Chapter 17
Saskatchewan Gaming Corporation—Preventing Cyberattacks

1.0 Main Points

Cybercrime continues to be a significant risk for many organizations, costing Canadians about $3 billion in economic losses each year.[1] Cyberattacks can be carried out from anywhere in the world using the internet, and do not require physical access to a business.

At July 2021, the Saskatchewan Gaming Corporation had effective processes, except in the following areas, to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games. SaskGaming needs to:

- Maintain well-defined cybersecurity action plans based on robust, evidence-based risk assessments. SaskGaming included some cybersecurity risks in its corporate-wide risk register, but the risk analysis was insufficient to support effective action plans to address all significant security risks including certain security deficiencies found during our audit.

- Improve its configuration of its IT network, servers, and workstations. During the audit, we were able to access some of SaskGaming's systems and sensitive data without detection. Attackers not only can manipulate inappropriately configured networks or devices to deny access, but also can access, copy, modify, or delete sensitive systems and data.

- Update certain password requirements and conduct complete quarterly privileged-user reviews. Strong password requirements and regular review to ensure users only have access to IT systems and data they need reduces the risk of unauthorized access. These controls are particularly important for privileged users who often have access to view and make changes to all IT systems and data.

- Update its 2017 IT security assessment plan to reflect changes in its practice and to align with IT industry standards. Without robust security assessments (e.g., periodic penetration tests), SaskGaming increases the risk that it will not identify and adequately address new and evolving cybersecurity threats and vulnerabilities in a timely manner.

- Analyze information from security assessments and attempted cyberattacks to better identify and assess cybersecurity risks. SaskGaming collected information from its security assessments, but did not analyze this data. Analyzing as much security intelligence as feasible can help identify weaknesses an attacker might use to get into the IT network, which supports creating cost-effective cybersecurity action plans.

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

We also found SaskGaming had some strong cybersecurity controls. It tracked its IT assets, separated gaming machines from its corporate network, and kept its IT systems up-to-date (i.e., applied timely security patches). In addition, SaskGaming provided regular training to its employees about cybersecurity, and periodically tested their understanding.

Maintaining effective cybersecurity programs reduces the risk of attackers disrupting operations or breaching IT systems and sensitive data, which can result in reputational damage, significant financial costs, and lost profits.

2.0 INTRODUCTION

SaskGaming, a Crown corporation, 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 made its Finance and IT Department responsible for managing and securing all technology assets, including preventing cyberattacks. The Department employs 14 full-time equivalent IT positions to support its workforce of more than 700 employees. These IT positions are responsible for both IT security and operational activities. The Department also contracts with various suppliers to help it fulfill its IT responsibilities.

We audited SaskGaming's processes to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games.

A cyberattack is the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.[2]

2.1 Importance of Cybersecurity

Effective cybersecurity programs to prevent cyberattacks are more important than ever as criminals continue to exploit the world's increasing dependence on IT systems. Per the Canadian Internet Registration Authority's *2020 CIRA Cybersecurity Report*, about three in 10 organizations saw an increase in cyberattack volume during the COVID-19 pandemic in 2020, and further increases are expected.[3] In addition, several high-profile cyberattacks at casinos in Canada and around the world caused outages in recent years, demonstrating cyberattacks can significantly impact casino operations.[4,5]

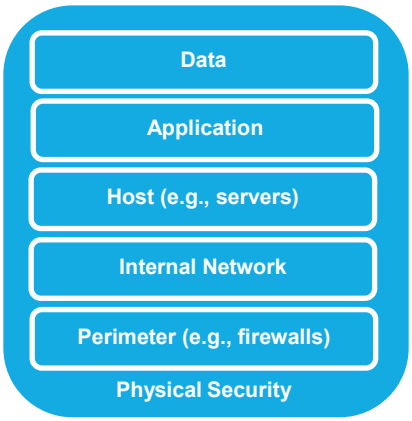
To protect against the many ways an attacker may attempt to gain access to systems and data, many organizations apply a defence-in-depth strategy as outlined in **Figure 1**. The principle of defence-in-depth is that layered security mechanisms as a whole increase system security.

