "back to the past" —a solid status quo. Crisis leaders, however, must see beyond the holes in the fence. Their strategy will focus on getting "back to the future" and the opportunities that await."

During an emergency event, a company's leader should artfully manage the company's approved crisis management plans and resources. The leader should oversee the effective implementation of emergency response procedures, business continuity plans, crisis communication strategies, and recovery plans. This includes timely decision making and support for those directly impacted by the crisis.

While a good crisis manager carries out management plans and allocates resources, a crisis leader demonstrates creative human skills, some of which are innate while others are learned. Demonstrating leadership during a crisis means exhibiting those skills that make people want to trust and follow you. Leading during a crisis requires the ability to demonstrate high levels of caring, decisiveness, and persistence against all odds.

II. CAN A CORPORATE LEADER BE A GOOD CRISIS MANAGER, BUT A POOR CRISIS LEADER

The performance of many senior leaders during a major event often demonstrates a detailed knowledge of the content and application of a company's emergency plans which contributes to the safe and adequate resolution of the emergency. However, as a crisis leader they may be rated only as 'adequate' because they never achieved the appropriate balance between acting and analyzing. A good crisis leader builds strong teams who possess detailed knowledge of a company's emergency plans and are skilled at executing them. Having strong teams in place should free leaders to exercise leadership and develop strategy, which is precisely what staff want and expect of them in a crisis.

Example: In response to an explosion at a school in Northern Ontario I was sent in to act as the Incident Commander for the pipeline company involved. At the corporate Emergency Operating Center (EOC) a relatively new Senior Manager had been assigned to lead the crisis as the Emergency Operations Center Director. Being a strong crisis manager he was well aware of the procedures and policies of the organization. During my regular updates with the EOC from the field, he constantly questioned the tactical response plans and recovery methods of the response team on site. This led to delays in key decisions at the most critical times of the incident and additional stress on the team because of his failure to put trust in their experience. Furthermore, despite being the Crisis Leader, he was unable to supply the strategic vision or guidance needed to lead the whole incident because he was caught up in the tactical details.

[1] Jim Truscott, "*Dancing With The Tiger: The Art of Business Crisis Leadership," Published by MissionMode Solutions, 2010-2012, page 3.*

III. What Qualities are Expected of a Good Leader?

Leaders must demonstrate resolve and decisiveness in order to move an issue along and build confidence in the workforce. Circumstances during an emergency situation can be fast-moving and change quickly. It is often stated that about half the information received in the "golden hour" or the first hour of a major emergency turns out to be wrong. In all likelihood, 95% of emergencies never escalate to a crisis level. This means that the crisis teams must react quickly and have confidence that the leadership will be ready to guide, assist and support them.

A good crisis leader never overlooks the human element. I have also seen instances where a crisis manager, while near perfect in the *application* of the emergency plans, overlooks the human element because the overall well-being of employees and the general public may not be spelled out in those technical plans. An important aspect of a crisis leader's abilities can be demonstrated through their concern for both the people impacted by the crisis and those dealing with the crisis.

Example: One could argue that BP's early response to the oil spill in the Gulf of Mexico or the early communiqués from the Maine & Atlantic Railway during the Lac-Mégantic train derailment should have been more focused on the human tragedy of those events. A caring organization should not appear to be emphasizing the technical aspects of incidents above concerns for the human impact.

The crisis leader must do everything possible to ensure everyone's personal safety. This should also be the organization's first priority, demonstrating to all those involved that safety comes before profit and that every reasonable step will be taken to reduce personal risk. This approach can also limit liability. Actions of care and concern are well appreciated by employees, the general public and the press – all of whom will be judging the crisis leader in the court of public opinion after the emergency is over – if not sooner.

In caring about people, good crisis leaders must take care of themselves and their families as well as their staff. They must be able to recognize when it is time to take a step back; to pause and consider whether everything is being done to support the efforts and well-being of everyone. Being overtired, overstressed or even hungry can affect the leader's ability to make decisions, provide guidance or offer support to those who need it. Knowing when to take a rest or a quiet meal break will enhance the effectiveness of the thinking process, provide space to ponder next steps and fuel the energy to execute these steps with confidence.

