Executive Council—Protecting Information Assets Follow-up

Summary

The Government of Alberta uses a variety of information technology systems to provide programs and services, and to host and process personal information.[1]

In our *October 2008 Report*, we recommended that Executive Council establish a central security office to oversee information security for the organizations using the government's shared computing infrastructure. We also made seven IT security recommendations directly to Service Alberta and three recommendations jointly to Service Alberta and Infrastructure.

In 2010, we reported that Service Alberta implemented the Corporate Information Security Office, and that the CISO then developed, implemented and communicated 10 IT security directives to ministries. Service Alberta and the Ministry of Infrastructure developed and communicated physical and environmental standards for shared data facilities (SDF) that store the government's information systems and data. The ministries then started work on implementing those standards in SDFs throughout Alberta.

What we found

In our 2012 follow-up to the remaining recommendations we found that Service Alberta (see page 67):

- had fully implemented eight of the original 11 IT security recommendations
- could not fully implement the three remaining recommendations without changes to the current decentralized IT governance model, because it lacked the authority and responsibility for overseeing IT security for some government entities

Service Alberta does not have the authority or ability to monitor and enforce IT security throughout the government. Because IT security standards, monitoring and enforcement are not consistent throughout government, there is a risk that public information assets are not properly secured. As security is only as strong as its weakest link, a security issue in one government entity creates a risk to all government entities.

We conclude that IT governance could be improved and made more consistent across government, even though the current decentralized approach to IT management will make improvement challenging. We therefore make a new recommendation to Executive Council, to assess the risk to public information assets across government and to determine how best to ensure risks are properly mitigated.

Why this is important to Albertans

Albertans need to:

- access online services and accurate government information when needed
- know that the IT systems the government and publicly funded entities use are secure, and that they protect personal and government information from unauthorized use

Albertans expect government and publicly funded websites and systems used to provide programs and services to be available when needed. They expect the data they process and host to be secure from potential attack. They also expect the government will maintain adequate security standards to protect these applications and systems, and that all technologies used to deliver programs and services are implemented and maintained in a manner that safeguards confidential government and personal information.

[1] For the purpose of this recommendation, the Government of Alberta refers to all ministries, their departments, and the agencies, boards and commissions that are part of the consolidated financial reporting process for each ministry.

What needs to be done

Four years after our initial recommendation, our original findings and concerns are still applicable to the government as a whole. We expect that Executive Council, through a risk assessment, will determine how to improve corporate IT governance by setting consistent IT security requirements throughout the government and ensuring they are met, to adequately protect all public information assets.

Findings and recommendations

Assess risks and improve oversight of public information systems

Background

The Government of Alberta creates, uses and manages large volumes of sensitive and confidential information. This information is created on thousands of devices and is processed and hosted in electronic form on servers throughout the government, and at government and third-party data centres throughout the province. This data, and the devices on which it is created, processed and stored, are collectively known as "information assets."

In our *October 2008 Report* (no. 4—page 53), we recommended that Executive Council establish a central security office to oversee all aspects (develop, communicate, implement, monitor and enforce) of information security for organizations that use the government's shared information technology infrastructure.