[2] cyber.gc.ca/en/glossary (2 September 2021).
[3] cira.ca/cybersecurity-report-2020 (1 March 2021). CIRA is a non-profit organization that manages the .ca internet domain and builds online security policies, programs, products, and services.
[4] Auditor General of Ontario, (2019), *Technology Systems (IT) and Cybersecurity at Ontario Lottery and Gaming Corporation*, p. 710.
[5] Silverstein, E., *Recent Closing of Three Tribal Casinos Provides Cyberattack Lessons.* www.casino.org/news/recent-closing-of-three-tribal-casinos-provides-cyberattack-lessons/ (24 January 2021).

Figure 1—Defence-in-Depth

The diagram to the right illustrates the common layers where security may be implemented. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.

Due to the ongoing discovery of new security weaknesses and given that no security mechanism is foolproof, securing only one layer (e.g., perimeter) is inadequate. It is important security be addressed at all layers based on assessed risk (i.e., defence-in-depth).



Source: Diagram adapted from The Business Forum, *Antivirus Defense-In-Depth Guide* (2015).

Due to the increasing occurrence and significance of cyberattacks globally, various organizations developed frameworks to help companies implement effective cybersecurity programs. One generally accepted framework is the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST). NIST's Framework includes five functions for an effective cybersecurity program as shown in **Figure 2**. For this audit we focused on the first two functions: Identify and Protect.

Figure 2—Five Functions from NIST's Framework for Improving Critical Infrastructure Cybersecurity

Function	Category
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management
Protect	Identity Management and Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
Detect	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Response Planning Communications Analysis Mitigation Improvements
Recover	Recovery Planning Improvements Communications

Source: The National Institute of Standards and Technology. www.nist.gov/cyberframework/online-learning/components-framework (28 November 2020).
Grey shading indicates functions included in our audit's focus.

Not maintaining effective cybersecurity programs to prevent cyberattacks increases the risk of attackers gaining access to IT systems and data.[6] Attackers with unauthorized access expose companies to disrupted operations, potential loss and exploitation of corporate data, and personal data breaches of its employees and customers.

Processes to prevent cyberattacks can save time and money because restoring IT systems successfully hacked is expensive and time-consuming. For example, in 2020, the global average total cost of a data breach was $3.86 million USD (2019: $3.92 million USD), and 280 days average time to identify and contain a breach (2019: 279 days).[7]

2.2 Importance of Protecting SaskGaming's IT Systems

SaskGaming depends on many IT systems to operate table games, slot machines, food and beverage services, and show lounges, as well as administrative/supportive functions (e.g., casino bank, payroll, accounting, security, IT). For example, SaskGaming uses these IT systems to manage game content, exchange cash and casino tender (e.g., slot machine tickets), and manage player rewards programs offered to its customers. SaskGaming gives employees and certain suppliers access to IT systems to carry out their work, and customers access to check their player rewards. If SaskGaming's gaming-related systems are breached or disrupted, there is a high risk of monetary loss.

SaskGaming's profits support people, programs, and services throughout Saskatchewan. Each year, one-half of its net income is paid to specific First Nations and Métis organizations.[8] In addition, each year it pays a dividend to the Crown Investments Corporation of Saskatchewan. Over the past three years, SaskGaming served millions of customers and earned millions in net income as shown in **Figure 3** below.

Figure 3—SaskGaming Customer and Financial Information from 2018–19 to 2020–21

	2020–21*	2019–20*	2018–19
Customers served (millions)	0.40	2.75	3.25
Revenue ($ millions)	30.9	114.1	118.6
Net income (loss) ($ millions)	(13.4)	40.2	44.9
Net income paid to First Nations and Métis organizations through the General Revenue Fund ($ millions)	--	20.1	22.4
Dividend to Crown Investments Corporation of Saskatchewan ($ millions)	--	13.3	18.0

Source: SaskGaming Annual Reports and corporate records.
* Note: results for 2020–21 are much lower than historical results due to impacts from casino closures related to the COVID-19 pandemic. The pandemic also impacted results for 2019–20, but to a much lesser extent.

