Alberta's Cybersecurity Strategy

Protecting Alberta's digital assets

Alberta

Cybersecurity Division, Technology & Innovation, Government of Alberta

Alberta's Cybersecurity Strategy – Protecting Alberta's Digital Assets

Contents

Message from the Minister of Technology and Innovation

In many ways, this Cybersecurity Strategy is at the centre of everything we do.

Albertans depend on the integrity and strength of our digital infrastructure every time they access a government service, whether they are applying for income support or renewing a driver's licence. Digital systems and solutions underpin nearly every service we deliver.

This is why, more than ever, our ability to meet the needs of Albertans means taking a proactive approach to managing, mitigating, and responding to the wide array of cyber threats Alberta faces every day. We take regular stock of our practices and strategies to understand how they can improve, then integrate those learnings across the organization. We test new products and processes thoroughly ahead of implementation, adjusting where required. We look for ways to optimize our efficiency while respecting public tax dollars. We learn from global leaders.

Alberta's Cybersecurity Strategy is the culmination of these actions, and outlines the ways our Cybersecurity division works to improve its response to Alberta's evolving security needs every day.

Now, Alberta's government is looking to take this work one step further through the CyberAlberta Community of Interest, a group led by our Cybersecurity division. Protecting our own networks is no longer enough: CyberAlberta's goal is to help as many organizations as possible in their pursuit to improve their own cybersecurity approach. More than 200 private, public, and non-profit organizations have already come on board and I look forward to seeing security improve as membership climbs.

The cyber threat we face has changed significantly in recent years. Despite these challenges, Alberta's government strives to deliver services Albertans can trust without hesitation.

We look forward to continuing that standard of excellence as we implement this strategy.

Nate Glubish
Minister
Technology and Innovation

Message from the Chief Information Security Officer

The Government of Alberta has made significant changes to how it delivers digital services, with a focus on accelerating service digitization and enabling remote work through mobile solutions. These changes have increased the government's attack surface, introducing new risks and vulnerabilities to manage.

To facilitate faster solutions delivery, the government has adopted new agile approaches and modern technologies that can deliver solutions in a matter of weeks or even days. To ensure that these solutions are secure by design, the government has implemented a DevSecOps model, integrating code development, security design and testing, and operationalization activities, which provides clear security specifications to develop and implement secure digital solutions.

Through this process, the government has learned that being agile and accepting some level of risk is often more effective than extensive planning and testing processes that can take months or years to produce usable products. This approach has reduced costs and improved customer satisfaction.

After almost two years of adapting to this "new normal," the government has updated its Cybersecurity Strategy to identify, manage, and respond to cyber threats. The strategy also includes plans to engage with stakeholders across Alberta to strengthen the province's overall cybersecurity posture, that is to say, our ability to protect our digital assets and respond to cyber attacks.

This Cybersecurity Strategy is a cornerstone of the government's commitment to protecting Alberta's information and technology assets, and the government is proud to lead efforts to secure this information on behalf of Albertans.

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

Introduction

Digital Assets refer to any form of digital content, information, or data that has value or importance to an individual or organization. This can include digital documents, images, audio and video files, databases, software applications, online accounts, cryptocurrency, and other digital resources that are owned or controlled by an individual or organization.

The Government of Alberta (GoA) established its Cybersecurity program in response to a report from the Office of the Auditor General in 2008. The Cybersecurity division oversees the security of all digital assets for the government and works collaboratively with Alberta stakeholders to strengthen Alberta's cybersecurity posture.

The government recognizes that Alberta's digital assets are critical and must be protected from damage, loss, unauthorized use, and disclosure. The Cybersecurity Strategy prioritizes the efficient and effective management, control, and protection of these assets. The strategy focuses on six objectives:

- securing information assets,
- raising stakeholder awareness,
- implementing proactive threat identification and treatment,
- implementing proactive cybersecurity events detection and response,
- establishing effective disaster recovery protocols, and
- continually improving security controls to counter cyber threats.

Cybersecurity Division Scope

The Cybersecurity division is responsible for protecting the GoA's digital assets, as well as advising and facilitating access to cybersecurity services and information for Alberta public and private organizations. The division also assists in educating Albertans about the threat of cyberattacks and how to protect themselves. The program focuses on shared learning, continuous improvement, and strengthening Alberta's overall cybersecurity posture.

Previously, the program only covered the GoA organization itself (GoA proper, with government agencies completely excluded). As we recognize that many Alberta public and private organizations lack access to cybersecurity resources and knowledge, the GoA has committed to expanding its program to assist and support Alberta stakeholders in protecting their digital assets.

