THE CIP EXCHANGE

Workshop Edition

A forum for sharing views and information about critical infrastructure protection FALL 2009

Resilience Revisited

Yossi Sheffi from MIT discusses new vulnerabilities in the supply chain

DALHOUSIE UNIVERSITY Faculty of Management School of Public Administration

CONTENTS

EDITORIAL

Editor: Kevin Quigley

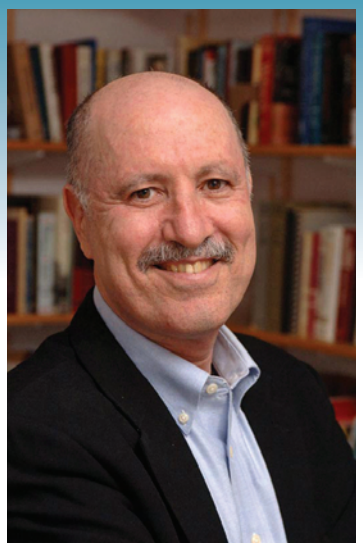
Copy Editor: Janet Lord

Design: Dalhousie Design Services, Roxanna Boers, Designer

Workshop Photography: Dalhousie Photography, Daniel Abriel

Additional Thanks: Ron Pelot

Dr. Yossi Sheffi is a professor at the Massachusetts Institute of Technology, where he is the Director of MIT's Engineering Systems Division and the MIT Center for Transportation and Logistics. He is an expert in systems optimization, risk analysis and supply chain management. He is the author of dozens of scientific publications and two books: a textbook on transportation networks optimization and *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage* (MIT Press, October 2005). Professor Sheffi is also an active entrepreneur, having founded five successful companies. In 1997 he won the Distinguished Service Award given by the Council of Supply Chain Management Professionals. In 2002/03 he was on sabbatical in the Judge Institute of Management Studies at Cambridge University, UK. He is also a life fellow of Cambridge University's Clare Hall College. In 2006 the Government of Aragón, Spain, awarded him the PLAZA Award for the most significant contribution to the economy of Aragón.



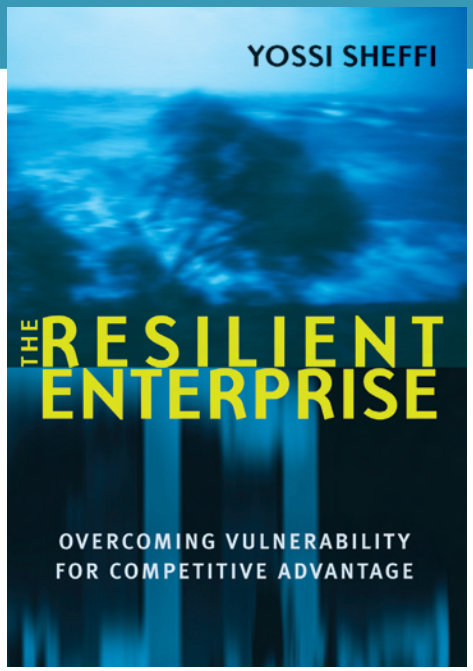
Yossi Sheffi

Kevin Quigley interviewed Dr. Sheffi by email in October/November 2009.

KQ: How has the economic downturn influenced your thinking on resilience?

YS: The economic downturn did not change my thinking; it exposed companies that were less prepared and consequently suffered more and some went out of business or needed government bailout (*e.g.*, GM and Chrysler). Companies that had good visibility into their supply chain and good collaborative relationships with their trading partners were able to recognize the magnitude of the slowdown faster than others and were also able to recognize the recent demand pick-up better than others.

Companies that had lean supply chains were not caught up with a lot of excess inventory that tied up cash and therefore did not need as much credit, which, at times last year, was difficult to come by.



The credit crisis that was part of the financial crisis added a special dimension of procurement and supplier choice considerations. For example, the trade-off between having a single supplier and multiple ones changed. Before the crisis there were many good reasons to limit the number of suppliers and go to a single supplier, one of which was that by concentrating the volume with a single supplier the company was a large customer of that supplier and got more attention, access to innovation, etc. With the financial crisis, it turns out that you cannot squeeze suppliers for which you are a big customer since they will fail and leave you stranded…

KQ: Over the last decade we have experienced numerous high-profile, large-scale operational failures due to, for instance, acts of terrorism, IT failures, natural disasters, labour disputes and pandemics. Considerable effort has been made to improve organizational resilience. What lessons about resilience—if any—do we seem unable or slow to learn?

YS: The overriding lesson that companies are not learning is that investment in resilience and risk management is an on-going process, not a one-time event. Clearly, companies get ready for Y2K, for the Avian Flu, but when the event is over, risk management and preparations go down in the priority list. It may be natural, but few companies are ever-vigilant. Many companies took specific actions, but it is clear that as the immediate threat passes or events fade from memory, so do preparations.

KQ: What impact will fuel price fluctuations have on global supply chain management?

YS: This is a tough issue. As the price goes up, remote outsourcing locations become less attractive and near-outsourcing locations, such as Mexico for the U.S. and Eastern Europe for Western Europe, may see an increase in outsourcing activities. Most experts agree that in the long run the price trend is up, but it will and does fluctuate. These fluctuations can be dealt with through hedging, but this is always a bet, which may help or hurt the bottom line.

KQ: Cases of piracy have been receiving increased attention. How serious is this threat to North America's global supply chains? What should companies do? What should governments do?

YS: Piracy is still a very small phenomenon compared to the volume of goods flowing over the high seas. It is still something that companies can insure against and it does not cause companies to miss deadlines or be out of stock. Governments are doing the right thing by patrolling the dangerous waters of Somalia, as the declining number of successful cases of piracy seems to indicate.

KQ: In *The Resilient Enterprise* you noted that government interventions during crises can often magnify problems. How can governments improve their responses to crises?

YS: I am not sure this can be done. Democratic systems are particularly bad at emergency response since they involve a lot of posturing and worry about who gets the credit for what. (Think about the U.S. Congress.) Some of the best response happens under less democratic regimes. For example, one of the best responses was that of Pakistan to the 2005 earthquake—ending up with efficient supplies of emergency material and solid organization of many aid agencies and foreign government help.

KQ: Former U.S. Secretary of Homeland Security Michael Chertoff has said that cyber security is his greatest short-term concern. President Obama's Administration seems ready to increase the profile of cyber security as a primary security concern. Is this warranted?

