Vancouver 2010 Olympics
Lessons Learned: Cyber

Robert Pitcher, Cyber Incident Handler
robert.pitcher@ps.gc.ca
Public Safety Canada
FIRST Conference
15 June 2011
Agenda

- Canadian Cyber Incident Response Centre
  - Roles and Responsibilities

- 2010 Games
  - Overview

- Olympic Exercises
  - Bronze, Silver, Gold

- 2010 GC Technical Working Group
  - V2010 Cyber Preparedness Report/Matrix

- CCIRC Readiness
  - Operational Rhythm
  - Incidents
Canadian Cyber Incident Response Centre (CCIRC)

- CCIRC is the national focal point for dealing with cyber based threats to Canada’s Critical Infrastructure.

- In 2010, CCIRC was focused mainly on federal government network protection.

- Provides stable, 24/7 coordination and support across the GOC, and to key national players in the event of cyber based emergencies

- National operations centre with the following mandates:
  - Reporting of real or imminent threats, vulnerabilities and incidents against the GOC
  - Threat and vulnerability identification and analysis
  - Distribution of cyber based publications (Alerts/Advisories/Cyber Flashes/Information notes)
  - Technical analysis, investigations, and coordination

- Supported by the GC Information Technology Information Management Plan (IT IMP)
CCIRC Partnerships

The Cyber Triage Unit (CTU)

- Led by the CCIRC, works to ensure a rapid and focussed response to a cyber incident.
- The CTU is responsible for the following:
  - Analysis of incidents and warnings reported from federal, national, and international sources;
  - Assessment of the nature of an incident to identify a primary department and support roles; and
  - Exchange of information between departments.

The international Community

- **Allies**: Close partners
- **FIRST**: Forum of Incident Response and Security Teams
- **IWWN**: The International Watch and Warning Network (Multiple Countries)
- **Objective**: International cyber community providing a global picture for threat identification, analysis and information exchange.

Other

- Provincial/Canadian Electrical Sector/Telecommunications/Banking
The Vancouver 2010 Olympic and Paralympics Winter Games (V2010) were held in British Columbia in February and March of 2010.

Approximately 6500 athletes and officials from 82 nations participated in 86 events in fifteen disciplines.

25,000 volunteers

6000 law enforcement, 5000 Canadian Forces, 4800 private security officers

119 agencies contributing police/peace officer from across Canada

43 days of aircraft patrol

205,000 accreditations (Olympic family, security workforce, VANOC, volunteers, etc.)
C&C: A complicated Affair...

Vancouver 2010 Integrated Connectivity Schematic
Key Stakeholders

Vancouver 2010 Key Cyber Stakeholders

DND
- Networks/Security
- Games Cyber Security

CCIRC
- GOC NOC
- Games Cyber Security

PS-GOC

VANOC
- Cyber Security (TOC)
- Information Security Manager

IC
- Networks/Security
- CTCP

Vancouver

SSBC CSC
- Service Desk
- Security Incidents
- Security Manager

EComm
- Service Desk
- Security
- IT Manager

ISP
- Telus, Rogers, Shaw, etc

BELL
- Games Security

Provincial

Federal

Limited Distribution

Industry

24h per day ops
CTCP / CTEPA
Service Contracts
Special Hosting Services
Wireless / Spectrum EMI issues
Incidents, threats and vulnerabilities sharing

Prepared by: Defence Research and Development Canada
Olympic Exercises

- The National Exercise Division of Public Safety Canada held three Olympic Exercises:
  - Bronze: Table Top
  - Silver: Validation
  - Gold: Confirmation

- These were large scale exercises involving both physical and information based assets and architecture

- Exercise Gold: 140 agencies, 45 coordination centres, 2000 participants

- Primary goal was to exercise incident identification, and reporting, to a centralized location for coordination and situational awareness

- IT IMP – Information Technology Incident Management Plan validation was primary deliverable
Lessons Learned: V2010 Exercises

- Cyber portions of readiness exercises need to be incorporated early
- Organizers concentrating on physical threats
- Education and understanding of the impacts of cyber issues for GOC and senior management
- Updating/Development of SOP’s/Annex’s for special events
- Departmental reporting procedures need to be validated before major events
- Exercise notes
  - Cyber based exercises require technical components
  - Coordination of exercise controllers key to success
  - Limit exercise to focused events (2 to 3 vectors)
IT Security Working Group

- Co-chaired by Public Safety, the Royal Canadian Mounted Police, and the Privy Council Office

- Membership included numerous federal departments with security or regulatory mandates relevant to the Olympics.
Lessons Learned: Working Group

- Limited success due to large size
- Critical time spent determining departmental roles/mandates
- Group eventually disbanded as an authoritative body
- Focus shifted to identifying key issues and gaps
- Departments surveyed to determine self-assessed readiness
- Result: Matrix showing Departmental Readiness in key areas
Goal: V2010 Cyber Security Matrix

Objectives:
- not a comprehensive technical review, risk assessment, or audit of IT security.
- goal was to provide departments with the framework to conduct self assessments
- designed to identify challenges and issues which could impact the ability of departments to detect and respond to serious cyber incidents during V2010.
Questions: V2010 Cyber Security Matrix

Questions designed to identify or characterize:

- critical tasks/mission areas
- most critical IT assets, services and information
- topology and host configuration information
- physical and network access management
- monitoring of hosts and links
- Monitoring of vulnerability releases, or regularly scans of assets
- patch management process
- virus scanner, host intrusion prevention system, vulnerability scanner, etc.
 Continued...

- Network zoning
- network operations centre, computer emergency response team, help desk (for points of contact)
- Process for review of logs and/or intrusion detection system alerts
- network geographic and physical deployment
- relationships with ISPs and vendors
- TRA status
- cyber incident management, accidental or malicious (including communication details with ISU, ISPs, others.)
Matrix Results

- Preparedness results grouped into categories:
  - Planning
  - Monitoring and detection
  - Reporting – horizontal alignment and coordination
  - Analysis of risk
  - Acceptance of risk/mitigation measures by senior management
Recommendations

- Incident reporting quick reference guide is essential.
- Teams should operate at a heightened state of readiness during V2010.
- Additional human resources must be identified.
- Must raise cyber awareness of CIOs and senior management of the key departments.
CCIRC: Operational Rhythm

- For the duration of the games, CCIRC was on an increased operational manning status

- Dedicated responders, technical support, and managers assigned to Olympic coverage, and vice-versa with regular operations

- 24 hour points of contacts with partner security agencies (RCMP/DND/CSIS/CSEC)

- International notifications of the upcoming Games

- Conference call with key stake holders three times a week
V2010 Incidents

- A copy of VANOC’s web site, hosted in a European country, leveraged interest in the luge accident to distribute a fake video CODEC malware. VANOC and CCIRC collaborated to identify and take down the perpetrating Ukrainian site.

- Search engine optimization (SEO) poisoning with Olympics themes was used to distribute malware/crimeware. VANOC identified this activity, resulting in a CCIRC cyber security awareness bulletin.

- Minor virus infections were reported and handled locally, but shared amongst stakeholders. Support was offered across organizations if required.

- There was rapid de-confliction of “cyber attack” reports, such as misinterpretation of the SEO poisoning events as actual attacks on the Games IT infrastructure.
General V2010 Lessons Learned

- Establishing trust and credibility
- Access to right subject matter experts (SMEs) key
- Not all levels of government have computer emergency response team capability
- Stakeholder buy-in varied (Private and Public Sector)
- Value of cyber information sharing
- Threat and risk assessments
- Minimize formal and complex audits