Chapter 22
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 September 2025, Saskatchewan Gaming Corporation implemented the one outstanding recommendation to strengthen its processes for preventing cyberattacks from affecting IT systems and data it uses to support and deliver casino games. We found SaskGaming maintained clear action plans to address significant risks of cyberattacks it identified.

An effective cybersecurity program can help reduce the risk of a successful cyberattack and the total time and associated costs to recover from it.

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, 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, and is responsible for managing and securing all its technology assets, including preventing cyberattacks.

2.1 Focus of Follow-Up Audit

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

We concluded, for the 12-month period ended July 31, 2021, Saskatchewan Gaming Corporation had effective processes to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games except for areas reflected in our seven recommendations.[2] By 2024, SaskGaming implemented six recommendations.[3]

[1] Public Safety Canada, *National Cyber Security Action Plan: 2019–2024*, p. 1.
[2] *2021 Report – Volume 2*, Chapter 17, pp. 127–142.
[3] *2024 Report – Volume 1*, Chapter 16, pp. 187–191.

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 recommendation, 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 interviewed key staff responsible for IT security and examined risk assessments, action plans, and reports related to cybersecurity.

3.0 STATUS OF RECOMMENDATION

This section sets out the recommendation including the date on which the Standing Committee on Crown and Central Agencies agreed to the recommendation, the status of the recommendation at September 5, 2025, and Saskatchewan Gaming Corporation's actions up to that date.

3.1 Clear Actions Planned to Address Cybersecurity Risks

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—Implemented

Saskatchewan Gaming Corporation maintained clear action plans to address significant risks of cyberattacks that may affect IT systems and data used to support and deliver casino games.

SaskGaming reviews its list of cybersecurity risks annually. We found SaskGaming updated its list of risks in 2025, as expected. It assessed 11 significant cybersecurity risks (e.g., information security or data breach, unauthorized access, malicious software), including the likelihood of each risk occurring and the impact each risk would have on its gaming operations.

SaskGaming identified controls in place to mitigate each risk and planned actions to further reduce the risks to acceptable levels. For example, it planned to implement further controls to help prevent the risk of data loss, improve processes to collect and analyze security information, and update security policies and training to continue supporting its employees to use good security practices. It also identified who is responsible to implement the planned actions for each risk and by when.

SaskGaming reported quarterly to its Board about the cybersecurity risks and progress toward implementing planned risk-reduction actions.

Well-defined action plans to address significant cyberattack risks can help prevent unauthorized access or breach of key IT systems and data.