

# The Art & Science of Resilience

Presentation to DRIE  
Ottawa – December 7th, 2011

# Introduction

- Part 1 – Albert will talk about emergency evacuation and emergency contingency planning
  - Part 2 – Steve will discuss ‘understanding the client’ and how that guided our methodology
  - Part 3 – Ian will discuss the BIA and BCP
- Using relevant parts of several approaches resulted in a best of breed approach and hopefully, outcome



# Case Study

- Public Space
- Critical Infrastructure
  - National Monuments & Icons\*
  - Showcase for Canadian and global culture & heritage
  - Tourists, schools, families & VIPs are frequent visitors
- Major events close to Museums
  - Canada Day, Blues Fest...
- Major Exhibits – high value, one-of-a-kind
- Global media interest
- Complicated building designs
- Complicated supply chain
- Two sites in two different provinces



*\* In some countries, this is a separate CI Sector. In Canada, it comes under the “Government Sector”*

# Context – Evacuation Planning

- Transition from Fixed Point to Zone Coverage
  - Plans existed, but they needed to be challenged and updated
  - Management Priority – Visitor, employee, contractor & volunteer safety
  - Visitor Services want the experience to be positive
- More efficient use of Security and Host resources



# Challenges

1. Dynamic Floor Loading
2. Public and non-public spaces
3. Vastness – time and space



# Egress

1. Determining number of employees needed
2. Designing safety & flexibility into the system
3. Moving meeting points – why?
4. Returning after the incident



# Business Continuity - Art & Science

- Challenges
    - Busy people
    - Multiple planning requirements
    - Low tolerance for safety and security risk
  - Satisfactory vs. Optimal solution
    - Plans are useable “out of the box”, and are tested, maintained and adjusted when the environment changes
    - Processes are repeatable and sustainable with CMCC resources
- Maintaining preparedness is one step on the journey to having high quality plans and procedures, so that visitors and asset owners have total confidence in the CMCC Team



# Understanding the Operating Environment

- Why is Client doing BCP? Business driver(s)...
- Where is the organization on its business process capability maturity evolution?
- Risk exposure of assets and organization
- Existing resilience
- Project Environment
- External Environment...



# Design guided by Client's context

- Appropriate data gathering techniques
  - Questionnaires, surveys, one-on-one interviews, workshops...
  - Quality of legacy documents
- Availability of, or capacity to introduce, automation support:
  - Feasibility of BCP being externally-hosted?
  - Automated notification process / software...
- Information & Reporting
  - Opportunities for validation - one final report or iterative reports
  - Audiences for reports & their needs
- Deliverables in both French and English
- Optimum use of visualization for time-sensitive responses (i.e., evacuation)



