January 7, 2013

2013 Information Security Program for the BC Government

Ian Bailey, Chief Information Security Officer

Office of the Chief Information Officer

BRITISH COLUMBIA
Ministry of Citizens' Services and Open Government

Table of Contents

Office of the Government Chief Information Officer

Information Security Program

The greatest technology challenge facing organizations today is to keep the information in their care safe from any form of unwanted intrusion. This is certainly the case for the British Columbia government, whose priority is to provide needed programs and services to citizens everywhere in the province. Citizens want safe, secure online services they can access at their convenience, without fear of their personal information being viewed or acquired without authorization.

To meet this objective, government must also accommodate itself to the rapid and constant advances in technology that enable citizens to conduct both their personal and business activities on a variety of available mobile devices. Government workers would like to have more flexibility in their choice of work tools and to use the same or similar devices in the workplace that they use in their personal lives. The widespread availability of mobile technology also means that workers can experience more flexibility in their work arrangements. Government must balance all of these considerations.

The Information Security Branch within the Office of the Government Chief Information Officer views information security as an essential service delivery enabler – meant to ensure that business flows, and that the information within that business is protected. This 3rd Edition of the Information Security Program for 2013 outlines a four-year vision designed to support government's business objectives, while at the same time, improving the information security posture and risk management practice of the BC government.

The four enterprise security objectives identified in our 2013 plan are: Know threats and risks of the government information and infrastructure; Enable seamless protection over boundaries; Enable information-centric safeguards; and Enable a secure Open Government for improved citizen engagement. These four objectives are all delivered within the Information Security Branch's overarching tenet of continuous improvement of current information governance and protection of government information assets.

Sincerely,

Ian Bailey
Chief Information Security Officer

Information Security Program for the BC Government

Overview

Information management and technology play a crucial role in government service delivery. Protecting government information and supporting technology infrastructure is essential to government's operations.

The Information Security Program describes how information protection measures will continue to meet the security requirements defined in the corporate policy and the Information Security Policy.

The identified projects are the results of brainstorming sessions in the Information Security Branch and consultations with Ministry Chief Information Officers, Ministry Information Security Officers, Risk Management Branch, and branches within the Office of the Government Chief Information Officer as well as the analysis of corporate direction and technology advancement.

Vision and Mission

The Information Security Program is focused on achieving the following vision and mission of the Information Security Branch, Office of the Government Chief Information Officer.

Vision: Leaders in Information Protection – Security, Trust, Excellence

Mission: Enable Government to provide services in a trusted and secure manner

Principles

To meet the changing demands and protect government proactively against potential threats and vulnerabilities, the 2013 Information Security Program adopted the following guiding principles to define and implement its program:

Assume no trust on any network boundaries

The conventional concept of security perimeter is disappearing due to consumerization and the proliferation of powerful mobile devices. Security has been invested in the trusted internal network but there are no longer enough controls to filter out unauthorized devices on the internal network and the assumption of a trusted internal network is no longer valid. No trust on any network should be assumed and consistent controls for information should be applied.

Adopt an information-centric approach

Based on the zero trust idea, the centre of the protection is information, rather than network or servers. Information owners should identify and classify their information and apply proper controls, which can be transparent to the underlying network. Example controls for the protection of information would be encryption, traffic analysis with data loss prevention solutions, and virtualized access to information. On top of the current perimeter controls, these information-centric controls should be implemented.

Embrace security analytics

The threat landscape is changing rapidly due to sophisticated evolving and targeted attacks. It has become more important to understand the threats and have awareness of the vulnerabilities that exist within the government environment. The Big Data phenomenon improved tools for analytics and security should embrace this technology to better understand threats and vulnerabilities so that security can identify new threats earlier and provide the Chief Information Security Officer and ministries with the necessary lead time to address the new threats.

Changing demands and matured roles

The role of the Chief Information Security Officer is becoming increasingly strategic as enterprise security matures and security functions become more standardized and commoditized. A significant portion of government information management and technology services are being outsourced and effective governance over the outsourced services is becoming more crucial to the success of secure service delivery. The planned outsourcing of the operational information security will require the Information Security Branch to play a central governance role in the management of the government information security operations.

To proactively position itself, the Information Security Branch plans to transform the branch to the following direction:

From an IT-focused role to a mature business-driven discipline

The security organization is recognized as a strategic partner that manages the information risks. Nowadays, it is commonly accepted that security initiatives may not always have an obvious Return-On-Investment, but security investments can provide tangible benefits in risk reduction and regulatory compliance. This evolution means that executives view the

Information Security Branch as a mature organization, with established processes, technologies, and measurements.