In 2020–21, SaskGaming spent about $4.4 million (2019–20: $7 million) on IT services, including new, and upgrades to, IT systems of $0.7 million (2019–20: $2.7 million). In 2021–22, it plans to spend about $6.2 million on IT services, including new, and upgrades to, IT systems worth $1.4 million.

[6] Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (28 November 2020).
[7] IBM Security, *Cost of a Data Breach Report 2020*. www.ibm.com/security/data-breach (20 September 2021).
[8] As required by *The Saskatchewan Gaming Corporation Act*, one half of SaskGaming's net income is paid into the General Revenue Fund which in turn pays grants totalling the same amount to the First Nations Trust, Community Initiatives Fund and Clarence Campeau Development Fund.

Having effective cybersecurity programs to prevent cyberattacks reduces the risk of attackers disrupting SaskGaming's operations or breaching SaskGaming's employees' or customers' personal data. Attackers with unauthorized access could expose SaskGaming to risk of undetected modifications to casino games. Such modifications could potentially damage SaskGaming's reputation if customers become concerned that cyberattacks could affect games running fairly, potentially reducing future revenues.

Furthermore, financial costs of successful cyberattacks at SaskGaming would reduce its profits used to support people, programs, and services in Saskatchewan.

3.0 AUDIT CONCLUSION

We concluded, for the 12-month period ended July 31, 2021, Saskatchewan Gaming Corporation had effective processes, except in the following areas, to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games. SaskGaming needs to:

- **Maintain well-defined cybersecurity action plans based on robust, evidence-based risk assessments to further reduce the risk of unauthorized access, breach, or interrupted service that could result from cyberattacks**
- **Implement stronger configuration of IT network, servers, and workstations to better protect them from security threats and vulnerabilities**
- **Update certain password requirements and conduct complete quarterly, privileged-user reviews to sufficiently restrict access to IT systems and data**
- **Update its IT security assessment plan to reflect changes in its practice and to align with IT industry standards**
- **Analyze information from security assessments and attempted cyberattacks to better identify and address cybersecurity risks**

Figure 4—Audit Objective, Criteria, and Approach

Audit Objective: Assess the effectiveness of Saskatchewan Gaming Corporation's processes, for the 12-month period ending July 31, 2021, to prevent cyberattacks from affecting IT systems and data it uses to support and deliver casino games.

A cyberattack is the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

The audit did not include assessing SaskGaming's processes to detect and respond to cyberattacks or physical security (e.g., physical locks on doors to enter the casino buildings or restricted areas within the buildings, security alarm systems, or video surveillance) of SaskGaming's assets for delivering casino games.

Audit Criteria:

Processes to:

1. **Identify risks that could result in cyberattacks**
   - Maintain an inventory of authorized IT systems and devices (e.g., network, application)
   - Continuously assess likelihood and impact of cyberattacks
   - Set strategies for reducing cyberattack risks to acceptable levels

2. **Protect IT systems from cyberattacks**
   - Securely maintain IT network (e.g., network segregation, firewalls, properly configure devices and software)
   - Properly control use of system privileges (e.g., network, application)
   - Regularly train staff about cybersecurity (e.g., risks, strategies, policies)
3. **Monitor IT security practices adequately prevent cyberattacks**
   - Routinely test network controls operate as expected (e.g., vulnerability scans, penetration testing, integrity checkers)
   - Analyze attempted cyberattacks to identify vulnerabilities and threats
   - Report timely to senior management and the Board

Audit Approach:

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook—Assurance* (CSAE 3001). To evaluate SaskGaming's processes, we used the above criteria based on related work, reviews of literature, and consultations with management. SaskGaming's management agreed with the above criteria.

We examined SaskGaming's policies and procedures, risk assessments, action plans, and reports related to cybersecurity. We interviewed key staff responsible for IT security. We hired an external consultant to assess network and system controls related to cybersecurity.

4.0 KEY FINDINGS AND RECOMMENDATIONS

4.1 IT Assets Sufficiently Tracked

SaskGaming sufficiently tracks its IT assets.

