Chapter 5
Central Services—Data Centre Security

1.0 Main Points

The Ministry of Central Services (Central Services) provides information technology (IT) services to government ministries and some other government agencies (clients). Central Services uses a data centre, operated by a third-party service provider, to deliver IT services to Central Services clients on its behalf. The data centre houses computer network equipment and servers that support client systems and data.

Each year, we examine whether Central Services has effective processes to secure the data centre. For the period January 1, 2015 to December 31, 2015, Central Services addressed three of our five recommendations. However, the remaining two areas continue to require attention. We found that Central Services had effective processes to secure the data centre except it needs to:

- Properly update and configure all network equipment and servers
- Have an approved and tested plan to recover critical systems and data in the event of a disaster

As a result, there is continued risk that systems and data will not be available to clients when required, or that systems or data may be inappropriately modified or accessed.

2.0 Introduction

This chapter reports the results of our 2015 audit of whether the Ministry of Central Services had effective processes to secure the data centre. See **Section 6.0 Glossary** for the definition of IT terms used throughout this chapter.

Central Services is responsible for developing, implementing, monitoring, and enforcing IT security policies and standards for its clients.[1] In addition, it is responsible for buying and providing IT goods and services.

It is also responsible for providing a secure data centre to house client applications and data. Central Services is to provide guidance, policies, and monitoring to help clients protect their IT applications and data.

Central Services' clients include 15 ministries and 10 government agencies (see **Section 5.0** for details). Central Services has agreements with each of its clients. These agreements outline the specific IT services Central Services will provide to each.

Central Services provides its IT services primarily on a cost-recovery basis; that is, clients pay for services Central Services provides directly or obtains them through service providers on their behalf. In 2014-15, Central Services spent $121.8 million, recovering $107.5 million from its clients.[2]

[1] *The Ministry of Central Services Regulations, 2012;* this includes responsibility for IT information and records management.
[2] Ministry of Central Services, *2014-15 Annual Report*, p. 19.

As shown in **Figure 1**, Central Services provides some IT services directly; it engages service providers to provide others (e.g., operating the data centre) at an annual cost of $27 million.[3,4] While it uses a service provider, Central Services remains responsible for meeting the security requirements set out in its agreements with clients.

Central Services' agreement with its data centre service provider sets out the roles and responsibilities of both Central Services and the data centre service provider.

Figure 1—IT Services Central Services Provides to Clients

Central Services Provides Directly	Data Centre Service Provider Provides
❱ Developing and implementing IT security policies and programs for its clients ❱ Maintaining a help desk to respond to client requests (e.g., granting/removing access to systems/data, password resets) and to help resolve problems encountered by client staff ❱ Monitoring and following up on security threats identified by security tools (e.g., firewalls) ❱ Reviewing and following up on security information provided by its service providers ❱ Providing computers to client staff ❱ Supporting application development and change management	❱ Operating the data centre in which client applications reside; the data centre includes: - all servers that operate the network and host applications (that is, hold the computer programs that store and work with client information) - network and telecommunications equipment that allow computers to send/receive data - systems used to backup data ❱ Implementing physical security controls to prevent unauthorized access to the data centre ❱ Configuring, managing, and maintaining data centre and all related equipment as mutually agreed upon with Central Services ❱ Revisiting mutually agreed upon requirements on a periodic basis (e.g., every 12 months) ❱ Reporting annually to Central Services on compliance with agreed-upon requirements ❱ Remedying equipment not in compliance with agreed upon requirements or seeking Central Services' exemption to requirements. For example, Central Services may exempt a server from receiving security updates if there is a risk that applications on that server may not run properly with the latest server updates.

Source: Provincial Auditor of Saskatchewan (2016).

Central Services indicates that it delivers to its clients IT services covering thousands of electronic assets (e.g., almost 7,000 desktop computers and over 5,000 laptops) and 1,150 applications. Over 12,000 staff of its clients located throughout the province use these IT equipment and applications.

2.1 Importance of Effective Security Processes

Information technology allows people to access systems and data from anywhere in the world at any time. This opportunity creates a corresponding challenge—how to effectively secure systems and data against cyberattacks[5] that can come from anywhere including IT security breaches by those inside the network.

[3] Central Services or its predecessors directly operated a data centre from 2005 until December 2010. Following this, Central Services outsourced these services to a third-party service provider.
[4] *2014-15 Public Accounts of the Government of Saskatchewan – Volume 2*, p. 52.
[5] Cyberattacks include the unintentional or unauthorized access, use, manipulation, or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.

