TECHNOLOGY AND INNOVATION

Alberta's Cybersecurity Strategy

Protecting the Province's Digital Assets

Alberta

Technology and Innovation, Government of Alberta
May 4, 2024
Alberta's Cybersecurity Strategy: Protecting the Province's digital Assets
Prepared by the Cybersecurity Division

alberta.ca

Contents

Message from the Minister of Technology and Innovation

As more Alberta organizations continue to transition to digital services and implement cloud and mobile technologies, they potentially become vulnerable to malicious cyberattacks. Globally, cyber-attacks have become more frequent and more sophisticated every day. In 2023, our Cybersecurity division successfully blocked an average of 129 million daily potentially malicious attempts to connect to the Government of Alberta's network.

Alberta's Cybersecurity Strategy is of the highest importance to the Government of Alberta, and it ensures we are intentional in our protection, vigilance, response and deterrence against malicious attacks on our digital ecosystem. Trust is at the heart of this strategy – because Albertans need to be able to rely on the strength and integrity of our digital infrastructure every time they use an essential government service. Whether applying for a health care card, driver's licence, or income support payments, Albertans need to know they are protected whenever they interact with us.

In this increasingly digitized world, our Cybersecurity Strategy is our plan to stay ahead of online threats. We take a multi-layered approach to security, applying best practices and standards to monitor and detect cyber threats, as well as to respond and recover from incidents.

As leaders in the public sector cybersecurity community, we continuously adjust our approach by working with federal, provincial and territorial counterparts, adopting new tactics and exploring new tools to counter ever-evolving online threats.

Considering the numerous cyberattacks that have been reported in mainstream media alone, my ministry is exploring regulations to make it mandatory for organizations collecting the data of Albertans to report significant cybersecurity incidents to our government based on specific criteria.

In Alberta, we've grown the CyberAlberta Community of Interest to a group of more than 700 cybersecurity experts from public, private and non-profit organizations who work collaboratively on many initiatives to strengthen Alberta's cybersecurity defences. Our new CyberAlberta website (cyberalberta.ca) launched in March 2024, connects Alberta cybersecurity leaders, and supports organizations as they respond to threats.

A rapidly evolving cyber threat environment can make anyone a target. Despite these challenges, we are confident our cybersecurity strategy will enable us to deliver online services that are secure, safe to use and resilient – access which Albertans can trust.

The Honourable Nate Glubish
Minister of Technology and Innovation

Message from the Chief Information Security Officer

In today's digital landscape, cybersecurity is not just a necessity but a critical imperative for safeguarding sensitive information, protecting assets, and ensuring business continuity. As organizations face increasingly sophisticated cyber threats, a robust cybersecurity strategy is essential to mitigate risks and build resilience.

The Government of Alberta envisions a cyberspace that is protected, secure, and adaptable, with respect for privacy: a cyberspace where Albertans can flourish while using digital services with trust and safety.

My division's mission is to work in collaboration with Government of Alberta Ministries, Alberta Public Agencies, municipalities, post-secondary and K-12 institutions, Alberta businesses, and other partners to strengthen Alberta's overall cybersecurity posture.

We follow simple principles to realize our vision of cyberspace and our mission's goal, such as using a risk-based approach for cybersecurity, working together with other cybersecurity professionals across the province, watching cyberspace for any suspicious activities, and encouraging cyber education and awareness.

Our cybersecurity strategy outlines a proactive and holistic approach to address the evolving threat landscape and to continuously evolve and strengthen Alberta's overall cybersecurity posture. By prioritizing cybersecurity and fostering a culture of security awareness, we will mitigate risks, enhance resilience, and safeguard the trust of our stakeholders in an increasingly digital world.

Sincerely,

Martin Dinel – BSc, ISP, ITCP, CISSP
Chief Information Security Officer and Assistant Deputy Minister
Cybersecurity Division – Technology and Innovation
Government of Alberta

Executive Summary

Vision: Alberta will be a world leader in cybersecurity by 2028

To achieve our vision, we must stand up to the cyber threat on behalf of Albertans and Alberta businesses. We will do this with our seven cyber shields:

1. **Stand up for Alberta against cyber threats**

   Stand in the way of the threat and equip Albertans, and Alberta's public and private organizations, to better recognize and respond to cyber threats.

2. **Shared threat information across Alberta**

   The Government of Alberta facilitates the development and distribution of real-time cyber threat information and related advice to all Alberta stakeholders.

3. **Adopt cybersecurity best practices and standards**

   Alberta has a comprehensive cybersecurity compliance framework that provides clear direction to all stakeholders, ensuring the adoption of world-class standards.

4. **Risk-based approach to modern technologies**

   Alberta is a leader in understanding and adopting technologies that they can trust through agile, and yet stringent, risk assessment and management processes.

