Chapter 48
SaskPower—Managing the Risk of Cyber Incidents

1.0 Main Points

By August 2017, SaskPower took steps to improve its management of the risk of cyber incidents for the protection of the provision of power. It implemented two of three recommendations from our 2015 audit. It needs to finish implementing its risk mitigation strategies that reduce risk of cyber incidents to acceptable levels.

Without effective cyber security, SaskPower is at greater risk of a cyberattack that could affect its ability to deliver power, negatively impacting power-generating plants and/or transmission equipment, businesses who need power to operate, or public safety.

2.0 Introduction

SaskPower is the principal supplier of electricity in Saskatchewan, serving more than 520,000 customers. Its mission is to ensure reliable, sustainable, and cost-effective power.[1] It relies on various IT systems to deliver power and manage its businesses.

In 2015, we assessed SaskPower's processes to manage the risk of cyber incidents for the protection of the provision of power. Our *2015 Report – Volume 1*, Chapter 18 concluded that, for the 12-month period ended February 28, 2015, SaskPower had effective processes to manage the risk of cyber incidents for the protection of the provision of power except for three areas. We made three recommendations.

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance* (including CSAE 3001). To evaluate SaskPower's progress towards meeting our recommendations, we used the relevant criteria from the original audit. SaskPower's management agreed with the criteria in the original audit.

We examined SaskPower's policies and procedures, its IT risk registers, and other relevant documentation. We also interviewed staff responsible for monitoring and responding to cyber incidents.

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 August 21, 2017, and SaskPower's actions up to that date. We found that SaskPower implemented two recommendations and is making progress towards implementing the remaining recommendation.

[1] SaskPower, *SaskPower 2017 Annual Report*.

3.1 Cyber Threats Documented

We recommended that SaskPower document the most likely types of information technology threats that could lead to cyber incidents that would adversely impact its ability to provide power. (2015 Report – Volume 1; Crown and Central Agencies Committee agreement December 13, 2016)

Status – Implemented

SaskPower documented IT threats that could lead to cyber incidents and the related risks in its risk registers. The enterprise security and IT risk registers included SaskPower's assessment of the likelihood and impact of risks for assets critical to providing power (e.g., operational IT systems).

3.2 Cyber Risk Mitigation Strategy Progressing

We recommended that SaskPower confirm that its cyber risk mitigation strategy addresses the significant threats of cyber incidents that would adversely impact its ability to provide power. (2015 Report – Volume 1; Crown and Central Agencies Committee agreement December 13, 2016)

Status – Partially Implemented

SaskPower had not finished implementing its cyber risk mitigation strategies to address significant threats of cyber incidents to power provision.

SaskPower updates significant threats of cyber incidents in its risk registers annually. By March 31, 2017, SaskPower had classified many cyber security risks as high, and documented planned strategies to reduce the risks (e.g., logical and physical access controls) to a level acceptable to its senior management and Board. SaskPower plans to implement these strategies over three years because of the large volume and complexity of work needed.

Management received monthly progress reports to monitor implementation of these strategies. But, at August 2017, it could not confirm the effectiveness of the strategies as implementation of them was at an early stage.

Without implementing and confirming that its strategies address significant threats of cyber incidents, SaskPower faces increased risk that a cyber attack could jeopardize its ability to deliver power. Disruptions in power may damage power-generating plants and/or transmission equipment, adversely impact businesses who need power to operate, or put public safety at risk depending on the timing and extent of the security incident.

3.3 Adequate Guidance Provided for Identifying Cyber Incidents

We recommended that SaskPower provide its staff with guidance to assist in assessing when an information technology security-related event is considered a cyber incident, and requires the use of its incident command system response plan. (2015 Report – Volume 1; Crown and Central Agencies Committee agreement December 13, 2016)

Status – Implemented

SaskPower gave staff adequate cyber-security training. SaskPower refers all security incidents to employees with annual cyber security training for critical infrastructure.

SaskPower's training is designed to help staff assess when an IT security-related event is a cyber incident that requires use of the incident command system response plan. Its training materials define what constitutes a cyber incident, and how to identify and respond to these incidents.

We found staff use this guidance to determine when an IT security-related event is a cyber incident that requires use of the incident command system response plan. SaskPower did not identify any cyber incidents between September 2016 and August 2017.

In 2017-18, SaskPower plans to update its general IT incident-management procedures to include the definition of cyber incident and the incident command system response plan.