Chapter 16
Wireless Network Security Audit Follow Up

1.0 Main Points

In our 2010 Report – Volume 2, we reported on wireless network security at Saskatchewan Government Insurance (SGI) and made three recommendations. At March 31, 2012, SGI has implemented the recommendations. It provides staff with training on the safe use of wireless-enabled laptop computers. Also, it promptly updates and appropriately configures these computers to protect against known security risks and to reduce the risk of inappropriate access.

2.0 Introduction

SGI sells property and casualty insurance products such as home, farm, business and auto insurance in seven Canadian provinces. It operates as SGI CANADA in Saskatchewan, SGI CANADA Insurance Services Ltd. in Manitoba and Alberta, the Coachman Insurance Company in Ontario and as a major partner in the Insurance Company of Prince Edward Island in Nova Scotia, New Brunswick and Prince Edward Island. Also, SGI is the administrator of the Saskatchewan Auto Fund (Auto Fund) and is the sponsor of the Saskatchewan Government Insurance Superannuation Plan (SGI Pension Plan).

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 to 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.[1] 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 license issuers located in rural communities.

Unsecure wireless-enabled laptops increase the risks to SGI's corporate systems and data. For example, intruders could exploit security weaknesses in wireless-enabled laptops that connect to the corporate network. Such connections could result in the modification and unauthorized disclosure of corporate information including the theft of customer personal information.

In 2010, we assessed whether SGI had adequate wireless network security processes. Our 2010 Report – Volume 1, Chapter 15 (pp. 153-164) concluded that SGI had adequate wireless network security processes for the period October 1, 2009 to March 31, 2010 except for the three recommendations we made on securing laptops.

[1] "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.

3.0 Status of Recommendations

In this section, we set out each of our recommendations and SGI's actions up to March 31, 2012. We found that SGI has implemented our recommendations.

3.1 Providing Training on Using Wireless Enabled Laptops

We recommended that SGI provide training to employees with wireless-enabled laptop computers on how to use this technology securely. (2010 Report – Volume 1))

Status – Implemented.

In our 2010 audit, we found that SGI's security awareness program did not address the risks and training needed for users to securely use wireless-enabled laptop computers. Security awareness is an important part of information security. It helps users to understand security issues, security responsibilities, and to act accordingly. SGI has now incorporated wireless-enabled laptop computers into its security awareness program.

3.2 Installing Security Fixes

We recommended that SGI promptly update its laptop computers to protect against known security weaknesses. (2010 Report – Volume 1)

Status – Implemented.

In our 2010 audit, we found that SGI did not promptly update its laptops for known security weaknesses. SGI now has implemented processes to promptly update its laptop computers.

3.3 Logging Security Events

We recommended that SGI configure its laptop computers to reduce the risk of inappropriate access and to log such attempts. (2010 Report – Volume 1)

Status – Implemented.

In our 2010 audit, we found that SGI did not adequately configure its laptops to log and restrict security breach attempts. Logs provide the information necessary to investigate attempted inappropriate access to these computers and unauthorized alterations of their settings. SGI has now strengthened the security configurations of laptops including the enabling of event logging.