YS: Yes, it is warranted. Not only because we would like our email and Facebook to keep working. The main problem is that many physical facilities, such as the electrical grid, dams, traffic lights and even medical procedures are operated remotely using Internet Protocols in increasing numbers. A cyber attack can create real havoc in many systems that advanced societies rely on.

As the immediate threat passes … so do **preparations**

Democratic systems are particularly bad at **emergency response**

Plan Ahead

Public Safety Canada focuses on CI vulnerabilities caused by increasing interdependencies

by Nicole McDonald

Suki Wong

The future of critical infrastructure will be characterized by greater interdependence among countries and across sectors. The (draft) *National Strategy and Action Plan for Critical Infrastructure* was designed in anticipation of such a future, and provides a foundation on which to build trusted partnerships capable of managing emerging risks and supporting the information requirements needed to protect vital networks and systems.

These were among the key themes presented by Suki Wong, Senior Director with the Emergency Management and National Security Branch at Public Safety Canada (PS). Wong delivered the message to an audience of academics and practitioners at the CIP Initiative Workshop, *Exploring Risk Governance*, held in Halifax on October 30.

The security context dictates that organizations responsible for critical infrastructure (CI) must be able to exchange sensitive information with confidence, Wong stressed. With this in mind, the Canadian government strengthened the safeguards for protecting sensitive information shared by private sector CI owners and operators with the federal government. She highlighted the 2007 *Emergency Management Act* (EMA), for instance, which resulted in amendments to the *Access to Information Act* (ATIA). Information now provided to government from third parties concerning their systems and networks related to emergency management planning is exempt from disclosure under the ATIA, she noted.

While PS is quick to point to the EMA as a success in this regard, it recognizes there is still work to do. This exemption from disclosure currently applies at the federal level only. PS therefore plans to work with other levels of government to ensure reasonable policies, standards and procedures are in place to ensure information can be shared with other jurisdictions without inappropriate disclosure.

While protecting information is crucial, so too is the need to share information with stakeholders in a timely fashion, Wong noted. PS aims to disseminate CI information quickly and broadly, avoiding 'classified clearance' when it is unnecessary. In a follow-up conversation with the editor of *The CIP Exchange*, PS staff confirmed the department's efforts to enhance its online presence and to provide 'single window' web access to Government of Canada information regarding CI. This new 'one stop' site will be the focal point for unclassified information for PS's portfolio partners.

Additionally, PS plans to improve the quality of information by ensuring that international events, for instance, are interpreted more effectively for a Canadian audience. A pipeline bombing in Afghanistan, or any other country, is noteworthy within the security realm, Wong noted, but what does it mean for Canadian CI owners and operators, in particular?

Organizations responsible for critical infrastructure must be able to exchange **sensitive information** with confidence

Wong underscored that the combination of protection measures and improved information-sharing mechanisms will make the task of managing and mitigating risks more successful.

There will also be institutional changes. The government plans to establish sector networks for each of the 10 critical sectors identified in the plan. Similar to the approaches taken by the United States and Australia, sector networks will provide a formalized and consistent structure for information-sharing, she noted. Membership will be voluntary, but PS anticipates that it will include representation from private industry and different levels of government.

These networks will be reinforced by a national cross-sector forum, which will identify priorities and address vulnerabilities caused by inter-sectoral interdependence.

Each sector network will follow a systematic three-pronged approach. First, each sector will identify risks, which may or may not be unique to that sector. Second, the sectors will undertake risk assessments to prioritize their collective efforts. Finally, risk profiles will be developed to inform action to address those risks.

Wong recognizes that that this will be a difficult undertaking, but with government working closely with all the sectors and jurisdictions, stakeholders and academe, the outcome will be more successful.

To download an audio recording of Suki Wong's talk, please visit our website or click here.

To read more about the Draft National Strategy and Action Plan, visit the PS website (publicsafety.gc.ca) or click here.

Nicole McDonald is in the second year of the MPA program at Dalhousie University.

CIP Initiative's Second Workshop

By Kevin Quigley and Ron Pelot

Theme: Exploring Risk Governance: Assessing and Managing Complexity, Uncertainty and Interdependence in Critical Infrastructure

October 30, 2009,
in Halifax, Nova Scotia

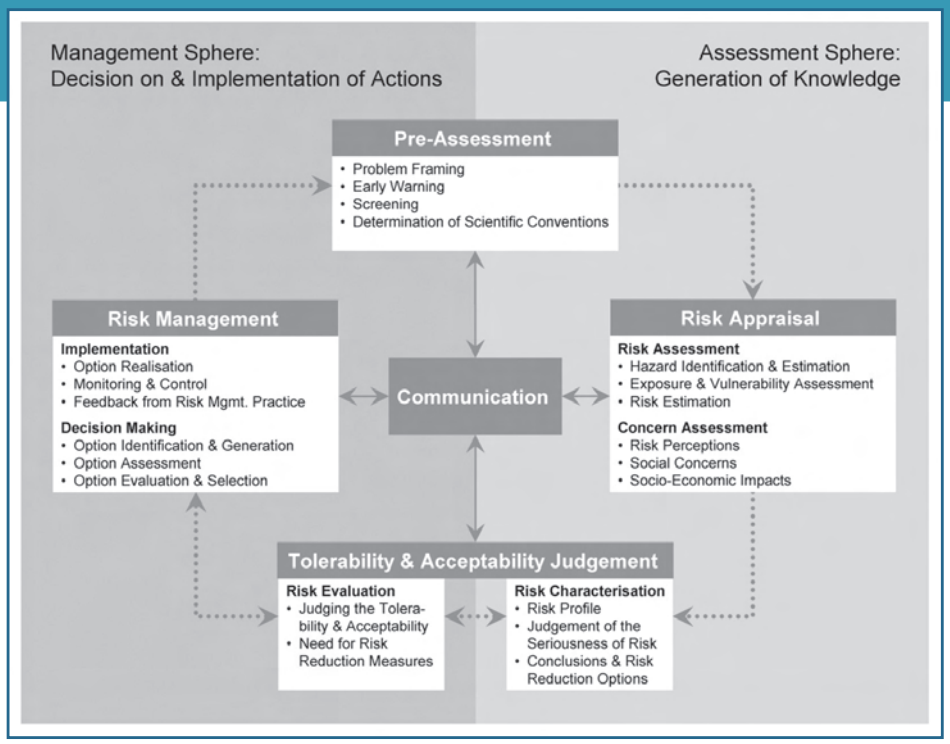
Rationale for the Workshop

Critical Infrastructure Protection—activities that enhance the physical and cyber security of key public and private assets—is garnering increased attention among governments and industry stakeholders largely due to the complexity and interdependence of the sometimes fragile systems upon which we rely. Failure in one system can have a cascading effect; it can cause multiple, simultaneous failures across industries and sectors. There is no single authority to take a binding risk management decision; instead the nature of the risk often requires collaboration and coordination between different stakeholders. The challenge is not merely a technical one. There are many social, legal, business and environmental obstacles that impede successful management of critical assets. These challenges require imaginative solutions that take a broad approach to understanding and managing risk.

