Chapter 7
SaskBuilds and Procurement—Responding to Cyberattacks

1.0 Main Points

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

Through its Information Technology Division, the Ministry of SaskBuilds and Procurement delivers IT services to nearly 30 government ministries and agencies (i.e., clients). It manages over 700 servers and over 300 applications on behalf of its clients.

Effective cyberattack response plans 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 critical government services (e.g., social assistance, child and family services, public safety alerts). Tested response and recovery plans help ensure corrective actions taken lessen the devastating impact of a cyberattack.

At August 31, 2023, the Ministry had effective processes, except in the following areas, to respond to cyberattacks. The Ministry needs to:

- Centrally and continuously monitor all security event logs to identify potential cyberattacks and to ensure these are managed in a timely and responsive way.
- Undertake periodic penetration testing, which involves simulating cyberattacks, to identify and address cybersecurity vulnerabilities and threats.
- Expand its testing techniques and continuously test its cyber incident response and recovery plans.

  Regular training and testing (e.g., walkthroughs, tabletop exercises, simulations) of response and recovery plans helps ensure personnel understand their roles and responsibilities to enact the plans appropriately to mitigate damage from security events, including ransomware, data breaches and cyberattacks.

The Ministry has a reasonable cyber incident response plan and several playbooks to respond appropriately to cyberattacks. These plans include processes to communicate with its clients and service providers and steps for rapid remediation and recovery.

Having comprehensive, up-to-date response plans can help reduce the associated costs and the total time the Ministry requires to recover from a cyberattack.

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

2.0 INTRODUCTION

The Ministry of SaskBuilds and Procurement Regulations assign the Ministry of SaskBuilds and Procurement responsibility for developing, implementing, monitoring, and enforcing IT security policies and standards. As part of its mandate, the Ministry delivers IT services to certain government ministries and agencies (i.e., clients) through its Information Technology Division—see **Section 6.0** for a list of its 29 clients at August 31, 2023, which includes all ministries except the Ministry of Health.[2] The Ministry does not provide IT services to the Government's Crown corporations like SaskEnergy, SaskTel, and SaskPower.

We audited the Ministry's processes to respond to cyberattacks.

A cyberattack is the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.[3] Attackers can interfere with the production and delivery of basic goods and services provided by the public sector. They can also undermine privacy by stealing personal information. Cyberattacks are one type of security incident that actually or potentially jeopardize the confidentiality, integrity or availability of an IT system.

The Ministry's clients' information (e.g., information about vulnerable adults and children, employee payroll information) must be protected from unauthorized use, disclosure, damage or loss; and must be available when needed, particularly during emergencies.

Due to the increasing occurrence and significance of cyberattacks globally, various frameworks exist to help organizations 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 that outline activities for an effective cybersecurity program as shown in **Figure 1**. Our audit focused on the last three functions: Detect, Respond, and Recover (from a cyberattack).

Figure 1—Five Functions from NIST's Framework for Improving Critical Infrastructure Cybersecurity

Function	Activities
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 & Procedures Maintenance Protective Technology

[2] eHealth Saskatchewan is responsible for managing critical IT services used to administer and deliver healthcare services in Saskatchewan. This includes responsibility for Saskatchewan's electronic health record and IT systems used by Saskatchewan Health Authority, Saskatchewan Cancer Agency, 3sHealth, and the Ministry of Health.
[3] www.cyber.gc.ca/en/glossary#c (7 December 2023).

Function	Activities
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 (7 December 2023).
Grey shading indicates functions included in the focus of our audit.

The **Glossary** in **Section 5.0** defines many of the IT terms used in this chapter.

2.1 The Ministry's Delivery of IT Services

The Ministry of SaskBuilds and Procurement utilizes a hosted data centre for its computer network equipment and servers supporting client systems and data, and manages over 700 servers and over 300 applications on behalf of its clients.

