# Saskatchewan Government Insurance

# 15

## Main points

Saskatchewan Government Insurance (SGI) makes extensive use of information technology (IT). This includes computers and networks including a large, system-wide network that provides most of SGI's personnel with access to email and significant amounts of information stored on network servers. We audited 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).

SGI has substantially limited its wireless security risks. Its corporate network is not a wireless network. SGI's wireless security risks are limited to its wireless-enabled mobile computers (i.e., laptops) and to wireless data transmission at certain rural motor licence issuers. SGI needs to provide employees with awareness training on the security risks of wireless-enabled laptops, promptly update its laptops to protect against known security risks, and strengthen its IT security settings.

# Introduction

Saskatchewan Government Insurance (SGI) sells property and casualty insurance in Saskatchewan. Its wholly-owned company, SGI Insurance Services Ltd. (SCISL), sells property and casualty insurance in Manitoba and Alberta.

Also, SCISL owns 100% of the issued shares of Coachman Insurance Company (Coachman) and 75% of the issued shares of Insurance Company of Prince Edward Island (ICPEI). Coachman sells property and casualty insurance including automobile insurance in Ontario. ICPEI sells property and casualty insurance including automobile insurance in Prince Edward Island, Nova Scotia, and New Brunswick.

SGI also manages the Saskatchewan Auto Fund (Auto Fund). The Auto Fund is Saskatchewan's compulsory automobile insurance program. It receives money from the motoring public and pays claims. The Auto Fund does not receive any money from the General Revenue Fund (GRF). Nor does it pay any dividends to the GRF or the Crown Investments Corporation of Saskatchewan. The financial results of Auto Fund are not included in SGI's financial statements.

SGI sponsors the Saskatchewan Government Insurance Superannuation Plan (SGI Pension Plan). The SGI Pension Plan is a defined benefit pension plan (closed to new members since 1978). The Board of Directors of SGI is responsible for administration of the SGI Pension Plan under *The Pension Benefits Act, 1992*. The primary objective of the SGI Pension Plan is to provide pensions to retired employees and the dependents of deceased pensioners and employees of SGI. SGI provides day-to-day management of the SGI Pension Plan.

The 2009 Annual Report for SGI includes its consolidated financial statements (including the operating results of the companies SGI owns) for the year ended December 31, 2009. Those statements report revenue of $390 million, net income of $52 million, total assets of $827 million, and retained earnings of $126 million.

The 2009 Annual Report for the Auto Fund includes its financial statements for the year ended December 31, 2009. Those statements report revenue of $686 million, net loss to the rate stabilization reserve of

$41 million, total assets of $1,496 million, a rate stabilization reserve of $67 million, and a redevelopment reserve of $21 million.

The annual report for SGI's Pension Plan includes its financial statements for the year ended December 31, 2009. Those statements report contributions from employees and SGI of $0.1 million, pension payments of $3 million, net assets of $36 million, and pension benefits owing of $37 million.

## Audit conclusions and findings

KPMG LLP is the appointed auditor for SGI, the Auto Fund, SCISL, Coachman, ICPEI, and SGI Pension Plan. Our Office worked with the appointed auditor using the framework recommended by the *Report of the Task Force on Roles, Responsibilities and Duties of Auditors*.[1] Our Office and KPMG LLP formed the following opinions.

**In our opinion, for the year ended December 31, 2009:**

- **SGI, Auto Fund, SCISL, Coachman, ICPEI, and the SGI Pension Plan had adequate rules and procedures to safeguard public resources**
- **SGI, Auto Fund, SCISL, Coachman, ICPEI and the SGI Pension Plan complied with authorities governing their activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**
- **the financial statements of SGI, Auto Fund, SCISL, Coachman, ICPEI, and the SGI Pension Plan are reliable**

The remainder of this chapter reports the result of our audit to assess the adequacy SGI's wireless network security controls.

[1] To view this report, see our website at www.auditor.sk.ca/rrd.html.

# Wireless network security audit

SGI makes extensive use of information technology (IT). This includes computers and a large, system-wide network that provides most of SGI's personnel with access to email and significant amounts of information stored on network servers.

SGI has limited its use of wireless network access. Wireless access is where computers communicate with each other without being physically connected by a wire or cable.[2] SGI's corporate network is not a wireless-enabled network. SGI's wireless security risks arise from its mobile computers (i.e., laptops) with wireless capability that connect to its corporate network and from wireless data transmission at certain motor licence issuers located in rural communities.

## Wireless networks and related risks

Networks that can be accessed by wireless devices involve additional security risks compared to networks that cannot be accessed wirelessly. For example, they can be easier to break into, especially poorly designed or implemented wireless networks.

Even if an agency has not set up a wireless network, many computers have wireless capabilities built in and can be used to set up informal or unapproved networks. And because wireless information is usually transmitted via radio waves and is potentially available to any computer 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 and security awareness.

Because of the risks associated with wireless access, SGI must effectively manage and monitor its wireless resources so that only approved and secure wireless activities take place.

[2] "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.

## Audit objective and conclusion

The objective of our audit was to assess whether SGI had adequate wireless network security processes for the period October 1, 2009 – March 31, 2010.