IV. Reputation and the Eye of the Media

Employees are looking for leadership. If they see that the leader is looking out for their safety and well-being, they are far more likely to follow willingly. But it is not just employees who are watching. The media's perception of the leader's performance is acute. If he/she is seen to be caring and concerned, then the organization's brand will also take less of a hit in the world of public opinion.

Example: Media quotes and communications regarding the early responses of senior leaders of BP or Maine & Atlantic Railway will be studied for years to come. What was said is not necessarily what people heard. Crisis communications must be a "No Spin Zone" Be up front, honest and communicate regularly.

Damage to an organization's brand can be more devastating to a company's recovery than damage to its physical assets. Plants, pipelines and drilling rigs can be rebuilt, but years of building trust with the general public, shareholders or government regulators can vanish with one poorly managed incident. Sometimes even the *perception* that the incident is being poorly managed can have an adverse impact, whether correct or not.

V. Stress in Perspective

The pressure induced by multiple and time-sensitive decision-making can cause severe stress for a senior leader during a crisis situation. Invariably, there will be different opinions that support specific actions or timings. This is normal and can be very productive especially when a different perspective is needed to solve an intractable problem. But sometimes differences of opinion and constant challenges can be counterproductive. A good crisis leader listens carefully to contrary perspectives and gives them due consideration. They also know when to stand their ground and go with their gut. This is not easy, but if all your viable options have been considered, and the safety of all involved has been prioritized, all it will cost you is money. Buildings can be rebuilt, but lost lives cannot.

VI. Critical Decision-Making During a Crisis Situation

In most crisis situations there is only going to be one chance of 'getting it right the first time.' Thinking and planning ahead and being well-prepared are

essential but the impact of some decisions about personal safety, protection of the environment, costs, and communications cannot always be anticipated. Some costs will be recoverable and some will not. A strong crisis leader will know the difference and manage the risks without paying undue attention to changing public opinions or the minute-by-minute musings of social media.

Crisis thinking is something that can be practiced, either by the experience of being involved in day-to-day emergencies or through emergency exercises. This enables crisis leaders to reduce their thinking time and react more instinctively. When a situation is perceived as 'typical,' people are likely to recognize the required 'typical' response. But be careful of focusing only on first perceptions. In the early stages of a crisis much of the information received may not be totally correct. The Crisis Leader should access the initial information, but take care not to over analyze it.

Effective internal and external communication is crucial, but getting the facts out correctly, early and often supplies valuable information to those who need to deal with the emergency. Communicating proactively is the best way to deal with issues that could damage the organization's image. To mitigate potential communication errors, many organizations use the 3-3-30 rule which requires messages consist of three short sentences and convey three key messages in thirty words or less. For example an early external communication to a pipeline rupture may look like:

> "XYZ *Energy Company has responded to the pipeline break at the Town of ABC. We have determined the site is safe. The cause of this incident is currently under investigation".*

Having this kind of pre-approved initial messaging can be critical in meeting the expectations of the public and the media at the onset of the crisis. Some organizations or agencies may also have multiple messages for various demographics, local cultures or even different languages.

During a crisis, sharing appropriate information in a timely fashion with staff, local authorities, the public and the media can be critical for achieving a coordinated and effective response, maintaining staff morale and safeguarding the organization's reputation. A good crisis leader will be one who can develop and capitalize on contacts with others and inspire them to co-operate and work together to achieve a satisfactory outcome.

From my experience an organization emerges successfully from a crisis situation, not because of the number of levels in their crisis management structure, but because of the number of leaders it has at those levels.

REFERENCES

[1] Jim Truscott, "Dancing With The Tiger: The Art of Business Crisis Leadership," Published by MissionMode Solutions, 2010-2012, page 3.

*Following 40 years of experience in the natural gas industry, holding positions of increasing responsibility in engineering, gas transmission and distribution field operations, operations training and emergency and security management, Bill is now President of Crisis Leadership Ltd. He has extensive knowledge and experience developing effective post incident investigation processes, crisis leadership training, workplace violence security response plans, and awareness-raising and education for emergency response and pipeline system security procedures.

Bill is an original member of the Technical Committee responsible for the development of CSA Standard Z246.1 Security Management for the Petroleum and Natural Gas Industry and sits on the Development Committee for CSA Standard Z246.2 Emergency Preparedness and Response for the Petroleum and Natural Gas Industry. He is the recipient of the 2013 Canadian Gas Association's Lifetime Safety Achievement Award.