Motivation

The impact of cyber threats is widespread and can disrupt any digital service, including utilities, telecommunication networks, banking systems, digital government services, and even healthcare services. These threats can also compromise personal information and undermine privacy.

The GoA recognizes that many public and private organizations, as well as individual Albertans, require assistance in protecting their digital assets from cyber threats. To address this need, the government is evolving its cybersecurity strategy to expand its services to external stakeholders.

Each year, the Cybersecurity division detects a growing number of more sophisticated cyber-attacks. Attackers are constantly investing in their capabilities, and organizations must respond by investing equally in their cybersecurity controls. This is particularly important given the expanding attack surface of organizations as they increasingly offer digital and mobile solutions, which creates new and complex cybersecurity challenges.

It's essential that the GoA remain vigilant and continue to invest in cybersecurity measures to protect its digital assets and maintain the trust of Albertans. The GoA is committed to working with stakeholders across the province to enhance cybersecurity and protect against cyber threats.

The Cyber Threat

The cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025, according Cybersecurity Ventures' "2022 Official Cybercrime Report".

The cyber threat landscape is diverse, and attackers can use various methods to gain unauthorized access to information systems. Exploiting software and hardware vulnerabilities, carrying out social engineering attacks, or taking advantage of individuals who fail to follow basic security practices are just a few examples of the techniques used by attackers. Once they gain access to a system, attackers can cause significant damage by stealing, corrupting, or disrupting information and system operations, or using the compromised system to launch further attacks on other systems.

Despite differences in attack tools and techniques, many cyber-attacks share four key characteristics that have contributed to their growing popularity over the years. First, they are often inexpensive, relying on low-cost or free tools available online. Second, they are relatively easy to execute, even for attackers with minimal skills. Third, even minor attacks can have a significant impact, making them highly effective. Last, attackers can evade detection and prosecution by hiding behind a web of computers and exploiting gaps in legal systems, making cyber-attacks low-risk for perpetrators.

Types of Threats

Accidental

Accidental attacks 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, knowledge, and understanding of cyber threats can also result in negligence on the part of an organization or staff, resulting in serious cybersecurity incidents. Due diligence must be used at all times and combined with a risk-based approach for cybersecurity decisions to improve the chances of an organization to counter the cyber threat.

Of the 2,221 cybersecurity incidents that occurred across the GoA in 2022, 76 per cent were due to malicious actors.

Disgruntled Employees or Rogue Contractors

Employees and contractors are provided with authorized access to the digital assets they require to perform their job functions. Controls are usually in place to control and monitor who uses the assets and how they use them, but in the event that an employee or contractor becomes disgruntled, or third-party contractors misrepresent themselves, they have the potential to become significant threats to the organization and can cause damage that is difficult to detect and prevent.

Cyber Crime

Criminals use or sell information stolen online, such as credit card numbers or credentials, and use malicious software designed to infiltrate or damage targeted systems. Even those who are diligent about practicing safe computing run the risk of information theft or fraud through third-party interactions.

Cyber Espionage

Cyber spies are well resourced, patient and persistent. They are often sponsored by nation-states to perform attacks against governments or other nation-states with competing interests. Their purpose is to gain political, economic, commercial or military advantage. Organizations with a presence in cyberspace are vulnerable. Reports from around the globe confirm that some attacks have succeeded in stealing industrial and state secrets, private data, and other valuable information.

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 take advantage of the world's dependence on cyberspace as a vulnerability to be exploited. Their tactics have the potential to morph into life-threatening attacks on critical infrastructure systems, such as taking control of emergency response, utility, or public health systems.

The Threat is Evolving

The evolution of cyber-attack tools and techniques has accelerated dangerously over the past few years. Attackers are sharing techniques and showing increased levels of creativity, finding new ways of breaking into the most up-to-date security controls. The GoA will continue to require a range of identification, protection, detection, response, and recovery controls, along with a strong cybersecurity awareness program supported by continued investment in cybersecurity staff, processes, and technology.

Artificial Intelligence (AI) is another tool being leveraged by threat actors to perform both reconnaissance and penetration activities. These tools must also be utilized by organizations as part of their cybersecurity arsenal to protect their digital assets.

Many of the attacks currently taking place come from nation-state sponsored actors who are hired by countries in direct competition with Alberta in various markets, such as oil and gas, agriculture, etc. These threat actors are attempting to break into provincial systems to gain access to information that will give them a competitive advantage that may disrupt Alberta government services, or impact public opinion about government and the services it provides.