About 15,000 public sector employees access information assets managed by the Ministry every day.

The Ministry contracts service providers to operate the data centre and to deliver certain IT services. In addition, the Ministry contracts a cloud service provider to host and manage some of its clients' systems and data.[4]

IT is an integral part of delivering many government programs and services. To deliver services effectively and achieve objectives, government ministries and certain government agencies rely on key IT controls delivered by the Ministry to keep their IT systems and data secure.

In 2022–23, the Ministry spent $150 million to maintain and deliver IT services.[5] At August 2023, it had 250 full-time equivalent staff dedicated to delivering IT services.

2.2 Importance of an Effective Cyberattack Response

Cybercrime in Canada, including cyberattacks via the internet, causes more than $3 billion in economic losses each year.[6] These crimes do not require physical access to an organization's premises.

While there are many different types of cyberattacks, **Figure 2** describes the three most common attacks affecting Canadian organizations.

[4] www.cyber.gc.ca/en/glossary#c (7 December 2023). Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere. Users access these resources via a computer network instead of storing and maintaining all resources on their local computer.
[5] Adapted from information provided by the Ministry of SaskBuilds and Procurement.
[6] Public Safety Canada, *National Cyber Security Action Plan: 2019–2024*, p. 1.

Figure 2—Three Most Common Cyberattacks Affecting Canadian Organizations

Cyberattack	Definition
Phishing	A cyberattack involving phishers (i.e., cybercriminals) pretending to be someone they are not (e.g., bank representative, government official, person from within the organization) to trick someone into sharing confidential information.
Malware	Malicious software designed to infiltrate or damage systems, networks and devices without someone knowing. Malware can take many forms, but once installed, the attacker may have access to an organization's sensitive information.
Unauthorized Access	Occurs when someone gains access to an organization's information, devices or networks without authorization.

Source: Innovation, Science and Economic Development Canada. www.ised-isde.canada.ca/site/cybersecure-canada/en/common-cyber-attacks (7 December 2023).

In 2022, Canada's foreign signals intelligence agency, the Communications Security Establishment, responded to almost 2,100 cybersecurity incidents affecting federal institutions, provincial services and critical infrastructure partners.[7,8]

Cybercrime has a major impact on organizations' economic security. The average ransomware payment in Canada during 2022 was over $250,000—this is in addition to other costs borne by organizations such as service disruptions, identity and intellectual property theft, IT recovery costs, and reputational damage.[9] The estimated total cost of an average data breach in Canada during 2022 was $5.6 million (2021: $5.4 million).[10]

IBM's 2022 data security report indicated that it took an organization an average of 277 days—roughly nine months—to identify and contain a data breach.[11] An incident going undetected for a substantial time can result in significant losses and damage to organizations and those they serve.

Once detected, a cyberattack requires corrective action, such as rapid remediation and threat containment, along with analysis and recovery of services in a clean state. These actions are crucial, yet often ineffective unless an agency has appropriate and tested response and recovery plans.

The systems and data the Ministry of SaskBuilds and Procurement manages on behalf of clients include several critical systems imperative to the government's delivery of essential services (e.g., social assistance, child and family services, public safety alerts, wildfire detection, correctional facilities, central payroll and payment processing). Inability to access these systems for a period of time can significantly impact Saskatchewan residents.

Effective cybersecurity programs that successfully respond to cyberattacks are more important than ever as cybercrime increasingly exploits IT systems. Given the increased level of interconnectivity between systems, the consequences of lengthy breaches are significant—once an attacker breaches one system, there is increased risk of further breaches in other systems.

[7] *Communications Security Establishment, Annual Report: 2022–23*, p. 27. The Communications Security Establishment (CSE) is Canada's technical authority for cybersecurity and information assurance. It alerts governments to the activities of foreign entities seeking to undermine national prosperity and security.
[8] www.cyber.gc.ca/en/glossary#c (7 December 2023). A cyber incident is any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.
[9] *Communications Security Establishment, Annual Report: 2022–23*, p. 17.
[10] IBM Security, *Cost of a Data Breach Report 2022*, p. 10.
[11] Ibid., p. 14.