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

Critical Infrastructure Protection and Antitrust Law

*André Brantz**

"People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices."

Adam Smith ~ Wealth of Nations

I. INTRODUCTION

Under competition laws, there is a presumption that competitors in the same business should not share information with each other. A more refined presumption is that they should not share information which may affect key business decisions (prices, outputs, investment, strategies). However, when competitors agree to share sensitive and confidential information, it can become easier for them to act in concert, thereby reducing, or even eliminating, competition.

Information-sharing can help identify threats and vulnerabilities, establish best practices, and detect or mitigate attacks. As better techniques evolve, it would be to everyone's benefit if they were shared. However, there is a perception or belief that sharing information with competitors may be viewed as a violation of antitrust laws. Indeed, there has been a call for a new antitrust exemption for such information exchanges in the United States. These calls have so far been rejected, presumably on the basis that there is no need for a new exemption from allegations of anti-competitive behaviour.

The goal of this article is to examine the extent to which sharing information on infrastructure protection may be perceived as anti-competitive conduct. A brief review of antitrust law in Canada and the United States will assist the reader in understanding and assessing the risks of potential antitrust violation.

II. CANADA

In March 2009 the Parliament of Canada enacted significant amendments to the Competition Act.[1] The conspiracy section, S. 45 of the pre-existing legislation prohibited not only cartel agreements such as price-fixing or market-sharing but all agreements which unduly restricted competition. It was argued that S. 45 had a chilling effect:

> "Because many business people understandably refuse to take any risk of committing a criminal offence, Section 45 often prevents the implementation of pro-competitive agreements such as strategic alliances which make more efficient use of resources."[2]

In response, it was observed that prosecutions under S. 45 had almost exclusively been against price-fixing, market-sharing and other similar cartels that did not generate pro-competitive effects. It was also argued that the Attorney General (today the Director of Public Prosecutions) would properly exercise his/her prosecutorial discretion and not prosecute beneficial strategic alliances even if there were some anti-competitive effects. Nevertheless, the Law was subsequently amended in 2009.

The 2009 amendments significantly changed the Law by creating a "two track" system for dealing with agreements between competitors.

Section 45.1 creates a "per se" criminal conspiracy offence with respect to agreements between competitors, or potential competitors to fix prices, allocate sales, customers or markets; or fix or control the production or supply of a product. Penalty for a breach of this provision can lead to a maximum of 14 years imprisonment and/or a $25M< fine.

Section 90 creates a new civilly reviewable matter in respect of agreements between competitors which prevent or substantially lessen competition (but which do not involve fixing prices, allocating sales, or reducing output). The Commissioner of Competition would apply to the Competition Tribunal for an order

[1] Competition Act (R.S.C., 1985c C-34)

[2] McCarthy Tetrault, August 2001 – Proposed Amendments to S. 45 of the *Competition Act*

prohibiting the impugned behaviour. This provision adopts the efficiency defence set out in the merger section where parties can demonstrate the agreement brings about "gains in efficiency that will be greater than, and will offset the effects of, any prevention or lessening of competition."

The Competition Bureau recognizes the need for transparency and predictability on how it analyzes competitor collaboration. Accordingly, after the 2009 amendments, the Bureau issued Competitor Collaboration Guidelines[3] ("the Guidelines") to assist businesses and their counsel in assessing whether a particular form of competitor collaboration is likely to raise concerns under the criminal or civil provisions of the Act.

While these guidelines do not specifically address the issue of information-sharing relating to protecting critical infrastructure, they deal with Information Sharing Agreements in general at para. 3.7 below:

> "In assessing information sharing agreements between competitors under section 90.1, the Bureau will consider the following factors, among others: the nature of the information exchanged (i.e., whether the information is competitively sensitive); the timing of the information exchange (e.g., whether the information relates to historical, current or future activities); whether the parties participating in the information exchange have market power or will likely have market power; the manner in which the information is collected and disseminated (e.g., whether the information is shared directly between the competitors or aggregated by a third party); and whether any anti-competitive effects are offset and outweighed by the efficiencies generated through the information sharing agreement."[4]
>
> 3.7.1 Competitively Sensitive Information
>
> An agreement to disclose or exchange information that is important to competitive rivalry between the parties can result in a substantial lessening or prevention of competition. For example, exchanging pricing information, costs, trading terms, strategic plans, marketing strategies or other significant competitive variables can raise concerns under the Act. Where competitors agree to share competitively sensitive information, it can become easier for these firms to act in concert, thereby reducing or even eliminating competitive rivalry."[5]

It is not possible to make a sweeping or blanket statement that all information exchanges relating to critical infrastructure protection will not raise antitrust concerns. The analysis of any conduct is extremely fact -driven. Recognizing that Guidelines cannot provide a comprehensive review of all competition issues that may arise from a given collaboration, firms are encouraged to seek guidance regarding future business conduct by requesting a binding written opinion from the Commissioner of Competition under S. 124.1 of the Act.