According to a recent 2022 Cybersecurity Workforce Study performed by (ISC)2, the world's cybersecurity workforce gap currently stands at 3.4 million cybersecurity workers.

Another Side of the Cyber Threat: Lack of Cybersecurity Expertise

The worldwide shortage of qualified cybersecurity professionals and experts will have a major impact on businesses and governments alike.

The GoA is feeling the effects of this shortage. It is becoming very challenging to attract, hire, and retain experienced and skilled cybersecurity personnel. Cyber talent is scarce while the need for cybersecurity resources continues to increase. Organizations are essentially competing for the same resources.

In addition to the shortage of new resources, the GoA faces the challenge of losing experienced staff to retirement. This is causing an increased vacancy rate in critical technical positions, as well as loss of critical knowledge within the business, making it more difficult to develop complete and secure digital solutions.

While the focus is often on the lack of human resources providing cybersecurity services, the lack of expertise goes further. Many Albertans are not aware of the risks or lack the expertise to protect themselves, which makes them vulnerable to cyber threats. Often, cybersecurity information is overly complex, making it difficult for non-experts to understand and act.

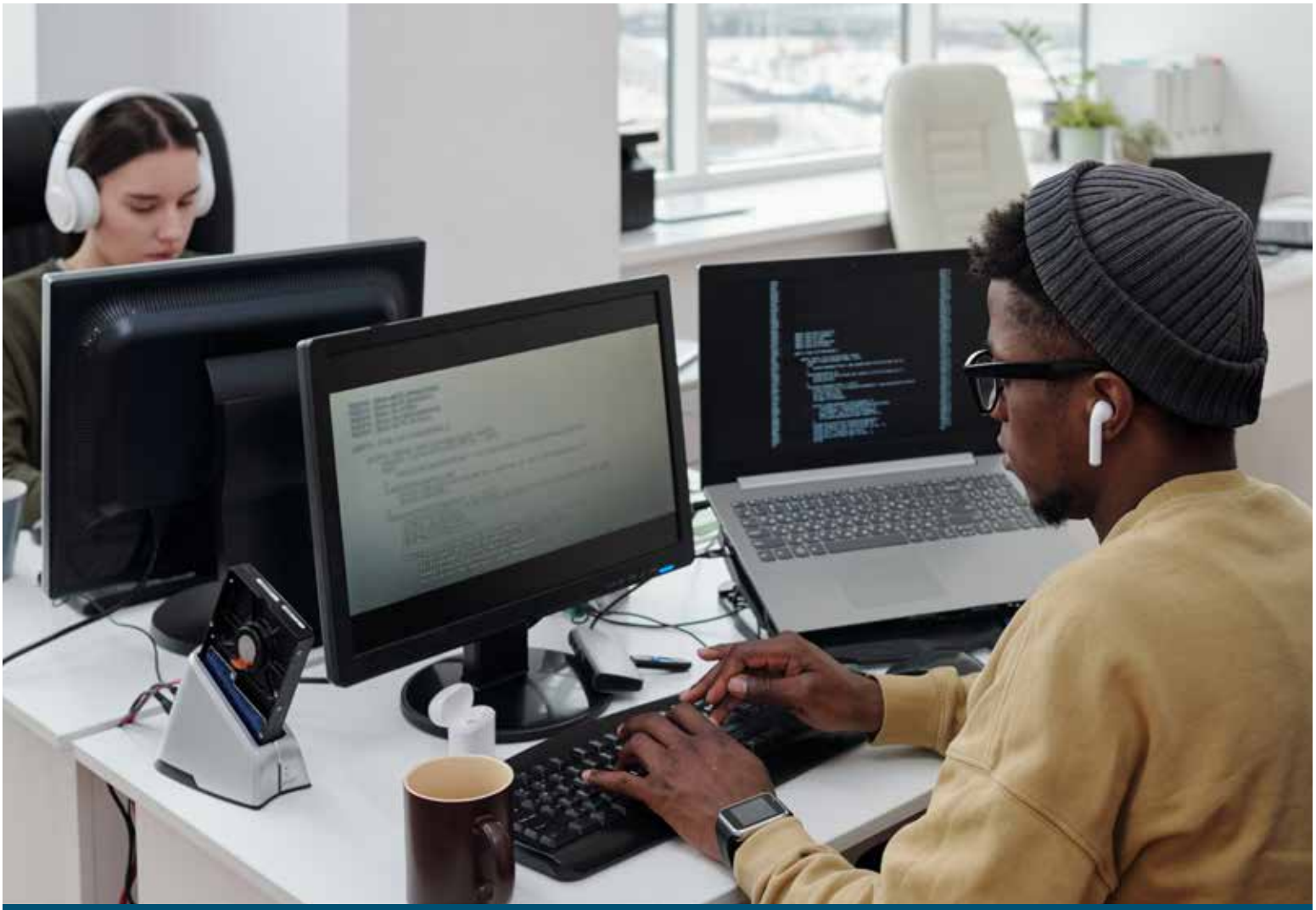
All of these issues contribute to a greater challenge for cybersecurity professionals, who must persuade people and organizations to take cybersecurity seriously even when they don't fully understand the threat. To address these challenges, it's important to increase awareness and simplify cybersecurity information. This can help ensure that more people and organizations have the knowledge and skills they need to protect themselves from cyber threats.