# Requirement

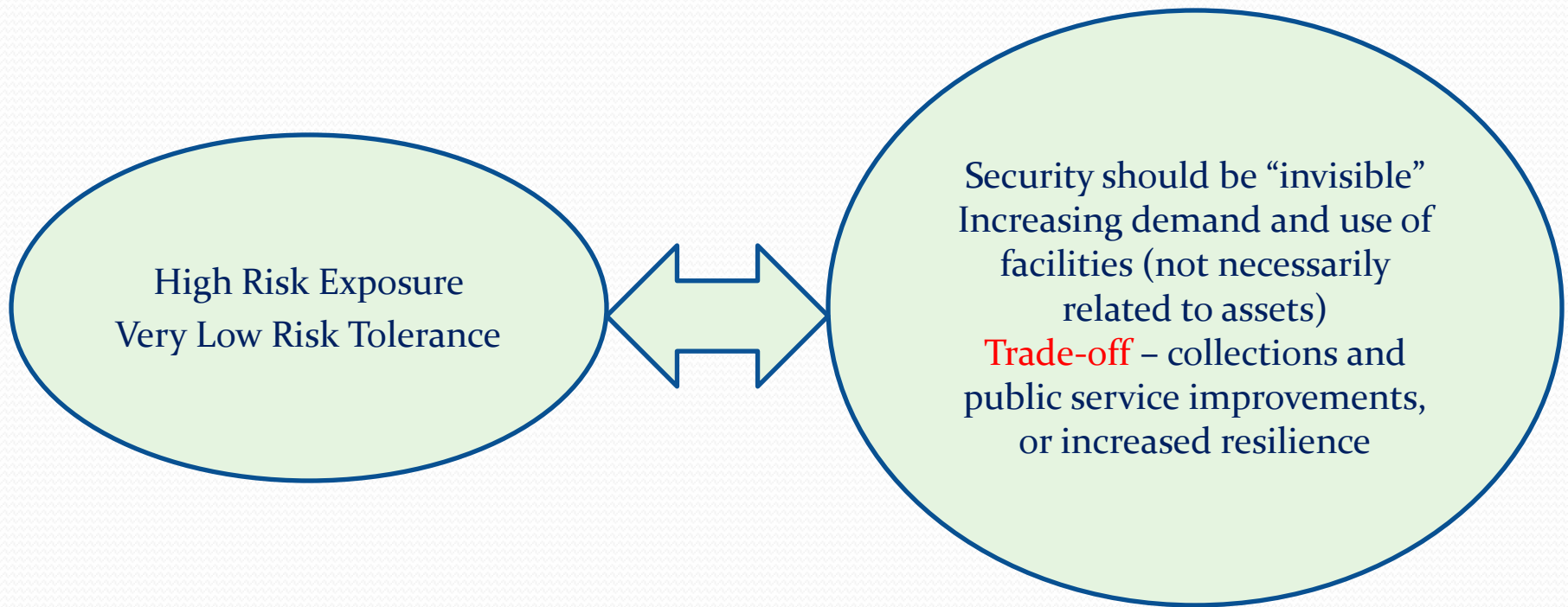
- Review and update evacuation, and emergency response plans (3 sites)
- Develop a CMCC BCP
- Specified timeline
- Reasonable time to develop proposal
- Site visits

# Response

- Able to propose a team-based approach with experience in risk, security (including physical, personnel, IT, and VIP protective services), emergency, continuity / disaster recovery and museum operations
- Able to include streamlined BIA/TRA as an integral part of process without jeopardizing the schedule or disrupting client workflow



# Decision Making Environment



# Stakeholder Analysis

- *Public (including children, families, people with special needs, schools...)*
- *First Responders (2 municipalities in separate provinces)*
- *Neighbours (including an industrial site)*
- *Dignitaries and VIPs (NCR – embassies, national & provincial associations)*
- *Partners (internal and external)*
- *Volunteers and part-time workers*
- *Asset Owners (e.g., private artifact owners / lenders, foreign institutions...)*
- *All levels of government (Federal, Provincial, NCC, Ottawa, Gatineau...)*
- *Local economy (business owners, transportation, tourism, hotels...)*
- *Media (all levels - local, national and international)*
- *Telecommunications and Internet Service Providers*
- *Financial and insurance service providers*
- *Investors, contributors*