SaskGaming uses a few systems and documents to maintain information about its IT assets, including more than 300 network devices such as firewalls and switches, over 100 servers, over 400 desktop and laptop workstations, and over 100 software applications. It tracks its IT assets in an IT system. The tracking system includes key information about each asset such as: asset tag (name), type, vendor, operating system, version, and location on the network. IT maintenance tools and network diagrams maintain additional information about updates needed and relationships between the assets. SaskGaming's disaster recovery plan maintains information about how long operations can manage without the IT assets. SaskGaming uses all of this information to help manage asset security updates and maintenance.

IT staff add assets to the tracking systems and documents when the assets are purchased or developed, and remove assets at disposal. IT staff are involved in all significant purchases or new development of IT assets. IT staff also complete routine scans and maintenance that help to identify issues with asset tracking. We found the inventory lists complete and accurate based on the information we gathered from network scans and other testing.

Maintaining accurate information about IT assets promotes timely maintenance and disposal of assets, and can help to identify and remove any unauthorized assets (e.g., laptops, software) on the network.

4.2 More Detailed Analysis and Planning for Cybersecurity Risks Needed

SaskGaming includes some risks relating to cybersecurity in its corporate-wide risk register, but does not complete a sufficiently detailed risk analysis to clearly support effective action plans to address all significant cybersecurity risks.

SaskGaming set a corporate-wide risk management policy.[9] The policy includes roles and responsibilities for risk management of the Board, management, and employees. The policy also sets out requirements for an annual risk assessment process including: determining impact and likelihood of risks; setting risk-tolerance levels; developing plans to address risks; ongoing monitoring of risk in daily operations; reporting on actions taken; and aligning with strategic planning and budgeting processes. SaskGaming used a top-down approach to develop and update its corporate-wide risk register (i.e., focus on corporate-wide risks affecting strategic goals and objectives).[10]

SaskGaming provided guidance in its risk framework for how to assess the impact and likelihood of identified risks to support a corporate-wide ranking process. Each year, it identifies its top six risks for more focused action and monitoring.

IT staff are involved in preparing information to support the corporate-wide risk assessment process. Three of the top six risks SaskGaming identified in its 2021–22 corporate-wide risk assessment relate to cybersecurity, including:

- Business interruption (e.g., IT systems needed for operations not available)
- System and information security (e.g., unauthorized changes to IT systems or data)
- Physical security (e.g., unauthorized device attached to network to enable remote access)

SaskGaming's Finance and IT Department also includes assessment of risk as part of its annual department plan. For 2021–22, the Department risks included some related to cybersecurity (e.g., limited staff skills development and cross-training, limited succession planning in the IT department, limited formal cybersecurity program tied to its corporate business continuity plan). The plan did not describe impact and likelihood of the risks or set out clear action plans to reduce risks to acceptable levels.

SaskGaming did not complete an in-depth assessment of cybersecurity risks to expand on its corporate-wide and departmental risk-assessment processes. That is, it did not clearly define and assess specific cybersecurity risks, and set out well-defined action plans to reduce any significant gaps identified. It used some processes to try to manage the various cybersecurity risks it faces, such as:

- Holding weekly meetings where IT employees can raise new risk area awareness and are required to report progress toward addressing previously identified risks.

[9] SaskGaming's corporate-wide risk management policy meets the requirements of the subsidiary risk policy set by its parent, Crown Investments Corporation of Saskatchewan (CIC), at www.cicorp.sk.ca/pub/Reports/Subsidiary%20Crown%20Policy%20Manual/policy-manual---version-4.pdf (8 September 2021).

[10] Opposite to the top-down approach is the bottom-up approach that focuses on key operational and tactical risks on a business unit basis. www.cicorp.sk.ca/pub/Reports/Subsidiary%20Crown%20Policy%20Manual/policy-manual---version-4.pdf (8 September 2021).

- Maintaining a list of action items, which may address some identified risks.
- Following a five-year technical architectural roadmap (2019–24) that briefly sets out IT projects and timelines, some of which may relate to cybersecurity action items (e.g., cyber incident handling, network segmentation, endpoint protection, encryption).
- Using a 2017 cybersecurity action plan that sets out very broad goals for developing a cybersecurity program (e.g., update IT-related policies, build cybersecurity framework, integrate cybersecurity into core learning, invest in network security enhancements). However, this plan is outdated and lacked details on key actions, timing, and resources required.