Assumptions and Considerations

While predicting what cyberspace or cyber threats will look like in the future can be challenging, the GoA must seek to understand the forces that shape the future to lead, influence and adapt to the evolution of its environment. The following are assumptions and considerations that will influence its future plans:

- The GoA recognizes the value of digital government services and agrees to prioritize their development.
  - We recognize that the migration to digital and mobile solutions also increases the attack surface.
- The volume and sophistication of cyber-attacks will continue to increase, especially with the emergence of AI and quantum technologies.
  - This will require ongoing increased stakeholder awareness, secure technology implementation, coordinated threat monitoring and incident responses, tested system resilience, and a strong cybersecurity workforce.
  - By leveraging AI in a responsible and ethical manner, the GoA can enhance its cybersecurity capabilities and improve its ability to respond to threats in a timely and effective manner.
- The supply chain the organization depends upon to provide digital services is controlled and maintained by independent third parties, making the organization susceptible to vulnerabilities left unmanaged by these third parties.
  - This threat and resulting risks must be identified, assessed, tracked and managed.
- New vulnerabilities, including zero-day exploits, will continue to be identified at a rate that is greater than the ability of organizations to respond in a timely manner.
  - Automation, including AI, should be leveraged where possible.
- The demand for digital solutions is growing and along with the importance of time-sensitive customer requirements.
  - The GoA must prioritize compliance with standards and best practices while leveraging automation to increase efficiency and reduce the risk of human error.

- The quantum technology threat to encryption systems will not become real for five to ten years
  - The GoA assumes that encryption of data in use, in transit and at rest, along with the control of an organization's encryption keys, will continue to be an effective security control to protect information.
- Social engineering attacks (mainly email phishing) will continue to be a primary attack vector for threat actors.
  - Awareness, improvements to authentication systems, and AI will be leveraged to identify these attacks.
- The worldwide shortage of cybersecurity talent will continue to challenge organizations.
  - This will impact organization's ability to identify, attract, and retain qualified cybersecurity staff.
  - Significant effort will be made to develop new cybersecurity talent across the province.
- The increasing use of AI and deep fakes for misinformation, disinformation, and manipulation presents a significant challenge for society.
  - The GoA must play a role in educating stakeholders to recognize and respond to these new threats.
- Differences in security requirements and risk tolerance across organizations demonstrates that one-size-fits-all security approaches are not effective.
  - Risk-based solutions tailored to particular organizations, user types, and even different age groups help in reducing the threat to organizations.
- Critical infrastructure services throughout Alberta are controlled by digital systems often accessible across the internet. The security of these systems is crucial to safeguarding the well-being of Albertans and the economic prosperity of Alberta.
  - The upcoming federal Bill C-26 will require critical infrastructure operators to comply with new regulations, and the GoA will provide assistance in the form of advice, communication, and coordination where appropriate to assist operators in meeting their obligations.
- Political tensions between nations are increasingly playing out in cyberspace, and it is important to recognize the potential impact of such conflicts. Cyber warfare can disrupt government and critical infrastructure services, impacting citizens' well-being, and affecting the economy.
  - The GoA will continue to proactively identify and assess threats, protect digital assets, monitor and detect cybersecurity threats, and respond and recover from any successful threats or incidents.
- The impacts of the pandemic and other global events on Alberta's economy will continue to be felt over the next several years.
  - This will result in increased pressures on budgets, requiring the GoA to continue to do more with less.
  - The focus of the Cybersecurity division will continue to be on leveraging existing investments to their full potential.