5. **Access to cybersecurity services and technology for all**

   Alberta's public and private organizations can quickly gain access to cybersecurity services and technologies that they can trust.

6. **Alberta's critical infrastructure is protected**

   The well-being of Albertans and Alberta's economic prosperity is ensured by our protected and resilient critical infrastructure systems.

7. **Alberta has a flourishing cybersecurity industry**

   Alberta is a centre of excellence for the development of cybersecurity talent, and a leader in cybersecurity innovations and solutions.

The Context

The mission of the Cybersecurity division is to work collaboratively with Alberta public and private organizations to strengthen Alberta's overall cybersecurity posture.

The Ministry of Technology and Innovation's Cybersecurity division is responsible for overseeing all aspects of information and technology security for the Government of Alberta (GoA).

The GoA recognizes that information and technology are critical assets, and that the management, control and protection of these assets have a significant impact on digital and physical service delivery, including Alberta's Critical Infrastructure. The assets must be protected from unauthorized use, disclosure, damage, and loss.

Alberta's Cybersecurity Strategy sets priorities for how the government can efficiently and effectively address the protection of Alberta's digital assets. It outlines the objectives and the outcomes that cybersecurity initiatives must focus on to iteratively strengthen Alberta's cybersecurity posture.

Cybersecurity Services Scope

Alberta public agencies, businesses, and people need help to protect their digital assets from cyber threats. The Cybersecurity division offers services to all information and technology assets in the GoA, and to Alberta's public and private organizations and people.

While the Cybersecurity division is directly responsible for planning and operating the cybersecurity program across the GoA, the division's role with Alberta's public and private organizations as well as with Albertans is one of a leader, facilitator, and connector.

Motivation

Every year, Cybersecurity Services detects a growing number of more sophisticated attacks. Attackers are seriously investing in their capabilities, and organizations must respond by investing equally in theirs. Cyber threats affect us all. Sophisticated attackers can disrupt digital services, from utility services or telecommunication networks, to banking systems, government services, critical infrastructure, or health care services. Cyber threats also undermine our privacy through theft of personal information.

Strategic Assumptions and Considerations

Predicting what cyberspace or cyber threats will look like in the future is challenging. We must seek to understand the forces that shape the future to lead, influence and adapt the evolution of our environment:

- Ongoing migration of services to digital – emphasizing mobile technologies, and cloud hosting – will also continue to increase the attack surface for threat actors.
- The continuous increase in volume and sophistication of cyber attacks requires increased stakeholder awareness, and a professional and agile cybersecurity workforce.
- New system and application vulnerabilities will continue to be identified at a rate that is greater than the ability of organizations to resolve them in a timely manner.
- The threat coming from supply chain, including code libraries, must be managed. It may come in the form of compromised goods and services, or third-party partnerships.
- Increasing threat to our democratic process due to misinformation and disinformation campaigns will continue to create more issues.
- A cornerstone to securing fast and agile digital solutions delivery is the adoption of cybersecurity standards and best practices throughout the entire lifecycle of the solution.
- Data encryption will continue to be an effective control to protect information for the next five to 10 years; however, we continue to prepare for the future quantum threat to our cryptographic controls.
- AI technologies, including deepfakes, machine learning, large language generators, and other automation is expected to be both a disrupter and an enabler for cybersecurity.
- Social engineering attacks will continue to be a primary attack vector used by malicious threat actors to gain access to internet-exposed digital systems and services.
- Differences in security requirements and risk tolerance across organizations demonstrate that one-size-fits-all security approaches are less effective than risk-based solutions tailored to organizations.
- The worldwide shortage in cybersecurity skills continues to be an issue. Attracting and retaining qualified cybersecurity personnel will continue to be a challenge.
- Critical infrastructure across Alberta is controlled through digital systems. These must be secured to ensure the well-being of Albertans and Alberta's economic prosperity.
- We expect that political tensions between countries will increasingly move towards cyberspace, with threat meant to disrupt government services and critical infrastructure services.
- The impacts of the pandemic on our economy will continue to be felt over the next several years. This will continue to result in increased pressures on the budget, requiring us to do more with less.

The Threat

The GoA's vision of Alberta's Cyberspace is one that is secure, safe, and resilient, while prioritizing privacy: a cyberspace where Albertans can thrive while confidently and safely utilizing digital services.

Cyber attacks come in different forms, like exploiting systems weaknesses, using social engineering to deceive people for information, or gaining unauthorized access to systems. After compromising a system, attackers can steal data or money, disrupt services, or turn the system into a tool for further attacks. These attacks are popular because they share four key traits:

- Inexpensive – Low-cost, leveraging free tools available across the internet.
- Easy – Attackers with basic skills can cause damage.
- Effective – Even minor attacks can cause extensive damage.
- Low risk – Attackers can evade detection and prosecution by hiding in a web of computers and exploiting gaps in legal systems.

