Chapter 18
SaskPower—Managing the Risk of Cyber Incidents

1.0 Main Points

The Saskatchewan Power Corporation (SaskPower) is the principal supplier of power in Saskatchewan with its mission to deliver power in a safe, reliable, and sustainable manner. SaskPower uses information technology to deliver power and manage its business. SaskPower recognizes increasing its reliance on technology can help it provide services more efficiently and reliably, and improve interaction with its customers.[1]

In 2012, Public Safety Canada reported that the frequency and severity of cyberattacks is accelerating.[2] Sophisticated individuals may be able to disrupt electronic controls of power grids, water treatment plants, and telecommunications networks.

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 the following. It needs to improve documentation of threats that could lead to cyber incidents, and confirm that its cyber risk mitigation strategy addresses the significant threats. Without complete documentation of threats that could lead to cyber incidents and confirmation that its cyber risk mitigation strategy address all significant threats, SaskPower may be more susceptible to successful cyberattacks.

SaskPower also needs to provide its staff with guidance to assist in assessing when an information technology (IT) security-related event is considered a cyber incident. Inconsistent determination of when to treat an IT security-related event as a cyber incident may result in SaskPower not appropriately responding to incidents.

2.0 Introduction

SaskPower operates under the mandate and authority of *The Power Corporation Act*. It is responsible for serving more than 500,000 customers in Saskatchewan.[3]

This chapter describes the results of our audit on the effectiveness of SaskPower's processes to manage the risk of cyber incidents to protect the provision of power.

2.1 Importance of Cyber Security

Cyber incidents (which can include cyberattacks) include the unauthorized or unintentional access, use, manipulation, interruption, or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.[4] Cyber security protects IT

[1] SaskPower, *SaskPower 2013 Annual Report*, p. 46.
[2] Public Safety Canada, *Canada's Cyber Security Strategy*, p. 3.
[3] SaskPower, *SaskPower 2013 Annual Report*, p. 1.
[4] Public Safety Canada, *Canada's Cyber Security Strategy,* p. 3.

systems and data from cyber incidents and reduces the likelihood and impact of cyberattacks on operations.

In common with other electrical companies, SaskPower uses IT systems to deliver power and manage its business. SaskPower recognizes that technology enablement (i.e., increasing its reliance on technology) can help it provide services more efficiently and reliably, and improve how it interacts with customers.[5]

SaskPower uses computer hardware and software to operate and control its power distribution (these are referred to as Operational Technology or OT). In addition, it uses various IT systems such as the Supervisory Control and Data Acquisition (SCADA) system[6] to enable it to operate and control its power distribution facilities remotely.

As SaskPower increases its reliance on technology, it increases the risk of cyber incidents significantly impacting and disrupting its operations. As noted in its *2013 Annual Report*, SaskPower acknowledges that its power facilities are exposed to the risk of man-made events (including cyberattacks).[7]

Without effective cyber security, SaskPower is more susceptible to successful cyberattacks (where attackers gain access to or use of an IT system). Attackers could potentially use these successful cyberattacks to jeopardize SaskPower's ability to deliver power – an essential need in today's society. Disruptions in providing power could potentially 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.

3.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether SaskPower had effective processes to manage the risk of cyber incidents for the protection of the provision of power. Our audit covered the 12-month period ended February 28, 2015.

We did not assess the physical security of SaskPower's assets critical to providing power.

We examined SaskPower's documentation setting out its policies and processes for the detection of, monitoring for, and responding to cyber incidents that may affect its cyber assets (e.g., control centres, power transmission stations). We reviewed evidence (e.g., results of exercises, compliance assessments, reports to management and the Board) to assess whether SaskPower had followed its procedures.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate SaskPower's processes, we used criteria based on our related work, reviews of literature including reports of other auditors, and consultations with management. SaskPower's management agreed with the criteria (see **Figure 1**).

[5] SaskPower, *SaskPower 2013 Annual Report*, p. 46.
[6] Ibid., p. 19.
[7] Ibid., p. 69.

Figure 1—Audit Criteria

1. **Identify risks of cyber incidents**
   - 1.1 Identify systems involved in the provision of power that would be targets for cyber incidents
   - 1.2 Assess likelihood and impact of cyber incidents for targets identified
   - 1.3 Establish a strategy for reducing cyber incident risks to an acceptable level

2. **Mitigate identified cyber incident risks**
   - 2.1 Establish mitigation procedures for targets identified
   - 2.2 Incorporate lessons learned into risk management strategy for cyber incidents
   - 2.3 Establish detection processes for targets identified
   - 2.4 Minimize administrative user access for targets identified
   - 2.5 Maintain a response plan for cyber incidents

3. **Respond to cyber incidents**
   - 3.1 Continuously monitor to detect cyber incidents
   - 3.2 Respond promptly to cyber incidents when they occur
   - 3.3 Report timely to senior management and the Board of Directors

We 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 the following.

