Presentation for the Pacific Northwest
Intergovernmental Audit Forum

IT Security Audits
The JUSTIN System

Addressing Reporting Risks

OFFICE OF THE
Auditor General
of British Columbia

Topic areas

- The JUSTIN System
  - What is JUSTIN?
  - What information is in JUSTIN?
  - What environment does JUSTIN operate in?
  - What did we report?
- Risk of Reporting
  - What were the issues around reporting?
  - What steps were taken to decide when to report?
  - What happened when we reported?

OFFICE OF THE
Auditor General
of British Columbia

What is JUSTIN?

Policing
Investigates crimes/ Recommends charges

Crown Counsel
Approves charges/ Prosecutes offenders

Judiciary
Schedules cases/ Tries cases

Court Services
Maintains court registry/ Manages and administers court documents

Corrections
Provides community supervision for released offenders/ Custody for serious offenders

OFFICE OF THE Auditor General of British Columbia

What information is in JUSTIN?

- Reports:
  - ongoing investigations and awaiting crown decision
  - awaiting trial, in process of trial, and finished trial
  - never tried and not guilty verdicts
- All criminal police investigations
  - Details of investigations
  - Accused, witness and victim contact information
  - Witness ‘Will Say’ statements

OFFICE OF THE
Auditor General
of British Columbia

What did we report?

Penetration Testing

- Gained access to JUSTIN information in other systems

User Access to Police Reports

- Over 3,330 users have access
- Users can print and save to external devices

System Security

- Firewall allows thousands of Non-JUSTIN users to reach JUSTIN
- Servers aren’t secured
- Unsecured computers are able to connect directly to the database

OFFICE OF THE
Auditor General
of British Columbia

What did we report?

Application, Database and User Management

- Downloads from the database can be made without detection
- Non-government computers can connect to the production database

Incident Detection and Response

- Proper detection and investigation of unauthorized access is not possible

OFFICE OF THE
Auditor General
of British Columbia

What were the issues around reporting?

Client Reporting Risks

- Witness safety
- Witness reluctance to testify
- Employee safety
- Increased hacker activity

OAG Reporting Risks

- Stress and anxiety of people involved in a legal case
- Public confidence in the judicial system
- Police confidence in record protection
- Inability to show wrongful disclosure

OFFICE OF THE
Auditor General
of British Columbia

What steps were taken in deciding whether to report?

System could become a target

- Critical security controls must be in place before reporting

Consider the potential risks of reporting that were not fixable

- System not properly secured for years
- Risks from previous slide –
  - Judicial integrity
  - Public confidence
  - Witness, victim and employee safety

OFFICE OF THE
Auditor General
of British Columbia

What steps were taken in deciding whether to report?

- Public report or In-camera
- Expert opinions:
  - Former special prosecutor
  - Police complaints expert
  - Law enforcement executive
  - Lawyer

OFFICE OF THE
Auditor General
of British Columbia

What happened when we reported?

- Reported January 2013 – regular media attention
  - To date, no negative effects evident
- Important to undertake:
  - Due diligence in assessing risks of reporting
  - JUSTIN was a high risk audit
  - JUSTIN experience is not a model for all IT security audits
  - IT security audits have different levels of risk
  - Each is considered based on its risk and profile

OFFICE OF THE
Auditor General
of British Columbia

Summary

Due diligence in addressing reporting risk:

- Report content and level of detail for the public report
- Risk of reporting analysis
- Clear and open communication with the client
- Seek the advice of experts
- Delay reporting to allow time for addressing critical controls
- Assess each report separately

OFFICE OF THE
Auditor General
of British Columbia