Saskatchewan Telecommunications Holding Corporation

13

Main points **162**

Introduction **163**

Related companies and pension plan 163

Audit conclusions and findings **163**

Better controls for the sale of prepaid cellular service cards required 164

Better security for customer credit card information required 165

Processes to manage intellectual property—a follow-up **166**

Background 166

Action on recommendations 167

Wireless network security **168**

Wireless networks and related risks 168

Audit objective and conclusion 169

Key findings by criteria and recommendations 170

Maintain effective management of wireless security 170

Secure wireless infrastructure 171

Monitor wireless security 173

Glossary **176**

Selected references **178**

Main points

Saskatchewan Telecommunications Holding Corporation (SaskTel) markets and supplies a range of voice, data, internet, wireless, text, image, security and entertainment products, systems and services.

SaskTel needs better controls to protect itself against losses from the sales of prepaid cellular service cards to distributors. It also needs to improve security over customer credit card information.

Many of SaskTel's activities and services involve the use of intellectual property. We followed up on our 2007 audit of SaskTel's processes to manage intellectual property. We found that SaskTel had complied with our recommendations.

SaskTel makes extensive use of information technology (IT) to deliver its products and services. SaskTel's IT environment includes a large, system-wide network that provides most of SaskTel's personnel with access to email and significant amounts of information. We audited the security of wireless access to these resources, focusing on the wireless security controls at SaskTel's head office and Regina data centre (wireless access is where computers communicate with each other without being physically connected by a wire or cable). We found that SaskTel did not have adequate wireless network security controls for the period August 1, 2008 – January 31, 2009. We make seven recommendations.

SaskTel, the companies it owns, and its pension plan had reliable financial statements; complied with the law; and had adequate rules and procedures to safeguard their public resources, except for the matters described above.

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.

Related companies and pension plan

At December 31, 2008, 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%)
- DirectWest Canada, Inc. (100%)
- SecurTek Monitoring Solutions Inc. (100%)
- Hospitality Network Canada Inc. (100%)
- Saskatoon 2 Properties Limited Partnership (70%)

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

Each year, SaskTel gives its annual report including its audited consolidated financial statements and the audited financial statements of each of the above-listed companies and pension plan to the Legislative Assembly. 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 followed the framework in the *Report of the Task Force on Roles, Responsibilities and Duties of Auditors*.[2] KPMG LLP and our Office formed the following opinions.

[1] SaskTel, 2007 Annual Report, p.52.
[2] To view this report, see our website at www.auditor.sk.ca/rrd.html.

In our opinion, for the year ended December 31, 2008:

- **The financial statements of SaskTel and each of the above-listed companies and the Saskatchewan Telecommunications Pension Plan are reliable**
- **SaskTel and each of the above-listed companies and the Saskatchewan Telecommunications Pension Plan had adequate rules and procedures to safeguard public resources except for the matters described in this chapter**
- **SaskTel and each of the above-listed companies and the Saskatchewan Telecommunications Pension Plan complied with authorities governing their activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**

In this chapter, we also include the results of our audit to assess the adequacy of SaskTel's wireless network security controls and a follow-up of our audit of SaskTel's processes to manage intellectual property.

Better controls for the sale of prepaid cellular service cards required

SaskTel needs better controls to protect itself against losses from the sale of its prepaid cellular service cards.

SaskTel hired a company (the distributor) to sell SaskTel's prepaid cellular service cards. SaskTel supplied the cards to the distributor. The distributor arranged for the sale of the cards through retailers, paid commissions to retailers, and charged SaskTel a commission for its services. The distributor was required to pay SaskTel the face value of the cards less commissions.

When SaskTel made its agreement with the distributor, SaskTel did not ensure it had adequate controls to prevent losses on money owed to SaskTel by the distributor. SaskTel should have required the distributor to provide adequate security to protect SaskTel against losses.

During the year, the distributor failed to pay SaskTel for amounts it owed for the sale of SaskTel's cards. As a result, SaskTel recorded a loss of $6.4 million on the amounts owed by the distributor.

1. We recommend SaskTel have adequate controls to prevent losses from the sale of its prepaid cellular service cards.

Management of SaskTel told us that the agreement with the prepaid card distributor was terminated and the process for creation and distribution of prepaid cards has been moved in-house and with this, the risk associated with having one supplier collecting money on SaskTel's behalf has been eliminated. Management told us that as part of moving the process in-house controls were increased and SaskTel now distributes cards to retail outlets and dealers directly. In addition, management told us contracts have been signed with each retailer/distributor with credit requirements and invoicing is done as cards are shipped and credit terms are monitored according to normal credit policy and procedures.

Better security for customer credit card information required

SaskTel needs to improve security over customer credit card information.

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.