The processes above support ongoing communications about cybersecurity risks, define staff to lead the work, set some timeframes to complete actions, and support monitoring of ongoing work. However, the processes do not clearly define all significant, unmitigated cybersecurity risks or clearly link the risks to action plans expected to reduce those risks to acceptable levels. Also, the roadmap and action plans did not include sufficient details about planned projects to clearly understand the scope of planned work and how it relates to identified cybersecurity risks. For example, plans do not clearly define the cybersecurity risks related to unauthorized access and expected actions, such as how to further segregate the network or encrypt assets (e.g., laptops) to address those risks.

We found several security deficiencies during the audit as described in **Sections 4.3** and **4.4** that indicate some unidentified cybersecurity risks, some risks requiring further assessment, or certain controls that are not reducing risks as expected.

Without detailed assessments (see **Section 4.6**) to identify all significant cyber risks and clear alignment to current, well-defined action plans to address those risks, SaskGaming is at an increased risk of cyberattacks. Cyberattacks could result in unauthorized access or breach of IT systems and data or significant disruption to operations, causing significant financial costs, asset or revenue loss, or damage to SaskGaming's reputation.

1. **We recommend 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.**

4.3 Stronger Network and IT Device Controls Needed to Restrict Access

While SaskGaming had a number of controls in place to prevent unauthorized access to its systems and data, some access controls were not sufficiently robust (e.g., network segmentation, wireless network configuration, workstation configuration, encryption).

Network: SaskGaming and its service providers use established processes for building and updating IT equipment such as firewalls and the intrusion detection system (IDS).[11]

[11] SaskGaming uses service providers to host certain IT systems, as well as to help it monitor activity on its network.

We found network equipment running up-to-date software and routines. We found SaskGaming appropriately located firewalls and IDS sensors in the network.

SaskGaming uses firewalls to prevent unauthorized individuals from entering its network. While it also restricted certain access within the network using firewalls (e.g., to gaming machines), these restrictions were insufficient to reduce risk of unauthorized access to some key systems (e.g., to support gaming operations). Good practice suggests the use of network segmentation to limit movement across a network in the event an attacker gains unauthorized access. SaskGaming also inadequately restricted ability to copy data from its network to an external source once users, including unauthorized users, access the network.

SaskGaming allows staff to use a wireless network to connect to its network; however, it did not adequately configure the wireless network to appropriately restrict access. The ease of access that a wireless network brings also creates a more open attack surface, as a wireless network only requires the attacker to be in proximity to the network, and does not require physical access.

Service providers help SaskGaming monitor user access and movement within its network. IT staff received alerts about unusual activity detected and monthly summary reports about activity. This monitoring does not detect and alert SaskGaming about all unauthorized activity including the deficiencies we describe in this section and **Section 4.4**. For example, strong monitoring practices can alert if it appears an attacker is using a laptop to gain unauthorized access to the wireless network and then to IT systems to copy large amounts of sensitive data from the network to the attacker's laptop. This type of alert provides the organization time to stop the attack.

Servers: SaskGaming and its service providers use standard processes to set up and update servers. We found servers had up-to-date software.

We found SaskGaming routinely completed backups of its systems and data at established intervals (e.g., nightly incremental backups, weekly full backups). It tested backup effectiveness including through its annual disaster recovery exercise. It updated its disaster recovery plan annually, or as needed.

However, we found SaskGaming made backup copies of certain data that did not have adequate encryption or internal access control. Restricting internal access to and properly encrypting backed up data limits a user's ability to view or copy data in a readable format.

Workstations: SaskGaming uses standard processes to set up and update desktop and laptop workstations. We found the workstations had up-to-date software.

We found workstations allowed users more access to IT systems and data than required to do their jobs. Insufficient access restrictions can result in users accessing unauthorized IT systems and data and/or elevating their privileges to increase their access further. In addition, attackers may exploit employees to gain unauthorized access to sensitive systems and data. Granting the minimum required user access for each employee to carry out required work reduces this risk.