3.0 AUDIT CONCLUSION

We concluded, for the 12-month period ended August 31, 2023, the Ministry of SaskBuilds and Procurement had effective processes, except in the following areas, to respond to cyberattacks. The Ministry needs to:

- **Centrally and continuously monitor all security events to identify potential cyberattacks**
- **Undertake penetration testing on a periodic basis to identify and address cybersecurity threats**
- **Expand its testing techniques and continuously test its cyber incident response plans**

Figure 3—Audit Objective, Criteria, and Approach

Audit Objective:

The objective of this audit was to assess whether the Ministry of SaskBuilds and Procurement had effective processes, for the 12-month period ending August 31, 2023, to respond to cyberattacks.

Audit Criteria:

Processes to:

1. **Identify potential or actual cyberattacks**
   - Maintain event logs for review
   - Monitor network devices that report unusual network activity
   - Require service providers to provide timely notification of any cyber risks and related potential impacts
   - Routinely test network controls operate as expected (e.g., vulnerability scans, penetration testing, integrity checks)
2. **Secure operations during a breach**
   - Maintain cybersecurity response plan (including incident triage and escalation)
   - Plan for assembling a breach response team to prevent additional data loss
   - Stop additional data loss and assess extent and cause of breach
   - Promptly notify appropriate stakeholders (i.e., clients, service providers, law enforcement)
3. **Resolve and recover from a breach**
   - Remediate vulnerabilities and confirm resilience
   - Restore systems and data (based on tested plans)
   - Conduct post-incident reviews and implement improvements
   - Communicate results with appropriate stakeholders (i.e., clients, service providers)

Audit Approach:

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

We examined the Ministry's policies, procedures, event logs, and reports relating to responding to cyberattacks. We interviewed key staff responsible for responding to cyberattacks. We hired an external consultant to analyze the Ministry's processes to respond to a cyberattack and to help assess the processes against good practice.

4.0 KEY FINDINGS AND RECOMMENDATIONS

4.1 Certain Event Logs Not Centrally and Continuously Monitored

While the Ministry of SaskBuilds and Procurement monitors its network to identify possible cyberattacks or security incidents, it does not centrally collect and monitor all the event logs and therefore assess all identified potential threats 24/7.

The Ministry uses two separate groups of IT security experts and two separate event tracking processes to monitor for security events on its network. A service provider monitors event logs from various network devices 24/7 and Ministry staff monitor network activity using different monitoring software tools than the service provider uses. However, Ministry staff do not perform their monitoring 24/7.

Identified events that indicate possible cyberattacks or security incidents (e.g., gaining network access through connection of an unauthorized device) are investigated and dealt with immediately.

Using the event logs, the service provider identifies and analyzes areas of potential security concerns and reports them to Ministry management for further investigation and mitigation. The service provider communicates minor issues to the Ministry on a weekly basis. It immediately communicates to the Ministry, any issues it considers significant and works with the Ministry to respond to the security concern; this includes reporting any concerns identified after normal business hours. For example, the service provider would report multiple failed login attempts from a single location as a potential security concern to the Ministry.

From September 2022 to August 2023, the service provider analyzed about 2,800 potential security incidents out of several million security events logged.

The service provider reported about 150 security incidents to the Ministry. Seven of these were assessed as high/critical by the service provider.

The service provider categorizes incidents into three categories: high, medium, and low. Security severity levels consider impact to the business, level of security breach into the network, and complexity to contain and resolve the situation. According to the contractual arrangement with the service provider, the service provider's response will be quicker the higher the severity level.

Between September 2022 and August 2023, the service provider identified seven high/critical incidents and reported them to the Ministry. The Ministry addressed and resolved all seven within a reasonable time.