2. We recommend SaskTel have adequate controls to ensure customer credit card information is securely transmitted and stored.

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.

Processes to manage intellectual property—a follow-up

Background

In 2007, we audited SaskTel's processes to manage intellectual property. Intellectual property refers to creations of the mind, such as inventions, symbols, names, pictures and designs. Patents, trademarks, copyrights, and industrial designs are examples of specific rights regarding intellectual property.[3]

Intellectual property is important to SaskTel. SaskTel uses intellectual property in many ways in carrying on its businesses: providing telephone, cell phone, internet, and television services, and providing telephone directories and home security to its customers.

In Chapter 11 of our 2007 Report – Volume 1, we reported our results. We concluded that SaskTel had adequate processes to manage intellectual property except for matters described in six recommendations (see Exhibit 1).

On January 19, 2009, the Standing Committee on Crown and Central Agencies considered the chapter and agreed with our recommendation.

In March 2009, we completed our review of SaskTel's actions on our recommendations. SaskTel has complied with all our recommendations.

Exhibit 1—Audit recommendations

1. We recommend that SaskTel should develop a plan for managing intellectual property. The plan should:
   - ♦ identify intellectual property assets
   - ♦ be proportionate to importance of intellectual property assets to the objectives and risks of SaskTel
   - ♦ describe approach/activities to manage intellectual property assets and risks
   - ♦ include training and resource allocation
2. We recommend that SaskTel include intellectual property issues in its risk management framework.

[3] Canadian Intellectual Property Office, p.3.

3. We recommend that SaskTel consistently document intellectual property agreements with its subsidiaries.
4. We recommend that SaskTel establish centralized responsibility for maintaining original contracts.
5. We recommend that SaskTel implement a system to assist it to comply with the intellectual property rights it has acquired.
6. We recommend that SaskTel monitor its progress in achieving its plan for managing intellectual property.

Action on recommendations

SaskTel has implemented a plan for managing intellectual property. The plan describes intellectual property in general and identifies types of intellectual property important to SaskTel. The plan reflects the importance of intellectual property to SaskTel. The plan describes SaskTel's approach for managing intellectual property by setting out guiding principles and outlining activities. The plan also identifies corporate resources for managing intellectual property.

SaskTel uses a formal risk management framework. SaskTel has now explicitly included intellectual property risks in its framework.

SaskTel requires that it now document agreements with its subsidiaries on intellectual property matters. Such agreements help in managing intellectual property and also help protect rights.

SaskTel has established centralized responsibility with its legal department for maintaining original contracts, although some agreements remain in different departments or areas for practical reasons. SaskTel is continuing to take steps to help ensure that it manages and tracks contracts.

SaskTel has improved its processes to comply with the intellectual property rights it has acquired. It has improved its usage of existing tools to manage software licenses. At the same time, SaskTel is evaluating new tools to assist with this task. SaskTel has created a new position with responsibilities related to this area. SaskTel's department objectives now explicitly address software compliance.

SaskTel requires the intellectual property plan and the related risk report on intellectual property to be reviewed annually by SaskTel's executive. This constitutes adequate monitoring.

Wireless network security

SaskTel makes extensive use of information technology (IT). 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.

This audit examines the security of wireless access to these resources. Wireless access is where computers communicate with each other without being physically connected by a wire or cable.[4]

Wireless networks and related risks

Networks that include wireless access involve additional security risks compared to 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) together with other controls such as training.

Poorly designed or implemented wireless networks can be relatively easy to break into. And because radio signals are hard to control, wireless signals may extend outside SaskTel's offices. This would make it easier for someone to attempt to break into the network.

SaskTel provides wireless access in many locations. Also, many computers used by SaskTel have wireless capability. It is important that SaskTel 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

[4] "Wireless" is sometimes used to refer to cellular technology. In this audit we are referring to electronic communications using the IEEE 802.11 standard, often referred to as Wi-Fi.

associated with wireless networking, SaskTel must effectively manage and monitor its wireless resources so that only approved and secure wireless activities take place.

Audit objective and conclusion

The objective of our audit was to assess whether SaskTel had adequate wireless network security controls for the period August 1, 2008 – January 31, 2009. We focused on the wireless security controls at SaskTel's head office and Regina data centre. This audit did not include handheld devices such as Blackberries. We followed *The Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants in carrying out this audit.

We used the criteria outlined in Exhibit 2 to assess SaskTel's controls. The criteria are based upon the National Institute of Standards and Technology, the Payment Card Industry Standard, and the wireless security testing section of the Open-Source Security Testing Methodology Manual. The selected references at the end of this chapter set out the sources of the criteria. SaskTel agreed with the criteria.