Goals of the Workshop

- Create a cross-sectoral and cross-jurisdictional space in which participants can access and share diverse and expert perspectives on protecting critical infrastructure and explore technical as well as managerial issues.

- Employ the recent International Risk Governance Council Framework to



International Risk Governance Council Framework

Source: Renn and Walker (2008), *Global Risk Governance: Concept and Practice Using the IRGC Framework*. Dordrecht: Springer. Chapter 1, Page 59. Reproduced with kind permission from Springer Science and Business Media.

provide a coherent structure to the workshop while at the same time examine and test the utility of this new framework. (See figure above.)

- Focus on understanding the nature and characteristics of different risks and threats to critical infrastructure and examine distinct and appropriate approaches to managing them.

- Consider future prospects for shared dialogue and collaboration on this subject.

Format

The workshop started with a keynote address by Suki Wong from Public Safety Canada. From there, the day was divided into four stages, each reflecting one part of the International Risk Governance Council Framework: (1) Pre-assessment; (2) Risk Appraisal; (3) Tolerability and Acceptability Judgment; (4) Risk Management. Stages one, two and four were presented as panels. The panelists each started with a brief presentation. The moderators then facilitated a discussion between the panelists and the audience.

Stage three was presented as breakout sessions. Participants joined one of three groups. Once the breakout sessions were over the workshop reconvened, at which point the individual groups reported back on the discussions to the entire workshop.

Audience participation was encouraged at all stages of the workshop.

The Audience

The audience at the workshop included academics, as well as public and private sector representatives that have an interest in and/or responsibility for managing and securing critical infrastructure.

The workshop was designed to allow for a broad and divergent discussion. The format—keynote, panels and breakout sessions—organized along the lines of the IRGC framework, and coupled with an audience drawn from academe as well as the public and private sectors, lent itself to a lively exchange of ideas on the subject.

Some Observations

Participants contributed numerous observations about risk governance and CIP. We offer five separate observations here. For us, they were the points that stood out most prominently, and related also to some of our own work. We do not suggest this list is exhaustive, and we encourage everyone to read the more extensive articles on the different stages prepared by the workshop rapporteurs.

IT Security: Laying the Groundwork for a More Informed Response?

"Half a fence is no fence at all," one person commented. In other words, partial security measures leave the system vulnerable. If one chooses to secure systems, however, the security measures can be expensive to build *and* maintain. At the same time, the IT context suggests so many vulnerabilities that it is simply not possible to protect all systems completely.

Some prioritization and risk assessment are therefore required. New technologies will be untested, and prone to operational failures and security lapses. Older systems will succumb to inventive hackers or human, if not technical failures. What likely emerges is a tiered approach to managing risks associated with systems. In short, we must protect mission-critical assets, and accept greater risk exposure to secondary systems. Mission-critical assets will still be vulnerable, of course. We must therefore be careful to interpret early signals of security lapses and commit to a meaningful learning

Risk appraisal should incorporate **social** concerns

process with appropriate institutional support for it.

This can start at the top. One of the oft-cited failures in the management of Y2K, for instance, was the lack of executive level leadership on the IT issue. CIOs were rare in the early to mid-1990s. As a result, management boards were often not well informed about Y2K. This contributed to, at times, overreaction, and at times, underreaction to the problem.

A cyber security czar can help to bring some perspective to the top as well as mobilize some resources and a coherent strategy. Placing security responsibilities with one person can also help to clarify the person's responsibilities. In contrast, asking one person to focus simultaneously on IT innovation *and* security potentially gives them competing priorities with no roadmap.

The new U.S. Administration is building up the capacity for cyber security leadership at the White House. If this position and the associated office takes hold and shows some success, it might be difficult for Canada to resist creating a similar position, not least due to coordination issues between the two governments.

Integrating the Social and Technical: Two Solitudes?

CIP often focuses on protecting the built environment without explicitly incorporating the human element into the assessment or solutions. When people are included in the evaluation procedure, it is typically as a formal measurement, such as in lives lost, injuries or people displaced. On a different front, significant attention has been paid to improving emergency response in recent years through better communication, planning, information use and coordination, to name a few thrusts. The focus of such initiatives is primarily concerned with addressing people's needs in the aftermath of a major incident.

The workshop encompassed both perspectives, as the stage two panel comprised leaders in each of these facets of CIP. Excellent discussions ensued, but it was apparent that there is little overlap between these two spheres of dealing with disasters. One could argue that this is not only to be expected but also fitting, for a number of reasons. Protection can be viewed as dealing with the "upstream" phases of detection, interdiction and target hardening, while the focus on people is paramount for the response and recovery phases. Furthermore, a broad holistic model does not always lead to better insight, nor sufficiently pointed preparatory actions.

However, the dichotomy can also engender serious impediments to effective CIP. For one thing, the risk appraisal step should incorporate social concerns, as illustrated in the IRGC model, and typically would benefit from input by diverse stakeholder groups, not just the regulators or owners of the infrastructure. While this principle is well known, it is not often put into practice. However, there are other more subtle interactions between these arenas. People are not just entities to be protected; they play a complex interactive role in CI protection and response. They volunteer during emergencies, with their skills, energy and goods. Pervasive communication devices and social media (e.g. Facebook, Twitter, YouTube) are playing an increasingly important role in disseminating crucial information in emergency situations, whether it's danger detection, situational developments or tracking of individuals, as well as improving collective responses.

Bridging groups or programs that are focused on their respective technical or social aspects of risk management would benefit the field tremendously through more effective use of resources dedicated to CIP and improved consensus on prioritizing the risks we face while developing more resilient systems and populations.

Partial security measures leave the system vulnerable

Risk Tolerance: The Holy Grail of Risk Governance?

Few had problems understanding the importance of determining risk tolerance, nor did they struggle to enumerate the reasons why it is so difficult to articulate in a coherent way. Several social, political, psychological and economic factors were identified as constraints acting against our individual and/or collective ability to determine a stable solution for risk tolerance.

