Chapter 29
Saskatchewan Telecommunications—Wireless Network Security Follow Up

1.0 Main Points

We audited Saskatchewan Telecommunication's (SaskTel) wireless network security controls in 2009 and made seven recommendations. We reported our first follow-up of this audit in 2011. This chapter reports our second follow-up, which is of management's actions on our recommendations to March 31, 2013. We found that SaskTel has implemented six of our seven recommendations relating to wireless training, setting roles and responsibilities, configuring equipment, assessing risks, maintaining an inventory of devices, and logging activity. It still needs to perform regular wireless security scans and address related issues.

2.0 Introduction

In 2009, we audited processes SaskTel used for wireless network security controls. We reported the results of our audit in our *2009 Report – Volume 1*, Chapter 13. We concluded that SaskTel did not have adequate wireless network security controls at its head office and the Regina data centre for the period from August 1, 2008 to January 31, 2009 and made seven recommendations.

In 2011, we examined SaskTel's actions on our recommendations from the audit. At that time, we found that SaskTel had many actions planned or underway to respond to these recommendations. We reported that follow-up in our *2011 Report – Volume 1*, Chapter 16.

In March 2013, we again examined SaskTel's actions on the recommendations. To conduct this review, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook - Assurance*. To evaluate SaskTel's progress towards meeting our recommendations, we used the relevant criteria from the original audit. SaskTel's management agreed with the criteria in the original audit. This chapter describes the results of our follow-up of management's actions to March 31, 2013.

3.0 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 personnel with access to email and significant amounts of information stored on network servers.

Networks that include wireless access involve additional security risks compared with networks that do not have wireless access. Wireless access is available in many locations in SaskTel. Because wireless information is usually transmitted via radio waves and is potentially available to those within range of the signal, there is greater risk of unauthorized access. This risk can be reduced, but it requires careful network and device implementation (for example, using an appropriate design, requiring appropriate encryption, and keeping hardware and software up-to-date).

SaskTel provides wireless access in many locations. 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. Because of the risks associated with wireless networking, SaskTel must effectively manage and monitor its wireless resources so that only approved and secure wireless activities take place.

4.0 Status of Recommendations

This section sets out our recommendations and SaskTel's actions up to March 31, 2013. We found that SaskTel has adequately implemented six of the outstanding seven recommendations.

4.1 Employees Trained to Use Wireless Devices Securely

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

Status – Implemented

SaskTel has provided employees with information regarding the use of wireless devices and has posted this information on its corporate Intranet. SaskTel has also added wireless information to a mandatory security training program that it provides to all SaskTel employees, contractors, and subsidiaries. SaskTel has also taken steps to make staff aware of the need to use wireless devices securely and it continues to update its staff using an ongoing security awareness program that covers wireless security topics.

4.2 Wireless Roles and Responsibilities Included in Information Security Policies and Procedures

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

Status – Implemented

SaskTel has now developed and approved policies that describe roles and responsibilities relating to wireless.

4.3 Configured Wireless Network and Network Devices to Reduce Information Technology Security Risks

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

Status – Implemented

SaskTel has improved how it configures its wireless network and wireless devices to increase security. IT administrators now use encryption to communicate with devices over the network. SaskTel has also installed an intrusion prevention system to help identify suspicious activity on the network. In addition to this, SaskTel has implemented a technology that prevents employees from connecting to wireless networks while being connected to the corporate network.

4.4 Wireless Risks Assessed and Addressed

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

Status – Implemented

SaskTel assessed risks relating to wireless in order to develop related policies and procedures. SaskTel developed a classification strategy to help determine what corporate wireless devices it should authorize for use on the network. SaskTel also implemented a wireless intrusion prevention system. SaskTel based these steps on its assessment of wireless risks.

4.5 Inventory Maintained of Wireless Devices on Network and their Users

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

Status – Implemented

SaskTel currently maintains an inventory of wireless devices that connect to the wireless network. SaskTel uses software to manage the wireless devices authorized to access its wireless network. This software is monitored regularly by SaskTel staff.

4.6 Wireless Activity Logs Adequately Monitored

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

Status – Implemented

SaskTel has implemented a wireless intrusion prevention system that staff use to monitor wireless activity and ensure that only authorized users have access to SaskTel's wireless network. SaskTel has adequate monitoring capabilities and processes for the type of wireless access they provide to staff. Management advised that proactive monitoring will remain part of SaskTel's strategy. SaskTel also collects activity logs and stores them centrally. SaskTel has plans to replace its wireless architecture.

4.7 Need to Regularly Perform Wireless Security Scans and Address Weaknesses Found

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

Status – Not Implemented

SaskTel performed ad hoc wireless security scans to identify inappropriate wireless activity. It did not carry these out on a regular basis. SaskTel should also perform site surveys to ensure that it has established and measured appropriate coverage and range for the wireless network.