Saskatchewan Telecommunications Holding Corporation

16

Main points

This chapter sets out the results of our 2010 audits of Saskatchewan Telecommunications Holding Corporation (SaskTel), the companies it owns, and its Pension Plan and our follow-up on SaskTel's wireless network security.

Security for credit card information

SaskTel accepts payments from customers using credit cards. SaskTel needs to improve security over customer credit card information.

Wireless network security follow-up

SaskTel provides wireless access to its network. In 2009 we audited whether SaskTel had adequate wireless network security controls. We concluded that SaskTel did not have adequate wireless network security controls and made seven recommendations. In 2011, we followed up on management's action on our recommendations. We found that SaskTel has many actions planned or underway to improve wireless security, but that it needs to complete these actions.

Introduction

Saskatchewan Telecommunications Holding Corporation (SaskTel) markets and supplies a range of voice, data, internet, wireless, text, image, security and entertainment products, systems and services.[1] SaskTel provides these products and services through its companies listed below.

This chapter discusses the results of our 2010 audits of SaskTel, the companies it owns, and its Pension Plan and our follow-up on SaskTel's wireless network security.

Related companies and pension plan

At December 31, 2010, SaskTel owned the following companies with active operations (percentage of SaskTel's ownership is set out in parenthesis):

- Saskatchewan Telecommunications (100%)
- Saskatchewan Telecommunications International, Inc. (100%)
- DirectWest Corporation (100%)
- SecurTek Monitoring Solutions Inc. (100%)
- Hospitality Network Canada Inc. (100%)
- Saskatoon 2 Properties Limited Partnership (Saskatoon 2) (70%)

Also, SaskTel sponsors and administers the Saskatchewan Telecommunications Pension Plan.

SaskTel did not prepare financial statements for Saskatoon 2 for the year ended December 31, 2010. SaskTel sold its interest in Saskatoon 2 in January 2011. For additional information on SaskTel and its companies, see SaskTel's website at www.sasktel.com.

Audit conclusions and findings

Our Office worked with KPMG LLP, the appointed auditor, to carry out the audit of SaskTel, the above-listed companies, and pension plan. We

[1] SaskTel, *2009 Annual Report*, p.52.

followed the framework in the *Report of the Task Force on Roles, Responsibilities and Duties of Auditors*.[2]

The following are our opinions for the above-listed companies[3] and Pension Plan for the year ended December 31, 2010:

- **They had adequate rules and procedures to safeguard public resources except for the matter described below**
- **They complied with authorities governing their activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**
- **The financial statements are reliable**

Better security for customer credit card information required

In our 2009 and 2010 – Volume 1 Reports, we recommended SaskTel have adequate controls to ensure customer credit card information is securely transmitted and stored.

SaskTel accepts payments from customers using credit cards. SaskTel stores, processes, and transmits customer credit card information. SaskTel does not have adequate controls, including those defined by the credit card industry, to provide reasonable assurance that customer credit card information is securely transmitted and stored. As a result, unauthorized access of customer credit card information could occur without ready detection.

Management of SaskTel told us that it is working to strengthen its controls and to fully implement the standards required by the credit card industry.

Status – We continue to make this recommendation.

[2] To view this report, see our website at www.auditor.sk.ca/rrd.html.
[3] We did not form an opinion for Saskatoon 2. As noted above, SaskTel sold its interest in Saskatoon 2 in January 2011.

Wireless network security follow-up

Background

SaskTel makes extensive use of information technology. This includes computers and networks, including a large, system-wide network that provides most of SaskTel's employees with access to email and significant amounts of information stored on network servers.

Networks that include wireless access have additional security risks compared with networks that do not have wireless access. Wireless access is available in many locations in SaskTel. In addition, many computers used by SaskTel have wireless capability. SaskTel must ensure that its wireless infrastructure provides mobile computing without compromising the confidentiality, integrity, or availability of sensitive and critical corporate information.

We audited SaskTel's wireless network security controls. In our 2009 Report – Volume 1 (Chapter 13), we reported the results of our audit. We concluded that SaskTel did not have adequate wireless network security controls at its head office and Regina data centre for the period August 1, 2008 – January 31, 2009. In 2011, we examined SaskTel's actions on our recommendations from the audit.

