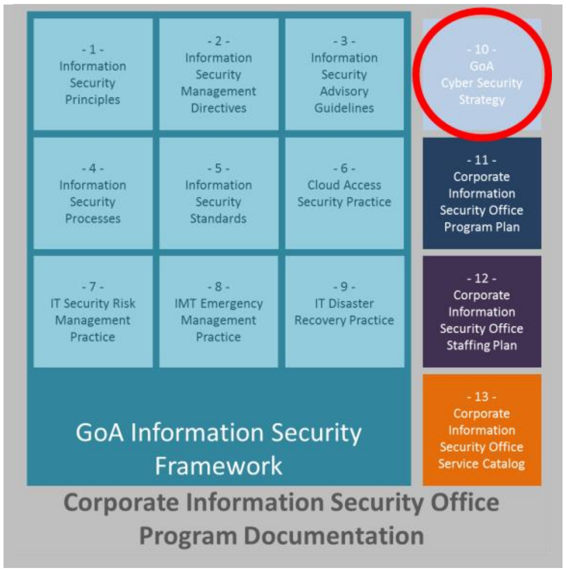
Corporate Information Security Office


- 1 - Information Security Principles
- 2 - Information Security Management Directives
- 3 - Information Security Advisory Guidelines
- 10 - GoA Cyber Security Strategy
- 4 - Information Security Processes
- 5 - Information Security Standards
- 6 - Cloud Access Security Practice
- 11 - Corporate Information Security Office Program Plan
- 7 - IT Security Risk Management Practice
- 8 - IMT Emergency Management Practice
- 9 - IT Disaster Recovery Practice
- 12 - Corporate Information Security Office Staffing Plan
GoA Information Security Framework
- 13 - Corporate Information Security Office Service Catalog
Corporate Information Security Office Program Documentation

Government of Alberta's Cyber Security Strategy

PROTECTING THE PROVINCE'S INFORMATION ASSETS

Public

Prepared by

Corporate Information Security Office
Service Alberta
Government of Alberta

Version 1.20

January 19, 2017

Message from the CISO

The prevalence of the Internet and the proliferation of web-based services have opened limitless opportunities for Albertans. We use the Internet, computers, cell phones and other mobile devices every day for personal or professional activities. A world without the Internet has become increasingly difficult to imagine – let alone living in one!

Cyberspace is the conglomeration of the Internet, all of its inter-connected networks, and all services and information made available through the Internet. Cyberspace offers many advantages, such as the ability to get information or services we require anywhere and anytime, or the ability to communicate with loved ones or colleagues over a myriad of channels as required.

Our quality of life is improved by these services; however, our increased reliance on cyber technologies has made us more vulnerable to attacks from faceless individuals who can potentially impact our lives from anywhere in the world, and often out of reach of any law enforcement services that could protect our rights as individuals.

The same data and devices that make our lives easier also make it easier for attackers to gain access to information that could impact or destroy our lives and the lives of our loved ones.

The Government of Alberta's Cyber Security Strategy is our plan for identifying, managing and responding to cyber threats. It is a cornerstone of the Government of Alberta's commitment to protecting the Province's information assets.

Martin Dinel, ISP, ITCP, PMP, CISSP
Chief Information Security Officer (CISO)
Service Alberta

Introduction

Cyber Security is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (*ref. Oxford Dictionaries*).

In response to the Office of the Auditor General's October 2008 report, the Executive Council and Service Alberta established a Corporate Information Security Office (CISO). The CISO was assigned the responsibility of overseeing all aspects of information security for the Government of Alberta's information and information technology systems.

The **Mission** of the CISO is to work in collaboration with ministries, public agencies and service partners to ensure that the Province of Alberta's information assets and services are secure, safe and resilient.

The Government of Alberta (GoA) recognizes that information is a critical asset and that the management, control, and protection of this information have a significant impact on services delivery. Information assets must be protected from unauthorized use, disclosure, damage, and loss; and must be available when needed, particularly during emergencies and times of crisis.