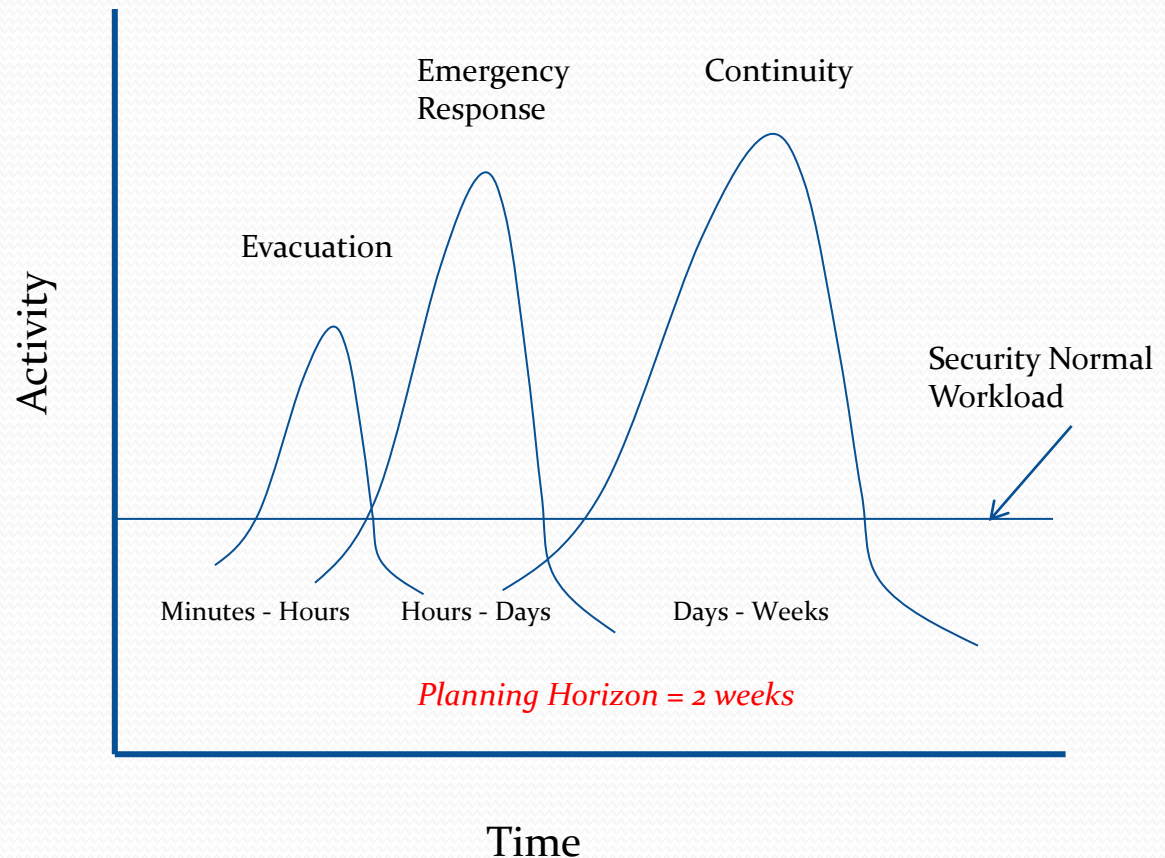


## Resilience / Escalation Concept

- **Evacuation** – pre-planned measures; automatic response; verbal direction; **Security Control Centre (SCC)** monitors situation; on-scene “commander”, until manager on scene; damage, hazard & risk assessment...
- **Emergency Response** – verbal direction, hazard, impact & risk assessment; if longer than 2-4 hours, **SCC controls response; may activate EOC** and shift work, etc...; EOC Commander keeps flexible; may have to delegate authority; keep COO and executive informed...
- **Continuity, Response & Recovery** – verbal direction; if consequence management longer than 2-4 days, could be written Incident Action Plan; ongoing risk assessment; suspend some services to create capacity; separation of duties – managing response and planning recovery in parallel; etc...

## Decision Making

- Time
- Resources
- Information
- Authority
- Gut feel
- Experience



# All Hazards BIA/RA Framework

- Decision Making
- Communications (Internal & External)
- Top 2 or 3 critical services; critical support services
- Loss of use of, or access to, facilities
- Loss of access to, or loss of, critical records, information and/or IT infrastructure
- Extended absenteeism (e.g., up to 35% of work force)
- Surge Capability (internal arrangements)
- Surge Capacity (external arrangements)
- Supply Chain Resilience

