Chapter 5
Central Services—Data Centre Security

1.0 Main Points

The Ministry of Central Services, through its Information Technology Division (ITD), provides information technology (IT) services to government ministries and some other government agencies (clients). ITD uses a data centre, operated by a third-party service provider, to deliver its data centre services to ITD clients on its behalf. The data centre houses computer network equipment and data storage.

Each year, we examine whether ITD has effective processes to secure the data centre. For the period January 1, 2014 to December 31, 2014, ITD addressed two of our past seven recommendations. However, the other areas continue to require attention. We found the ITD had effective processes except it needs to:

- Better secure IT equipment and systems
- Have an approved and tested plan to recover critical systems and data in the event of a disaster
- Complete policies that set a minimum IT security standard for clients to follow and provide security reports that better inform clients whether the ITD is effectively securing their systems and data

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

2.0 Introduction

The Ministry of Central Services Regulations, 2012 make the Ministry of Central Services responsible for developing, implementing, monitoring, and enforcing the Government of Saskatchewan's IT security policies and standards. The Ministry has assigned to ITD these responsibilities along with the responsibility for direct delivery of IT services to primarily government ministries and several agencies.[1] It refers to those ministries and agencies as its clients (see **Section 6.0** for ITD's client list at December 2014).

ITD delivers IT services involving use of electronic assets (e.g., almost 7,000 desktop computers and over 5,000 laptops) and 1,400 applications.[2] Over 12,000 staff[3] from its clients located throughout the province use these electronic assets and applications. The **Glossary** in **Section 7.0** defines many of the terms used in this chapter.

This chapter reports the results of our 2014 audit of whether ITD had effective processes to secure the data centre. We perform this audit annually to support our audits of ITD's clients.

[1] Prior to May 2012, the Information Technology Office was a separate ministry that provided IT services to clients.
[2] Source: Information Technology Division.
[3] http://cs.gov.sk.ca/ITServices/ (8 April 2015).

2.1 IT Services Provided Directly by ITD

ITD has agreements with each of its clients outlining the specific IT services it will provide. ITD is responsible for providing certain IT services directly to clients, including:

- Developing and implementing IT security policies and programs for its clients
- Managing the relationship between ITD and 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 ITD's service providers
- Providing computers to client staff
- Providing application development and change management

2.2 Certain ITD Services Provided Through its Service Provider

ITD has engaged a third-party service provider to deliver data centre services to ITD clients on its behalf.[4] Even though it uses a service provider, ITD remains responsible for meeting the requirements it has agreed to with clients.

ITD's agreement with the service provider sets out the roles and responsibilities of both ITD and the service provider. Under this agreement, ITD pays the service provider $30 million annually.[5]

The service provider is responsible for operating the data centre. The data centre includes all servers that operate the network and host applications (i.e., hold the computer programs that store and work with client information). The data centre also includes network and telecommunications equipment that allow computers to send/receive data, systems used to backup data, and mass storage devices used to store client systems and data. The service provider is also responsible for implementing strong physical security controls to prevent unauthorized access.

ITD and its service provider have agreed on how the data centre and all related equipment are to be configured, managed, and maintained. ITD and its service provider revisit these requirements on a periodic basis (i.e., every 12 months).

ITD requires the service provider to annually report on its compliance with the agreed-upon requirements. Any equipment not in compliance with the agreed-upon requirements must either be remedied by the service provider or exempted by ITD from

[4] ITO directly operated a data centre from 2005 until December 2010.
[5] *2013-14 Public Accounts of the Government of Saskatchewan – Volume 2*, p. 54.

established requirements. For example, ITD may exempt a server from receiving security updates if there is a risk that applications on that server may not run properly if the latest server updates are applied.

2.3 Relationship Between ITD and Clients

Section 3 of *The Ministry of Central Services Regulations* makes the Ministry responsible for developing, implementing, and enforcing security policies and standards for its clients with respect to IT, information management, and records management. In addition, it is responsible for developing, procuring, and providing goods and services related to IT (i.e., it is a service provider). The Ministry carries out this mandate, as it relates to IT services, through ITD.

ITD signed agreements with its clients to describe roles and responsibilities and the services it is to provide. As described in **Section 2.0**, ITD's clients include ministries and 10 government agencies (see the list of clients in **Section 6.0**).

ITD operates on a cost recovery basis for client services; that is, it is reimbursed by clients for the services it provides. It may also receive funding for specific client-wide initiatives (e.g., computer modernization project). In 2013-14, ITD spent $121.1 million, of which it recovered $112.8 million from its clients.