Types of Threat

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

Negligence
Lack of resources and knowledge of cyber threats can result in negligence from an organization or staff, leading to serious cybersecurity incidents.

On average, companies take about 204 days to identify and 73 days to contain a breach according to IBM's Cost of Data Breach Report for 2023.

ibm.com/reports/data-breach

Insider Threat
Employees and contractors are given the access they need to perform their functions. Controls are in place to monitor digital assets, but if staff becomes disgruntled or misrepresent themselves, they could become threats to the organization, causing damage that is difficult to detect and counter.

Cyber Crime
Criminals use malicious software or coordinated attacks designed to infiltrate or damage targeted systems, usually, with the goal to make a profit (e.g.: ransomware).

According to estimates from a Canadian Cybersecurity Network report, there will be approximately 3.5 million unfilled cybersecurity jobs worldwide by 2027

canadiancybersecuritynetwork.com/talent-why-growing-canadas-cybersecurity-talent-is-so-important

Cyber Espionage
Cyber spies are well resourced, patient, and persistent. Often sponsored by nation-states their purpose is to gain political, economic, commercial, or military advantage.

Cyber Terrorism & Hacktivism
Terrorists and activists are using the internet to support recruitment, fundraising and other propaganda activities. Hacktivists often 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, with the potential to result in life-threatening attacks on critical infrastructure systems.

The Cyber Threat is Evolving

The evolution of cyber attacks has accelerated dangerously in recent years. Attackers are increasingly creative, sharing techniques, and finding new ways to bypass the latest security controls. AI is being used both by malicious actors to devise new attacks, spread misinformation, or compromise critical systems, and by defenders to enhance their ability to detect and counter threats.

Aging and often unsupported technology in legacy systems is becoming a critical attack vector for threat actors. Would-be-attackers now leverage AI technologies to quickly identify the presence of older and unsupported technologies, and they leverage known vulnerabilities and related exploits to compromise systems and either disrupt services or access information without authorization.

Alberta stakeholders must maintain a range of monitoring and response controls and a robust cybersecurity awareness program, supported by ongoing investment in cybersecurity personnel, processes, and technology.

Many current attacks originate from nation-state actors sponsored by countries competing with Alberta in markets like oil and gas, and agriculture. These actors aim to steal valuable information for a competitive edge or to disrupt government services and sway public opinion.

The global shortage of cybersecurity professionals continues to pose a significant threat. This shortage affects both businesses and governments, as the demand for cybersecurity expertise continues to grow, leading to fierce competition for the same limited pool of resources.

The Strategy

“The key to the Alberta’s Cybersecurity Strategy is to shift our posture from passive to proactive – a posture where identify and manage cyber threats before they become incidents.” -- Martin Dinel, CISO, Government of Alberta

The cybersecurity 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-de-fensive security posture is not enough to protect against continually evolving cyber attacks. The GoA’s cybersecurity environment must continuously evolve and adapt to changing cyber threats.

The Cybersecurity division adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This framework establishes a risk-based approach to managing cybersecurity by providing a standard set of controls, clear desired outcomes, and compliance criteria. This allows the government to communicate using a common language for managing and communicating cybersecurity risks to stakeholders. The framework can then be used to prioritize risk treatment actions, helping to set expectations across the organization.

Shield 1:
Stand up for Alberta against cyber threats

Key Performance Indicators:

- Number of CyberAlberta led meetings and speaking engagements, including workshops
- Number of external incidents facilitated by CyberAlberta
- Number of GoA Cybersecurity incidents
- Number of malware and phishing attacks prevented by GoA cybersecurity controls
- Number of GoA-led penetration testing exercises performed
- Number of GoA systems vulnerabilities discovered by penetration testing and vulnerabilities scans
- Number of GoA digital systems vulnerabilities resolved

1. Support Alberta's public and private sectors

Alberta's public agencies, businesses, and citizens are under continuous attack from threat actors. Many of these stakeholders are unable to protect themselves in a consistent manner due to a lack of cybersecurity expertise or resources. The primary platform to share and collaborate on critical security events within the province is the GoA's CyberAlberta Community of Interest (COI).

GoA Action Plan

The GoA plays a crucial role in leading the CyberAlberta COI, aiming to boost the province's cybersecurity. CyberAlberta liaises with the various levels of Canada's governments, with law enforcement agencies, and with cybersecurity partners to gather, formulate, and offer guidance while facilitating collaboration amongst Alberta stakeholders.

The COI serves as a platform for informing and involving Alberta's stakeholders in enhancing cybersecurity. We plan to establish sub-committees focusing on key areas like developing cyber talent and securing digital infrastructure. By fostering partnerships between government, post-secondary institutions, K-12 schools, and public and private organizations, CyberAlberta strengthens collective defenses against cyber threats. Members can discuss security issues, share information, and devise strategies to address and prevent cyberattacks promptly. This initiative ensures timely sharing of cybersecurity insights, enhancing overall preparedness to counter emerging threats.