The Future We Are Building

The GoA's vision is of an Alberta cyberspace designed to ensure the utmost security, safety, and resilience of its systems, safeguarding Albertans' privacy by design. Empowering Albertans to confidently use the cyberspace for all their online activities, without fear of data breaches, cyber-attacks, or unauthorized access knowing there is robust and reliable infrastructure in place.

To realize the full potential offered by cyberspace, the GoA must ensure safety, security and resilience of the environment while promoting cyber threat awareness and cybersecurity knowledge. This complex, resource-intensive effort requires research, development, and investment, along with ongoing operational enhancements. In keeping with its vision, the GoA is committed to creating a cyberspace that is:

Secure

Digital assets must be secure and protected from damage, loss and unauthorized access or use. The privacy of Albertans must continue to be a top priority.

Safe

Information and technology must provide a safe environment for Albertans to interact with government. Data integrity must be maintained, and digital services must remain malware-free.

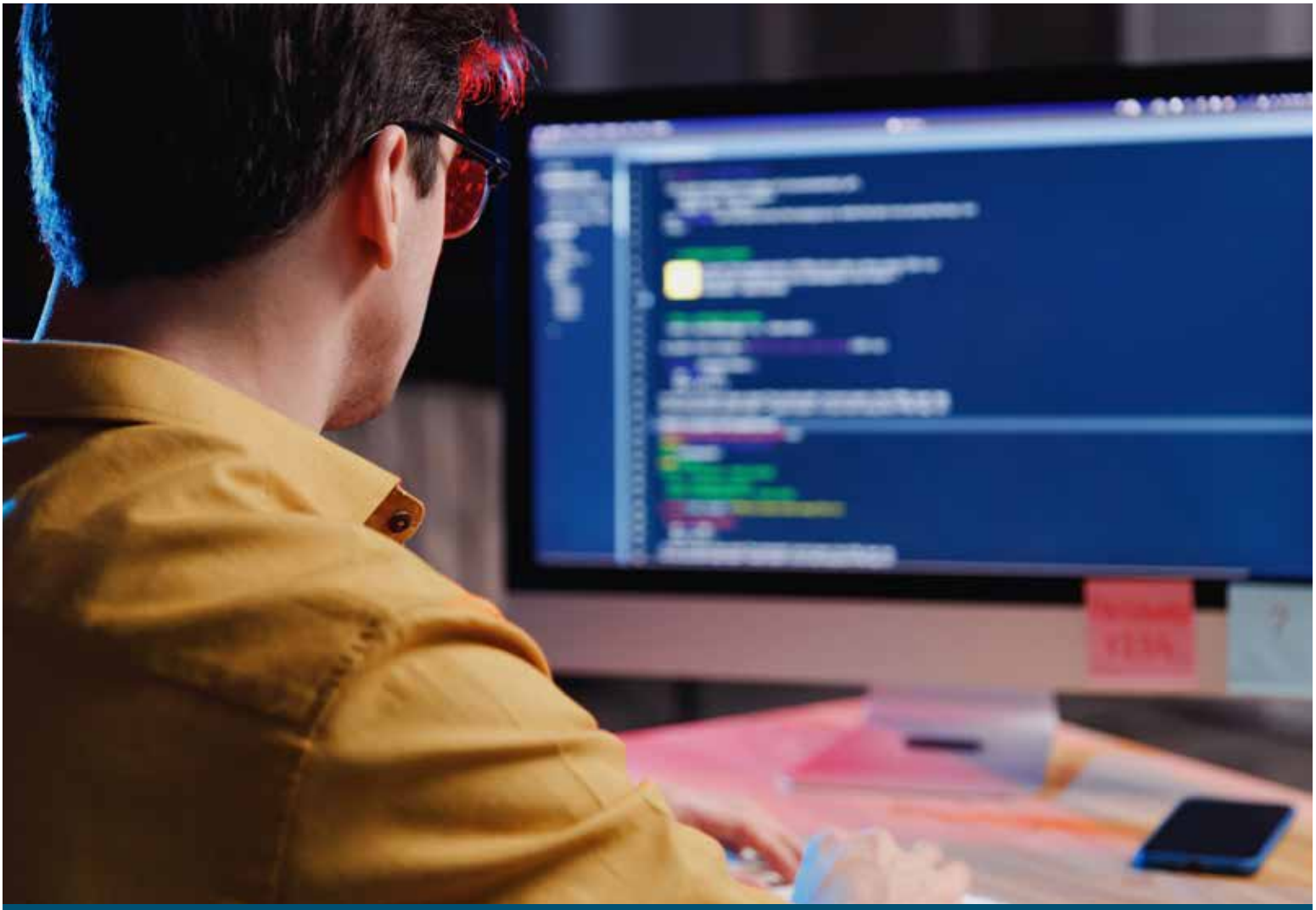
Resilient

When disaster strikes, critical systems and services must remain available to Albertans. In the event of system loss due to disaster events, systems and data must be recovered in a timely manner.