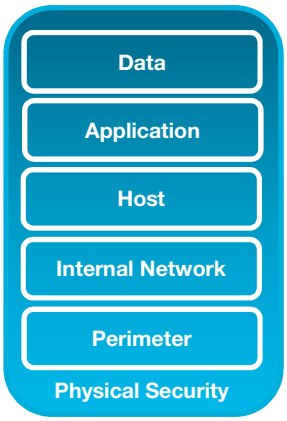
Public Safety Canada has reported that the frequency and severity of cyberattacks is accelerating.[6] Employees inside organizations perpetrate purposely an estimated 31% of IT security breaches; actions of employees inadvertently cause another 23% (e.g., accidentally opening a malicious email).[7]

The Saskatchewan Government is not immune to the threat of security breaches; nor can it ever fully protect itself against all cyberattacks. Human error or intentional malicious acts will always make systems and data susceptible to attacks. However, well-secured systems can better defend against attacks, detect potential failures, and limit loss if a breach of systems and data occur.

To protect against the many ways that an attacker may attempt to gain access to systems and data, many organizations apply a defense-in-depth strategy as outlined in **Figure 2**. The principle of defense-in-depth is that layered security mechanisms as a whole increase security of systems.

Figure 2—Defense-in-Depth

The diagram to the right illustrates the common layers where security may be implemented. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system. Due to the ongoing discovery of new security weaknesses and given that no security mechanism is foolproof, securing only one layer (e.g., perimeter) is not adequate. It is important that security be addressed at all layers based on assessed risk (i.e., defense-in-depth).



Source: Diagram from The Business Forum, Antivirus Defense-In-Depth Guide (2015).

The data centre includes the components reflected in the diagram in **Figure 2**. Central Services is responsible for physical security of the data centre, and the security of the perimeter, internal network, and hosts (i.e., servers). Security for each of these layers help protect the systems and data that reside within the data centre against hacking. Clients are responsible for the security of their applications (i.e., systems) and data.

A weakness involving one or more clients or the data centre can pose risks to all client applications and data within the data centre. For example, employees may inadvertently introduce virus threats to the network, or data centre staff with access to install programs on the network (e.g., system administrators) may inadvertently, or purposefully damage data or access it without proper authority.

Central Services must make certain its data centre service provider implements effective security processes, and its clients adhere to effective security requirements. Without effective security controls, someone could gain unauthorized access, inappropriately access confidential information, inappropriately modify systems or data, or perform acts that could affect availability of systems and data.

[6] www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, p. 3 (19 March 2016).
[7] IBM, *IBM 2015 Cyber Security Intelligence Index*, (2014).

3.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of our audit was to assess whether the Ministry of Central Services had effective processes to secure the data centre for the period of January 1, 2015 to December 31, 2015.

The audit did not assess the effectiveness of security controls (e.g., user access controls) for specific client applications (e.g., financial accounting or payroll applications) because this is the responsibility of clients and not Central Services.

We examined both Central Services' and its data centre service provider's controls and processes used to secure the data centre, including network device configuration, server patch levels, and physical security at the data centre. We interviewed Central Services and service provider staff. We also examined Central Services' agreements, minutes, reports, and policies.

To conduct our audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate Central Services' processes, we used criteria (see **Figure 3**) based on the work of other auditors and literature listed in the selected references. The criteria are primarily based on *The Trust Services Principles, Criteria, and Illustrations* authored by the Chartered Professional Accountants of Canada and the American Institute of Certified Public Accountants. Central Services management agreed with the criteria.

Figure 3—Audit Criteria

1.	**Demonstrate management commitment to security**
1.1	Have an effective agreement with its service provider
1.2	Effective threat and risk assessments are performed
1.3	Management approves effective policies and procedures
1.4	Management effectively monitors security including its service provider
2.	**Protect the data centre from unauthorized access**
2.1	Effective user access controls protect the data centre from unauthorized access
2.2	Effective physical security controls protect the data centre from unauthorized access
3.	**Ensure the availability of data centre**
3.1	Effective backup processes exist and are followed
3.2	Effective disaster recovery plans exist and are tested
4.	**Ensure the integrity of systems and data**
4.1	Effective change management processes exist and are followed
4.2	Effective operational processes exist and are followed

We concluded that, for the period of January 1, 2015 to December 31, 2015, the Ministry of Central Services had, except for the following areas, effective processes to secure the data centre. Central Services needs to:

- **Adequately secure all key servers and network equipment**
- **Have an approved and tested plan for the data centre in the event of a disaster**

4.0 Key Findings and Recommendations

In this section, we set out our key findings and recommendations.