III. UNITED STATES

In April 2000, the U.S. Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") issued Anti-trust Guidelines for Collaborations among Competitors.[6] The preamble states that notwithstanding that the Federal agencies had brought relatively few cases against competitor collaborations in the last two decades, there was still "a perception that anti-trust laws are skeptical about agreements among actual, or potential competitors which may deter the development of pro-competitive collaborations."

On April 10, 2014, the DOJ and the FTC issued a joint policy statement on the sharing of cyber-security information.[7] In explaining how their analytical

[3] Competitor Collaboration Guidelines, Dec. 23, 2009 www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03177

[4] *Supra at 3*

[5] *Supra at 3*

[6] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, Antitrust Guidelines for Collaborations Among Competitors (2000), http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf

[7] Department of Justice and Federal Trade Commission: Anti-trust Policy Statement on Sharing of Cyber-security Information April 10, 2014, www.justice.gov/atr/public/guidelines/305027.pdf

framework applies to information-sharing, the DOJ and the FTC seek to "make it clear that they do not believe that antitrust is – or should be – a roadblock to legitimate cyber-security information-sharing.

This policy statement refers to a previous antitrust analysis on cyber threat information-sharing that was issued in October 2000 when the DOJ issued specific guidance in a business review letter (advisory opinion) to the Electric Power Research Institute Inc (EPRI).[8] According to the 2014 policy statement this letter is still relevant as the legal analysis in that matter is still appropriate. The DOJ business review letter is available online at http://usdoj.gov/atr/public/busreview/6614.htm.

In 2000 EPRI sought a business review letter with respect to its proposed information exchange. The EPRI indicated that the energy companies planned to exchange two principal types of information: best practices (including methodologies for conducting vulnerability assessments, stress tests and plans to identify, alert, and prevent cyber-security breaches) and product vulnerability information.

The EPRI also adopted a number of measures to prevent any anti-competitive effects, including:

1. Ensuring all information related directly to physical and cyber security;
2. Prohibiting the discussion of specific prices for cyber security equipment and systems;
3. Prohibiting the exchange of company-specific competitively sensitive information;
4. Prohibiting the use of the program as a conduit for discussions by vendors, manufacturers, and security providers with respect to any exchange participants; and
5. Ensuring neither the EPRI nor any participant recommended the products or systems of any particular manufacturer or vendor.

The DOJ concluded that it had no intention to challenge the proposed information-sharing arrangement. It also stated: "To the extent that the information exchanges result in more efficient means of reducing cybersecurity costs and thus savings redound to the benefit of consumers, the information exchanges could be pro-competitive in effect."

The 2014 Policy Statement explains that in examining the information exchanges, the antitrust agencies will typically examine information-sharing agreements under a rule of reason analysis which considers the overall competitive effect of an agreement.

> "Rule of reason analysis focuses on the state of competition with, as compared to without, the relevant agreement. The central question is whether the relevant agreement likely harms competition by increasing the ability or incentive profitably to raise price above or reduce output quality, service or innovation below what likely would prevail in the absence of the relevant agreement."[9]

By and large, the construction of the rule of reason inquiry has remained unaltered since it was first articulated by the US Supreme Court in Chicago Board of Trade v. United States in 1918.[10]

The agencies will consider the extent to which competitively sensitive information likely would be disclosed to competitors. Thus the nature and detail of the information disclosed and the context in which information is shared are highly relevant. The statement goes on to add "…it is less likely that the information sharing arrangements will facilitate collusion on competitively sensitive variables if appropriate safeguards governing information sharing are implemented to prevent or minimize such disclosure."

