Chapter 16
Saskatchewan Gaming Corporation—Preventing Cyberattacks

1.0 Main Points

Cybercrime in Canada, including cyberattacks via the internet, causes more than $3 billion in economic losses each year.[1]

Effective cybersecurity programs are critical as cybercrime increasingly targets and can exploit government IT systems and networks resulting in data breaches, significant recovery costs, reputational damage, and disruption to the delivery of services.

By February 2024, Saskatchewan Gaming Corporation implemented six of seven recommendations we made in 2021 to improve its processes for preventing cyberattacks from affecting IT systems and data it uses to support and deliver casino games.

We found SaskGaming better restricted access to its network, servers, and workstations by improving security set-up (configuration) of those devices. It also included all privileged-user groups in its periodic user access reviews, enforced password expiry on all accounts, and increased its use of multifactor authentication to access IT systems. SaskGaming also updated its IT security assessments to reflect current practice and closer align with IT industry standards.

SaskGaming contracted a service provider to help it better gather and analyze security information from its systems. However, SaskGaming needs to maintain clear plans for reducing all significant cybersecurity risks to acceptable levels based on robust risk assessments.

Having an effective cybersecurity program can help reduce the risk of a successful cyberattack and the total time and associated costs SaskGaming requires to recover from it. Cyberattacks could cause significant disruption to gaming operations, as well as lead to substantial financial costs, asset or revenue loss, and reputational damage.

2.0 Introduction

Saskatchewan Gaming Corporation, a subsidiary of Lotteries and Gaming Saskatchewan, operates two casinos (one in Regina and another in Moose Jaw) under *The Saskatchewan Gaming Corporation Act*. It offers a variety of casino games (e.g., slot machines and table games), food and beverage services, and entertainment.

SaskGaming's profits support people, programs, and services throughout Saskatchewan (e.g., First Nations and Métis organizations, general government programs).

SaskGaming depends on many IT systems to operate. SaskGaming is responsible for managing and securing all its technology assets, including preventing cyberattacks.

[1] Public Safety Canada, *National Cyber Security Action Plan: 2019–2024*, p. 1.

2.1 Focus of Follow-Up Audit

This chapter describes our first follow-up audit of management's actions on the recommendations we originally made in 2021.

In 2021, we assessed Saskatchewan Gaming Corporation's processes to prevent cyberattacks. We concluded SaskGaming had effective processes, except in the areas reflected in our seven recommendations, to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games.[2]

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

To carry out our follow-up audit, we used an external consultant to assess network and system controls related to cybersecurity. We interviewed key staff responsible for IT security and examined policies and procedures, risk assessments, action plans, and reports related to cybersecurity.

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 February 28, 2024, and Saskatchewan Gaming Corporation's actions up to that date.

3.1 Formal Planning for Addressing Cybersecurity Risks Needed

We recommended Saskatchewan Gaming Corporation maintain well-defined action plans clearly addressing all significant risks of cyberattacks that may affect IT systems and data used to support and deliver casino games. (*2021 Report – Volume 2*, p. 134, Recommendation 1; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Partially Implemented

Saskatchewan Gaming Corporation did not have a current comprehensive plan setting out actions to address all significant cybersecurity risks.

In 2022, SaskGaming created a Cyber Security Action Plan to address recommendations we made in 2021, as well as recommendations related to an external cybersecurity maturity assessment completed in 2022. However, it had not updated the Plan since that time.

[2] *2021 Report – Volume 2*, Chapter 17, pp. 127–142.

In 2023, SaskGaming listed and reviewed its top cybersecurity risks monthly, including observing whether the level of risk changed. However, SaskGaming did not document details of its risk assessment, such as likelihood and impact of each risk or the remaining risk level after considering relevant controls in place. It also did not set out formal action plans to reduce risks to acceptable levels, where required.

Without a well-defined annual action plan, based on detailed risk assessments, that clearly addresses all significant risks of cyberattacks, SaskGaming is at increased risk of unauthorized access or breach of its IT systems and data.