From IT expert to business facilitator

As business begins to realize that it owns risks to its applications and infrastructure, it increasingly involves security as a business facilitator to help make the right decisions. *Research and consulting functions* are increasingly important in the corporation as functional and operational groups trust the judgment and respect the opinion of the Information Security Branch. Providing mediation between different functional groups is also becoming more important and appreciated.

From technology-centric to people-focused

Technology is necessary and important; however, it is no longer sufficient as the sole protection. User behavior analysis and metadata analytics are increasingly important. Information risk awareness is an important piece of the mandate of the branch. This transformation requires skills and abilities for risk analysis, incident management, compliance, and awareness communication.

From local security to global risk management

As business migrates to the Internet and Web 2.0 services rapidly, the security landscape is becoming significantly more complex. Local mitigation of security risks is not sufficient to protect government information and infrastructure. Collaboration with other jurisdictions and the private sector is becoming more important. Coordinated information sharing amongst other governments is crucial to identify potential risks and to respond to current attacks or incidents effectively and efficiently.

From invisibility to being in the spotlight

Due to high-impact security breaches and the compliance requirements from legislation and industry regulations such as FOIPPA and PCI DSS, information security is on top of the corporate agenda. Corporate executives need an awareness of current levels of security controls to steer government appropriately. The branch needs to communicate the value of information security to executives using the language of *good governance, regulatory compliance, citizens' benefits,* and *business impact*. Overall, this change results in more management visibility than ever.

Corporate Direction and Alignment

With three strategic documents *Citizens @ the Centre: B.C. Government 2.0, IM/IT Enablers Strategy,* and *Being the Best*, government has demonstrated its strategic direction, how it will conduct its business and how employees will perform their work. Creating an environment that protects government information and enables government to achieve these strategic objectives is a key responsibility of the Information Security Branch, therefore excerpts from these documents are included here to add context to the strategies and activities within the Information Security Program.

Citizens @ the Centre: B.C. Government 2.0 identifies three strategic shifts that government needs to make:

- Citizen participation: engaging British Columbians more directly with their government, particularly through improved access to government data and sharing of information.
- Self-service: expanding opportunities for citizen self-service by improving and modernizing the government's online service offerings so they are shaped less by the structure of government and more by citizen needs.
- Business innovation: taking a more corporate approach to technology planning and innovation for the benefit of citizens and public service employees.

The *IM/IT Enablers Strategy* was developed by the Government Chief Information Officer to support the vision of the *B.C. Government 2.0* defined above. Current version (v1.5) of the *IM/IT Enablers Strategy* defines seven primary enablers: Integrated Planning, Privacy and Information Sharing, Identity Information Management, Strategic Procurement, Network, Web 2.0/Gov 2.0, and Standards and Guidelines; and four underlying enablers: flexible work tools, hosting, information security and connectivity necessary to achieve the vision within *Citizens @ the Centre*.

Being the Best has been the human resource plan for government for years. Recently, the BC Public Service Agency published its sixth edition of the plan, which promotes cultural shift in three ways: becoming a workforce of trusted professionals that embraces open communication, a collaborative work environment, and flexibility and choice in work styles and tools; supporting the diversity, professional development and career aspirations of its employees; recognizing employees' safety, health and work-life balance have an important influence on their professional success and productivity. These shifts will achieve the three goals behind this plan - Building internal capacity, Managing for results, and Increasing our competitiveness - through lean thinking, the diversity strategy and the health strategy.

The *Being the Best* plan is well aligned with the strategic direction of *B.C. Government 2.0*: open communication, a collaborative work environment, and flexibility and choice in work styles and tools.

Information and technology management is a crucial enabler of the *B.C. Government 2.0* strategy and the *Being the Best* human resource plan. It is important for the Information Security Program to be aligned and tightly integrated with their strategic objectives and the *IM/IT Enablers Strategy*.

Current Information Security Environment and Trends

The security environment changes as technology and business requirements evolve. There are technologies mature enough to form a mainstream and drive service delivery restructuring. Recent surveys performed within the government information security community have confirmed major threats and opportunities from the technological and environmental changes.