In light of this fact, public administration scholars might argue that clearer accountability for managing certain risks is an appropriate halfway house. In short, while it may not be easy to determine tolerance, we should make it someone's job to determine appropriate levels of risk tolerance and then hold them to account.

While the tendency to develop clearer rules and accountability may be in the DNA of bureaucracies, it does not provide a fully satisfactory answer. As noted at the outset of this article, risk governance refers to risks for which "there is no single authority to take a binding risk management decision; instead the nature of the risk often requires collaboration and coordination between different stakeholders."

Some flexibility and learning seem to be required. More scenario planning in the boardroom and emergency management drills on the ground may help. These exercises provide potentially important opportunities for developing a shared understanding of threats and opportunities, and how best to respond to them.

The Aim of Risk Management: Normalize or 'Shock Therapy'?

Many noted that formal risk management is often neglected; people pursue it for a time, and then competing priorities overtake it. While an institutional presence—such as a risk management committee armed with a risk management strategy—may help to keep the subject on the radar, there is likely more to it.

Many suggested that risk must be incorporated into policies and practices throughout the organization; staff must be trained and aware of their roles, for instance. In short, risk management must be integrated into regular planning, not treated separately or left to one organizational unit.

There are many advantages to this integration strategy and, in particular, the ability to perhaps get away from template-driven risk management, in which risk becomes a somewhat surreal management process driven by the functional authorities and not by operational realities.

> What we understand to be a risk is **directly** related to what we value

Ironically, we may not want to become too comfortable with our risk management plans. As Cultural Theorists[1] would remind us, what we understand to be a risk or danger is directly related to what we value. Both of these concepts—risk and value—are functions of organizational culture. These concepts are not easily detected, yet they are pervasive. Often organizations select specific risks to manage, yet overlook others. In large bureaucracies, for example, risk management often means responding to risks with more regulations and subdivision of tasks. The opportunity costs of these decisions are often neglected. A shock to the system, or an outsider's perspective, can help to bring blindspots such as these to our attention.

The IRGC Framework: Using it in Different Ways

The IRGC framework was a useful way to organize the workshop. Most panelists and participants stuck to the script, discussing (more or less) the stages at the appropriate time. The IRGC figure published in the program acted as a 'cheat sheet' that helped to remind people of the key points at each stage. The survey data from the participants seem to confirm that there was a high level of satisfaction with the framework: 82.6% of those asked agreed that it was helpful for the discussion of CIP (see page 8).

As a learning and planning tool, this framework can be used differently from the way in which we used it, notably with the following variations. First, we could use one problem in particular and examine it through the four stages, engaging multiple stakeholders in the process. (Indeed, the framework was seemingly designed for this purpose.) Second, and relatedly, participants could be provided with more data, possibly in advance, in order to generate a more informed dialogue among participants. Publishing background information on each subject planned for discussion, and distributing such a document in advance would likely be helpful. Third, we covered a lot in one day, but the benefits could be greatly enhanced with more time to elaborate on certain aspects. The tolerability and acceptability breakout discussions, in particular, raised a number of interesting questions that were worth pursuing further. For instance, if we met once a week over a three-week period, we could capture and benefit more from our collective learning over that period, resulting in stronger and better informed discussion as we worked our way through the process.

For more information on the IRGC and Ortwin Renn, the framework's author, see page 17.

We would like to thank sincerely all panelists, participants and rapporteurs for engaging with us on these important subjects on October 30. We hope you found it rewarding.

Kevin Quigley and Ron Pelot are the principal investigators of the CIP Initiative at Dalhousie University. Comments welcome at cip@dal.ca.

[1] See, for example, Douglas, M. (1982), *In the Active Voice.* London: Routledge; Douglas, M. (1992), *Risk and Blame: Essays in Cultural Theory.* London: Routledge.

Survey says...

By Judy Baroni

Workshop participants were employed largely in the public sector, including organizations that manage publicly-owned infrastructure. There was some representation from the private sector. From academe, there were faculty members and graduate students.

The School of Public Administration surveyed workshop participants at the end of the workshop. Of the approximately 50 participants, 23 completed surveys. We obtained these results.

Will you be able to apply ideas from today's workshop to your workplace situation?
Yes: 86.9%

Was the IRGC framework helpful for today's discussion of CIP?
Yes: 82.6%

Overall how would you rate your satisfaction with today's CIP workshop?
Very Satisfied: 47.8%
Somewhat Satisfied: 47.8%

Would you recommend this workshop to a colleague?
Yes: 95.7%

Do you use other CIP Initiative products?
Yes, or plan to in the future: 68.8%

Would you be interested in attending future workshops hosted by the CIP Initiative?
Yes: 91.3%

Judy Baroni is a research assistant at the School of Public Administration, Dalhousie University.

WORKSHOP SESSIONS

Stage 1: Pre-assessment

By Trevor Fowler

PANELISTS:

Dwight Fischer, Dalhousie University
Ben Sapiro, TELUS Security Labs
Nart Villeneuve, Munk Centre for International Studies, University of Toronto

MODERATOR:

Kevin Quigley, School of Public Administration, Dalhousie University

The first stage of the workshop examined the pre-assessment phase of risk governance, focusing in particular on the emerging cyber security landscape.

Dalhousie CIO Dwight Fischer outlined the often competing priorities in the university IT environment: the need to secure often highly sensitive data with the need to support an open and decentralized culture that resists heavy-handed regulation. 'Cloud computing' has only added to the complexity, he noted, making potentially crucial data even more difficult to protect.

Ben Sapiro asserted that cyber risk assessment should be framed as a business problem informed by hard data rather than a technological problem.

Cyber risk assessment should be framed as a business problem

He cautioned that most people have only a rudimentary understanding of risk, and that we need to work harder to develop more sophisticated means of measuring and explaining security risk to businesses. Citing evidence from a recent TELUS-Rotman survey, he noted that over half of the respondents did not consult a security professional in building their business systems; 74% reported issues with spyware and malware (though only 3% reported sabotage); and 40% did not believe a background check was necessary for new employees, yet government has reported that 30% of its IT risks originate from people inside the organization.

Participants came from the public and private sectors

Nart Villeneuve contrasts those who frame the cyber threat environment as a pending 'Armageddon' with those who wilfully neglect to address even the most basic IT security practices, believing them to be unnecessary. The truth lies somewhere in between, he noted. Indeed, threats are often not elaborate, external attacks on infrastructure, Villeneuve said, but rather, sustained, low-level attacks to gain critical information about systems and organizations' reactions to attacks.