4.1 Need to Adequately Secure Servers and Network Equipment

We recommended that the Ministry of Central Services adequately configure and update its server and network equipment to protect them from security threats. (2012 Report – Volume 2; Public Accounts Committee agreement September 23, 2014)

Status – Partially Implemented

Adequate Network Configuration Needed

Central Services continues to lack information from clients about the classification (e.g., level of sensitivity) of the data residing on servers within the data centre. Central Services needs this information so that it can work with its clients to determine the appropriate security level for the data (i.e., provide stronger security controls for confidential information such as social insurance numbers). Once it knows the appropriate level of security, it must work with its service provider to place applications and data on servers, within a network structure designed to provide the required level of security.

By December 2015, Central Services had not finished documenting which client data resides on which particular servers. It also had not established separate parts of the network to differentiate security controls based on data classification. Without this work complete, Central Services and clients may not have effective security controls implemented for protecting applications with sensitive data.

As in prior years, Central Services used firewalls to help protect its data centre from hackers. Central Services located data centre firewalls at appropriate locations, and monitored reported security events. However, we found that the firewalls (at the data centre and at client locations) were not properly configured. For example, Central Services' data centre firewall rules did not sufficiently restrict access to the data centre because Central Services did not effectively define the firewall rules that its service provider must follow. Central Services indicated that it plans to review and update the rules for the data centre firewall in 2016. Inadequate firewall rules increase the risk of a security breach.

Updating of Network Devices Needed

We also found firewalls at client locations and network devices (e.g., switches) were not receiving software updates, or were no longer receiving user support. This means these devices were not patched for known vulnerabilities, dating back to 2013 for client firewalls. This increases the risk of a security breach.

Timely Updates of Servers for Security Vulnerabilities Needed

At December 2015, Central Services noted over 100 of the 1,000 servers, which it manages on behalf of clients, used unsupported versions of operating software. Using unsupported software means security updates (e.g., Windows updates or patches) are not available for these servers, which increases the risk of security breaches and availability issues.

During 2015, Central Services told clients which of their applications had underlying components (i.e., server hardware, server operating systems, or databases) that the related vendor no longer supported. Central Services recommended clients either upgrade the component(s) to a supported level, or formally document acceptance of the risk. Where a client accepts the risk, Central Services needs to ensure there is no other client information on the unsupported server that requires increased protection.

Central Services worked with some clients during 2015 to upgrade servers and databases to vendor supported levels. However, by December 2015, not all clients had formally documented their acceptance of the risk related to unsupported components.

Although Central Services' data centre service provider updated most servers, on at least a quarterly basis, we found patching on all servers was not complete for all known vulnerabilities. All 10 servers we tested were missing updates (some related to updates [patch releases] made available in 2012). We found Central Services did not ask its staff or its service provider to do these updates.

Also, it did not have a documented risk analysis as to why these servers did not need the missing updates. Security updates address known security vulnerabilities. Attackers wanting to hack into systems can exploit these vulnerabilities to gain unauthorized access to applications and data.

4.2 Complete and Tested Disaster Recovery Plan Required

We recommended that the Ministry of Central Services have a disaster recovery plan for the data centre and client systems. (2006 Report – Volume 3; Public Accounts Committee agreement April 3, 2007)

Status – Partially Implemented

As in prior years, Central Services did not have a complete and tested disaster recovery plan for the data centre. At December 31, 2015, Central Services' agreement with its data centre service provider continued to require the service provider to provide only best efforts recovery service in the event of a disaster. If a disaster occurred, it is not clear:

- How long it would take Central Services' data centre service provider to recover client applications and data so that clients can use them
- If best efforts recovery would meet client needs, or

- How much the recovery would cost Central Services or its clients.

As a result, some of Central Services clients with critical client systems (e.g., student loan system, correctional information system, courts management/fines collection system) do not have disaster recovery plans.

A few Central Services' clients[8] have signed separate disaster recovery agreements with other service providers to restore specific critical systems and data if a disaster occurs. However, the recovery of critical client systems remains dependent on the availability of certain equipment and systems within the core data centre (e.g., network switches, firewalls, network storage, network drives, email) to recover business operations following a disaster. As a result, having multiple agreements for disaster recovery does not result in an effective enterprise approach to disaster recovery for the data centre.

