

National CIO Subcommittee on Information Protection (NCSIP)



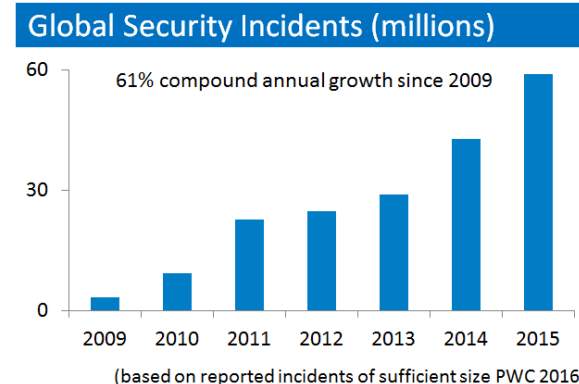
Gary Perkins, Chair



Key messages



- incidents are increasing in frequency and are more sophisticated and targeted than ever
- no organization globally is immune to attack
- organizations will be judged not only on their ability to prevent but detect and respond
- security is not just an IT problem, it's business enterprise risk
- security is a boardroom issue



Appointments



■ Chair

- Gary Perkins BC (incoming)
- Kent Schramm ON (outgoing)

■ Vice Chair

- Vacant (incoming)
- Grant Streeter NB (outgoing)

■ Secretary

- Martin Dinel AB (incoming)
- Grant Streeter NB (outgoing)

Meeting Updates



- Monthly teleconferences
 - very good participation
- In-person meetings
 - Fredericton (May 2016)
 - Edmonton (November 2016)
- Ask
 - ensure there is an NCSIP representative assigned (Nunavut does not have one, Quebec and New Brunswick are TBD)
 - encourage participation in monthly conference calls
 - support travel to in-person meetings

New Brunswick In-Person Meeting



- Shared Threat & Risk Assessment
 - sharing threat/risk assessments for Microsoft Office 365 (O365), Box, Android for Work
- Information Security Classification
 - exploring adoption of a common scheme or cross-mapping across Canada
- Cloud Security
 - dependence on classification
- Mobile Device Security
- Security Awareness
- Outsourcing / Vendor / Supply Chain Security
- Business Continuity and Disaster Recovery

Edmonton In-Person Meeting (future)



- Security Strategy
- Information Security Classification
 - cross-mapping jurisdiction classifications (done)
 - determine viability of common classification
 - at a minimum leverage cross-mapping
- Cloud Security
 - review results of Microsoft O365 risk assessment
 - review shared TRAs including Box, Mobile
- Digital Government
- Threat and Risk Assessment
- Threat Intelligence Sharing
- Passwords
 - inappropriate for remote access

NCSIP Sub-working Groups



- Investigations & Forensic
 - monthly teleconferences
 - share modern techniques and opportunities with evolving demands posed by investigations and forensics needs

- Security Awareness
 - meeting as required
 - continue to share successful education and awareness techniques, messages, and materials

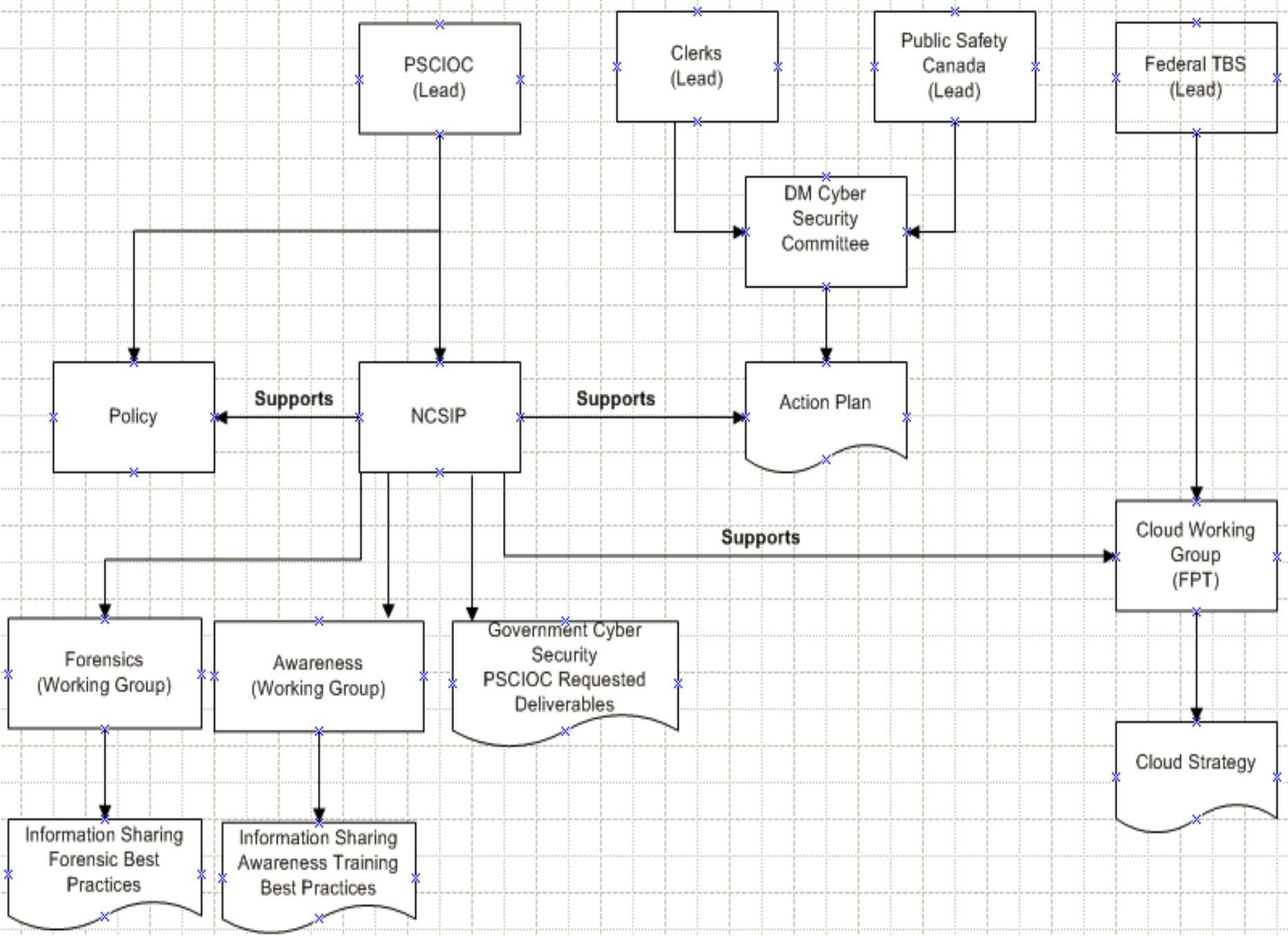
Discussion



- NCSIP recommends
 - centralized travel funding
 - centralized tools
 - collaboration, conference, email distribution
 - leadership training and development
- PSCIOC members
 - are your needs met?
 - do you require additional information or presented in different ways?

Questions?





2016 Cybersecurity Skills Gap

Too Many Threats

\$1 BILLION:

PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014¹

97%



BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY²

MORE THAN

1 IN 4



ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK³

\$150 MILLION:

AVERAGE COST OF A DATA BREACH BY 2020⁴

1 IN 2

BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES⁵

74%

BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM⁶

Too Few Professionals

2

MILLION:

GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019⁷

3X



RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14⁸

84%

ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED⁹

53%



OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES¹⁰

77%

OF WOMEN

SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.¹¹

89%



OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.^{12**}

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer-Member Study. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