2. Provide clear and adapted cyber guidance for Alberta stakeholders

Security professionals face significant challenges due to the rapid pace of technological advancement and the increasingly creative tactics of attackers. Simply waiting to respond to incidents isn't sufficient; organizations must proactively address threats before they escalate. Many organizations struggle with implementing effective cybersecurity measures due to a lack of expertise and resources. Individuals in Alberta also need guidance to safeguard their digital assets, such as their identity, devices, and online presence, from cyber threats.

GoA Action Plan

Providing direction and guidance can accelerate an organization's cybersecurity efforts and skill development. In 2022, the GoA implemented a Cybersecurity Compliance Assessment Framework, aligned with the NIST CSF. Regular assessments of this framework's controls occur every few months, providing leaders with insights into cybersecurity strengths and weaknesses, helping to prioritize improvements. This framework could spark discussions within CyberAlberta, leading to an Alberta-wide compliance framework. This would aid in comparing maturity assessments, identifying priorities for COI members, and seeking guidance from organizations with mature controls.

Recognizing that not all organizations need the same level of control maturity, the COI plans to create a flexible framework suitable for all sizes. Moreover, this framework could be used in procurement to ensure that cybersecurity products and services meet required standards, safeguarding organizations from supply chain vulnerabilities.

Albertans also need cyber guidance. The CyberAlberta team is collaborating with service providers, school boards, and the Ministry of Education to integrate cyber safety into the K-12 curriculum. This includes offering cybersecurity micro-certification for grades 9 to 12, potentially creating job opportunities or meeting post-secondary education requirements. They also aim to educate seniors on cyber threats through online materials and in-person sessions.

Furthermore, despite security controls, uninformed staff pose a significant risk to their organization. User training is crucial. When individuals understand their role in protecting assets and how to recognize and respond to cyber threats, organizations significantly improve security. CyberAlberta prioritizes cybersecurity awareness and training, developing materials for Albertans, organizations, and cybersecurity teams, such as playbooks, and a variety of threat reports.

3. Work with federal government on National threat blocking

Canada's cyberspace is unfiltered, with a large portion of its traffic belonging to threat actors. When organizations come under attack, they are often left to fend for themselves, working to block incoming threats. If they manage to repel these attacks, the threat actors typically move on to target another Canadian entity.

GoA Action Plan

The GoA's Cybersecurity division will continue to collaborate with other provinces, territories, and the federal government to improve Canada's cyberspace. One significant initiative, proposed by Alberta and gaining momentum, is the National Cyber Threat Blocking. Traditionally, organizations would spot threat actors via their IP addresses and block them from their networks. Under this new initiative, suspicious IPs would be reported to a national program. If the IPs meet specific criteria signaling malicious activity, they would be blocked at the national level, preventing threat actors from moving between Canadian targets. This initiative not only enhances cybersecurity but also leads to a cleaner, safer, and faster Canadian cyberspace.

Shield 2:
Shared threat information across Alberta

Key Performance Indicators:

- Number of individual intelligence reports analysed by CyberAlberta
- Number of published CyberAlberta threat intelligence reports (emergent threats)
- Number of published CyberAlberta digital threat landscape reports (research focused)
- Number of published CyberAlberta CyberMinutes articles (cyber news items)

4. Cybersecurity regulations to help, not impede

The primary objective of CyberAlberta is to enhance the overall cybersecurity framework within the province. In some cases, regulations may be necessary to ensure the implementation of best practices and standards or to support initiatives that can fortify Alberta's security posture.

For example, sharing information about cyber threats, both attempted and successful, is essential for the program's success. Tracking significant cybersecurity incidents supplies other organizations with valuable data to defend against similar attacks and helps measure the effectiveness of the CyberAlberta program, guiding future efforts. Voluntary reporting is not something that can be counted on to achieve the program's outcomes. Regulations may be required to ensure that incidents and related data are reported to the program in a timely and effective manner.

GoA Action Plan

CyberAlberta will contemplate introducing certain regulations to boost the province's security posture; nevertheless, collaboration with other government levels and potentially international jurisdictions will be sought to discuss the need for regulatory simplification or harmonization to alleviate negative impacts on Alberta stakeholders. With the global rise in cybersecurity regulations, businesses operating beyond the province and internationally might have to comply with various provincial, federal, or international regulations, where conflicts may sometimes arise. CyberAlberta aims to mitigate this issue.

Cybersecurity is exploring regulation to make it mandatory to report significant cybersecurity incidents based on a specified criteria. CyberAlberta is also collaborating with the Canadian Centre for Cyber Security (CCCS) to ensure that forthcoming regulations under Bill C-26 align with or complement those being considered by the Government of Alberta.