Like the other panelists, Villeneuve stressed the importance of understanding the vulnerabilities inherent in distributed, interdependent IT systems. He warned that more sophisticated hackers exploit trusted relationships as a means of infiltrating systems; the hackers intercept and corrupt emails between trusted colleagues, for instance. The current climate requires more international institutions to which academics can report security breaches when they are discovered, he noted.

The session included several interesting exchanges. Sapiro, for instance, argued that one need not concern oneself with a hacker's motivation; it can often be an unnecessary distraction. Rather, one should focus on addressing the vulnerability in one's system. Villeneuve disagreed. He argued that motivation tells us what the hackers will do with the compromised data—a key insight, he suggested.

Drawing from the current debate over the need for a 'cyber-czar' in the U.S., the notion of a Canadian cyber-czar drew mixed reviews. Some noted that we should focus on policies that keep pace with changes in technology and security realities. There was also disagreement on the role of standards and regulations. Some argued that clearer regulations enable more effective management; others argued increased awareness is the key.

Ben Sapiro

For those awaiting a 9/11-type cyber attack, again, the participants were not convinced. They noted that poor IT security practices cost us every day, but doubted there would ever be a cyber security event on the scale of 9/11 to crystallize for lay people the seriousness of the issue.

Trevor Fowler is in the second year of the MPA program at Dalhousie University.

Most people have only a **rudimentary understanding** of risk

Stage 2: Risk Appraisal

By Reama Khayat

PANELISTS:

Benoît Robert, Centre risque et performance, École Polytechnique de Montréal
John Webb, Nova Scotia Emergency Social Services

MODERATOR:

Ronald Pelot, Industrial Engineering, Dalhousie University

"The only thing harder than preparing for an emergency is trying to explain why we didn't," noted John Webb of NS Emergency Social Services. In a short sentence Webb captured the complexity and importance of risk appraisal.

The lunchtime panelists combined their expertise to provide technical as well as social insights into the challenge of understanding and responding to cascading infrastructure failures brought about by systems interdependence.

Understanding interdependencies in critical infrastructure requires different types of information, Benoît Robert noted. Robert's research centre is therefore developing flexible mapping tools that integrate both broad analysis and precise information requirements in order to facilitate a multidisciplinary approach based on collaboration by multiple stakeholders.

Researching in the field has significant challenges, he noted. Acquiring and integrating confidential data has risks. A leak can bring about liability issues for those who acquired the data and potentially threaten healthy market dynamics; businesses consider information to be a source of competitive advantage and could suffer significantly if strategic information were released to the market. Proper analysis and communication are also crucial; we have to be careful to avoid the dangers of using poorly interpreted data. This raises the question of who assumes the cost of acquiring, managing and updating critical information.

> "The only thing **harder** than preparing for an emergency is trying to explain **why we didn't**"

Robert also emphasized people's tendency to ask for and gather information perhaps too indiscriminately, which creates a sort of data excess. "Too much information kills information," he stated, highlighting the need to identify only good information that is worth analyzing. Dr. Robert concluded that governments should clearly specify and justify information requests when seeking to understand systems interdependence.

John Webb underscored the importance of forming strong partnerships with those who know what is happening on the ground in emergency management operations. He highlighted the province's successful relationships with the Red Cross and the Salvation Army, citing their ability to work effectively with the most vulnerable.

Both Webb and Robert agreed that the protection of critical infrastructure is much higher on the priority list for many stakeholders than it had been formerly. With some irony, Webb admitted that emergencies—such as 9/11, Swiss Air, Hurricanes Juan and Katrina as well as the more recent H1N1 Pandemic—help keep critical infrastructure protection on the radar.

For Webb, emergency response is about protecting people and keeping them safe before, during and after emergencies. Yet people have different expectations, which governments have not always been adept at predicting. "The two major concerns for many people after disasters are pets and meds," he noted. This realization led to the establishment of the Disaster Animal Response Team, for example. Having dealt with over 70 midsized emergencies, ESS benefits from lessons learned. "We're getting good because we've made a lot of mistakes," Webb conceded.

Reama Khayat is in the second year of the MPA program at Dalhousie University.

Stage 3: Tolerability and Acceptability Judgment

Breakout Session One

By Reama Khayat

LEAD:

Wayne Boone, Norman Paterson School of International Affairs, Carleton University

Participants agreed that both tolerability and acceptability were dynamic concepts. Organizations should strive to determine a working standard for risk tolerance and acceptance, but they should also remain flexible, recognizing that as circumstances and experiences change so too will the perception of the consequences of operational failures. External stakeholders can also exert more influence on issues as they gain traction; this introduces new perspectives that must be accommodated.

Participants suggested that most organizations place more emphasis on those things that are concrete and measurable in risk appraisal. As the risks begin to influence the strategic mission of an agency, however, the less tangible aspects—the ethical, social and political dimensions—have more influence in our understanding of the risk.

Organizations should strive to determine a working standard for **risk tolerance** and **acceptance**...

Sessions had a mix of professors, graduate students and practitioners

For most of the session the group considered whether risk assessments are simply superficial 'checklists' or something more probing. Checklists can offer a false sense of security, one person noted; regulatory compliance conducted through a checklist, for instance, fails to encompass our full understanding of security and risk management.

Participants agreed that learning through different risk processes and events informs our willingness to accept and tolerate risks. This gave way to a more rigorous examination of what separates 'lessons learned' from 'lessons identified.' Participants were concerned that organizations tend to place more emphasis on the identification rather than the application of lessons. Most agreed that a meaningful learning experience can only be achieved through iterative processes of analysis and application, considering the lessons from multiple perspectives.

Reama Khayat is in the second year of the MPA program at Dalhousie University.

Breakout Session Two

By Jared Abbott

LEAD:

Jim Bruce, SAIC

Participants noted the value of cost-benefit analyses as a starting point for prioritizing risks and determining trade-offs in risk decisions. Still, such tools have limitations. The value of non-quantifiable aspects to individuals' lives (happiness, well being, etc) is not necessarily integrated into cost-benefit analyses.

The group discussed the extent to which people's perception of risk can be influenced by such factors as control, gender, media, culture, region, rumours, age, life experiences and feelings of private emotional anxiety. Several examples were discussed.

Helplessness and pessimism were also considered. Participants noted that the complex and interconnected nature of modern society can lead to feelings of helplessness in attempting to manage risks. This, unfortunately, can lead to a failure to act, which in itself is a risk. Indeed, opportunity costs are often neglected in risk analysis.