This cyberspace will also be supported by the GoA's Cybersecurity division, which aims to be the *leading cybersecurity authority* in Alberta and a recognized national leader, leading and facilitating a strong Alberta cybersecurity posture.

The division strives to foster a cybersecurity-first culture within the government and the province's stakeholders, driving proactive risk management and continuous improvement. Its vision is to be the premier cybersecurity authority in Canada, known for cutting-edge technology, rigorous standards, and collaborative approach. By prioritizing the protection of GoA proper, the division ensures that critical information systems and services across the province remain secure, resilient, and trusted, enabling the GoA to deliver high-quality services to the citizens of Alberta.

The Cybersecurity division is committed to understanding and managing risks, responding to incidents and threats, and advising, guiding, and educating stakeholders on cybersecurity best practices. Through close collaboration with Alberta stakeholders, it works to ensure that the province's digital assets and services are secure, safe, and resilient, with a special focus on GoA proper. The division's ultimate mission and goal is to *protect the confidentiality, integrity, and availability of Alberta's critical digital assets, thereby safeguarding Albertans and promoting the province's economic and social well-being.*



Strategic Approach

"The key to the Government of Alberta's cybersecurity strategy will be to adapt security controls to proactively identify and manage cyber threats before they become incidents."
Martin Dinel, GoA CISO

The cybersecurity landscape has changed, and traditional security measures are no longer enough to protect against evolving threats. To address this, the GoA adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which uses a risk-based approach to manage cybersecurity.

The NIST CSF has five key functions: Identify, Protect, Detect, Respond, and Recover. By using this framework, the government can communicate cybersecurity risks and prioritize actions to reduce them. The risk-based approach ensures that the right controls are applied in the right situations, and that security personnel provide information and recommendations to business decision-makers. More information on the NIST CSF can be found on the NIST website at www.nist.gov/cyberframework.

Strategic Cybersecurity Pillars

The following strategic pillars guide and support the GoA's cybersecurity program:

Expand the CyberAlberta Program

Many of Alberta's public agencies, businesses, and citizens are vulnerable to cyber-attacks due to a lack of cybersecurity expertise or resources. The absence of a platform for sharing and collaborating on critical security events further compounds the problem. The GoA has taken the initiative to address this issue by creating the CyberAlberta Community of Interest (COI), led by the Cybersecurity division and formed with cybersecurity leads from across Alberta's public and private organizations.

With the goal to strengthen the province's overall cybersecurity posture, the COI will focus on three critical cybersecurity challenges over the next three years, namely:

- Developing new cyber talent across the province.
- Establishing a cybersecurity compliance framework to assist Alberta's public and private organizations in developing their cybersecurity programs.
- Creating procurement mechanisms for cybersecurity-related goods and services that can be used by any CyberAlberta member across the province.

To achieve this goal, the Cybersecurity division will act as advisors to the province and facilitate collaboration and communication among stakeholders. By doing so, the GoA can leverage its unique position to engage and lead a community of interest focused on collaboratively enhancing the cybersecurity posture of the province.

A great example of this approach involves the coordination and facilitation of activities regarding the compliance of Alberta's Critical Infrastructure Operators to Bill C-26 announced by the Government of Canada in spring 2022.

Operationalize Risk-Based Cybersecurity Controls Framework

The GoA provides services to Albertans, which requires secure and resilient digital systems. The Cybersecurity division provides expertise and skills to ensure the safety of these services. All security decisions are based on risk information and recommendations from cybersecurity experts, with an enterprise perspective rather than just a cybersecurity lens.

Albertans trust the GoA to protect their information assets, and the Cybersecurity division has developed the Information Security Management Directives (ISMD) along with the IMT Cybersecurity Controls Framework to document and assess the maturity of basic controls that must be implemented within GoA systems. These controls are aligned with the NIST Cybersecurity Framework.