5. Create a centralized threat intelligence network

Numerous threat intelligence feeds are available, often containing duplicated reports. Moreover, not all intelligence is relevant to every organization. Sorting through these reports, identifying those applicable to an organization, and crafting tailored messages for executives and actionable guidance for technical staff is a considerable challenge. Many organizations lack the resources to sift through these reports or the expertise to comprehend and effectively address the threats they contain.

GoA Action Plan

The GoA aims to establish a robust threat intelligence network, collating sources relevant to Alberta stakeholders. This involves crafting straightforward threats explanations and providing actionable advice for their identification and mitigation to cybersecurity teams across the province. Additionally, the GoA will develop concise executive messaging, enabling cybersecurity professionals to effectively communicate threats and resources needs upwards without disrupting their technical duties.

6. Research and report on threats and new technologies

Not all identified threats are immediately exploitable. Great examples of this would be the threat associated with Quantum computing, and the potential threats posed by Artificial Intelligence systems used for reconnaissance and for attacks by threat actors.

GoA Action Plan

CyberAlberta's Threat Intelligence team will proactively identify, and research identified threats, how to recognize them, and how to treat or resolve them when treatment is possible and available. The team will prepare reports on the overall threat landscape to the province of Alberta, ensuring that Alberta stakeholders are well-informed and able to recognize and face the threats.

The CyberAlberta team will also explore, sometimes even test, and always document relevant cybersecurity technologies and new strategies and techniques, publishing documents to promote knowledge of these across Alberta's cybersecurity community.

Shield 3: Adopt cybersecurity best practices and standards

Key Performance Indicators:

- Number of GoA internal cybersecurity standards documented or updated
- Number of cybersecurity standards published by CyberAlberta
- Number of cybersecurity playbooks published by CyberAlberta
- Number of GoA internal Cybersecurity Controls Framework audits performed
- Percentage of GoA internal Cybersecurity Controls assessed as “compliant”

7. Encourage the adoption of proven cybersecurity best practices and standards

Cybersecurity needs vary among organizations, influenced by the size and expertise of their cybersecurity teams, the organization’s risk tolerance, and the sensitivity and criticality of the data they collect and manage. Unfortunately, many organizations adopt solutions without fully grasping the value or sensitivity of their assets, potentially leaving them vulnerable. This lack of expertise can lead to unintended exposure of digital assets, risking system compromises and privacy breaches.

GoA Action Plan

Albertans rely on the GoA to safeguard government information assets. To achieve this, the Cybersecurity division created a NIST CSF aligned control framework to evaluate compliance with international cybersecurity standards. This framework helps the organization identify strengths and weaknesses in cybersecurity controls, guiding ongoing improvement efforts. This framework leverages a Zero Trust Architecture, ensuring that all users, regardless of their position inside or outside the GoA, are rigorously authenticated, authorized, and continuously validated.

The CyberAlberta Community of Interest will examine this framework closely, aiming to develop a flexible provincial framework over the next few years. The framework will be later leveraged to help identify weaknesses in each organization’s environment, leading to better prioritization of efforts to improve the organization’s posture. It will also be leveraged to identify best practices across the province, as well as to help secure the organizations’ supply chains by requiring vendors and service providers to match or exceed the compliance level of the organizations requesting their services.

8. Cybersecurity throughout the solutions' lifecycle leveraging DevSecOps

Over the past five years, there's been a growing demand to digitize government services. The popular strategy for this is agile development, where small functionalities are delivered rapidly and built upon over time. This approach brings together all the necessary services, skills, and expertise when needed. However, several challenges have arisen for cybersecurity professionals. There's a global shortage of cybersecurity resources, and the need for faster solution delivery has led to the use of a wider range of tools and technologies. This, combined with ongoing attacks on digital services, makes it harder for professionals to conduct timely security assessments, offer mitigation recommendations, and address vulnerabilities in both new and old applications.

GoA Action Plan

To tackle this challenge, Cybersecurity Services need to transform and become part of solution delivery teams with minimal impact on resources and budgets. A DevSecOps approach – integrating development, security, and operations related functions to secure the entire application lifecycle – is required. This approach will ensure that all solutions are secure by design by:

- Providing security design and specifications to development teams at the project's start, covering systems authentication, authorization, logging, and other controls.
- Speeding up automated security assessments by categorizing systems using historical data to identify vulnerabilities faster, assess risks quicker, and offer mitigation recommendations based on application parameters and past risks.
- Equipping development teams with automated testing tools to ensure compliance with security design specifications before implementation.
- Engaging ethical penetration testing teams before critical and web-facing applications go live, ensuring thorough testing and remediation.