The statement then goes on to look specifically at cyber-security threat information-sharing and identifies three important considerations:

1. "Cyber threat information can improve efficiency and help secure our nations networks of information and resources."
2. Cyber threat information typically is very technical in nature. The agencies note that the "nature of the information being shared is very important to the analysis" and "sharing of this

[8] http://usdoj.gov/atr/public/busreview/6614.htm

[9] Supra at 7

[10] *Chicago Board of Trade v. United States* 246 US 231 Supreme Court 1918

information is very different from the sharing of competitively sensitive information such as current or future prices and output or business plans."

3. Is the exchange of information likely to harm competition? "Generally speaking, cyber threat information covers a limited category of information and appears unlikely in the abstract to increase the ability or incentive of participants to raise price or reduce output quality, service or innovation."

The Policy Statement concludes by saying that "properly designed sharing of cyber threat information should not raise anti-trust concerns." Of course, if an information-sharing agreement is being used as a cover to fix prices, allocate markets, or otherwise limit competition, antitrust issues could arise. In sharing information about protecting critical infrastructure, the shared information should be tightly circumscribed and limited only to the extent necessary to realize the stated goal.

Notwithstanding concerns having been voiced for many years over the risk that sharing threat information might be viewed as an unlawful anti-competitive practice, the United States has not sought legislative amendment or exemption but has opted to proceed by a re-statement of analytical guidelines. Indeed, a legislative exemption would create a new body of law that would upset decades of case history and undoubtedly lead to years of new litigation.

In conclusion, exchanges of information about critical infrastructure protection are both desirable and feasible. The sharing should be tightly circumscribed, and open only to the extent necessary to realize the stated protection goal. It remains to be seen whether the "rule of reason" analysis followed by the U.S. Courts will become relevant in Canada but it is quite likely.

*Andre Brantz is a lawyer who for 22 years was a Competition Officer with the Competition Bureau where he was involved in the enforcement of the civil and criminal provisions of the Competition Act. He also supervised and participated in the preparation of complex economic analysis on the competitive impact of mergers on the Canadian market. He then spent 10 years in the Competition Law Division of the Canadian Department of Justice where he was responsible for criminal prosecutions and immunity applications in conspiracy and fair business cases which included misleading advertising, mass marketing fraud as well as civil competition matters where remedial orders were sought and obtained.

Although retired, Mr. Brantz consults for various international organizations and conducts staff training, capacity building, training of judges, and the drafting of legislation and operational guidelines for Competition Agencies in developing countries.

Using Open Source Data to Better Understand Impacts of Critical Transportation Infrastructure Disruption: Lessons From Simulating a High-Profile Highway Disruption

Trevor R. Hanson, PhD, P.Eng. Assistant Professor*
UNB, Dep't of Civil Engineering

This article summarizes the approach, methodology, analysis and results for one of the critical infrastructure scenarios that considered the potential effects of a four-day independent truckers strike on the import and export of food, fuel, and other goods via the Trans-Canada Highway (TCH) at St-Jacques, New Brunswick, near the Quebec border. The goal was to develop a better understanding of the significance of this route to the New Brunswick and regional economy and its sensitivity to disruption. A detailed account of this study, including the specific methodology, is available from the author upon request.

I. INTRODUCTION

Transportation and public safety agencies are continuing to adapt to the risk of catastrophic disruptions to critical transportation infrastructure and the resulting impacts on economies and supply chains. In addition to understanding this risk, agencies need to understand the mechanisms of disruptions at a micro-level to help them tailor a local response to the disruption. This can assist in quantifying second- and third-order effects of the disruption on local, regional, and provincial economies.

The Security Directorate of the New Brunswick Department of Public Safety contracted researchers at the University of New Brunswick (UNB) to develop "worst-reasonable case scenarios" for disruptions to critical transportation infrastructure in New Brunswick, then to quantify the impacts of the disruptions. The UNB Gregg Centre for the Study of War and Society contributed to the initial development of the scenarios, and then contracted the UNB Transportation Group to provide the technical expertise in transportation engineering to flesh out the scenarios and develop the analysis. One constraint was the analysis needed to be done using "open source" data, which includes non-confidential data that can be accessed freely through the internet, by direct observation, or acquired without a security clearance.