Our willingness to help others in danger can also depend on the amount of risk voluntarily taken on by the individuals in danger. Miners trapped in a mine may elicit more sympathy than hikers who have lost their way on a trail. This distinction has specific implications; some would suggest that the hikers be held liable for the search and rescue costs, whereas many would agree that the miners should be compensated for their pain and suffering.

Failure to **act** is in itself a risk

The participants extended the analysis to contrast personal with organizational risk. Individuals may not see much risk in contracting H1N1, for instance, but their sickness can pose significant risk to their organizations if they spread the illness among their colleagues.

Given all these considerations, the group turned its attention to risk thresholds, focusing on the question of how one establishes appropriate standards. The group discussed the importance of increasing participation in the consultation process as a way of securing more stable solutions. That disaster plans should use volunteers' input in creating plans as well as implementing them was offered as an example.

Jim Bruce leading the discussion

Thresholds must also be **adaptive**

Thresholds must also be adaptive, it was noted; they can change over time. For instance, the army once accepted 10% casualties during training, one participant noted; that is no longer considered acceptable.

Jared Abbott is in the second year of the MPA program at Dalhousie University.

Breakout Session Three

By Trevor Fowler

LEAD:

Andrew Hosie, Marsh Canada

Tolerability and acceptability constitute an organization's 'pain threshold', Hosie noted at the start of the session. Participants ranked numerous risks, measured by the risks' impact on an organization's ability to function. A tolerance scale with labels ranging from 'insignificant' to 'catastrophic' was provided as a tool to guide people's reasoning. The group considered power outages and employee health and safety practices, for instance.

Participants contrasted public-sector practices with those of the private sector. They suggested that private-sector organizations are likely to prioritize according to financial impact, which can include dollars, but also brand disruption, employee morale and health and safety. Public-sector organizations, on the other hand, often have to respond to situations that are crucial to the organization's mission but not easily translated into dollars, including broad social concerns and (sometimes fickle) public perception of risk management standards. Indeed, when risks cannot be easily translated into dollars, it can be difficult to achieve consensus on how to prioritize risks.

When risks cannot be easily translated into dollars, it can be difficult to achieve **consensus** on how to prioritize risks

A lively discussion focussed on the importance of dynamic models that can account for changes in risk tolerance over time. In some instances, the consequences of operational failures can change during the time of the failure. How long can an organization last without power, for instance? Without transportation? Without health care? Our capacity to tolerate these failures may change as the failure continues. Some participants contended that the dimension of time can be included on the tolerance scale noted above, associating increased duration with increased severity. Others were less sure. Some noted that risk events sometimes impact internal and external stakeholders differently, and that we often neglect this distinction in risk assessments.

Finally, Hosie stressed that when organizations engage in risk and tolerability assessments, they must establish a consensus with a diverse range of employees in order to avoid the sometimes narrow views put forward by homogeneous groups. Despite the inherent challenges in arriving at consensus on risk prioritization, Hosie underscored that it must be achieved within organizations in order to develop risk mitigation plans successfully.

Trevor Fowler is in the second year of the MPA program at Dalhousie University.

Public policy specialists exchange views with industrial engineers

Stage 4: Risk Management

By Jared Abbott

PANELISTS:

Andrew Hosie, Marsh Canada
John Parkin, Halifax Regional Municipality Police
Steve Snider, Halifax Harbour Bridges

MODERATOR:

David Stuewe, School of Public Administration, Dalhousie University

This session focused largely on how Halifax Harbour Bridges (HHB) manages risks. Steve Snider, General Manager and CEO at HHB, started by setting the context: 55% of HRM traffic crosses the two Halifax bridges; a catastrophic failure could take two to three years to repair.

In fact, the bridges routinely face many threats, from aging infrastructure, to naturally occurring events (e.g., weather), to person-made events (e.g., car accidents, deliberate acts of destruction).

As a result, HHB deploys several risk management strategies. They range from mundane acts, such as posting warnings about weather concerns, to more dynamic ones, such as continuous training and relationship building with stakeholders. Information-gathering is crucial, Snider noted. Bridge patrols, weather stations and CCTV cameras were all cited as tools HHB uses to inform their approach to risk management.

Snider also noted the importance of bringing in outside expertise. With this in mind, HHB contracted with Marsh Canada to review HHB's risk management practices.

Andrew Hosie, who worked with HHB on the review process, reinforced Snider's view; Hosie noted potential risks at HHB that were at times overlooked. He noted a possible risk associated with the bridge's salt supply, for instance, without which the bridges could not remain open in bad weather conditions.

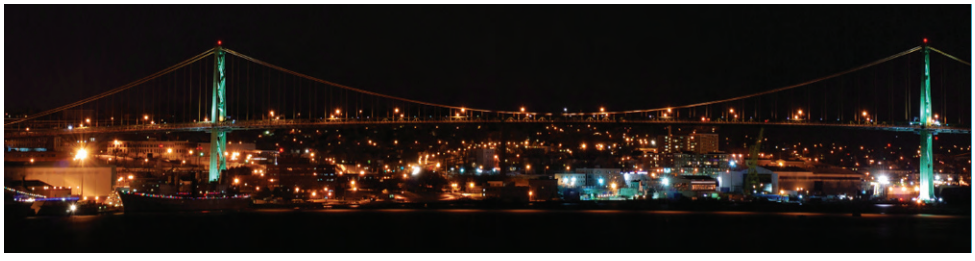
Hosie surveyed key HHB employees asking each to describe the operation of the bridge and to list possible risks. This exercise allowed Hosie and the HHB employees to develop 63 risk factors and scenarios, and ultimately generated a risk map of the top 20. The map helped decision-makers select optimal risk management plans for HHB.

John Parkin commented that risk management in a complex setting inherently requires trust in partnerships; these partnerships must be developed and maintained. He highlighted the value of conducting joint exercises with key partners in order to have a clear understanding of who is responsible for what in an emergency. He cited numerous learning experiences.

An audience member noted that one challenge with such emergency management drills is to ensure that there is some degree of spontaneity; over-rehearsed drills and including only the players with which the organization is already familiar reduces the effectiveness of the events; they can fail to capture the unpredictable element of emergencies.

