Chapter 30
SaskEnergy Incorporated—Securing its SCADA System

1.0 Main Points

SaskEnergy delivers natural gas to the people of Saskatchewan. To help it do so, it uses information technology assets like supervisory control and data acquisition (SCADA) systems to control and monitor the physical transportation of natural gas through pipelines. Strong security processes are needed to protect SCADA against risks associated with unintentional actions by staff or actions with malicious intent.

By March 20, 2015, SaskEnergy had implemented five of the seven recommendations we made in our 2013 audit of SaskEnergy's processes to secure its SCADA system. SaskEnergy needs to do more work to securely configure and monitor security of its SCADA system.

2.0 Introduction

In 2013, we assessed SaskEnergy's processes to secure its SCADA system. This chapter describes our follow-up of management's actions on the recommendations we made in our *2013 Report – Volume 1*, Chapter 19*.* In our report, we concluded that SaskEnergy did not have effective processes to secure its SCADA system used to control and monitor natural gas distribution. We made seven recommendations.

To conduct this review engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate SaskEnergy's progress towards meeting our recommendations, we used the relevant criteria from the original audit. SaskEnergy's management agreed with the criteria in the original audit. We reviewed SaskEnergy's policies and procedures, plans, and reports and interviewed SaskEnergy staff. We also reviewed SaskEnergy's controls to secure its SCADA system, including computer patch levels, physical security, and access to the SCADA system.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Crown and Central Agencies agreed to the recommendation, the status of the recommendation at March 20, 2015, and SaskEnergy's actions up to that date. We found that SaskEnergy had implemented five recommendations and is working to address the remaining two.

3.1 Security Framework Improved

We recommended that SaskEnergy Incorporated complete a threat and risk assessment of its supervisory control and data acquisition system. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy hired a consultant to help it carry out a threat and risk assessment for its SCADA system in early 2014. The assessment identified a number of risks and SaskEnergy developed plans to address those risks. SaskEnergy continues to work on implementing these security plans as described below.

We recommended that SaskEnergy Incorporated implement complete policies to protect the confidentiality, integrity, and availability of its supervisory control and data acquisition system based on a threat and risk assessment. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy adopted a policy framework based on industry best practice (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 62443). It used its policy framework and the results of its SCADA threat and risk assessment to create and update its SCADA security policies. For example, this included developing a SCADA security policy, SCADA incident management plan, change management policy, and an antivirus patch management policy. Management advised us that it plans to continue updating its policies with any changes that result from implementing its security plans.

3.2 Processes to Protect SCADA System from Unauthorized Access Progressing

We recommended that SaskEnergy Incorporated configure its supervisory control and data acquisition system network to protect it from security threats. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Partially Implemented

SaskEnergy's SCADA security plans included modifying the network architecture (e.g., how firewalls, encryption, and intrusion detection systems are used) and changing the configuration of network devices, servers, and workstations. SaskEnergy began implementing the most critical parts of the plans first. For example, it implemented a firewall for its SCADA network. However, as of March 20, 2015, it had not yet completed all network architecture and computer configuration changes required to effectively secure its SCADA system. It expects to complete this work in 2015.

We recommended that SaskEnergy Incorporated monitor the security of its supervisory control and data acquisition system. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Partially Implemented

SaskEnergy installed a new monitoring tool on its SCADA system in late 2014. This tool gathers information from various points within the SCADA network to enable SaskEnergy staff to monitor system security. During early 2015, SaskEnergy staff began to use the tool and attended training to expand their knowledge so that they can increase the use of this tool in the future. As SaskEnergy completes the implementation of changes to its network architecture and computer configurations, it plans to expand the use of this tool so that it can effectively conduct real-time security monitoring of its SCADA system.

We recommended that SaskEnergy Incorporated effectively restrict physical access to its facilities. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

We recommended that SaskEnergy Incorporated effectively restrict access to its supervisory control and data acquisition system. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy improved restriction of physical access to its facilities and access to its SCADA system. It implemented certain controls such as a requirement to lock doors to all parts of its facilities during the day as well as at night, and to lock user accounts on computer systems when staff are not using the computers. It communicated these policies to its staff. It also added controls to prevent non-authorized use of the SCADA equipment (e.g., locked USB ports). In addition, SaskEnergy had plans to continue strengthening and automating its access controls to further reduce risk.

3.3 Business Continuity Plan Tested

We recommended that SaskEnergy Incorporated test its business continuity plan for its supervisory control and data acquisition system to verify its effectiveness. (2013 Report – Volume 1; Crown and Central Agencies Committee agreement March 12, 2014)

Status – Implemented

SaskEnergy developed processes for testing its business continuity plan annually in 2013. It tested and updated its plan in 2013 and 2014.