Background

From September 6 – 8, 2005, independent truckers in New Brunswick undertook a wildcat strike in response to high fuel prices. According to media reports [1-3], the strike began at St-Jacques, NB near the Quebec border, but also spread to 10 locations throughout NB. Of these, the St-Jacques strike was estimated to have been the largest, with approximately 300-500 trucks participating for up to three days. Drivers parked their loaded trucks on the side of the highway and created a blockade on the highway. The intention of the blockade was to delay commercial vehicles only. The media reported localized shortages of fresh produce, perishable goods, and fuel, with some reports of people near Edmundston travelling to Maine to do their shopping [4]. Several large local companies dependent on trucking shipments reported facing layoffs or closure, or that their products were being blocked from delivery [5]. Even though protestors were reportedly waiving through passenger vehicles and delaying commercial vehicles only long enough to invite them to sign a petition, queues on the highway at the protest site were reportedly up to 15 km in length.

Though there was a general recognition at the time that this disruption had a widespread impact, the impact itself was not well understood: How much and what types of cargo were detained? How much delay was experienced by non-participating truckers and the general public? What would be the impact if this were to happen again and could it be mitigated with a better understanding of the mechanisms of the disruption? Answering these questions required employing approaches and data typically used in transportation engineering to manage traffic and infrastructure. One such approach was micro-simulation, which can use traffic volume data to simulate the arrival of vehicles at a location, and then uses software tools to interrupt

or delay the traffic and measure the results. The operational elements of the disruption could be organized into a series of steps that could be programmed into a simulation. Probabilities associated with each operational element of the disruption could be estimated or determined from open source data, then adjusted to explore a worst-reasonable case scenario.

II. METHODOLOGY

Developing a worst-reasonable case scenario requires each element of the possible disruption to be explored and evaluated in terms of whether the scenario is possible or would result in alternative actions which would limit the impact of the disruptions. A worst-reasonable case scenario was sought that would involve some type of prolonged disruption of the TCH at St-Jacques, yet not result in a complete diversion of commercial traffic to other less convenient routes or result in trucking companies holding back trucks at the distribution centres to protect perishable goods. An independent truckers strike similar in breadth and scope of the 2005 disruption was considered to be a worst-reasonable case scenario since:

- It had historical precedence and apparent widespread impact;
- Traffic was permitted to flow through the area, albeit delayed, meaning there would be little reason to hold back trucks at distribution centres or divert them to other routes;
- It was considered likely that the delay encountered by passenger vehicles and non-participating trucks at the protest location would be less than the delay incurred by taking alternate routes, leading to normal traffic volumes approaching this location;
- There was not one single point of disruption (such as a road washout) that had a single solution, rather it was the collective action of hundreds of independent operators, each of whom had the choice to participate or not;
- The end time to the disruption was not fixed.

The purpose of the original disruption was to make the point to elected officials and the general public in New Brunswick that it was cheaper for the independent truckers to park their vehicles on the side of the road than to operate their trucks, given the gas prices at the time. The disruption lasted three days. While other independent trucker strikes have lasted longer, such as one that occurred at a British Columbia port in 2005, this strike lasted a month. [6] It was an illegal disruption of the highway network rather than job action on private property. Although a longer disruption at this location is possible, there are a number of mitigating factors which suggest a worst-reasonable case would probably not last much longer than three days - the most critical being the highway's role in interprovincial trade which would probably elicit a rapid enforcement and political response.

Several types of open source data were obtained for this study, including:

- Media reports which described the detailed operations of the strike;
- Traffic counts and weights from the Province of New Brunswick;
- Publically available online resources including US Department of Transportation border crossing data and Transport Canada trucking company data.

Since detailed cargo information for the trucks on the highway was not available, a video log of traffic was taken at the same location as the protest and cargo types estimated from a visual inspection of the trailers in the video. For example, any truck that had a refrigerated trailer was assumed to be carrying "perishable" goods. Cargo capacities were also estimated based on maximum allowable vehicle weights for each type of truck class and assumed empty truck weights. Several parameters for the simulation needed to be assumed, including delay times and protest participation rates, though actual traffic volumes for 2012 were used. The simulation was completed using ARENA by Rockwell Automation and underwent a process of verification and validation of the model parameters. Simulation was beneficial because it permitted the adjustment of parameters (e.g. delay per vehicle) until the observations in the simulation generally matched the anecdotal observations in the media reports (e.g. queue lengths). This permitted a better understanding of what those parameters must have been to result in those observations.