The GoA's Cyber Security Strategy sets priorities for how the organization can efficiently and effectively address the management, control, and protection of the Province's information assets. It also outlines the objectives that future initiatives will focus on and identifies necessary components to iteratively improve the security posture of the GoA.

The GoA's Cyber Security Strategy has a simple concept: Secure GoA information assets against cyber threats, increase stakeholders awareness to minimize the threat of social engineering and human errors, and implement monitoring and intelligence services to ensure that threats are identified and that information security controls continue to evolve to meet the ever evolving cyber threat.

Motivation

Cyber threats affect us all. Attackers with basic skills can cause real harm. Sophisticated attackers can disrupt anything from our utility systems, financial or economic systems, to telecommunication networks. They can interfere with the production and delivery of basic goods and services provided by both the public and private sectors. They undermine our privacy by stealing personal information.

Dealing with cyber threats in isolation does not work. The GoA's Cyber Security Strategy ensures that stakeholders, including Government organizations, service providers and individuals, work together to address the threats.

Approximately **350,000 public sector employees** access the Province of Alberta's information assets every day. (*ref. Statistics Canada website, Public Sector Employment for the Province of Alberta*)

Every year, the CISO detects more sophisticated attacks and attack sources than the previous year. Attackers are investing in their capabilities, and we respond by investing more in ours.

The GoA recorded **259 security incidents in 2015.** 58% of these incidents relate to lost or stolen assets, 10% to infected workstations, 9% to unauthorized access, 9% to suspicious traffic, and 8% to account breaches. Many security incidents are also prevented by **blocking around 90% of emails** received by the GoA yearly (500 million email messages per year). These emails are blocked either because they are identified as spam, or because of identified malicious content.

Strategic Assumptions

While we cannot accurately predict what cyberspace or cyber threats will look like in the future; we must seek to understand the forces that shape the future in order to lead, influence, and adapt to the evolution of our environment. The GoA's Cyber Security Strategy is based on the following assumptions:

- Increasing volume and sophistication of cyber-attacks demand heightened stakeholder awareness, secure technology implementation, coordinated threat monitoring and incident responses, tested critical systems resilience, and a professional and agile cyber security workforce.
- Deepening dependence on information and communication technologies creates opportunities for greater productivity and innovation, but it also increases the number of users, devices, data, and processes requiring protection.
- Globalization of information and communication technology transcends geographic and political boundaries, resulting in increased threats to information assets as these threats may come from attackers located anywhere in the world.
- The accumulation of data in the "cloud", combined with distributed systems and remote access poses further security challenges.
- Mobile technology increases the risk of exposing sensitive data and processes to attackers.
- Differences in security requirements and risk tolerance across organizations suggest that one-size-fits-all security approaches are less effective than risk-based solutions tailored to particular organizations.

Cybercrime is a growth industry with an estimated annual cost of **$445B to the global economy**. Costs relating to cybercrime in Canada represent 0.17% of the country's GDP; cybercrime costs in the United States represent 0.64% of their GDP (*ref. McAfee.com 2014 Cybercrime report*).

Understanding the Cyber Threat

Cyber Threat is a possible danger that might exploit a vulnerability to breach security and cause possible harm. A threat can be "intentional" – i.e. planned with the intent to cause damage – or it could be "accidental" – i.e. system malfunction, natural disaster or user error (*ref. Wikipedia*).

Various types of attacks and exploits can be used to gain access to information in cyberspace. For instance, attackers can exploit software and hardware vulnerabilities. They can also coordinate attacks called "Social Engineering" where attackers trick people into providing information by getting them to open infected emails or visit corrupted websites that infect their computers with malicious software. They can also take advantage of people who fail to use basic security practices such as using complex passwords, updating their antivirus, or using only protected wireless networks.

Once they have gained access to a system, attackers can steal or change information stored within the system, corrupt system operations, or program the system to attack other computers on the network. These attacks often result in identity theft or theft of personal assets.