Status of recommendations

The following sections set out the recommendations (in italics) from our 2009 audit and SaskTel's actions to March 2011 to address the recommendations.

SaskTel has many actions planned or underway that relate to wireless security. Some of these are part of, or depend on, larger IT security initiatives that are underway and will take two or more years to complete. Management told us that it is allocating its resources to those areas it regards as presenting the highest risk.

Train employees to use wireless devices securely

We recommended that SaskTel train employees to use wireless devices securely. *(2009 Report – Volume 1)*

SaskTel has provided employees with some information regarding the use of wireless and has posted the information on the corporate Intranet. SaskTel is creating a mandatory wireless security training program that it plans to provide to all SaskTel employees, contractors and subsidiaries by the end of December 2011.

Status – We continue to make this recommendation.

Describe wireless roles and responsibilities

We recommended that SaskTel describe wireless roles and responsibilities in its information technology security policies and procedures. *(2009 Report – Volume 1)*

SaskTel is working on identifying the business requirements for wireless. It plans to develop wireless policies, including describing roles and responsibilities relating to wireless, reflecting its business requirements. It plans to complete this process in 2011.

Status – We continue to make this recommendation.

Properly configure wireless network and network devices to reduce security risks

We recommended that SaskTel properly configure its wireless network and network devices to reduce information technology security risks. *(2009 Report – Volume 1)*

SaskTel has introduced several improvements to how it configures its wireless network and wireless devices to improve security. It has set up a separate part of its network to manage wireless devices. IT administrators now use encryption to communicate with devices over the network. SaskTel has also piloted a new wireless architecture that would further improve security. The piloted system includes an intrusion detection system to help identify suspicious activity on the network. Part of the pilot included development of a classification strategy to determine what corporate wireless devices should be authorized for use on the network and configuration standards for each device. SaskTel will evaluate further deployment of the piloted system as it identifies its business requirements.

Status – We continue to make this recommendation.

Assess wireless risks and address them

We recommended that SaskTel assess wireless risks and address them. *(2009 Report – Volume 1)*

SaskTel has not carried out a full assessment of its wireless risks. SaskTel considered wireless risks in piloting a new wireless network architecture. SaskTel also considered wireless risks in creating a classification strategy to help determine what corporate wireless devices it should authorize for use on the network.

Status – We continue to make this recommendation.

Maintain an inventory of wireless devices

We recommended that SaskTel maintain an inventory of wireless devices on its network and their users. *(2009 Report – Volume 1)*

SaskTel does not maintain an inventory of wireless devices or a list of approved users. Management told us that they are considering alternatives for doing this, but are waiting until they have completed developing the business case for wireless and made decisions on wireless architecture.

Status – We continue to make this recommendation.

Adequately monitor wireless activity logs

We recommended that SaskTel adequately monitor wireless activity logs. *(2009 Report – Volume 1)*

SaskTel has not implemented processes to monitor wireless activity logs. Management told us that they plan to make decisions regarding monitoring logs when they complete their changes to SaskTel's wireless architecture.

Status – We continue to make this recommendation.

Regularly perform wireless security scans

We recommended that SaskTel regularly perform wireless security scans and address weaknesses found. *(2009 Report – Volume 1)*

SaskTel performs ad hoc wireless security scans to identify inappropriate wireless activity. SaskTel should ensure that it has established and measured appropriate coverage and range for the wireless network.

Status – We continue to make this recommendation.

Glossary

Access point—An electronic device that provides other devices, such as computers, with a point of entry into a network.

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

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

Intrusion detection system (IDS)—Software and/or hardware designed to detect a security breach by identifying inappropriate access or changes taking place within a computer or network.

Intranet— An intranet is a private computer network used to securely share any part of an organization's information.

Log—A record of computer, network, or application use.

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

Wireless architecture—The overall design of an organization's wireless network, both in terms of its physical components and in how data is meant to travel.

Wireless network—A network where computers communicate without being physically connected by a cable or "wire", for example, using radio signals.

This page left blank intentionally.