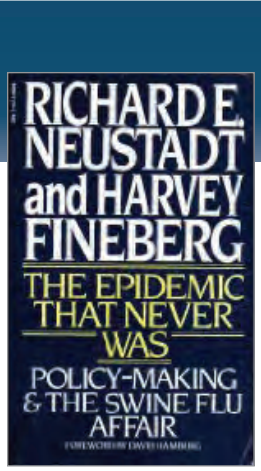
Two themes emerged strongly from the session. First, risk management should be integrated into the organization's culture, and employees must be encouraged to play an important role. Second, organizations must balance this integration process with a challenge function. Many agreed there is value to bringing a fresh set of eyes from outside the organization to offer some perspective on one's risk management plans.

Jared Abbott is in the second year of the MPA program at Dalhousie University.



BOOK Review

Reviewed by: Elisa Obermann



The Epidemic That Never Was: Policy-Making & The Swine Flu Affair

by Richard E. Neustadt and Harvey Fineberg

ISBN 9780394711478, Vintage Books edition published in 1983

Since the first known case in April 2009, swine flu (the H1N1 virus) has spread quickly: 3,764[1] hospitalized cases in Canada and 503,536[2] worldwide. Media coverage has painted a controversial picture: long lines for vaccines, vaccine shortages and waste, potential hospital bed shortages, two-tiered service delivery, body bags shipped to aboriginal communities, and a problematic relationship between the H1NI vaccine and the seasonal flu shot. Yet the media coverage itself has been criticized for its failure to place the story in its appropriate context. Experts agree, for instance, that there will be more deaths this year caused by seasonal flu than by H1N1. In short, uncertainty abounds. Key questions remain. How should governments respond to pandemics? And how, in particular, should they react to this media coverage?

There may be some merit in looking to the past for some answers. Indeed, flu virus scares are not new to governments in North America. In their book, *The Epidemic that Never Was: Policy-Making and the Swine Flu Affair*, Richard E. Neustadt and Harvey Fineberg detail the failings of the United States government's approach towards a suspected swine flu outbreak in the late 1970s, and in so doing draw some significant lessons that may be useful today.

How should governments **respond** to pandemics?

In early 1976, several isolated cases of swine flu were identified on a U.S. military base. These cases very quickly prompted executive level policy decisions and a sizeable inoculation program to combat a flu that never materialized. The result: significant drain on the public purse, liability issues, a skeptical public, vaccine side effects that included Guillain-Barré Syndrome (a disorder causing paralysis) and, ultimately, the termination of the U.S. swine flu immunization program.

Neustadt and Fineberg provide a compelling narrative of the events. They suggest that several forceful actors from a handful of government agencies led the charge to begin a sweeping national immunization program based on meagre evidence and little awareness of the possible effects of such a program. The government was highly reactive; it did too much, too quickly, they suggest. More evidence and analysis over time were needed, rather than proceeding to the 'nuclear option' as quickly as the government did. Neustadt and Fineberg also suggest that rather than acting purely in the public interest, many decisions were motivated by government's concern over being portrayed as hesitant and weak by the media.

Despite the government's mistakes, some aspects of the response were promising. Mark Moore from the Kennedy School of Government at Harvard University, for instance, has suggested that the speed with which the policies were adopted and the operation mounted was an impressive example of prompting inert bureaucracies to act in a time of perceived crisis.[3]

We must remember the potentially harmful consequences of **overreaction**

There are some limitations to comparing this case with the present day. While media may be more present

[1] Public Health Agency of Canada. (2009). Summary of FluWatch Findings for the week ending November 7, 2009. Retrieved from http://www.phac-aspc.gc.ca/fluwatch/09-10/w44_09/index-eng.php

[2] World Health Organization (WHO). (2009). Pandemic (H1N1) 2009—Update 74. 13 November 2009. Retrieved from http://www.who.int/csr/don/2009_11_13/en/index.html

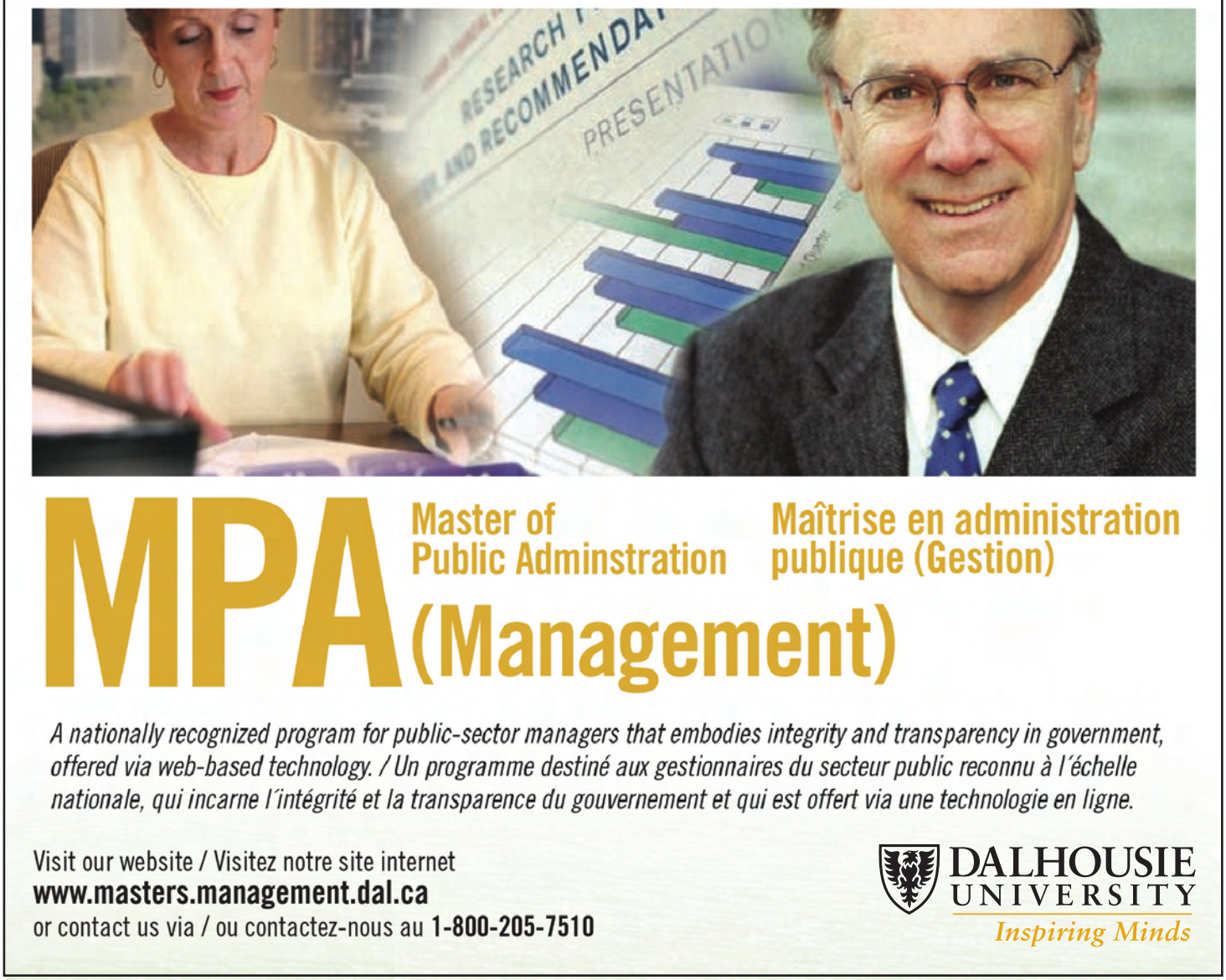
[3] Moore, M. (1995) *Creating Public Value: Strategic Management in Government.* Cambridge: Harvard University Press.