Powerful mobile devices and BYOD Mobile devices are becoming powerful enough to replace some notebooks and desktops due to their mobility and convenience. This shift is also happening in the government work environment to meet flexible work options and increase productivity. Along with the positive impacts, powerful mobile devices also bring significant threats to the workplace since their operating systems and application consumption frameworks are not designed for the enterprise environment but for the consumer market. Many organizations are launching initiatives like Bring-Your-Own-Devices (BYOD). These initiatives are aligned with the trend that new information technology emerges first in the consumer market and then spreads into business organizations, which is called "consumerization". This trend is also accelerated by the desire to have one device to deal with personal and business issues with information segregation. This trend is becoming increasingly visible.

Cloud Computing Cloud computing has become a mainstream service delivery vehicle. As data sovereignty and security have been critical areas of concern for cloud computing, cloud service providers are focusing on providing solutions that support the legal and security requirements in the Province for cloud services. Private cloud has a long history in government; however, it does not provide the same financial benefits as a public cloud does. The pressure to migrate government services to public clouds as a significant cost-saving option is increasing. It is important for government to be ready for seamless migration to cloud environments.

Identity Information Management Online trust is a major issue for services on the Internet. The identity assurance mechanisms and authentication capability are key ingredients of online

trust. Such demands drive the need for a trustworthy identity information management mechanism. To respond to the demands, the BC Services Card will soon be available for citizens and high security credential services will be in place within government.

Targeted and Sophisticated Cyber Attacks Cyber attacks have become commonplace and the nature of cyber attacks has been elevated to the nation-state level. This reality drives the need for federal and inter-provincial level collaboration in cyber security intelligence and preparedness against potentially high-profile cyber attacks.

Open Government In terms of information management, open government initiatives bring changes in two main areas: open data and open information. Open data makes government-owned data available for citizens so they can add value by processing it, which can result in better use of the government data. Open information proactively discloses government business which can lead to a more transparent government. The BC government has been proactive in this movement and has demonstrated leadership in the Canadian public sector.

Flexible Work Style Government needs to be innovative to conduct more business with fewer resources and to provide more flexible work arrangements to enable the growth of internal capacity and competitiveness. This requires seamless connectivity to government information and infrastructure regardless of device, location and time.