This audit did not include handheld devices such as Blackberries. We followed *The Standards for Assurance Engagements* published by The Canadian Institute of Chartered Accountants in carrying out this audit.

We used the criteria outlined in Exhibit 1 to assess SGI'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. SGI agreed with the criteria.

**Exhibit 1—Audit criteria**

To have adequate wireless network security controls, SGI should:

1. **Maintain effective management of wireless security**
   - 1.1 Assign responsibility for wireless security
   - 1.2 Maintain wireless security policies and procedures
   - 1.3 Maintain documentation of wireless architecture
   - 1.4 Require approval for wireless devices
   - 1.5 Maintain a current list of wireless approvals
   - 1.6 Use secure methods to administer wireless devices

2. **Secure wireless infrastructure**
   - 2.1 Securely configure wireless devices
   - 2.2 Deploy updates and security patches
   - 2.3 Encrypt wireless traffic
   - 2.4 Implement additional controls to secure networks accessible by wireless devices
   - 2.5 Implement security controls to limit unauthorized wireless activity

3. **Monitor wireless security**
   - 3.1 Maintain an inventory of wireless devices on the network
   - 3.2 Monitor wireless activity logs
   - 3.3 Monitor for unauthorized wireless activities

**We concluded that Saskatchewan Government Insurance had adequate wireless network security processes for the period October 1, 2009 – March 31, 2010 except for the specific matters on wireless-enabled laptop computers described below.**

## 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 SGI 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*

SGI has documented overall responsibility for IT and for networks through job descriptions. SGI has also approved IT security policies and procedures and has implemented a security awareness program. This program includes various components including a security awareness month with weekly articles, quizzes, contests, and a security self-assessment survey.

SGI's IT security policy requires that any requests for the use of wireless network technology be assessed for potential risks and approved by management. It also refers to appropriate wireless networking standards.

SGI has not deployed a wireless-enabled corporate network. It also has implemented procedures to promptly detect and investigate unauthorized electronic devices (e.g., portable computers, wireless devices etc.) that attempt to connect to its corporate network. Consequently, SGI has substantially limited its risks from unauthorized wireless connections to its corporate network.

Because of the risks described below with wireless-enabled laptop computers, we expected SGI's IT security policy to govern their use. We expected the policy would cover providing wireless capability to staff specifically authorized to use it. In addition, we expected SGI's security awareness program to address the risks and training needed to securely use this wireless capability. It does not.

Management told us that it had approved the use of wireless on SGI's laptop computers.

**1. We recommend that Saskatchewan Government Insurance provide training to employees with wireless-enabled laptop computers on how to use this technology securely.**

### *Secure wireless infrastructure*

*We expected SGI to:*

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

SGI needs to strengthen the security of its wireless-enabled laptop computers.

Insecure wireless-enabled laptops increase the risks to SGI's corporate systems and data. For example, a user of an insecure wireless-enabled laptop could connect, accidentally or intentionally, to an outside wireless network while connected to the corporate network. Such a connection provides a way into the corporate network. SGI's corporate network defence systems may not readily detect this kind of unauthorized access. At the time of our test, we did not detect (at SGI's head office) accessible wireless signals from external sources.

In addition, a wireless-enabled laptop that is not promptly updated for known security weaknesses and that does not properly log and restrict security breach attempts is at a higher risk of compromise when used away from the office. For example, users could access internet sites from hotel rooms, airports, etc. that appear to offer legitimate web access, but instead contain security threats. If intruders were to exploit laptop security weaknesses and gain account user names and passwords, they may be able to use computer connections trusted by the corporate network to compromise it when a user returns to the office.

SGI adequately secures, through password protection and hard drive encryption, the capability to use and access stored data on the laptops. It also promptly updates the virus protection software on its laptop computers. However, it does not promptly patch its laptops for known security weaknesses or adequately configure its laptops to log and restrict security breach attempts. Logs provide the information necessary to investigate attempted inappropriate access to these computers or unauthorized alterations of their settings.

2. **We recommend Saskatchewan Government Insurance promptly update its laptop computers to protect against known security weaknesses.**

3. **We recommend Saskatchewan Government Insurance configure its laptop computers to reduce the risk of inappropriate access and to log such attempts.**

The wireless infrastructure at motor licence issuers located in rural communities encrypts the data to and from SGI using a virtual private network. This technology is effective in protecting the confidentiality and integrity of transmitted data.

### *Monitor wireless security*

*We expected SGI to:*

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

As stated earlier, SGI does not have a corporate wireless-enabled network. To safeguard its corporate network from wireless risks, SGI has implemented controls to promptly detect and investigate any unauthorized electronic devices (e.g., portable computers, wireless devices, etc.) being connected to its corporate network. These controls are very effective at protecting SGI's corporate network from unauthorized wireless devices.

During the audit, we checked each floor of SGI's head office for unauthorized wireless activity. We did not find any examples of internal wireless activity. This test also confirmed that SGI had no wireless

devices connected to its network and, as noted earlier, we found no wireless activity originating from external sources.

## 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.

**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.

**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.

**Virtual private network**—A private network that is configured within a public network (e.g. the Internet) to provide secure site-to-site connections for data transmission.

**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.