We found SaskGaming inadequately set up its remote access process (e.g., virtual private network) to restrict data flow between an employee's internet activity from activity on SaskGaming's network. In addition, it did not use sufficient encryption on devices such as laptops for employees who may work with sensitive systems and data. Protecting laptops through encryption helps reduce the risk of compromise in the event that laptop is lost or stolen.

During the audit, as a result of the deficiencies noted above, we were able to obtain unauthorized access to some of SaskGaming's systems and data without detection. Data accessed included sensitive information about some of SaskGaming's employees and customers.

Without adequate configuration of its network, servers, and workstations, SaskGaming increases its risk of unauthorized access to its systems and data. A breach of its systems and data could result in revenue loss or financial costs reducing SaskGaming's profits.

2. **We recommend Saskatchewan Gaming Corporation adequately configure its network, servers, and workstations to better protect them from security threats and vulnerabilities.**

We also noted several physical security deficiencies during our audit work. For example, we found certain IT equipment inadequately locked up, lack of visitor logs for certain IT rooms, and insufficient backup power supply. Inadequate physical security controls can result in unauthorized access to IT systems and data resulting in cybersecurity breaches, as well as risk of damage or unavailability of IT systems and data.

4.4 User Access Review and Password Requirements Need Strengthening

Although SaskGaming follows established processes to grant and remove access to its systems and data, it needs to strengthen its password requirements and include all privileged-user groups in its review of user access.

Managers complete a standard form to approve employees' access to IT systems and data before IT staff give access. When an employee leaves, IT staff receive an automatic notification from the payroll system, then remove the employee's access. We found SaskGaming adequately granted and removed user access for its employees except as noted below.

Managers review appropriateness of IT system access for all staff semi-annually and request changes as needed. IT staff review access quarterly for employees with more sensitive access to systems and data (i.e., privileged access). We found SaskGaming completed reviews as expected, except for a group of privileged users who were not included in the quarterly reviews, potentially resulting in more users than required having access to certain systems (e.g., over 15 privileged users for one system that were not reviewed).

SaskGaming uses unique identifiers and passwords to access its systems and data. We found its password standards (set out in policy) consistent with accepted practice by the IT

industry (e.g., minimum eight characters, complexity such as numbers and special characters, change every 90 days, lock after five attempts). However, we found SaskGaming did not require certain sensitive accounts' passwords to be updated every 90 days as expected by its policy. For example, we found accounts where passwords had not been updated in more than nine years. Accounts without appropriate password settings are a potential access point for unauthorized access or malicious software into the SaskGaming network.

In addition, we found SaskGaming does not require multifactor authentication (MFA), except for certain remote access methods. MFA adds a layer of protection to the sign-in process by requiring users to provide additional identity verification listed in **Figure 5**. This stronger authentication method could help to reduce risk of unauthorized access, especially for privileged accounts, sensitive data, and remote access. The more layers of security between an organization's information and cyber criminals, the better.

Figure 5—Examples of Identity Verification Used in Multifactor Authentication (MFA)

Identity Verification Type	Identity Verification Method
Something you know	Password PIN Security questions
Something you have	Card with chip Texted codes
Something you are	Fingerprint Retina scan

Source: Adapted from www.cyber.gc.ca/sites/default/files/publications/what_is_mfa6_e_0.pdf (7 October 2021).

Without sufficiently strong controls to manage who can access IT systems and data, and how, SaskGaming may have increased risk of unauthorized access to its IT systems and data. Unauthorized access can result in inappropriate use, modification, or loss of systems or sensitive data, causing financial and reputational harm.

3. **We recommend Saskatchewan Gaming Corporation include all privileged-user groups in its quarterly user access reviews.**

4. **We recommend Saskatchewan Gaming Corporation update all user account passwords as often as required by its password policy.**

5. **We recommend 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.**

4.5 Sufficient Cybersecurity Guidance and Training Provided

SaskGaming provided sufficient guidance and training to its staff about cybersecurity.

SaskGaming maintained an appropriate IT security policy, as well as policies for acceptable use, privacy, and other specific IT topics. Its employees had ongoing access to the policies on its intranet.