ITD's clients are each responsible for their own IT systems and data. In addition to providing a secure data centre to house client systems and data, including data entrusted to its clients by the public, ITD is to provide guidance, policies, and enforcement to help clients protect systems and data. Therefore, ITD needs to help clients understand security risks associated with their IT systems, including the impact on the IT systems of other clients, and recommend actions to address these risks.

3.0 Importance of Effective Security Processes

IT 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[6] that can come from anywhere including IT security breaches by those with access to the network.

Organizations need effective security processes to protect the confidentiality, integrity, and availability of systems and data. Public Safety Canada has reported that the frequency and severity of cyberattacks is accelerating.[7] This includes an estimated 28% of IT security breaches perpetrated by employees inside organizations.[8]

Saskatchewan 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 are better able to defend against attacks, detect potential failures, and limit loss if

[6] 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 www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf p. 3 (19 March 2015).
[7] Ibid.
[8] PWC (2014). *US cybercrime: Rising Risks, Reduced Readiness – Key Findings from the 2014 US State of Cybercrime Survey*, p. 9.

systems and data are breached. For these reasons, effective security processes are of vital importance.

To protect the security of systems and data against hacking, ITD needs to ensure that its service provider implements effective security processes and that ITD's clients adhere to effective security requirements. This is because a weakness involving the service provider or ITD client staff could pose risks to all client data. For example, system administrators (i.e., privileged users) can use their greater system access to install programs on the network to steal information, or virus threats can be inadvertently introduced to the network by employees. 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.

4.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of our audit was to assess whether the Information Technology Division of the Ministry of Central Services had effective processes to secure the data centre for the period of January 1, 2014 to December 31, 2014.

The audit did not assess the effectiveness of security controls (e.g., user access controls) for specific client systems (e.g., financial accounting or payroll systems). We assess security controls in our audits of ITD's clients.

We examined both ITD's and its service provider's controls and processes used to secure the data centre, including network device (e.g., firewall, switch) configuration, server patch levels, and physical security at the data centre. We interviewed ITD and service provider staff. We also examined ITD's 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 ITD's processes, we used criteria (see **Figure 1**) 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* published by the Chartered Professional Accountants of Canada and the American Institute of Certified Public Accountants. ITD management agreed with the criteria.

Figure 1—Audit Criteria

1. **Demonstrate management commitment to security**
   - 1.1 Have an agreement with its service provider
   - 1.2 Threat and risk assessments are performed
   - 1.3 Management approves policies and procedures
   - 1.4 Management monitors security
2. **Protect the data centre from unauthorized access**
   - 2.1 User access controls protect the data centre from unauthorized access
   - 2.2 Physical security controls protect the data centre from unauthorized access
3. **Ensure the availability of data centre**
   - 3.1 Backup processes exist and are followed
   - 3.2 Disaster recovery plans exist and are tested
4. **Ensure the integrity of systems and data**
   - 4.1 Change management processes exist and are followed
   - 4.2 Operational processes exist and are followed

We concluded that, for the period of January 1, 2014 to December 31, 2014, the Information Technology Division of the Ministry of Central Services had effective processes to secure the data centre except that it needs to:

- **Better restrict access to IT equipment and systems**
- **Fully secure all key servers and network equipment**
- **Have an approved and tested plan to recover systems and data in the event of a disaster**
- **Provide security reports that better inform clients whether the Information Technology Division is effectively securing their systems and data, including consequences of any issues**
- **Complete security policies that set a minimum IT security standard for clients to follow**

5.0 Key Findings and Recommendations

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

5.1 Threat and Risk Assessment Processes Followed

We recommended that the Information Technology Division of the Ministry of Central Services follow its established processes to identify and manage risks related to the data centre. (2014 Report – Volume 1; Public Accounts Committee agreement September 23, 2014)

Status – Implemented

ITD updated its IT risk management policy in February 2015. The policy continued to require a risk officer to maintain a risk register that identifies, describes, categorizes, and assesses key risks. The risk officer is expected to provide status updates on the progress to address key risks to the Ministry's Executive Committee.

We found ITD staff revisited and updated the risk register in February 2015 and presented it to the Ministry's Executive Committee.

5.2 ITD Monitored its Service Provider

We recommended that the Information Technology Division of the Ministry of Central Services monitor whether its service provider meets its security requirements. (2011 Report – Volume 2; Public Accounts Committee agreement June 25, 2012)

Status – Implemented

ITD's agreements with its service provider included requirements for configuring and maintaining server and network equipment. ITD required the service provider to provide security reports, called compliance scan reports, to confirm security requirements were met.