III. DISCUSSION OF RESULTS

The methodology permitted a clearer understanding of the mechanics of the protest actions, and how those actions translated into delays of passenger vehicles and delivery of goods. Though it was not the intent of the protestors to disrupt passenger vehicles, the delays to commercial vehicles produced long queues in both directions. The simulation and associated analysis was completed for both directions (eastbound and westbound) and provided results by time of day and day of the week. It was possible to determine the amount of delay induced by the protestors at the

blockade that resulted in extensive highway queuing and to estimate the amount of cargo (and type) held in the roadside protest.

The following figures provide an estimate of the amount of cargo housed within the trucks of the roadside protests, assuming 50% loading eastbound and 45% loading westbound.

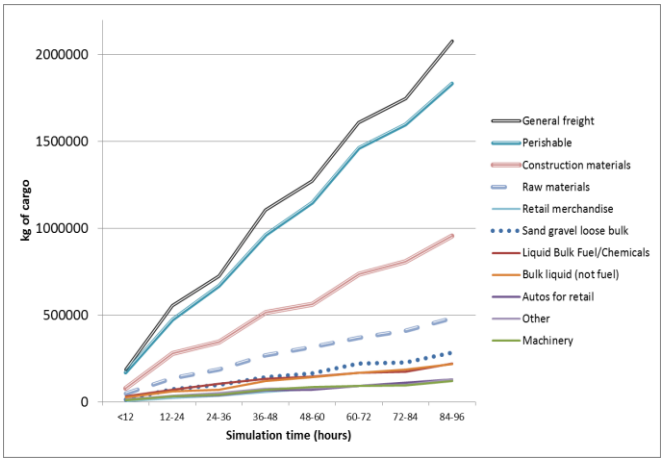

Figure 1 - Estimated cargo in protesting trucks by simulation time (both directions)

By the end of the fourth day of the simulation, there was an estimated 1.8 million kg of perishable goods sitting in the roadside protest, with 1 million kg inbound to New Brunswick. Values of this magnitude represent a considerable disruption of food supplies for the province and beyond, as well as to businesses dependent on food exports. This contextualizes the concerns of shippers and receivers noted in media reports in 2005.

IV. Lessons Learned From the Study

There were several lessons learned from this study in terms of how the work was completed and the application of the work. The first was that verified and validated model outputs from the simulation provided results consistent with anecdotal observations at the time of the original disruption. This occurred even though the underlying assumptions could not be validated due to limited information describing the particulars of the 2005 protest.

The second lesson was that understanding the sensitivity to changes in model parameters (such as increasing the delay per truck), could provide practical lessons for those monitoring similar situations in real time. For example, monitoring vehicle delay times during a disruption could help predict whether there may be a traffic jam later, even if the highway typically operates below capacity and in a rural environment. This would need to be studied on a location by location basis as traffic volumes and peaks would differ between locations.

The third lesson is that transportation data is becoming increasingly open source, though not always routinely accessible. Some jurisdictions post traffic counts and other information online, others provide it when a request is made. In the absence of information, it can be possible to infer information through direct observation. Knowledge of transportation engineering and planning practice was instrumental in developing reasonable assumptions, obtaining relevant open source data, and preparing the simulation.

Lastly, it is likely that the vulnerabilities of the transportation network were already known to those looking to exploit them and to those trying to protect them, though the magnitude of the negative effects of the 2005 disruption may not have been readily evident to either party prior to the protest starting. The media reported that the main goal of the protestors was to attract government attention and public sympathy for their situation. They appeared to structure their protest in a way that they hoped would accomplished this (e.g. waving through cars at their blockade and delaying only commercial vehicles to invite them to join the protest), but the tactics resulted in considerable queuing and highway delays to all vehicle types. Had authorities known such a disruption would have resulted in the delay of potentially 1.8 million kg of perishable goods, with queues of 10-15 km, would their approach to managing the disruption have been different? This and other questions relating to the impacts of supply chain disruptions highlight the need to conduct detailed level analysis which can explore the spatial and temporal impacts of such disruptions.

Looking to the future, agencies concerned about impacts to critical transportation infrastructure should consider a proactive approach of conducting micro-simulation or other detailed analysis exercises on elements of their network, in addition to overall risk management. There may be opportunities for retrospective evaluation of disruptive events provided a detailed and quantifiable account of disruption parameters is maintained.