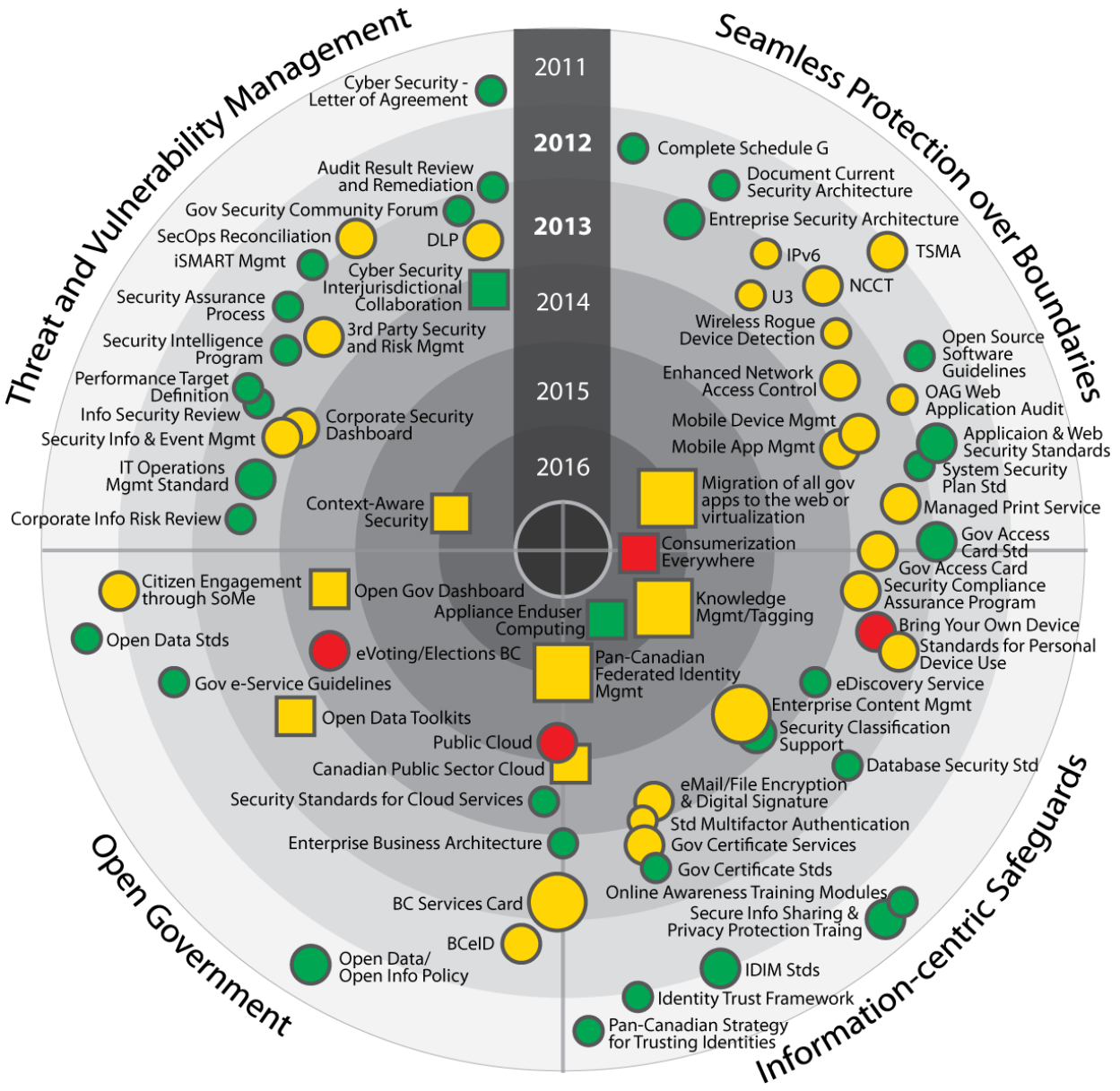
Four Enterprise Security Objectives

Based on a review of the strategic plan of the Office of the Government Chief Information Officer and the Ministry of Citizens' Services and Open Government, the Information Security Branch has applied the guiding principles and developed a set of four enterprise security objectives:

1. Know threats and risks to the government information and infrastructure.
2. Enable seamless protection over boundaries.
3. Enable information-centric safeguards.
4. Enable a secure Open Government for improved citizen engagement.

These four enterprise security objectives will be delivered with the Information Security Branch's overarching tenet of continuous improvement in government's information security posture.

To support the four enterprise security strategic objectives, the Information Security Branch has identified a series of internal initiatives to be undertaken in the branch or corporate initiatives to be supported by the branch. The coloured circles in Figure 1 represent such initiatives.



Enterprise Value
Enterprise value represents the potential benefits that can be derived. (circles: ISB action items, squares: items for anticipated deployment)

Deployment Risk
Deployment risk represents the likelihood of operational failure.

High Value | Medium Value | Low Value | High Risk | Medium Risk | Low Risk

Value is assessed by effect on expenditure, performance, availability, and functional benefits.

Risk is assessed by technical maturity, security vulnerabilities, architectural interoperability, and skill availability.

Figure 1. 2013 Information Security Program Activities

In Figure 1, each quadrant represents an enterprise security objective. Relevant activities and initiatives are shown in coloured circles in each quadrant in a chronological order. The squares indicate technological trends or services that government may adopt to meet its business objectives. Both circles and squares are shown in three different sizes depending on their values. The colour of the circles and squares represents the risk level of the activity or initiative, which is measured by technical maturity, security threats and vulnerabilities, architectural interoperability, and skill availability. This diagram shows activities and initiatives planned or performed between 2011 and 2016.

Planned activities and initiatives in each enterprise security objective are listed in the following sections. In the list, an item with "*"denotes a project directly supporting the *IM/IT Enablers Strategy*.

Know threats and risks to the government information and infrastructure

The level of security risks and threats around government is increasing as cyber security attacks are more targeted and sophisticated. Some of these attacks are allegedly sponsored by nation-states. The correct understanding and precise knowledge of the current threat and vulnerability level of government becomes more crucial than ever. Active monitoring, timely reporting and real-time adjustment capability of the information infrastructure and information usage is a key to improve the security posture of government.

The Information Security Branch needs to ensure active security monitoring and controlling capability and to develop governance tools to assure expected activities are happening.

The action items in support of this objective include:

- Develop a Security Assurance Process
- Develop performance targets for Information Security Review
- Develop a Security Intelligence Program
- Conduct annual Information Security Review
- Implement a Corporate Security Information and Event Management system
- Implement a real-time corporate security dashboard
- Manage the Corporate Information Risk Review process
- Reconcile the Security Operations capability
- Implement 3rd Party Security and Risk Management capability
- Implement audit result review and remediation capability

- Coordinate a government-wide security community forum embracing major IT alliance partners
- Support iSMART tool for government-wide security threat and risks assessments*
- Implement a Data Loss Prevention system*

Enable seamless protection over boundaries

Traditionally the network perimeter had worked as an effective security perimeter so that organizations had focused on the protection of this perimeter. Due to the rapid development of powerful mobile devices and business trends of consumerization, this perimeter is dissolving and becoming unclear. The protection requirements for the government information and infrastructure have not been changed. In the era of the dissolving boundary, the safeguards need to be more universal and transparent from underlying platforms.