SaskPower needs to document the most likely types of information technology threats that could lead to cyber incidents that adversely impact its ability to provide power, and confirm that its cyber risk mitigation strategy addresses the significant threats of cyber incidents. SaskPower also needs to give its staff guidance to help them consistently assess when an IT security-related event becomes a cyber incident.

4.0 Key Findings and Recommendations

In this section, we set out the criteria (expectations) in italics and our key findings along with related recommendations.

4.1 Need for Complete Documentation of IT Threats to Critical Cyber Assets—Operational Technology Systems

To identify risks of cyber incidents, we expected SaskPower to:

- *Inventory its assets involved in providing power that could be targets for cyber incidents (i.e., critical cyber assets – OT systems).*

- *Determine that the listing of critical cyber assets is complete (e.g., do a periodic review of them).*

- *Formally assess risks of critical cyber assets as targets for cyber incidents (including identifying potential vulnerabilities, the likelihood of identified risks, and impact on SaskPower). Vulnerabilities are weaknesses in the cyber assets that may allow attackers to gain access into the related OT system.*

- *Maintain a current written strategy for mitigating risks of critical cyber assets as identified as targets of cyber incidents.*

SaskPower has a policy that requires staff to update and review its critical asset inventory (i.e., listing of assets used to provide power throughout the province) at least every 15 months. Also, it has documented procedures to help it identify those critical assets, and the impact and likelihood of asset failure. The procedures require an assessment team to:

- Identify assets critical to providing power throughout the province.
- For each identified asset, document the critical nature of each asset based on the impact of failure of the asset would have on SaskPower's ability to provide power. SaskPower has documented criteria to help assess the impact of asset failure.
- Determine the likelihood of failure.

The assessment team is comprised of staff from several departments (e.g., plant services, enterprise services) and staff with expertise in processes to maintain power plants.

We found SaskPower used peer reviews (e.g., applicable electrical engineers), external third-party reviews (e.g., Public Safety Canada), and reviews and approvals from senior management to ensure completeness of its inventory of critical assets (i.e., its OT systems).

We found that, while SaskPower kept a current listing of what it had assessed as its critical assets, it had not specifically identified which of those assets could be potential targets for a cyber incident. Management indicated that they consider all of the critical assets (e.g., control systems, data acquisition systems, networking equipment) used in the provision of power to be most-likely targets for cyber incidents.

As part of its process to assess risks, SaskPower considered the significance of each identified critical asset at a site (e.g., transmission station) to its ability to deliver power, assessed the potential overall impact of the asset failure on the site, and then categorized and ranked the sites based on its impact assessment. Also, SaskPower's risk assessment documents the likelihood of failure of critical assets and its assessment of the potential impact of this failure on the Corporation and public safety (e.g., major consequence, significant consequence, minor consequence).

In March 2015, SaskPower provided its senior management and Board of Directors with a high-level summary of the potential threats it faced in relation to its assets that provide power, the impact of those threats, and the safeguards that it had in place to mitigate those threats (mitigation strategy). However, this high-level summary may not be complete. We found that SaskPower did not specifically identify potential weaknesses in and threats to its OT systems (e.g., unauthorized connections of these systems to the internet, use of USBs) that may allow an attacker to get into the critical cyber assets. In turn, SaskPower did not assess the likelihood of these types of cyberattacks (e.g., where attacker pretends to be an authorized user, viruses cause system not to operate as intended) that potentially could lead to a cyber incident.

Without fully documenting the types of information technology threats most likely to be used to cause a failure of assets critical to providing power, it is difficult for SaskPower to ensure it has the appropriate strategy in place to mitigate the risks.

1. **We recommend 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.**

2. **We recommend 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.**

4.2 Need for Guidance on Assessing Cyber Events

To mitigate risks of cyber incidents, we expected SaskPower:

- *To follow established mitigation procedures for critical assets assessed as having a high risk of being a target of cyber incidents. A critical part of reducing cyber incidents is to minimize administrative user access (i.e., powerful access that allows the user to make changes to system settings and functions) to high-risk targets.*

- *To follow established cyber incident detection processes. A detection process is based on established thresholds that define what is a cyber incident.*

- *To maintain a response plan for cyber incidents and respond to cyber incidents incorporating, to the extent possible, lessons learned from past cyber incidents.*

SaskPower has a detection and response plan for use in the event of an incident (including a cyber incident); it calls this plan the "Incident Command System" (ICS). ICS includes detailed procedures for both detecting and responding to incidents (including cyber incidents).