Acknowledgment

This report was made possible by funding from the Security Directorate of the New Brunswick Department of Public Safety through the Gregg Centre for the Study of War and Society at UNB. The input and insight from the members of the Security Directorate and its Critical Infrastructure Program was integral to the success of this project. The author is grateful for the support and involvement of Prof. David Charters of the UNB Gregg

Centre, Brody Hanson of the UNB Transportation Group, and UNB civil engineering student research assistant Jessica Bishop. The author also acknowledges the New Brunswick Department of Transportation and Infrastructure for providing data used in this report.

REFERENCES

[1] 500 trucks block NB highways; Truckers' anger over high gas prices directed at refineries; police negotiate to end blockade, in Times & Transcript. 2005: Moncton

[2] CBC. N.B. truckers protest gas hikes, clog highways. 2005 [cited 2013; Available from: http://www.cbc.ca/news/canada/n-b-truckers-protest-gas-hikes-clog-highways-1.523395.

[3] Canadian Press, Truck protest gears up, in Daily Gleaner. 2005: Fredericton.

[4] Banville, B., Wildcat trucker strike hits border; Maine stores selling basics to Canadians, in Bangor Daily News. 2005: Bangor. p. A1.

[5] Berry, S., Provincial government pressured to end truckers' blockades, letters reveal, in Telegraph-Journal. 2005: Saint John.

[6] CBC. B.C. truckers strike may soon end, Ottawa says. 2005 [cited 2014 January 2]; Available from: http://www.cbc.ca/news/canada/b-c-truckers-strike-may-soon-end-ottawa-says-1.541673

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

*Trevor Hanson, P.Eng. is an Assistant Professor of Civil Engineering at the University of New Brunswick and member of the UNB Transportation Research Group. His research has included developing a better understanding of policy issues by exploring them through an engineering lens, including, most recently, understanding the impacts of disruptions to critical transportation infrastructure. He has also undertaken research in rural intelligent transportation systems, rural older driver travel behaviour and safety, and active transportation.

RECENT CONTRIBUTIONS TO PROFESSIONAL LITERATURE
ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
SELECT TITLES

"Resilience of civil infrastructure systems: literature review for improved asset management"
by Leon F. Gay & Sunil K. Sinha
Security and Intelligence Studies Journal, Vol. 1, No. 1 (2013)
http://institutes.king.edu/fileadmin/DAM/SIS_Journal/files/SISJ_no1_Lukasic.pdf

"Implications of the West African Oil Rush for US National Security"
By Jessica Lukasik.
Security and Intelligence Studies Journal, Vol., 1, No. 1 (2013)
http://institutes.king.edu/fileadmin/DAM/SIS_Journal/files/SISJ_no1_Lukasic.pdf

"Protecting critical infrastructures through behavioural observation,"
William Hurst; Madjid Merabti; Shamaila Iram; Paul Fergus
International Journal of Critical Infrastructures, Vol.10, No.2, (2014)
http://www.inderscience.com/info/inarticle.php?artid=62972

"Information sharing and collaboration for critical infrastructure resilience - a comprehensive review on barriers and emerging capabilities"
by Boris Petrenj; Emanuele Lettieri & Paolo Trucco
International Journal of Critical Infrastructures, Vol.9, No.4 (2013)
http://www.inderscience.com/info/inarticle.php?artid=58172

"Comparative Islamist Perspectives on the Politics of Energy in the Middle East and Beyond"
By Emmanuel Karagiannis
Studies in Conflict and Terrorism, Vol. 37, Issue 8, August 2014
http://www.tandfonline.com/toc/uter20/current#.U8gtH0CGcSU

"Identification of Key Performance Indicators of Security Management for Thermal Power Plants"
Raj Sekhar Choudhury & Sutapa Das
Journal of Applied Security Research, Vol. 9, Issue 2 (2014)
http://www.tandfonline.com/doi/full/10.1080/19361610.2014.883271#.U4PYmnaGcSU

"EMS and Homeland Security."
BY Mac Kemp
Homeland Security Affairs Vol. X, Article 4 (2014)
http://www.hsaj.org/?article=10.1.4

"Security Levels of Critical Infrastructure"
by Kiril Stoichev
Journal of Applied Security Research, Vol. 9. Issue 3 (2014)
http://www.tandfonline.com/doi/full/10.1080/19361610.2014.913233#.U9JTyUCGcSU