The CyberAlberta COI will also lead efforts to implement a flexible provincial cybersecurity compliance framework to level the cybersecurity controls implemented by Alberta stakeholders, strengthening the overall cybersecurity posture of the province. Initially, the GoA's control framework will be leveraged to engage with the COI to develop the provincial framework.

Enhance Cybersecurity Awareness

Most cybersecurity issues are traced to human errors, often amplified by the continuous acceleration of technology changes, making it impossible for staff to keep up with. The most effective tool to mitigate against this weakness is user training. When users understand their role in protecting assets, the value of those assets, and how to recognize and respond to cyber threats, the organization's chances of keeping assets secure drastically improves. Cybersecurity awareness and training must be a high priority and start at the top of the organization.

GoA's first email phishing test was conducted in 2016 before the establishment of the Cybersecurity Awareness program. It resulted in 40 per cent of staff taking the training and 28 per cent test failure rate. In 2018, intake improved to 60 per cent while failure rate fell to 17 per cent. In 2022, intake increased to 78 percent while failure rate went down to 4 percent.

The GoA has made annual cybersecurity training mandatory for all staff and contractors across the organization. The training uses regularly updated and relevant content. Additionally, the Cybersecurity division performs annual social engineering tests to assess the success of the training program and identify areas for improvement. The new CyberAlberta COI will leverage the GoA's experience and training material to increase awareness among Alberta stakeholders.

Improve Authentication Systems

The first, and likely the most important security controls involved in all transactional systems – whether digital or manual – is the confirmation that all parties involved in the transaction are who they claim to be. These security controls are called authentication systems. The GoA prioritizes building secure and transparent authentication and authorization controls that protect user privacy, while also enabling seamless and convenient digital interactions. By doing so, the GoA can instill confidence and trust in digital services, empowering users to fully embrace these transformative technologies.

In the next year, cybersecurity personnel will research and assess password-less solutions, such as biometrics and more efficient and effective identity verification processes. The goal is to improve the security of provincial systems while making it easier and faster for verified users to access them.

Shift to Proactive Protection, Detection, and Response Controls

Technology is evolving at an unprecedented pace, and with it, the creativity and adaptability of attackers is on the rise. This poses significant challenges for security professionals in their quest to protect information assets. The traditional passive-defensive cybersecurity approach, where an organization waits for an alert or a breach to occur before responding, is no longer adequate in today's threat landscape. A more proactive and aggressive strategy is required to identify and mitigate threats before they escalate into full-blown issues.

To strengthen its cybersecurity defenses, the GoA needs to take a comprehensive

and sophisticated approach. This includes using advanced technologies such as AI, machine learning, and predictive analytics to identify and respond to potential threats in real-time. Additionally, employee training must be prioritized to ensure staff can identify and report potential security incidents in a timely manner.

The GoA also needs to adopt a more robust philosophy for configuring digital services, which is where Zero-Trust comes in. Zero-trust is a security model that assumes that all users and devices accessing an organization's resources, whether inside or outside the network perimeter, are untrusted and potentially malicious. It relies on the principle of "never trust, always verify" and requires continuous authentication and authorization for every access request. This ensures serious consideration of risks and benefits have been reviewed prior to solution selection and implementation. The Cybersecurity division established a Threat Hunting team last year, which works closely with Cybersecurity Operations and Vulnerability Management teams to proactively identify and treat vulnerabilities.

To achieve a more aggressive cybersecurity posture, the Cybersecurity division modernized its entire cybersecurity toolset, focusing on Microsoft's offerings, and added fraud detection systems to its arsenal. The division will continue to evolve its cyber arsenal and share lessons learned to help fast-track the implementation of proven solutions. This year, it will work with Microsoft and the GoA's Managed Security Services provider to automate some response processes, leveraging AI and other automation means. The goal is to automate routine and repetitive tasks, which were previously outsourced. Lessons learnt and successes will be shared with the CyberAlberta COI to help fast-track the implementation of secure controls and solutions across the province.

Assess Backup Solutions with Consideration to Cloud Migration

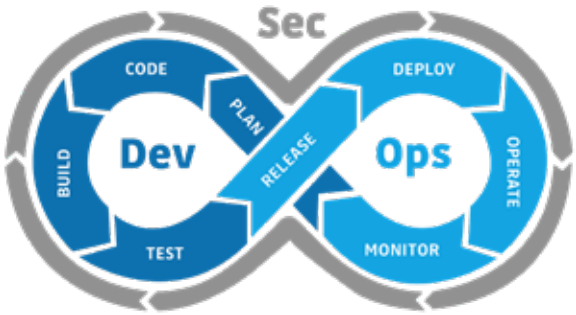
Over the past eight years, significant progress was made to structure and improve the GoA's disaster recovery framework. The framework helped to identify critical assets, to document and test recovery plans, and to train staff in their specific disaster recovery roles. The Cybersecurity division is now focused on optimizing the framework.