During 2014, ITD received and reviewed weekly compliance scan reports for network equipment and an annual report for servers. It also received weekly information from the service provider about patches applied to servers. The compliance scan reports showed that security requirements were not always met. For example, scan reports showed 54 servers not in compliance with configuration policies at the end of 2014 (as later described in **Section 5.4**).

5.3 Need to Better Restrict Access

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

Status – Partially Implemented

ITD continued to allow insecure methods for accessing systems and data. At December 31, 2014, ITD continued to maintain network accounts that did not comply with its password standards. For example, it allowed passwords for certain network accounts to not expire. Some of these accounts belonged to users with access to critical IT functions. Once a privileged user account and password are known, an unauthorized person could affect the performance of the server or the related network. We found some of these user accounts belonged to clients. As noted later in **Section 5.6**, ITD provided clients with reports that described how certain network user accounts did not comply with or required exceptions from password policies.

Also, at December 2014, ITD had over 1,000 non-user accounts with passwords not set to expire. The network and systems use these accounts to manage interactions between computers. ITD began to exempt these accounts from its 90-day password change policy, as well as implement stronger controls (e.g., longer and more complex passwords) to reduce the related risks. It had not completed this work by December 31, 2014. Weak password controls increase the possibility that a password may be compromised and used to gain unauthorized system access.

ITD allowed certain users to have local administration rights to the computers they use. Local administration rights enable users to change configuration settings that could impact a computer's security. For example, local administration rights allow users to install new programs on computers without authorization, which increases the risk of viruses and malware that can create availability issues for the network.

During 2014, ITD began updating operating systems on client desktop computers. Implementation of the updated operating system will allow ITD to reduce the number of users who had required local administration rights (e.g., to run older versions of applications) and permit improved monitoring of those users who have these rights.

ITD continued to lack processes to adequately secure remote access to certain network equipment and systems. For example, ITD allowed users to access the network from their home computers through older remote access methods. These remote access methods did not incorporate advancements in security practice (e.g., requiring two different ways of verifying a user during logon, such as something a user has, like a token, and something a user knows, like a password). ITD does not and cannot manage home computers to make sure they are effectively secured (e.g., using firewalls, antivirus software). As a result, ITD is at an increased risk of hackers compromising or using home computers to obtain access to the data centre without being physically present.

5.4 Need to Fully Secure Servers and Network Equipment

We recommended that the Information Technology Division of 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

As in prior years, ITD lacked information from clients about the classification (e.g., level of sensitivity) of the data it manages on behalf of clients. By December 2014, ITD had not established separate parts of the network that differentiate security controls based on data classification (i.e., stronger security controls for systems that collect confidential information such as social insurance numbers). ITD had begun to document which client data resides on particular servers so that it can work with its clients to determine the security level required for the data. We found not all servers were properly configured and updated. This puts client systems at risk including those systems that contain sensitive and confidential data.

At the end of 2014, ITD's records showed that, of the nearly 1,000 servers that it managed, 54 servers were not in compliance with configuration policies and 369 servers used unsupported operating systems. Use of unsupported operating systems means security updates (e.g., Windows updates) are not available for these servers. This increases the risk of someone hacking into the server to gain unauthorized access to systems and data. We found that some of the unsupported servers host sensitive and confidential client information (e.g., fine and offender information, information about vulnerable adults and children, information about post-secondary students and their families). As noted in **Section 5.6**, ITD has not obtained clients' acceptance of the risks related to storing this information on systems that did not comply with security requirements.

Security patches address known security vulnerabilities. Attackers wanting to hack into systems can exploit these vulnerabilities to gain unauthorized access to systems and data. Although ITD's service provider patched (i.e., updated) most servers, on at least a quarterly basis, patching on all servers was not complete for all known vulnerabilities.

Of 15 servers we tested, we found 10 servers were missing patches dating back to October 2009. For most of the missing patches on the 10 servers, ITD did not request its

service provider or ITD staff to apply the patches to the servers. Also, ITD did not have a documented risk analysis on why these servers did not need the missing patches.

By December 2014, ITD had started to document which particular client systems and data reside on which servers so that it can explain the related risks to its clients. Management advised us that it plans to provide the risk analysis related to unsupported servers to its clients in 2015.

As in prior years, ITD used firewalls to help protect its data centre from hackers. While ITD located data centre firewalls at appropriate locations, and monitored reported security events, the firewalls (at the data centre and at client locations) were not properly configured. For example, ITD's data centre firewall rules did not effectively restrict access to the data centre because ITD did not effectively define the firewall rules that its service provider must follow.