The action items of the Information Security Branch include:

- Develop standards for application and web security*
- Develop a standard for System Security Plan
- Develop guidelines for the use of open source software*
- Develop a standard for the Government Access Card
- Support the implementation of the Government Access Card
- Work within the Office of the CIO on the Managed Print Service
- Work with Technology Solutions Division to implement the enhanced network access control capability*
- Work with the Technology Solutions Division to implement the mobile device management capability
- Work with the Technology Solutions Division to implement the mobile application management capability
- Support the development of a migration strategy to IPv6*
- Work within the Office of the CIO on the Telecommunications Services Master Agreement (TSMA)*
- Work within the Office of the CIO on the Network Communication and Collaboration Transformation (NCCT) project
- Document the existing information security architecture
- Develop the Enterprise Security Architecture
- Support Technology Solutions Division to securely implement the U3 project
- Support Technology Solutions Division for the implementation of the wireless rogue device detection capability*

- Complete Schedule G and its appendices
- Keep the Cryptographic Standards updated with newly emerging technology and business demands*

Enable information-centric safeguards

As the protection perimeter becomes unclear, the focus of the protection moves from the infrastructure to the information. Regardless of the device or end-user environment, it is important to provide consistent controls to protect government information. Identity and access are the foundation of the information-centric control. Also important are the classification of information and knowledge management in a corporate manner.

The action items in support of this objective include:

- Work within the Office of the CIO to develop the BC Services Card
- Develop the Government Certificate Standards*
- Work within the Office of the CIO to develop the Government Certificate Service
- Develop a strategy for implementing email and individual file encryption and digital signatures in conjunction with the government certificate service
- Support government's corporate multifactor authentication implementation in conjunction with the government certificate service*
- Work within the Office of the CIO to develop the Identity Information Management standards, processes and frameworks*
- Develop a security standard for the use and deployment of cloud services*
- Develop and implement the strategy (standards/guidelines) to support personal devices for work (Bring-Your-Own-Device - BYOD)*
- Support the public cloud computing initiatives*
- Participate in the development of the Enterprise Business Architecture
- Develop a strategy for eDiscovery service provision
- Work within the Office of the CIO to develop the Enterprise Content Management strategy
- Support ministries' information security classification implementation*
- Develop a Security Compliance Assurance program
- Collaborate with the BC PSA and relevant branches to educate staff on secure information sharing and privacy protection
- Develop online security awareness training modules
- Develop a standard for database security

Enable a secure Open Government

To meet the citizens' demand, government is making its services available online and increasing the availability of government-owned information to the public. Government releases information more frequently to promote transparency.

The Information Security Branch participates in the corporate initiatives implementing "Open Government" and looks for more opportunities around the BC public sector. To support this direction the Branch will:

- Work within the Office of the CIO to develop the BC Services Card
- Work within the Office of the CIO to implement the BCeID services*
- Work within the Office of the CIO to develop Open Data and Open Information Policy*
- Develop security guidelines for government e-Services*
- Work with Elections BC on electronic voting

Continuous improvement

The inclusion of continuous improvement as an overarching tenet of the Information Security Program is a recognition that effective security management is an ongoing process that adopts new advances and meets changing needs. Continuous improvement allows us to keep pace with the factors influencing the security and risk profile of government's information and technology management.

The action items in support of this objective include:

- Continue to deliver awareness events designed to create a common level of understanding and awareness of security threats, risks and mitigation strategies
- Continue to develop materials, tools and a support structure to assist Ministry Chief Information Officers and Ministry Information Security Officers in meeting government's information security goals and objectives
- Conduct information security audits as necessary
- Review the purpose and outcomes of annual information security review process
- Conduct security investigations
- Continue to work with Technology Solutions Division to support new and existing service delivery

- Continue to make recommendations for the ongoing improvement of government's security posture, based on the results of security and privacy investigations, security threat and risk assessments and security incidents

Information Security Branch
Office of the Chief Information Officer
PO Box 9412 Stn Prov Govt
Victoria BC V8W 9V1
Fax: (250) 387-3240
Email: CITZCIOSecurity@gov.bc.ca
Web: http://www.gov.bc.ca/informationsecurity