Fraud detection systems, which are becoming increasingly efficient at spotting suspicious user behaviors and automating a response to these actions, are also becoming a prevalent control to help secure our digital systems against the threat actors.

Shield 4:
Risk-based approach to modern technologies

Key Performance Indicators:

- Number of published CyberAlberta threat intelligence reports focused on AI and new technologies
- Number of GoA digital services risk assessments performed
- Total number of risks in the GoA Cybersecurity Risk Register
- Number of new GoA cybersecurity risks identified
- Number of internal GoA Statement of Acceptable Risks approved

9. Risk-based approach to technology decisions

Cybersecurity units offer their specialized expertise as a service to their organizations. Most of the time, these organizations' primary focus isn't cybersecurity, a crucial point for cybersecurity leaders to grasp. While all business decisions rightfully remain within the purview of the business itself, it's the role of the cybersecurity team to ensure that cyber threats and risks are factored into these decisions.

GoA Action Plan

Organizations must effectively communicate their most critical assets—whether physical, human, intellectual, or otherwise—to their cybersecurity teams. This ensures these assets receive the necessary protection and monitoring. Regular risk assessments are vital to identify and understand the risks surrounding these assets, allowing for the implementation of appropriate safeguards and tested recovery plans to ensure resilience.

Within the GoA, our application inventory comprises over 1,300 applications. Each of these systems has undergone thorough security threat and risk assessments, with identified risks documented and managed through a corporate cyber risk register. CyberAlberta will encourage all Alberta organizations to adopt this best practice.

10. Quantum threat advice

The GoA standard for information security in the cloud mandates data encryption in transit and at rest, aligning with data sensitivity requirements. Whenever possible, the GoA controls encryption keys to prevent data compromise by third parties.

Quantum computers use various states for data beyond the usual 1s and 0s, allowing them to process larger amounts of data faster. For instance, while traditional computers would require around 300 trillion years to break an RSA-2048 bit encryption key, a quantum computer could do it in about 8 hours. Since the main security control used to protect GoA data is data encryption, Quantum computing is quickly becoming a serious threat consideration for most organizations.

GoA Action Plan

The Government of Alberta's Cybersecurity division is actively researching and documenting best practices to address the Quantum threat to cryptographic algorithms safeguarding our digital assets. Regular updates on this research are shared with our Community of Interest (COI). Additionally, the CyberAlberta team is formulating a coordinated Alberta-wide strategy to compile a comprehensive inventory of encryption methods used by organizations across the province. This initiative includes a roadmap to ensure these organizations are prepared to counter the Quantum threat and begin implementing Quantum-safe solutions to enhance their digital security. The plan is currently in progress and is expected to be published by end of summer 2024.

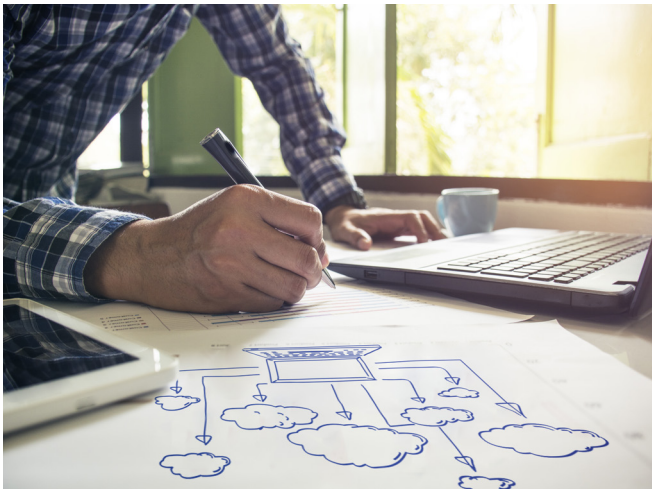
11. Artificial Intelligence threat advice

Artificial Intelligence (AI) can boost productivity and decision-making through augmented intelligence and by leveraging ongoing machine learning. However, improper implementation of AI can pose serious threats to organizations. These threats include data breaches due to sensitive information becoming part of public AI knowledge bases, the risk of using unverified data leading to flawed decisions, and the potential for threat actors to exploit AI for reconnaissance and automated attacks.

GoA Action Plan

The GoA is actively exploring and testing AI technologies to ensure that emerging threats are addressed while continuing to deploy AI tools and systems very cautiously. Insights from these investigations inform the development of new policies and technical controls, such as the Natural Language Generator (NLG) directive and guideline shared with the CyberAlberta Community of Interest in October 2023. Additionally, lessons learned from the various technology pilots performed by the GoA are utilized to enhance the configuration of AI and security systems within the organization.

CyberAlberta is committed to disseminating the GoA's key findings on AI technologies and its approach to AI tool adoption within the Community of Interest. This sharing aims to accelerate the secure adoption of AI tools, particularly for small organizations lacking IT resources, and to highlight potential issues for organizations considering AI adoption.