Employees sign-off annually that they understood and followed the IT security policies. During orientation and annual refresher courses, employees access training about SaskGaming's IT security policies through SaskGaming's online learning application. The application tracks attendance so the human resources department can monitor that all employees received the training. IT staff provide the training content. We found all but four out of 584 employees attended the most recent training. Informed employees are less likely to open email attachments containing malware that can infect a corporate IT network.

IT staff typically provide monthly updates about cybersecurity risks and good practice guidance, and upload these updates on SaskGaming's intranet. We found SaskGaming provided updates to staff, although less often than monthly due to casino closures caused by the COVID-19 pandemic. The updates covered a wide variety of security topics such as creating strong passwords, avoiding email scams, and securing use of mobile devices.

SaskGaming used an IT program to semi-annually test the effectiveness of its IT security training. Testing includes activities such as sending an email scam to see whether staff open the email and click the embedded link, or leaving an unidentifiable USB drive to see whether staff try to use it on their computer. The IT program provides a results summary so management can assess training effectiveness. It also sends a notice to employees who fail the test so they can refresh their training and reduce the risk of a real attack.

We found SaskGaming completed its last test in fall 2020, before the casinos ceased operations again due to the COVID-19 pandemic, and reviewed testing as expected. Generally, its employees demonstrated understanding of cybersecurity risks, given only three of about 200 employees tested replied or opened attachments.

SaskGaming sets a budget annually with provisions for funding for training. IT staff can attend more detailed cybersecurity training to maintain their specialized skill sets, although staff were unable to attend specific cybersecurity training in 2020–21 due to casino closures caused by the COVID-19 pandemic. IT staff submit requests for training to their supervisors for approval. We found the IT staff knowledgeable about SaskGaming's IT systems and cybersecurity. IT staff need advanced training to stay current about evolving cybersecurity risks to support development of strategies to reduce those risks and to plan general cybersecurity awareness training for all staff.

4.6 Security Assessments and Analysis Need Improvement

SaskGaming uses a variety of processes to assess its IT security effectiveness, but needs to better analyze security information to support improved risk assessment. It also needs to update its security assessment plans to reflect current practice and IT industry standards, which will improve the quality of information available to analyze.

SaskGaming uses a number of security monitoring practices to assess its current state of IT security. SaskGaming completes ongoing vulnerability assessments and periodic penetration tests to help identify security threats and vulnerabilities, and uses security event monitoring to alert it about potential unauthorized activities in real time. Penetration testing discovers real security weaknesses, while vulnerability assessments are good for security maintenance.

SaskGaming completed regular vulnerability assessments of its network to help identify security threats and vulnerabilities. It documented the expected frequency for these assessments in a test plan in 2017. We found it required some assessments less often (every six months) than good IT industry practice suggests (every four months) without a formal risk assessment to support the decision. We also found it completed some assessments more frequently than expected in its test plan (e.g., almost monthly instead of every six months).

SaskGaming completed some assessments directly, and used third-party service providers to provide other assessments. It tracked all of the assessments in an IT system to support investigation and remediation of identified issues.

However, we found some of the assessments did not utilize sufficiently useful test parameters for identifying potential vulnerabilities. Setting up the scanning tools to broaden these assessments would support better understanding and identification of risks, and detecting unauthorized assets. For example, internal scans using an active account can more thoroughly check servers and desktops.

SaskGaming indicated it plans to complete penetration tests to search for IT security weaknesses every four years; however, it has not documented this plan or rationalized the basis for testing every four years. SaskGaming last completed a penetration test in 2016. Good practice suggests the frequency of penetration testing may vary based on risk (cost-benefit), with many larger organizations running at least annual tests for their IT networks. Management advised us it delayed expected penetration testing in 2020 due to casino closures and related impacts caused by the COVID-19 pandemic. As of July 31, 2021, it had not made any firm plans for its next penetration test.

Third-party service providers also help to monitor SaskGaming's security logs and alerts (e.g., intrusion detection system, firewalls). SaskGaming tracked alerts it received from these parties in an IT system to support investigation and remediation of issues. We found alerts from one service provider were not timely to support management in responding (e.g., received more than 24 hours after incident). Management advised us it is working with its service provider to address this issue. SaskGaming did not receive any critical alerts during our audit period.