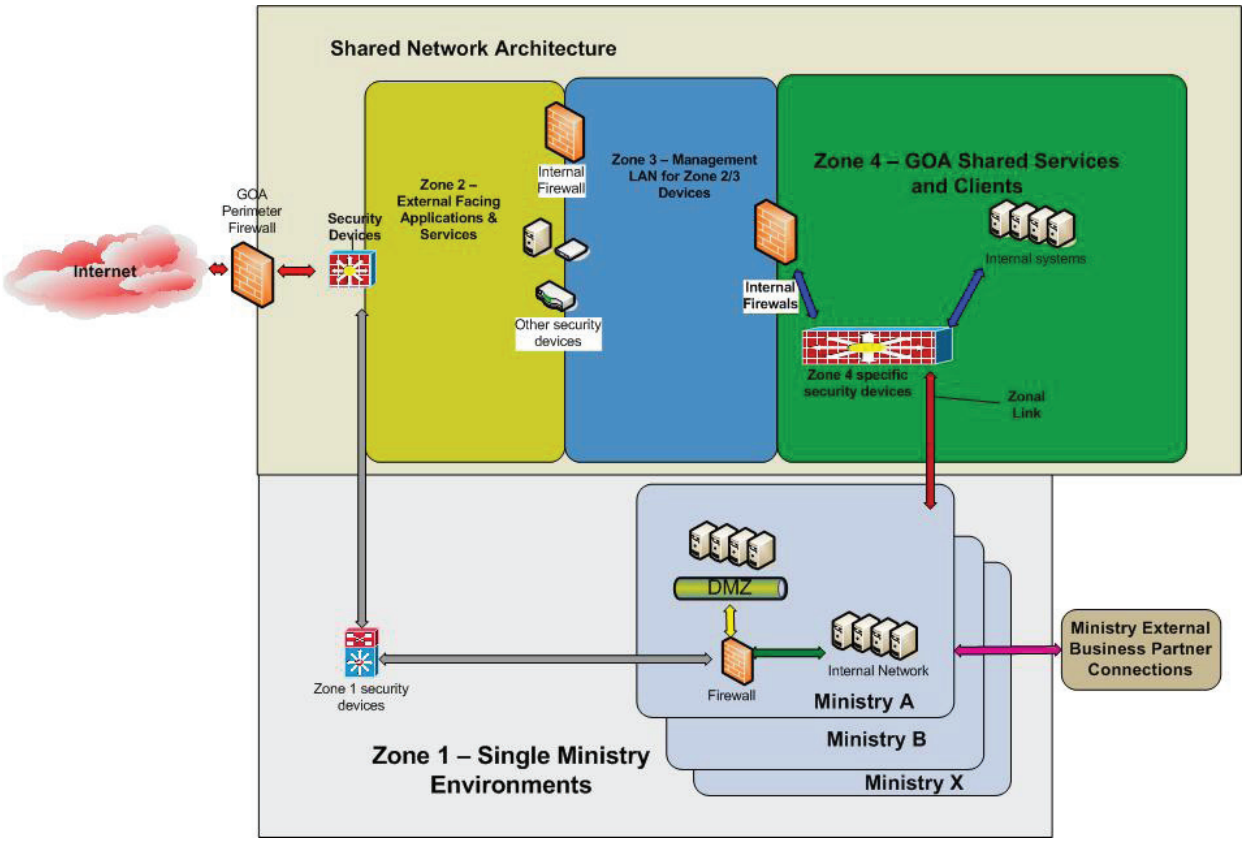
In response to our recommendation, Executive Council referred to the Information Management Technology Strategy giving Service Alberta the mandate to establish a central security office to oversee all aspects of information security for government's shared information technology infrastructure. Service Alberta subsequently created the Corporate Information Security Office and hired a director for it. In our *October 2010 Report* (page 77), we confirmed that the CISO had developed, implemented and communicated ten IT security directives, thus fulfilling the first half of the recommendation. Specifically, Service Alberta:

- developed, implemented and communicated IT security standards to government departments, through its directives
- implemented a system to prevent and monitor security issues for zones 2 to 4 of the government computing environment

However, to fully implement the remainder of our recommendation, Service Alberta would need to monitor and enforce compliance with its security directives.

The following diagram describes the government's IT security environment:

The Government of Alberta has established a zoned network architecture as a means to control security and perimeter access between the shared computing environment and departments, agencies, boards and commissions with separate networks and systems (i-domains and separate infrastructures).[2]



Internet—the internet zone includes agencies, boards and commissions that host their web applications and/or networks and data outside of the government's core computing environment.

Zone 1 includes departments and other consolidated reporting entities such as agencies, boards, commissions and Crown corporations that have chosen not to be part of the shared computing environment and instead manage their own infrastructure. There is perimeter protection from the internet in this zone, and from this zone into the other zones of the government's computing environment. These entities, though, are responsible for setting and meeting their own IT security policies, procedures and standards and are not part of the government's shared computing domain.

Zones 2 and 3 were designed to house services that have internet facing requirements. Zone 2 is partially exposed to the internet and Zone 3 contains systems that manage those services in Zone 2. This architecture provides additional layers of separation between the internet facing systems and the core government infrastructure.

[2] Diagram received from Executive Council

Zone 4 includes databases, desktops and other important information assets in the government's shared computing domain.

The zone architecture is set up such that each zone has its own perimeter protection. Traffic from one zone to another zone must pass through this protection layer. These protection mechanisms include firewalls and intrusion prevention sensors.

It is possible that security breaches from the internet and zone 1 can pass through to zones 2 through 4 as normal traffic is processed over the network. The Government of Alberta shared environment has implemented perimeter protection and other protocols to mitigate the risk of external security breaches impacting sensitive core systems. However, better coordination of security protocols and reporting from entities outside of the shared environment, including those in zone 1, with the Corporate Security Office, would further enhance overall security across all zones.

During our annual audits of financial statements, we review IT controls that support financial reporting throughout government. Through these audits, we are aware that certain entities do not know of or cannot comply with Service Alberta's 10 IT security directives. Further, some entities are unsure of what IT security standards they should follow or even who is responsible for their IT security. For example, some government entities have their systems within the government computing environment (zone 1), but do not receive security services from Service Alberta. Other government entities have their information assets hosted on the internet outside of the shared computing environment on the internet, where they are subject to additional security risks. Other than our annual audits to assess IT controls that affect financial reporting, no one monitors, assesses or enforces IT security in many of these publicly funded government entities. Further, IT control assessments do not typically look at non-financial but equally important systems that host other data such as health records, driver's licences or birth certificates.