In 2014, almost 15,000 Canadians were victims of **identity theft** for a reported loss of $74 million (*ref. Government of Canada, Canadian Anti-Fraud Centre website*)

While certain attack tools and techniques are more sophisticated or damaging than others, most cyber-attacks share four characteristics that account for their growing popularity. Cyber-attacks are often:

- **Inexpensive –** Many tools can be purchased for a low price or downloaded for free.
- **Easy –** Attackers with very basic skills can cause significant damage.
- **Effective –** Even minor attacks can cause extensive damage.
- **Low risk –** Attackers can easily evade detection and prosecution by hiding in a web of computers and exploiting gaps in legal systems.

Types of Threat

For the purpose of reporting and for awareness training, the GoA identified four categories of cyber threats:

Accidental

Accidental attacks are not intended to be malicious. They include systems malfunctions, user errors, natural disasters and other unexpected or unplanned events that may cause damage to or loss of information assets.

Yearly, approximately **200 security incidents** occur due to **user errors**. At a minimum, these errors result in an individual user's downtime and time spent by a support team in resolving the issue; other more serious incidents have resulted in data loss, compromised systems or unauthorized access to information assets.

Cyber Espionage

These attackers are normally well resourced, patient, and persistent. Their purpose is to gain political, economic, commercial, or military advantage. All organizations that have a presence in cyberspace are vulnerable to these types of attacks. Reports from across the world confirm that these attacks have succeeded in stealing industrial and state secrets, private data, and other valuable information. At times, cyber espionage can be used for military advantage, for instance, to sabotage an adversary's infrastructure or communication networks.

Cyber Terrorism & Hacktivism

Terrorists and activists are finding a niche in cyberspace. They are using the Internet to support recruitment, fundraising, and other propaganda activities. Hacktivists demonstrate their skills by defacing or taking down websites. Terrorists are taking advantage of the world's dependence on cyberspace as a vulnerability to be exploited. Terrorist cyber-attacks have the potential to morph into life-threatening attacks, for instance, taking control of emergency response, utility, or public health systems potentially endangering lives.

Cybercrime

Individual and organized criminals are taking advantage of the opportunities offered by cyberspace.

In the U.S. in 2010, approximately 5,600 robberies were perpetrated for $43M with 22% of the criminals being brought to justice and put in jail; in the same year, over **300,000 cybercrimes** occurred for a total of **$1.1B in damages** and only 0.5% of the cases being prosecuted resulting in less than 1/3 convictions (*ref. InfoWorld, January 2012*).

Criminals use or sell information stolen online, such as credit card numbers, computer accounts information, and malicious software designed to infiltrate or damage targeted systems. Even those who are diligent about practicing safe computing are at the risk of getting their information stolen through third parties they share information with.

Cyber Threat is Evolving

The average age of hackers dropped from 24 to **17 years old** in the past year (*ref. Mirror, December 2015*).

The evolution of cyber-attack tools and techniques has accelerated dangerously over the past few years. Attackers have found new ways to share information amongst themselves and have become better educated. This results in an increased level of creativity and agility that enables them to constantly find new ways of breaking into the most up-to-date security measures and technologies.

Protecting information in cyberspace is a constantly evolving challenge. To address this challenge, the Government of Alberta will continue to require a range of monitoring, responses, and awareness supported by continued investment in cyber security programs.

The Future We Strive For

Cyberspace is the online world of computer networks and the internet (*ref. Merriam-Webster dictionary*).

The GoA has the ability to influence what cyberspace will look like and how it will be used over the next several years. The CISO strives for an environment that is safe and secure. A cyberspace that offers opportunities to Albertans and promotes confidence in our Government's services.

The GoA's **Vision of Cyberspace** is one that supports secure, safe, and resilient systems while protecting privacy by design: a cyberspace that we can use with confidence to serve Albertans.

Cyberspace – and primarily the Internet – has transformed nearly every aspect of daily life. A trusted digital infrastructure will provide a platform for innovation, better communication, improved services, and more effective decision making. In order to realize the full potential offered to Albertans by the cyberspace, the GoA must ensure safety, security, and resilience of the environment while promoting cyber threat awareness and cyber security knowledge. This complex, resource-intensive effort will require substantial research, development, and investment, along with ongoing operational enhancements. The Cyber Security Strategy provides the foundation for those efforts.