The migration of services to the cloud has changed the GoA's disaster recovery approach. While on-premise systems continue to be recovered using on-premise backups, the organization is now relying on the high availability and reliability of cloud solutions to ensure availability of cloud-based digital services. This approach carries some risks regarding the recovery of assets that may have been deleted or modified by error, and to address these risks, the Cybersecurity division will assess and reconsider its current backup strategy and solutions.

Ensure Security throughout the Digital Assets' Lifecycle

To ensure the security of digital assets, organizations need to implement strong security measures at every stage of the asset's lifecycle. This includes from creation to disposal, to maintain the integrity, confidentiality, and availability of the asset. Consistently focusing on security can help organizations mitigate the risk of cyber threats, protect their assets, and maintain the trust of their stakeholders.

The demand to digitize government services faster has increased over the past five years, with the most popular development strategy being agile development. The DevSecOps approach – integrating the development, security and operationalization of systems as part of one complete process – brings together all the services and skills needed to develop and implement solutions at the right time.



Leverage Threat Intelligence to Evolve Security Controls

Although the source of future cyber threats or new technologies that may enhance security protection cannot always be predicted, the GoA can use threat intelligence, data analysis, and research to improve and evolve its security controls to counter the ever-evolving cyber threat.

To achieve this, a new Threat Intelligence and Reporting team was established last year, with the aim of identifying security data collections and reporting them in a more useful and actionable manner. The team also conducts research on both threats and technology advancements to ensure the organization's digital assets remain well protected. The information gathered and reported by the team is shared with the CyberAlberta COI parties, along with advice to strengthen Alberta's overall cybersecurity posture.

In the coming years, the Cybersecurity division will continue to monitor quantum computing, which poses a threat to encryption systems used to protect data in transit and at rest. The team will also research password-less technologies to improve authentication systems and investigate how machine learning and AI can be used to automate or orchestrate more of the province's cybersecurity responses and actions.

Develop New Cybersecurity Talent

Due to the significant worldwide shortage of cybersecurity talent and professionals, organizations have to become more creative in finding ways to attract and retain staff.

The Cybersecurity division implemented a very successful two-year work experience program to fast-track training of four candidates through teaching materials and on-the-job experience. This program will be expanded and offered to the rest of the province, along with all artefacts developed to run the program.

The issue of cyber talent shortage will be a key focus of the CyberAlberta COI. The goal is for the province to become a centre of excellence for the development of skilled cybersecurity professionals, while satisfying the resources requirements of Alberta stakeholders. Approaches that are being considered include the development of a provincial post-secondary cybersecurity curriculum, leveraging short boot camps to develop new cybersecurity talent, and a K-12 cyber safe program with a focus on grade 9-12 cyber skills development leveraging micro-certification.

Moving Forward

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

Alberta's Cybersecurity Strategy is the organization's plan for securing the GoA's digital assets, while also assisting and supporting Alberta stakeholders to achieve this same goal. The strategy's success will be measured by tracking, assessing, and reporting the results and progress achieved by the Tactical Plan supporting this strategy.

The GoA recognizes that digital services are critical to the daily lives of Albertans, and the organization is prioritizing the digitization of more services to make them easily accessible. However, this increased reliance on digital services has also increased the threat surface for cyber attackers. The Cybersecurity division plays a crucial role in the GoA's Cybersecurity Strategy by collaborating with external organizations and stakeholders to ensure that the latest threat intelligence information is available to all parties involved.

Cybersecurity is a responsibility shared among all information stakeholders, including Albertans, Alberta Public Service employees, the private sector, and service partners. The GoA's Cybersecurity Strategy promotes awareness of cyber threats and strong security practices and encourages stakeholders to adapt their behavior and implement the necessary processes and technologies to meet security standards.

To ensure that Alberta stakeholders are ready to address emergent attacks, the Cybersecurity division collaborates with federal and provincial jurisdictions, local police, and law enforcement authorities. Sharing information and working collaboratively is essential to eliminate and mitigate common cyber threats throughout Alberta.

If you have any questions, concerns, or feedback regarding Alberta's Provincial Cybersecurity strategy, please email goa.cybersecurity@gov.ab.ca.