Recommendation: Assess risk and improve oversight

11 RECOMMENDATION

We recommend that Executive Council:

- assess the risks to public information assets throughout the government
- determine if the government has adequate IT security policies, standards and controls to mitigate risks
- determine who is responsible and accountable to ensure that public information assets are adequately protected. Specifically:
  - who is responsible for monitoring compliance with IT security requirements
  - who is responsible for ensuring or enforcing compliance with security requirements
  - what actions should be taken when non-compliance is identified
  - how is compliance to security requirements demonstrated

Criteria: the standards for our audit

The government should:

- know what the risks are to public information assets
- have adequate IT security policies, procedures, standards and controls to mitigate risks to public information assets

Further, the government should:

- know who is responsible and accountable for the security of public information assets in all ministries and their government entities
- be able to demonstrate that public information assets are adequately protected from unauthorized use, change, disclosure or loss

Our audit findings

Key findings

- Service Alberta developed and implemented IT security directives and then communicated them to all ministries.
- It is not clear if all ministries or government entities are following the security directives, as regular reporting from the entities is not gathered.
- The government does not have sufficient assurance mechanisms for publicly funded agencies, boards and commissions to demonstrate they adequately protect public information assets.
- More consistent corporate oversight is needed across government, to ensure public information assets are adequately protected.

We assessed the design and implementation of the IT security directives, SDF[3] standards and their respective supporting procedures and standards. We found they would be adequate to provide a minimum level of security for the government if properly implemented and consistently followed.

Service Alberta can monitor only those devices that it hosts in the shared network portion of the government network (zones 2 to 4), and does not have the authority to enforce its security standards on non-Service Alberta owned or administered devices. Ministries and other government entities also use devices in zone 1 of the government's network. A security issue in any zone opens the information assets of all ministries and all zones within the network to unnecessary security risks.

Other government entities have information assets outside of the government's computing environment. These entities may not have adequate monitoring for or protection against security issues, attacks or unauthorized access. We don't know whether their security protection is adequate because there is currently no one assessing it. Further, not all government servers that host and process important and possibly confidential or critical information are located in government SDFs. Thus, network devices and servers in about 800 locations within the computing environment that host government data are not as well protected. And other devices and servers belonging to government entities are in other locations or third-party data centres outside of the computing environment. Owners of devices and servers in locations less secure than the government's secure SDFs introduce additional risks.

In our initial recommendation to Executive Council in 2008, we found that no one single government function had the authority and responsibility to:

- design security for the government as a whole, including agencies, boards, commissions and post-secondary entities
- evaluate the effect of weak security in one part of the government and its impact on the rest
- detect attempted intrusions or respond to potential security threats across the government
- continually monitor the government for threats and vulnerabilities and develop remediation plans
- enforce the solutions required to keep the government secure

[3] Shared data facilities

Although Service Alberta developed IT security directives and standards, and is monitoring for compliance to them in zones 2 to 4 of the shared computing environment, some departments and government entities have yet to demonstrate compliance. Steps should be taken to ensure sufficient oversight so entities are not putting the government at risk.

Service Alberta provides a suite of services—shared computing infrastructure—to government organizations. Service Alberta is responsible to ensure the shared infrastructure is secure and reliable. However, under the current decentralized approach to IT governance, Service Alberta does not have the authority to ensure that organizations using the shared infrastructure meet minimum baseline security requirements within their own applications, systems and computing environments. The government uses a decentralized approach to information technology. This "federated" or "trusted" IT environment allows ministries and other government entities to join the government's computing environment quickly and share resources such as printing and email.

A decentralized, federated approach may work well for program delivery, but it poses significant challenges for IT security. The government's existing decentralized computing environment creates inherent vulnerabilities and risks to the information of government and Albertans. Information security is only as strong as the weakest link—if one part of the government doesn't have adequate security controls in place, it can affect other parts of the government that have well-designed security controls. Because information security throughout government is not consistently enforced, all public information assets may be exposed to unnecessary risks.

Audits and reporting to date have not revealed evidence of significant security breaches. However, regular and more rigorous reporting of compliance to the Government of Alberta directives by all entities and departments would provide better assurance that security breaches can be avoided or mitigated in the future.

There is a gap in the government's corporate IT governance, which results in an inability to:

- monitor for security incidents throughout all government ministries—including the departments and publicly funded agencies, boards and commissions that are a part of their consolidated financial reporting process
- ensure all government entities meet and follow adequate IT security standards to protect public information assets
- take appropriate action when IT security standards are not being followed

Events subsequent to the audit

Executive Council has recently formed the Deputy Minister Information Management and Technology Committee to provide a cross-government venue for the review and approval of strategies and policies of government IT management and technology services. Included in the Committee's mandate is the oversight of systems and processes in place to address IT security. We will follow up on the work of this committee in due course.

Implications and risks if recommendation not implemented

Without adequate security policies, the ability to monitor and enforce them throughout government, or the need for government entities to demonstrate they adequately protect public information assets, government information and the personal information of Albertans is at risk of unauthorized use or disclosure.