In keeping with its Vision, the GoA is committed to creating:

A Cyberspace that is Secure

The GoA's IT infrastructure and systems must be secure and must protect information assets from damage, loss, and from unauthorized access or use.

A Cyberspace that is Safe

GoA's information and information systems must provide a safe environment for Albertans to interact with. Data integrity must be maintained within the systems, and data and systems must remain malware free. Secure and safe connectivity should be available from almost anywhere and anytime, ensuring user confidentiality while using online GoA services.

A Cyberspace that is Resilient

In the event of single systems or wide-spread disasters, critical systems and services to Albertans must remain available. In the event of loss of systems due to disaster events, all systems and data must be recoverable, and be restored in an organized and timely fashion.

A Cyberspace that Protects Privacy

The privacy of Albertans must be protected. Monitoring of the GoA environment must be focused on the protection and use of assets instead of user activities.

Guiding Principles

A **Principle** is a fundamental truth or proposition that serves as the foundation for a system of belief or behavior or for a chain of reasoning (*Ref. Oxford Dictionaries*).

The GoA is committed to protecting the Province's information assets and to providing leadership by ensuring that public sector organizations working with these assets have implemented adequate policies and controls to manage security risks.

The following three principles communicate the Government's expectations for Alberta's public sector organizations to be accountable for ensuring that the Province's information assets are protected using a risk-based approach.

As of December 2015, the GoA has a total of **19 Ministries** accessing the Province's information assets. There are also **over 300 Public Agencies** using subsets of the same information assets.

Principles

Adequate Information Security Policies and Framework

Public sector organizations must have appropriate information security policies approved by their management for protecting information and information technology systems. These policies must be communicated across the organization. They must be based on a generally accepted framework for Information Security such as ISO 27000. They must also identify the elements of the framework that are required for the organization based on factors such as the nature and size of the organization, and the complexity of their systems. The GoA's information security framework is based on ISO 27000.

Monitoring and Managing Information Security Risks

Public sector organizations must have a process to identify, monitor, and manage their information security risks. The complexity of this process will depend on the nature and size of the organization, and at a minimum, will require that the organization identifies its most important information assets; whether its security policy adequately protects those assets, and whether necessary controls have been implemented to protect those assets. This includes identifying systems or applications that are critical to the organization's operations and ensuring that all critical systems have Disaster Recovery Plans implemented and tested on a regular basis.

Reporting Information Security Risks

Public sector organizations must have a process to report the status of their information security policies as well as the status of significant information security risks to their Minister. These organizations should have an annual report that includes a copy of their Information Security Policy, evidence that the agency has implemented the policy, and an Information Security Risk Registry. Organizations must report security risks or incidents to their Minister upon detection, since a significant risk has potential to result in a significant security incident or breach that may affect public security, public confidence, or result in unforeseen costs. Ministers shall determine how reporting provided by public sector organizations will be used to supplement Information Security Risk and Compliance reporting that each Ministry provides to Service Alberta.

Purpose of the Principles

The Principles will be applied along with the Strategies defined in this document to ensure that the GoA provisions information and technology services that are secure, safe to use, and resilient, while protecting user privacy.

These Principles and subsequent implementation by public sector organizations clearly state an expectation by the GoA that each organization is responsible for risk assessment of information assets in its control, ensuring that adequate policies are in place to protect those assets (from a confidentiality, integrity and availability perspective) by using a risk-based approach, and reporting the status of significant security risks to the Minister.

Albertans will benefit by knowing that the Province's public sector organizations are accountable for protecting information assets and technology systems, and for ensuring that systems essential to delivering critical services will remain available or can be restored in the event of a disaster.

GoA's Cyber Security Strategy

The **Cyber Security Strategy** defines the high level approach that will be used to reach our Cyberspace and Cyber Security Vision while satisfying the CISO's Mission.