Shield 5: Access to cybersecurity services and technology for all

Key Performance Indicators:

- Number of GoA cybersecurity related agreements made available to Alberta stakeholders
- Number of GoA cybersecurity products or services risk assessments published by CyberAlberta

12. Common procurement practices leveraging Alberta-wide agreements

Cybersecurity and IT procurement processes usually take around three to four months to prepare, followed by a month of evaluations and another one to two months of negotiations with the chosen vendor. This assumes the organization has the resources and expertise to identify needs and assess proposals. These processes can expose security needs and weaknesses, and smaller organizations often miss out on good deals due to their size and limited resources. Each Alberta organization performing these procurement mechanisms concurrently and independently also results in repetition of related costs for no valid reasons.

Another procurement related issue comes from open source products. Threat actors leverage these products for attacks, and often, cyber-defenders could leverage the same products to better protect their organizations, but shy away from them because their organization does not allow for non-vendor supported products.

GoA Action Plan

The services needed by the GoA's Cybersecurity division are often required by all Alberta organizations. By tapping into the CyberAlberta Community of Interest, the province's procurement processes could benefit from a more comprehensive list of requirements and the collective purchasing power of the entire province. This could lead to better financial deals, making services and products accessible to smaller organizations that might not afford them otherwise.

Creating pre-approved agreements for certain services, like digital forensics for ransomware attacks, could offer quicker access to services at agreed-upon rates. This saves time and avoids costly negotiations during urgent situations.

CyberAlberta will also ensure that consideration for open source products is always given in order to implement solutions that could help organizations to reduce time to implementation and costs.

13. Simplify and centralize cybersecurity tools and logging

Vendors, service providers, and internal procurement processes often complicate cybersecurity tool acquisition. Every vendor claims their product is superior and tries to convince cybersecurity leaders of their expertise. Procurement processes prioritize finding the cheapest product without much regard for integration or ease of use. This leads to cybersecurity teams managing a complex environment with numerous tools, each covering a small part of the system, through multiple monitoring consoles. Training cybersecurity staff to manage these tools as experts also becomes a significant issue.

GoA Action Plan

A significant factor in the success of the GoA's cybersecurity toolset modernization was simplifying and consolidating tools and services, accompanied by in-depth training on a select few tools. Rather than chasing after the absolute best products, we prioritize investments in tools that seamlessly integrate and are respected leaders within their categories. Our focus is on reducing the number of monitoring consoles to just one, simplifying management.

CyberAlberta will advocate for this approach within the Community of Interest, guiding members to trusted tools known for their compatibility. Additionally, we will facilitate connections with organizations capable of supporting implementation, operations, and training requirements.

Shield 6: Alberta's critical infrastructure is protected

Key Performance Indicators:

- Number of CyberAlberta members identified as Critical Infrastructure Operators
- Number of GoA digital systems identified as Critical Infrastructure Systems

14. Liaise between Alberta Critical Infrastructure Operators and the federal government

While the federal government has authority over national critical infrastructure services, they don't necessarily have a deep understanding of Alberta critical infrastructure operators, and they rarely interface with other Alberta stakeholders that don't support critical infrastructure services.

GoA Action Plan

The GoA, through its CyberAlberta program, maintains strong connections with cybersecurity leaders across both public and private sectors in Alberta. This positioning enables effective communication between Alberta stakeholders and the federal government, facilitating clarification on cybersecurity concerns and potential future regulations. Moreover, CyberAlberta can advocate on behalf of Alberta organizations when challenges and issues present themselves, and they can provide support for national initiatives that may impact Alberta stakeholders.

15. Provide ability to test cybersecurity measures for critical infrastructure

Critical Infrastructure Operators oversee highly complex and sensitive digital environments. Even minor changes or configuration tests in such environments carry substantial security implications, potentially leading to catastrophic events that threaten the welfare of Albertans and the economic prosperity of Alberta. Unfortunately, these operators often lack the resources, capabilities, or capacity to establish secondary testing environments for safely evaluating infrastructure changes under controlled conditions.

GoA Action Plan

CyberAlberta is committed to collaborating with Critical Infrastructure Operators, Alberta's cybersecurity vendor community, and the CyberAlberta Community of Interest to explore viable solutions for enabling operators to test controls and configuration changes outside of critical production environments. Our aim is to pool resources and budgetary allocations at the provincial level to drive this initiative forward. By coordinating activities effectively, we will ensure that all organizations in need of such services can access them. Our goal is to meet their requirements with minimal investment of time and resources.