Exhibit 2—Audit criteria

To have adequate wireless network security controls, SaskTel should:

1. **Maintain effective management of wireless security**

   Assign responsibility for wireless security
   Maintain wireless security policies and procedures
   Maintain documentation of wireless architecture
   Require approval for wireless activities
   Maintain a current list of wireless approvals
   Use secure methods to administer wireless devices

2. **Secure wireless infrastructure**

   Securely configure wireless devices
   Deploy updates and security patches
   Encrypt wireless traffic
   Implement additional controls to secure networks accessible by wireless devices
   Implement physical security controls to limit unauthorized wireless activity

3. **Monitor wireless security**

   Maintain an inventory of wireless devices on the network
   Monitor wireless activity logs
   Monitor for unauthorized wireless activities

We conclude that Saskatchewan Telecommunications Holding Corporation 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.

As a result, SaskTel's systems and data at these locations are at increased risk of disclosure, modification, or loss.

Key findings by criteria and recommendations

We describe below what we expected (in italics) and our key findings and recommendations for each criterion.

Maintain effective management of wireless security

We expected SaskTel to:

- *Assign responsibility for wireless security*
- *Maintain wireless security policies and procedures*
- *Maintain documentation of wireless architecture*
- *Require approval for wireless activities*
- *Maintain a current list of wireless approvals*
- *Use secure methods to administer wireless devices*

SaskTel has documented overall responsibility for IT and for networks though job descriptions. However, SaskTel has not clearly documented roles and responsibilities for wireless security within the agency. Not documenting specific roles and responsibilities for wireless security decreases SaskTel's ability to carefully manage this area. We discuss this further in this section in connection with security policies and procedures.

SaskTel has a general security awareness program. It has processes to keep track of whether all employees receive security awareness training. As we conducted the audit, several SaskTel staff members asked us for identification. This demonstrates security awareness. However, SaskTel's security training does not include any specific content on secure wireless practices (although we observed that in some cases, employees who were approved to use the wireless network received security reminders). Given its level of wireless activity, SaskTel should educate its staff on wireless security and tie it to approved wireless policies and procedures (discussed below).

3. We recommend SaskTel train employees to use wireless devices securely.

SaskTel should improve its IT security policies and procedures to more fully address wireless security. The security policy and procedures prohibit unauthorized wireless access to the network. They also state that SaskTel may grant employees wireless access for established business needs. The security procedures call for "occasional" sweeps (examinations) for places where unauthorized wireless access is available ("rogue access points"). However, the policies and procedures should more clearly set out specific roles and responsibilities relating to wireless. The security policies and procedures should require regular or scheduled checking for unauthorized wireless use. In addition, SaskTel should consider adopting a security standard to guide its use of wireless. We examined examples of SaskTel's wireless network hardware and found that SaskTel had not set these up to meet security specifications. Following a specific security standard would assist IT employees in setting up and operating wireless network devices securely and consistently (we discuss configuration further under the second criterion).

4. We recommend SaskTel describe wireless roles and responsibilities in its information technology security policies and procedures.

SaskTel maintains documentation of its wireless architecture. SaskTel requires employees who wish to use the wireless network to obtain approval. SaskTel maintains a list of approvals. The list is not complete.

SaskTel does not use secure methods to configure and manage wireless devices. We discuss this further in the next section.

Secure wireless infrastructure

We expected SaskTel to:

- *Securely configure wireless devices*
- *Deploy updates and security patches*
- *Encrypt wireless traffic*
- *Implement additional controls to secure networks accessible by wireless devices*

- *Implement physical security controls to limit unauthorized wireless activity*

SaskTel needs to secure its wireless infrastructure. This includes both the physical security of devices and their electronic settings. SaskTel did not make wireless access points physically inaccessible. This increases the risk that unauthorized individuals could modify settings to reduce security. SaskTel advises it is considering new devices and locations for the devices that would reduce accessibility.

We found several examples where SaskTel had not set up devices to reduce security risks. For example, SaskTel does not disable (by default) wireless access devices in laptop computers. It should do this. When SaskTel uses wireless on a computer, it must manage the related security risks. For example, that same computer can readily be modified to function as a way into the network (a wireless "network access point") without authority and adequate protection. Also, if a user of a wireless device uses it to access an external signal, it can compromise the network. We observed that it was possible for an employee within SaskTel's premises to connect to an external wireless access point using an unsecure connection while remaining connected to the corporate network. This is a high security risk.

Even where users are not currently connected to the corporate network, risks exist. Users may access sites (for example, in public locations) that appear to offer legitimate web access, but instead contain security threats. When a computer that has been compromised connects once again to the network, it puts the network at risk as well. SaskTel should disable wireless access devices in laptops unless specifically required for business reasons or implement other methods to reduce these risks.

SaskTel should also ensure that it sets signal power settings on wireless devices no higher than required. We found devices were set too high such that wireless signals could be accessed from nearby public locations. This increases the likelihood of inappropriate access.