It is not clear how long clients could operate effectively in recovery mode, or what the costs of operating under such conditions on a longer-term basis would be. Also, lack of effective disaster recovery plans could result in critical IT systems, data, and services not being available to the Government and the people of Saskatchewan when needed.

Management advised us that Central Services continues to analyze alternatives for disaster recovery services including for the core data centre and critical client systems.

4.3 Access Better Restricted

We recommended that the Ministry of Central Services adequately restrict access to systems and data. (2012 Report – Volume 2; Public Accounts Committee agreement September 23, 2014)

Status – Implemented

By December 2015, Central Services used more secure methods for accessing systems and data. At December 31, 2015, network accounts complied with its password standards. Central Services removed local-administration rights to computers (which enable users to change configuration settings that could impact a computer's security) except where required to carry out daily operations. Central Services developed processes for monitoring users with these rights.

4.4 Client Security Reports Provided

We recommended that the Ministry of Central Services provide relevant and timely security reports to its clients. (2009 Report – Volume 3; Public Accounts Committee agreement June 18, 2010)

Status – Implemented

[8] Clients with separate disaster recovery agreements include the Ministry of the Economy for its gas and oil systems, the Ministry of Social Services for its children-in-care case management system, Saskatchewan Housing Corporation for its housing management system, and the Ministry of Finance for the government's financial management system.

In 2015, Central Services gave its clients information to help them make decisions about the security of their IT applications and data. The information included:

- Known security risks including security investigations completed (e.g., related to lost computers)
- Risks reported to and/or accepted by the client (e.g., user access rights greater than Central Services' policy)
- Network user accounts not used for an extended time period
- Applications with infrastructure components no longer supported by a vendor

4.5 Security Policy Approved

We recommended that the Ministry of Central Services establish information technology security policies for its clients. (2008 Report – Volume 3; Public Accounts Committee agreement December 10, 2008)

Status – Implemented

In October 2015, Central Services approved a new information security policy for its staff and clients. The policy establishes roles and responsibilities for both Central Services and its clients.

Central Services based this security policy on an accepted technical security framework – ISO/IEC 27002:2013.[9] It posted the policy on its intranet to make it accessible to clients. It made clients aware of the policy through meetings with them.

5.0 Central Services IT Client List at December 2015

Ministries	Agencies
Ministry of Advanced Education	Apprenticeship and Trade Certification Commission
Ministry of Agriculture	Financial and Consumer Affairs Authority of Saskatchewan
Ministry of Central Services	Global Transportation Hub Authority
Ministry of Education	Physician Recruitment Agency of Saskatchewan
Ministry of the Economy	Saskatchewan Legal Aid Commission
Ministry of Environment	Saskatchewan Grain Car Corporation
Executive Council	Saskatchewan Housing Corporation
Ministry of Finance	Saskatchewan Municipal Board
Ministry of Government Relations	SaskBuilds Corporation
Ministry of Highways and Infrastructure	Technical Safety Authority of Saskatchewan
Ministry of Justice	
Ministry of Labour Relations and Workplace Safety	
Ministry of Parks, Culture and Sport	
Public Service Commission	
Ministry of Social Services	

[9] ISO/IEC 27002:2013 gives guidance for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration an organization's information security environment.

6.0 Glossary

Application – A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Change Management – An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

Configure – To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Data Centre – A central location for computer network hardware and software, especially storage devices for data.

Disaster Recovery Plan – A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Firewall – Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up using **firewall rules** to only allow certain types of data through.

Network – A group of computers that communicate with each other.

Network Switch – Hardware that connects devices (e.g., computers, printers, servers) within a network.

Patch – An update to a computer program or system designed to fix a known problem or vulnerability.

Physical Access Controls – The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Server – A computer that hosts systems or data for use by other computers on a network.

User Access Controls – The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

7.0 Selected References

Chartered Professional Accountants of Canada and the American Institute of Certified Public Accountants (AICPA). (2014). *Trust Services Principles, Criteria, and Illustrations.* Toronto: Author.

International Organization for Standardization. (2013). ISO/IEC 270002:2013(E). *Information Technology – Code of Practice for Information Security Management; 2nd Edition*. Geneva: Author.

The Information Systems Audit and Control Association. (2012). *COBIT 5*. Rolling Meadows: Author.