3.2 Stronger Network and IT Device Controls Used to Restrict Access

We recommended Saskatchewan Gaming Corporation adequately configure its network, servers, and workstations to better protect them from security threats and vulnerabilities. (*2021 Report – Volume 2*, p. 136, Recommendation 2; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

Saskatchewan Gaming Corporation improved the configuration of its network, servers, and workstations to better protect them from security threats and vulnerabilities.

SaskGaming uses firewalls to prevent unauthorized individuals from entering its network and to restrict access within its network. We found key servers (e.g., to support gaming operations) had appropriately configured firewalls in place to prevent unauthorized access. SaskGaming also appropriately restricted access to its wireless networks. It used service providers to monitor for unauthorized user access and movement within its network or unauthorized file transfers to external sources.

SaskGaming encrypts workstations and data to reduce risk of unauthorized access to systems and data. We found it also restricted user access on workstations for staff to access only those systems and data required to do their jobs. In addition, SaskGaming adequately set up its employees' remote access to its network.

Adequate configuration of networks, servers, and workstations decreases the risk of unauthorized access to systems and data.

3.3 User Access Review and Password Requirements Strengthened

We recommended Saskatchewan Gaming Corporation include all privileged-user groups in its quarterly user access reviews. (*2021 Report – Volume 2*, p. 137, Recommendation 3; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

We recommended Saskatchewan Gaming Corporation update all user account passwords as often as required by its password policy. (*2021 Report – Volume 2*, p. 137, Recommendation 4; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

We recommended Saskatchewan Gaming Corporation implement further use of multifactor authentication to reduce, to an acceptable level, the risk of unauthorized access to IT systems and data. (*2021 Report – Volume 2*, p. 137, Recommendation 5; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

Saskatchewan Gaming Corporation included all privileged-user groups in its reviews, increased its use of multifactor authentication, and enforced password expiry requirements on all user accounts.

During 2023, SaskGaming began reviewing all users who can access sensitive systems and data to confirm whether access is still appropriate. For the two quarters we tested, SaskGaming included the expected user groups. Regular reviews of user accounts help ensure only users who require access to sensitive systems and data have access.

We also verified SaskGaming required all user account passwords be changed consistent with its policy. Complying with password policies help mitigate the risk of unauthorized access to sensitive systems and data.

In addition, SaskGaming implemented multifactor authentication for employee devices with network access (e.g., laptops), which electronically authenticates a user's identity using more than just a password and username (e.g., fingerprint, texted codes).

Appropriate IT access controls help to reduce the risk of inappropriate use, modification, or loss of key systems or sensitive data.

3.4 Improved Cybersecurity Analysis

We recommended Saskatchewan Gaming Corporation update its IT security assessment plan to reflect changes in its practice and align with IT industry standards. (*2021 Report – Volume 2*, p. 140, Recommendation 6; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

We recommended Saskatchewan Gaming Corporation analyze information from security assessments and attempted cyberattacks to better identify and address cybersecurity risks. (*2021 Report – Volume 2*, p. 140, Recommendation 7; Crown and Central Agencies Committee agreement November 10, 2022)

Status—Implemented

Saskatchewan Gaming Corporation sufficiently gathered and analyzed security information, as well as updated its IT vulnerability management policy to better align with IT industry standards.

SaskGaming updated its vulnerability management policy in 2023. It requires routine (e.g., monthly) scans of its network and IT systems to identify potential vulnerabilities. It also requires a service provider to test its security (i.e., penetration testing) at least every two years. While good practice suggests completing penetration tests at least annually, agencies must determine appropriate intervals based on assessments of their specific business risks, various security assessment processes in place, and ability to address issues identified by the testing.

We encourage SaskGaming to reassess the frequency of its penetration testing as its cybersecurity practices evolve.

In 2023, SaskGaming contracted a service provider to help analyze security information (e.g., firewall and IT-system logs) and to support incident response. We found SaskGaming acted timely on alerts from the service provider. The service provider also provided monthly reports about potential cybersecurity risks.

Robust security assessments and analysis help to identify cybersecurity risks timely and inform appropriate actions to reduce these risks.