today, governments generally are more sophisticated in their communication strategies; overreaction strictly to satisfy a hungry media seems short-sighted and arguably less likely. Moreover, organizations such as the World Health Organization might be more successful than before at acting as a check against any one government's (over)reaction.

Overall, Neustadt and Fineberg emphasize the value of sequential decision-making and the potentially detrimental effects that the media, fear-mongering and even individual personalities can have on policy-making. Through their analysis the authors underscore the importance of using a comparative and logical approach to determine the value of different courses of action. They also provide an approach for communicating flu risk with an eye to not arousing public fear unnecessarily and understanding the limitations of medical opinion.

Dealing with potential emergencies is a very tricky business. This book, published over 25 years ago, provides important lessons for policymakers. Although underreaction can present a risk to public health, we must remember the potentially harmful consequences of overreaction also.

Elisa Obermann is a recent graduate of Dalhousie University's Master of Public Administration program.



The International Risk Governance Council

Excerpts From the IRGC Website

The International Risk Governance Council (IRGC) is an independent organization whose purpose is to help the understanding and management of emerging global risks that have impacts on human health and safety, the environment, the economy and society at large. IRGC's work includes developing concepts of risk governance, anticipating major risk issues and providing risk governance policy recommendations for key decision makers.

IRGC focuses on emerging, systemic risks for which governance deficits exist and aims to provide recommendations for how policy makers can correct them. Many of these risks are complex, uncertain or even ambiguous. In most cases, the potential benefits and negative side-effects interconnect.

IRGC believes that by combining forces governments, academia, industry and international and large non-governmental organizations can together develop and implement the best options for governing global risks through coordinated and coherent policy making, regulation, research agendas and communication.

For more information on the IRGC visit its website (irgc.org) or click here.

Ortwin Renn, Author of the IRGC Framework

Ortwin Renn

Ortwin Renn is a professor and chair of environmental sociology and technology assessment at Stuttgart University. He has published over 250 articles and 30 books. His honours include an honourary doctorate from the Swiss Institute of Technology (ETH Zurich), the Distinguished Achievement Award of the Society for Risk Analysis and an Outstanding Publication Award from the American Sociological Association for the book, *Risk, Uncertainty and Rational Action*, which he co-authored with Jaeger, Rosa and Webler.

For more information on Professor Renn visit his website (http://ortwin.gingedas.net) or click here.

AG's Audit of Public Safety Canada

The November 2009 report of the Auditor General of Canada includes a chapter on emergency management and Public Safety Canada. To obtain a copy of the audit visit the AG's website or click here.

Financial support from the Canada School of Public Service to conduct this work is gratefully acknowledged. The views expressed in this publication are not necessarily those of the Canada School of Public Service or of the Government of Canada.

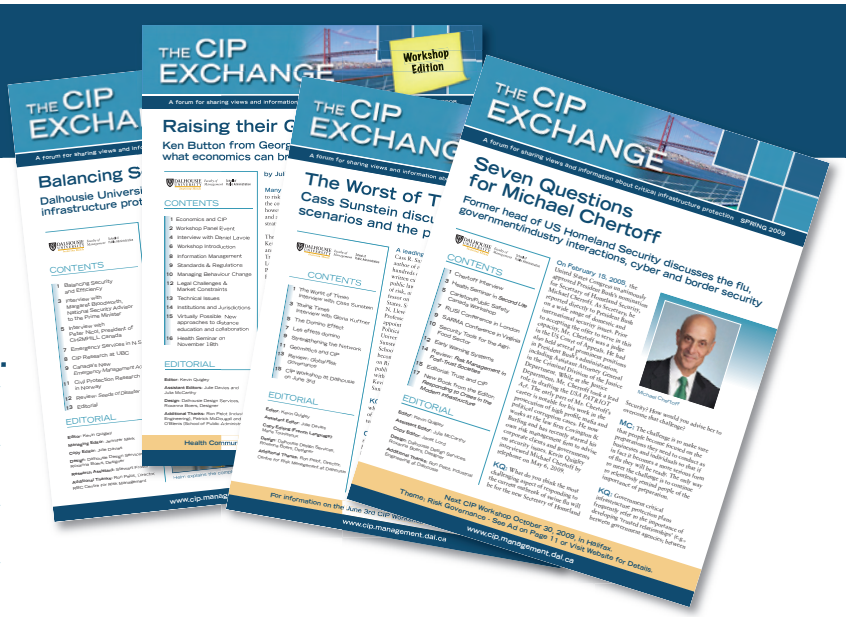
Sponsored by:

CANADA SCHOOL OF PUBLIC SERVICE
Your Partner in Learning

The articles contained in this publication were prepared by their authors who are solely responsible for their correctness and appropriateness. The views contained in this publication are attributed to their authors and not to this publication, Dalhousie University or the Dalhousie School of Public Administration.

Critical Infrastructure Protection at Dalhousie

BRIEF SUMMARY



THE CIP EXCHANGE

A semi-annual publication featuring . . .

- Interviews with leading commentators
- Research and event updates
- Workshop proceedings
- Book reviews and more

WHAT IS THE CIP INITIATIVE?

A national dialogue about how best to protect Canada's critical assets.
It includes:

- Panel events
- Workshops
- Second Life seminars
- On-line directory of experts
- On-line database of key publications NEW

Don't miss what's critical. Join the dialogue today.

CIP@DAL.CA

www.cip.management.dal.ca