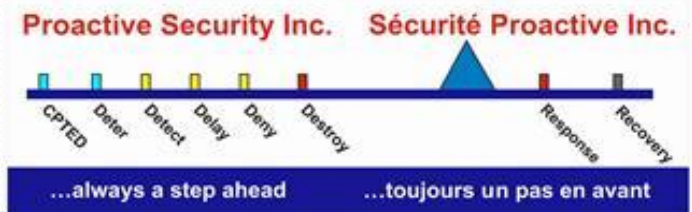


# Lessons Learned

- Understanding the context is critical
  - Being able to adapt methodology is important
  - Stakeholder analysis is an important aspect of BIA (e.g., to understand the supply chain and risk perception...)
  - Risk analysis should be an integral part of the BIA and BC/DR planning process
  - Common look and feel plans
  - Graphical plans for time-critical response
- Strive for excellence, not perfection



# Thank You - Questions



**Albert Bissonnette**

Security Management  
Security Risk Assessment  
VIP Protection  
Threat & Risk Assessments  
Major Events Security  
Business Continuity Planning  
Training & Communications  
Investigations...

**Ian Bayne**

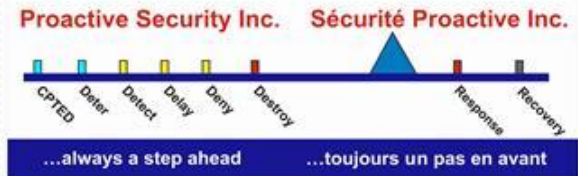
Risk-Informed Decision Support  
Capability Development & Gap Analysis  
Business Continuity Management  
Operational Readiness Assessment  
Critical Infrastructure Protection / Surety  
Strategic Planning  
All Hazards Risk Assessment Frameworks  
Incident Command System...

**Steve Ghadiali**

Business Impact Analysis  
Business Continuity Planning  
Enterprise Risk Management  
SWOT analysis  
Communications  
Governance & Strategic Planning  
Partner relationship management  
Automation support...

**Bob Marentette**

Security Management  
Decision Support  
Relationship Management  
Planning  
Relationship building  
Training ...



# Contact Information

Proactive Security / Sécurité Proactive Inc.

[www.proactivesecurity.ca](http://www.proactivesecurity.ca)

- Albert Bissonnette [ajmbissonnette@rogers.com](mailto:ajmbissonnette@rogers.com)
- Ian Bayne [irbayne@rogers.com](mailto:irbayne@rogers.com)
- Steve Ghadiali [steveg@smartdecisions.ca](mailto:steveg@smartdecisions.ca)
- Bob Marentette [rmarentette75@sympatico.ca](mailto:rmarentette75@sympatico.ca)

Telephone: 613 837-2173 Cell: 613 851-3171



# Terminology

## Evacuation & Emergency Response Planning

- Threat
- Hazard
- Vulnerability
- Plans focus on security (protection of people, assets & trust)
- Incident Command / Management System
  - Incident Commander
  - EOC Commander
- First Responders
- Critical Infrastructure Protection
  - Criticality Analysis

## Business Continuity / Resilience Management

- Risk-based gap analysis
- All Hazards Risk Management
- BIA
  - Critical Services
  - Critical Support Services
  - Minimum Acceptable Service Level
  - Normal Service Level (including peak periods)
  - Maximum Tolerable Downtime
  - Stakeholder risk perception
- BC – focus on services
- DR – focus on assets (e.g., IT, building operations)
- Organizational Resilience
- Surge Capability
- Surge Capacity
- Supply Chain



*Guideline: Use terms Client already uses; avoid jargon; use plain language. Many useful Resources [e.g., TBS/PS standards and best practices; Security Risk Management Body of Knowledge (SRMBOK, 2009); ASIS SPC-1 (2009) Organizational Resilience standard; CAN/CSA standards for risk, emergency & continuity management; ISO 27001/2 (IT Security & continuity); UK BSI 27999; benchmarks from other museums / art galleries...].*