Shield 7: Alberta has a flourishing cybersecurity industry

Key Performance Indicators:

- Number of CyberAlberta Community of Interest members
- Number of CyberAlberta external volunteers
- Number of hackathons and conferences sponsored by CyberAlberta
- Number of Cybersecurity Work Experience Program participants employed by GoA
- Number of cybersecurity Interns employed by GoA
- Number of pan-Canadian initiatives involving GoA Cybersecurity division staff

16. Alberta as a cybersecurity talent development centre of excellence

The Canadian Cybersecurity Network (canadiancybersecuritynetwork.com/talent-why-growing-canadas-cybersecurity-talent-is-so-important) organization estimates that the worldwide shortage of cybersecurity talent will reach 3.5 million by 2027. Organizations, especially small organizations with limited resources and the public sector, are having significant issues with attracting and retaining cybersecurity personnel.

GoA Action Plan

Since 2021, the Government of Alberta's Cybersecurity division has forged partnerships with post-secondary institutions and the Ministry of Advanced Education to spearhead novel talent development initiatives. These include a cybersecurity work experience program, an internship program, and the recent initiation of a cybersecurity apprenticeship program. While these initiatives are being refined within the government, they are also extended for implementation by members of the CyberAlberta Community of Interest.

Moreover, CyberAlberta collaborates closely with these institutions to enhance candidate attraction for diverse cybersecurity talent development programs and to standardize the cybersecurity curriculum, ensuring accessibility to prospective professionals. The overarching objective is to establish the province as a hub for cultivating skilled cybersecurity resources, effectively meeting the resource demands of Alberta stakeholders.

17. Lead pan-Canadian cybersecurity initiatives

Alberta boasts some of Canada's top cybersecurity talent. However, as organizations in Alberta confront a rising tide of attacks, it's all too common for teams to become inwardly focused. They may overlook the advantages of collaborating with other organizations and fail to recognize the potential benefits of spearheading joint initiatives to shape outcomes more effectively.

GoA Action Plan

The Cybersecurity division of the GoA is committed to advocating for Alberta's interests on the national stage. We will persist in introducing innovative ideas to bolster Canada's overall cybersecurity posture and take the lead on pan-Canadian initiatives and endeavors. Through these efforts, we aim to uphold Alberta's position as a recognized national leader in cybersecurity.

18. Support the development of new cybersecurity revenue generators

As the technology sector flourishes throughout the province, and as cybersecurity talent development initiatives advance, the landscape for cyber startups and the emergence of innovative cybersecurity revenue streams grows richer. It's imperative to establish robust support systems to foster these new revenue streams effectively.

GoA Action Plan

Under the CyberAlberta initiative, we are committed to collaborating with the community and various Technology and Innovation divisions to facilitate connections between organizations poised to pioneer new revenue streams in cybersecurity and relevant government resources. This includes leveraging platforms like Alberta Innovates and other government programs to provide essential support and resources.

Moving Forward

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

The very daily lives and routines of Albertans rely on the internet and digital services. The GoA, just like most global organizations, prioritizes the digitization of government services to facilitate easier, faster, and cheaper access to these services.

Cyber threat actors have realized that the threat surface of all organizations and of individuals has expanded significantly. This provides them with a greater opportunity to benefit from their skills and from poorly designed solutions to access to more data, and to benefit from this access.

Those who use the internet with malicious intent are becoming more dangerous as their skills and the technologies they use evolve and become simpler to use. Uneducated users with little or no hacking experience now have the tools and the ability to cause as much damage as an experienced hacker.

Alberta's Cybersecurity Strategy is the GoA's plan for securing the province's digital assets. By promoting awareness of cyber threats and strong security practices, the Strategy encourages Alberta stakeholders to adapt behaviours, and to implement processes and technologies required to meet strong security standards and the ever-evolving cyber threat.

Cybersecurity is a responsibility that is shared amongst all information stakeholders. Albertans, Alberta's public and private sector organizations, and service partners all have a role to play to strengthen Alberta's overall cybersecurity posture. We must continue to encourage our stakeholders to share cybersecurity and cyber threat information and work collaboratively towards our common objectives.

The Cybersecurity division collaborates with external organizations, such as the Alberta Provincial Security & Intelligence Office (PSIO), Canada's Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (CCCS), Canadian Security Intelligence Service (CSIS), the National CIO/CISO Subcommittee for Information Protection (NCSIP), province-wide local law enforcement authorities to ensure that we have the latest threat intelligence information and that all stakeholders are ready to address any emergent attacks. Furthermore, the Cybersecurity division shares information with federal and other provincial jurisdictions to ensure that knowledge and experience are leveraged to minimize expanded efforts and costs, while maximizing the work done by all jurisdictions to resolve common issues and threats. The participation of these stakeholders and partners is required to eliminate and mitigate the common cyber threat.

If you have questions, concerns, or feedback regarding Alberta's Cybersecurity Strategy, please forward them to GoA.cybersecurity@gov.ab.ca.