The cyber security landscape has changed drastically over the past few years. The rapid evolution of technology and the creativity and adaptability of attackers has made it increasingly difficult to protect information assets. A passive-defensive cyber security posture is no longer enough to protect against continually evolving cyber threats and attack methods. The GoA's Information Security environment must continuously evolve and adapt to the evolving cyber threat.

The approach used by the GoA to secure the Province's information assets is a proven standard approach:

- **Assess –** assess risks regarding assets;
- **Protect** – security controls are implemented based on assessed risks to prevent impacts to assets;
- **Detect** – monitoring controls detect when protection controls have been attacked or breached;
- **Respond** – plans, controls and tools are used to treat incidents and threats;
- **Recover** – recovery plans and tools are in place to ensure the organization can recover from attacks.

A risk-based approach to decision making is used to ensure that the right controls are applied in the right situations. Security personnel identify and assess risks, and provide this information to decision makers.

The GoA hosts **122 public facing websites** providing key services to Albertans. These valuable systems also pose a risk of being exploited by external attackers.

Strategic Pillars

The GoA's Cyber Security Strategy is built on three (3) strategic pillars:

Hardening of the GoA's Cyber Security Posture

Albertans trust that the GoA is able to provide them with services they need. They understand that the GoA requires their personal and corporate information to provide them with these services, and trust that their information will be protected against unauthorized access or changes, and against damage or loss. The GoA will implement the necessary measures and controls to ensure the protection of these information assets across the public sector.

392 of the business applications used by the GoA are classified as **Critical or Vital**, which means that disaster recovery plan have been prepared to ensure that they are recovered **within 3 days** of a disaster event.

Increasing Information Stakeholders Awareness

No matter what security controls or measures are in place, the main weakness of all information security programs is people. The best tools to mitigate this weakness are awareness and training. When people understand their role in protecting the assets, the value of these assets, and the continuous threat exposure relating to these assets, they start to understand the value of a security program.

To be successful, a security program must be given a high level of priority; to increase the level of priority, stakeholder awareness must start at the top of the organization.

Shifting Security Posture from Reactive to Proactive

The rapid evolution of technology and the increased creativity and adaptability of attackers presents serious challenges to security professionals. A passive-defensive cyber security posture is no longer enough to protect information assets. A more aggressive posture must be adopted to ensure threats are identified and dealt with before they become issues. Intelligence gathering and analysis is one of the most critical tools to accomplish this.

Specific Initiatives

Initiatives are sets of activities performed to achieve one or many objectives. Within the CISO, initiatives are managed as projects. Charters are developed outlining scope, objectives, deliverables, schedule, resources and budget. Status reporting mechanisms are established based on stakeholders' communication requirements.

The following CISO initiatives have been organized using the three (3) defined strategic pillars.

Hardening of the GoA's Cyber Security Posture

Initiatives under this strategic pillar are meant to improve the efficiency of security services and allow for user privacy. The CISO will formalize its services by streamlining, simplifying, and documenting its processes while setting expectations regarding its services by defining service level commitments. Roles and responsibilities will also be clarified and documented – for CISO specific roles and other stakeholders. Tools will be reviewed and assessed to ensure that the right tools are being employed and that tools that are not extensively used are decommissioned.

An important role of the CISO is to monitor compliance to the GoA Information Security Framework. A maturity-based model will be established instead of the "pass" or "fail" model that has been historically used. This new model will provide a more accurate status of Cyber Security at the GoA, and will also provide a clearer path to improving cyber security services. Once this model has been developed, it will be used to re-assess compliance across the GoA.
Priority will be given to Disaster Recover Planning activities over 2016.

The **Information Security Framework** is a set of artifacts developed and maintained by the CISO to protect the GoA's information assets. Artifacts include information security directives, policies, standards, guidelines, as well as material relating to the training and awareness program. The framework describes a total of **132 security controls** that are used to assess compliance to the framework across the GoA.