Although information from security assessments and alerts helps SaskGaming address specific issues identified in its IT systems, it did not analyze this data holistically to help it assess the quality of its overall security processes. Analyzing this data could help SaskGaming better identify and assess cybersecurity threats and risks.

We identified a number of control deficiencies during the audit as described in **Sections 4.3** and **4.4**. While some of these deficiencies appear to have action items showing management's plans to address them in the future, for several deficiencies, we did not see any evidence that management had yet identified the deficiencies. Regular penetration tests can help to identify such deficiencies to better support risk assessment.

Without robust security assessments about the effectiveness of implemented IT security controls, SaskGaming increases the risk that it will not identify and adequately address new and evolving cybersecurity threats and vulnerabilities in a timely manner. Unmitigated

cybersecurity threats and vulnerabilities could lead to unauthorized access to sensitive systems and data, resulting in financial losses or reputational damage.

6. **We recommend Saskatchewan Gaming Corporation update its IT security assessment plan to reflect changes in its practice and to align with IT industry standards.**

7. **We recommend Saskatchewan Gaming Corporation analyze information from security assessments and attempted cyberattacks to better identify and address cybersecurity risks.**

4.7 Regular Reporting on Cybersecurity-Related Risks

SaskGaming uses weekly meetings and quarterly updates about risks to report to management and its Board about cybersecurity.

SaskGaming's IT employees met weekly to discuss the status of existing and upcoming projects related to managing identified cybersecurity risks. As part of these meetings, it updated a list of action items to track progress toward these projects.

In addition, SaskGaming's corporate-wide risk management policy requires management to provide quarterly updates on the top corporate-wide risks, as well as ad hoc reports about any significant emerging risks or breakdown of controls immediately, if they occur. We found management provided quarterly updates on risks as expected by the policy. Management advised us that no such issues arose during the year to require ad hoc reporting to the Board.

More detailed assessments to identify all significant cyber risks as described in **Sections 4.2** and **4.6** will help SaskGaming confirm its quarterly updates to its Board include all relevant information about risks and mitigation strategies. Regular reporting on cybersecurity risks helps with allocating resources to manage these risks and monitoring the effectiveness of related risk strategies.

5.0 GLOSSARY

Application – A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup – A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Configure – To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Defence-in-depth – The practice of using layered security mechanisms to increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.

Disaster recovery plan – A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Encryption – The process of converting information or data into a code, especially to prevent unauthorized access.

Firewall – Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up using firewall rules to only allow certain types of data through.

Integrity checker – a tool used to detect unauthorized changes made to an IT system or data.

Intrusion detection system – Software and/or hardware designed to detect a security breach by identifying inappropriate access or changes taking place within a computer or network.

Intranet – a communications network within an organization employing the same technology as the internet.

Multifactor authentication (MFA) – Users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone when accessing accounts or apps.

Network – A group of computers that communicate with each other.

Penetration test – a security exercise to find and exploit vulnerabilities in an IT system.

Security vulnerability – An unintended weakness in a computer system exposing it to the potential exploitation such as unauthorized access or malware (e.g., viruses).

Server – A computer hosting systems or data for use by other computers on a network.

Unauthorized access – When someone gains access to a website, program, server, or other systems and data using someone else's account or other methods.

User access controls – The controls in place at an organization to restrict use of systems or data to those authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

Vulnerability assessment – A systematic review to identify, classify by severity, and recommend remediation actions for any known weaknesses of an IT system. Organizations generally use IT tools to help complete the review.

6.0 SELECTED REFERENCES

Auditor General of British Columbia. (2017). *An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls*. Victoria: Author.

Auditor General of Ontario. (2019). *Technology Systems (IT) and Cybersecurity at Ontario Lottery and Gaming Corporation*. Toronto: Author.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg: Author. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (28 November 2020).

Provincial Auditor of Saskatchewan. (2015). 2015 Report – Volume 1, Chapter 18, *SaskPower—Managing the Risk of Cyber Incidents*. Regina: Author.

Provincial Auditor of Saskatchewan. (2020). 2020 Report – Volume 1, Chapter 6, *eHealth—Securing Portable Computing Devices*. Regina: Author.