We also found client firewalls and network switches at the data centre were not patched for known vulnerabilities, dating back to 2013 for client firewalls and May 2014 for the network switches. Inadequate firewall rules and untimely patching increases the risk of a security breach.

ITD had plans to review and update its firewall rules as part of a network security modernization plan in 2014, but it advised that it could not continue this work due to resource constraints. Management advised us that ITD is considering how to implement its network security modernization plan over a longer period.

5.5 Complete and Tested Disaster Recovery Plan Required

We recommended that the Information Technology Division of 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, ITD did not have a complete and tested disaster recovery plan for the data centre including critical client systems (e.g., student loan system, correctional information system). These conditions could result in critical IT systems, data, and services not being available to the Government and the people of Saskatchewan when needed.

At December 31, 2014, ITD's agreement with its 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 for systems and data to be operational, if best efforts recovery would meet client needs, or how much the recovery would cost. As a result, certain ITD clients have signed separate disaster recovery agreements with service providers to restore specific critical systems and data if a disaster occurs.

Having multiple agreements for disaster recovery does not result in an effective enterprise approach to disaster recovery for the data centre. Also, the recovery of critical client systems is dependent on the data centre (e.g., network switches, firewalls, network storage, network drives, email) being available to continue business operations following a disaster. Management advised us that, at February 2015, it had drafted a request for proposal for disaster recovery services for the data centre.

5.6 Client Security Reports Being Drafted

We recommended that the Information Technology Division of 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 – Partially Implemented

Each of ITD's clients is responsible for its own systems and data. Accordingly, each requires timely and relevant information from ITD – their service provider – to be able to effectively monitor ITD's security services and to understand the security issues that could impact their systems and data.

As in prior years, ITD continued to provide its clients with monthly reports about network availability as well as firewall and intrusion detection system security alert statistics. These reports outline security services conducted by ITD. ITD also reported information specific to each client about any security investigations completed (e.g., related to lost computers), risks accepted by the specific client (e.g., granting additional access rights to users other than those allowed by policy), network user accounts that had not been used for an extended time period, and network user accounts with exceptions to password policies (e.g., passwords that do not expire).

However, these reports are not sufficient. For example, during 2014, ITD agreed with the service provider that certain servers would be exempt from specific security standards based on the nature of the client applications (e.g., clients required use of older, unsupported applications). This included servers that hosted confidential client information (e.g., information about vulnerable persons). ITD needs to better report risks to clients to inform client decisions on how to address the risks or to document the clients' acceptance of the risks.

By December 31, 2014, ITD had created a template for an annual security report to its clients. ITD intends the reports to summarize the impact of identified data centre weaknesses (e.g., untimely server updates) on client systems and data. ITD also expects to use the reports to explain to clients how risks—including those documented in exemptions from specific security standards—affect client information. ITD plans to start providing the new annual security reports to its clients in 2015.

5.7 Complete Client Security Policies Progressing

We recommended that the Information Technology Division of 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 – Partially Implemented

In past years, ITD developed or revised security policies and procedures for clients in a number of areas (e.g., physical security, access control, incident management). By December 31, 2014, ITD had not finalized or implemented these policies in accordance with its established planned dates.

During 2014-15, ITD continued to work with the Public Service Commission to finalize the draft IT acceptable use policy. ITD expects to adopt this policy when it is finalized. ITD advised us that it expects to approve the remaining policies in 2015-16. Management indicated that it plans to obtain client feedback and acceptance of the policies before it finalizes and implements them.

6.0 ITD Client List at December 2014

Ministries:
Ministry of Advanced Education
Ministry of Agriculture
Ministry of Central Services
Ministry of Education
Ministry of the Economy
Ministry of Environment
Executive Council
Ministry of Finance
Ministry of Government Relations
Ministry of Highways and Infrastructure
Ministry of Justice
Ministry of Labour Relations and Workplace Safety
Ministry of Parks, Culture and Sport
Public Service Commission
Ministry of Social Services

Agencies:
Apprenticeship and Trade Certification Commission
Financial and Consumer Affairs Authority of Saskatchewan
Global Transportation Hub Authority
Physician Recruitment Agency of Saskatchewan
Public Guardian and Trustee
Saskatchewan Legal Aid Commission
Saskatchewan Grain Car Corporation
Saskatchewan Housing Corporation
SaskBuilds
Technical Safety Authority of Saskatchewan

7.0 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.

8.0 SELECTED REFERENCES

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

International Organization for Standardization. (2013). ISO/IEC 27002:2013(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, IL: Author.