Following are the initiatives that fit this category:

- Managed Security Services Transition
- Cyber Security Toolset Standardization
- Development of the Cyber Security Services Catalog (with Service Commitments)
- Facilitation of Information Security Framework Compliance
- IT Disaster Recovery Planning Improvements
- 2nd Factor Authentication & Remote Access Improvements

Increasing Information Stakeholders Awareness

It is critical that the GoA achieves a higher level of awareness relating to information security across the organization to ensure that stakeholders can identify attacks and potential threats, and that they know how to respond to these.

> According to IBM's *2014 Cyber Security Intelligence Index*, 95% of all cyber security incidents involve **human error**.

The current internal online training tool is outdated and has not proven as effective as expected. As a result, new awareness and training methods are being developed and implemented, including both in class and on line training.

Initiatives under this category include:

- Implement a New In-Class Information Security Awareness Program
- Upgrade and Update Online Information Security Awareness Resources
- Upgrade Internal Training & Certification (CISO and MISO resources)

Shifting Security Posture from Reactive to Proactive

In order to shift its security posture from passive-defensive (reactive) to aggressive-offensive (proactive), the GoA must leverage existing internal and external sources of cyber threats intelligence and information, and create new and more advanced sources.

The cloud is being increasingly used for storing data and for accessing web-based application services. Policies, strategies, processes, and tools have to be developed and implemented to ensure that controls similar to the internal infrastructure are in place to make cloud usage safer.

Historically, security control tools offered little opportunity to manage information assets and user access proactively. Recently, these tools have evolved, providing new opportunities. These tools even go as far as offering the ability to fast-track the implementation of information classification programs. The GoA will evaluate and implement such tools over the next few years.

Following are the initiatives under this category:

- Develop Cloud Access Security Practice
- Define and Implement Cyber Threat Intelligence Services
- Update and Formalize an Information Security Risk Management Process
- User Access Controls Improvements

Moving Forward

Albertans are becoming more dependent on the Internet and on Cyberspace. New web-based services are becoming available every day along with new mobile technology that is making services easier to access, in turn, making our dependence on Cyberspace grow even faster.

As we enjoy the benefits offered by cyberspace, we must also recognize the threats that come with these benefits. Those who use the Internet with malicious intent are becoming more sophisticated and dangerous as technologies evolve. Newer technologies provide uneducated users, with little or no hacking experience, the ability to cause as much damage as any experienced hacker would.

The GoA's Cyber Security Strategy is our plan for securing the Province's cyber systems and for protecting Alberta's information assets. By promoting awareness of cyber threats and strong security practices, the GoA's Cyber Security Strategy will encourage all levels of the Government to adapt behaviour and implement processes and technologies required to meet the ever evolving cyber threat.

The Government began implementing new initiatives supporting the GoA Cyber Security Strategy in 2015, ensuring that Government systems are secure and that information assets are protected while providing access to authorized individuals. The initiatives may be adjusted and strengthened over the next few years based on changes to the environment.

Cyber security is a responsibility that is shared amongst all information stakeholders. Albertans, Government employees, the private sector, and service partners all have a role to play. The GoA's Cyber Security Strategy makes information security and the implementation of all initiatives a collaborative effort. The only way these efforts will be successful is if we all work together with a common set of objectives.

The CISO also works with external organizations such as the Alberta Security & Strategic Intelligence Support Team (ASSIST), the Canadian Cyber Incident Response Centre (CCIRC), various police services as well as external committees such as the National CIO/CISO Subcommittee for Information Protection (NCSIP) to ensure that cyber threat intelligence is kept up-to-date. Furthermore, the CISO shares information with federal and other provincial jurisdictions to ensure that knowledge, experience and efforts are leveraged to minimize expanded efforts and costs while maximizing expertise and experience involved in resolving common issues and threats. The participation of all of these stakeholders and partners is required to eliminate or mitigate the common cyber threat.

If you have questions, concerns or feedback regarding the GoA's Cyber Security Strategy, please forward them to ciso@gov.ab.ca

When it comes to the protection of the Province of Alberta's information assets, **everyone** has a role to play!