Only authorized users should be able to use wireless devices. SaskTel employed adequate access controls to help ensure only authorized users were able to access the network. However, SaskTel should ensure that it

locks out persistent unsuccessful attempts to access the wireless network.

SaskTel has implemented additional security controls to secure wireless networks. For example, SaskTel has placed a firewall to restrict access to its network. However, it should deploy sensors to detect suspicious wireless activity in the network.

SaskTel also needs to ensure that wireless security is not weakened through out of date devices or software. SaskTel does not have formal procedures to maintain or "patch" wireless hardware. It should implement such procedures. We noted that SaskTel maintained up-to-date virus protection on computers connecting to the wireless network.

Finally, IT administrators do not use secure methods to configure and manage wireless devices. When administrators communicate with wireless devices, for example, to change how the devices are set up, they do not use secure means of communication. They should use encrypted communication to help ensure that sensitive information such as usernames and passwords remain confidential. Further, SaskTel does not use a separate part of its network to administer security. Using a separate part of the network for management is a good security practice. We also found that administrators did not regularly change passwords required to manage these devices, contrary to security policies and procedures.

5. We recommend SaskTel properly configure its wireless network and network devices to reduce information technology security risks.

Monitor wireless security

We expected SaskTel to:

- *Maintain an inventory of wireless devices on the network*
- *Monitor wireless activity logs*
- *Monitor for unauthorized wireless activities*

SaskTel has not performed a risk assessment to help it appropriately manage wireless risks. SaskTel should perform a risk assessment and use it to decide what wireless devices to track and how closely. Nevertheless, SaskTel should maintain an inventory of wireless devices.

SaskTel has no way to track the devices that appear on its wireless network or the person assigned to the devices. Therefore, if wireless devices are used in an inappropriate way (for example, to allow inappropriate wireless activity), SaskTel is less able to remedy the problem. SaskTel should maintain an inventory of devices and settings.

6. We recommend SaskTel assess wireless risks and address them.

7. We recommend SaskTel maintain an inventory of wireless devices on its network and their users.

It is important when disposing of devices to ensure they do not contain sensitive information including configuration settings and passwords. SaskTel advises that it uses the manufacturer of its wireless devices to assist with secure disposal.

SaskTel needs to improve its logging and monitoring processes. Logs are records of who uses a device and how it is used. SaskTel sets up its wireless devices so that logs capture both traffic and management activity. However, SaskTel does not adequately monitor its logs, for example to identify attempts to break into its systems.

8. We recommend SaskTel adequately monitor wireless activity logs.

SaskTel has carried out scans looking for inappropriate wireless activity. The assessments found inappropriate or unauthorized wireless activity. However, SaskTel does not have regularly scheduled wireless scans. It should.

We examined each floor of SaskTel's head office and Regina data centre locations. We found many examples of unauthorized wireless activity. We found many examples where computers could be configured as access points. Also, we found many examples where wireless signals were not encrypted or used weak encryption. We could not tell, nor could SaskTel advise, whether these signals originated from computers that were on its network.

9. We recommend SaskTel regularly perform wireless security scans and address weaknesses found.

Management of SaskTel told us that it will address the audit recommendations related to Wireless Network Security (Recommendations 3 to 9) through the implementation of the SaskTel Corporate Security Program and the SaskTel PCI-DSS Compliance Program.

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).

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

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

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

IT infrastructure—An organization's computer and network assets.

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

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

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.

Rogue access point— An electronic device that provides other devices, such as computers, with a point of entry into a network, but which is not set up or authorized by the responsible agency.

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

Traffic—Information travelling over 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.

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.

Selected references

Canadian Intellectual Property Office. (2004). *Stand out from your competitors: Make intellectual property your best business ally*. Ottawa: Industry Canada.

Herzog, P. (2003). OSSTMM wireless 2.9.1. Wireless security testing section, open-source security testing methodology manual. Institute for security and open methodologies: Europe and USA.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). Information technology – Code of practice for information security management; 2nd Edition. Geneva: Author.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition. Rolling Meadows, IL: Author.

Karygiannis, T. & Owens, L. (2002). Wireless network security. 802.11, Bluetooth and handheld devices. Special publication 800-48. National Institute of Standards and Technology: Gaithersburg, MD.

PCI Security Standards Council. (2006). Payment card industry (PCI) Data security standard. Security audit procedures. Version 1.1. Release: September 2006. https://www.pcisecuritystandards.org/. (17 Nov 2008).

The Center for Internet Security. (April, 2005). Wireless networking benchmark, Version 1.0. Author.

The Information Systems Audit and Control Foundation. (2005). CoBiT4.0. Rolling Meadows, IL: Author.