ICS documents the processes used when an incident is detected including who would be involved in responding to an incident, the participants' responsibilities, the required communications regarding the incident, and the steps for planning the response to the incident. Also, the ICS set out expected detection activities, such as use of intrusion detection systems and anti-virus software and the review of security logs[8] and alerts.[9] We found that SaskPower has implemented the detection activities as set out in the ICS including periodic reviews of system logs and alerts. We noted various staff (e.g., system technicians) were assigned responsibility to review security logs and alerts. An IT security-related event is any observable occurrence in a system (e.g., a firewall blocking a connection attempt, failed log-on attempts).

While SaskPower used processes to detect and track various IT security-related events, we found that it did not have documented criteria that set out what IT security-related events it considered as cyber incidents (such as a series of failed log-in attempts in a short period). Without a clear and consistent understanding as to when an IT security–related event should be classified as a cyber incident, there is an increased risk that an IT security-related event identified in detection activities would not be appropriately

[8] Security logs track security-related information (e.g., log-in and log-out activity) on a computer system.
[9] A sound or message that indicates some predefined event has occurred or a selected operation is about to be performed.

addressed. That is, there is a risk that SaskPower's ICS response plan would not be invoked when needed and actions would not be taken to address the risk within an appropriate timeframe. Also, without documented guidance, there is a risk that IT security-related events may be inconsistently considered to be a cyber incident when more than one person assesses and monitors IT security-related events.

3. We recommend 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.

SaskPower requires approval for any changes to user access (e.g., addition of a new employee) to its OT systems including the systems used to operate and control power distribution. Also, on an annual basis, it requires a review of all user access to determine if access provided remains relevant. These user-access change procedures include administrative user access. We found SaskPower followed its user–access change procedures and appropriately restricted its administrative user access for its critical assets to a small number of employees.

We note that once the ICS is invoked, ICS includes procedures to categorize an incident into different levels (i.e., low, medium, high, and critical). Each level results in differing actions and involvement of staff to reflect the risk and severity of the incident.

Also, the ICS requires yearly training of the response team and a review of the incident response to incorporate lessons learned in future responses. We observed evidence that yearly training occurred. SaskPower regularly tests its response plan through test exercises. It completed testing exercises in 2013 and 2014. Management indicated that it is planning to conduct another exercise in 2015. Management stated that in the last three years, it had not detected a cyber incident, nor an interruption to the provision of power due to a cyber incident related to its OT assets used in the provision of power. As such, it had no need to invoke its ICS response plan.

4.3 Regular Reports to Management Occurring

To effectively respond to cyber incidents, we expected SaskPower to regularly monitor to detect cyber incidents. Once an incident is detected, we expected SaskPower to respond promptly, and report, on a timely basis, the incident to senior management and the Board of Directors.

SaskPower has established policies and procedures for regular monitoring of incidents that could impact its critical assets. As previously noted in **Section 4.2**, SaskPower's ICS clearly defines key roles and responsibilities involved in responding to incidents, including cyber incidents.

We found that SaskPower communicated ICS procedures to its employees and has made it readily available to staff for reference should an incident occur. The ICS outlines the required communication for each level of incident. Where the incident is defined as critical, this communication includes notification of senior management.

We found that, each month, SaskPower's Director of Enterprise Security gave senior management an update on security issues (e.g., security incidents, current investigations, industry security advisories). During 2014 and up to February 2015, SaskPower did not identify any cyber incidents related to assets used in the provision of power.

Also, SaskPower's Internal Audit Division gathers information on incidents occurring at SaskPower and reports them to a Committee of the Board of Directors. Management indicated that this reports would include significant security and cyber incidents, if any.

5.0 Selected References

Auditor General of Canada. (2012). *Report of the Auditor General of Canada to the House of Commons, Chapter 3, Protecting Canadian Critical Infrastructure Against Cyber Threats.* Ottawa: Author.

Auditor General Manitoba. (2014). *Annual Report to the Legislature, Chapter 8, Manitoba Hydro – Managing Cyber Security Risk Related to Industrial Control Systems.* Winnipeg: Author.

Australian National Audit Office. (2014). *Audit Report No.50 2013-14, Cyber Attacks: Securing Agencies' ICT System.* Carberra: Author.

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: Author. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (9 October 2014).

North American Electric Reliability Corporation. *Critical Infrastructure Protection Standards*. Atlanta: Author. www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (2 April 2015).

Provincial Auditor of Saskatchewan. (2014). *2014 Report – Volume 1, Chapter 7, Central Services – Information Technology Division – Data Centre.* Regina: Author.

Provincial Auditor of Saskatchewan. (2013). *2013 Report – Volume 1, Chapter 19, Securing SaskEnergy's SCADA System.* Regina: Author.

Public Safety Canada. *Canada's Cyber Security Strategy*. Ottawa: Author. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (22 October 2014).