We tested 10 incidents identified in event logs and found the Ministry or service provider appropriately followed up the incidents in a timely manner based on the assessed severity level.

We found the Ministry's processes to track and maintain event logs reasonable. For example, log data is retained for a sufficient number of months for auditing, investigation, and forensics support by the service provider.

We also tested the Ministry's processes to detect and log possible security incidents. We ran a number of test cases to determine whether the Ministry's monitoring processes detected the incident. **Figure 4** shows examples of the test cases we used. We found the Ministry adequately logged and detected the incidents tested. In certain instances, the Ministry would have notified the service provider.

Figure 4—Examples of Test Cases Used

- Password attack (attempted to gain access to the network through multiple password attempts)
- Shutdown of a server
- Change in privileged access (e.g., escalation of access, creation of new access)
- Addition of unauthorized device on the network
- Addition of unauthorized Wi-Fi access point
- Installation of unauthorized software

Source: Office of the Provincial Auditor of Saskatchewan.

The Ministry only communicates significant events identified through its monitoring to its service provider, who then investigates the events and notifies the Ministry whether it needs to take corrective action. A complete analysis of all identified events could help in detecting attack patterns.

Also, the Ministry does not perform its monitoring 24/7. This could result in the Ministry not identifying and dealing with security events timely. Undetected events could lead to loss of system availability or system compromise.

1. **We recommend the Ministry of SaskBuilds and Procurement centrally and continuously monitor all event logs to identify potential cyberattacks.**

4.2 Cyber Incident Response Plan Maintained

The Ministry of SaskBuilds and Procurement has developed response plans (Cyber Incident Response Plan and playbooks) to use in the event of a possible cyberattack or security incident.[12]

The Ministry's response plans document the steps to take after a cyberattack. The Ministry most recently updated the response plans in 2023 and intends to update them annually.

The Response Plan includes definitions of what a possible incident would be; the personnel involved in the response, including their roles and responsibilities; the response timeframe based on the assessed severity of the incident; the steps to contain (i.e., stop additional data loss) and recover from the incident; and the documentation and follow up required after the incident has been dealt with.

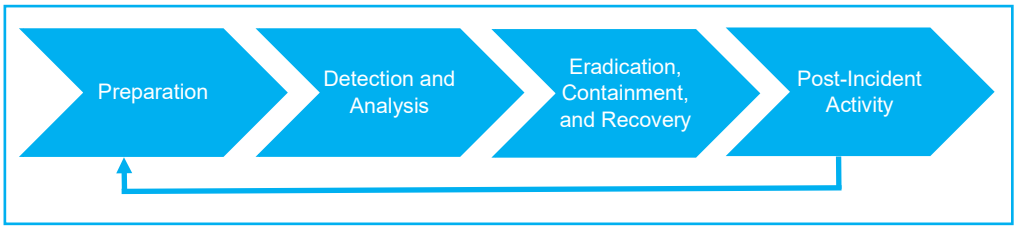
The Ministry also developed several incident response playbooks as guidance in specific situations (e.g., unauthorized access, denial of service attack, ransomware attack).

We found the Ministry's Response Plan and playbooks reasonably document the necessary steps to respond to a cyberattack or security incident. The Ministry appropriately

[12] A playbook is a document typically part of overall cyber response plans or disaster recovery plans documenting key aspects, including response and recovery steps to enact during a crisis.

used guidance from the National Institute of Standards and Technology (NIST), as described in **Figure 5**, to develop its Response Plan and playbooks.[13]

Figure 5—Incident Response Life Cycle



Source: Adapted from nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, p. 21.

The Ministry's Response Plan specifies the roles and responsibilities of its response team—the Computer Security Incident Response Team (CSIRT), which would be activated on the same day of detecting an incident determined to be high or critical by the Ministry. The team appropriately includes staff throughout the Ministry, including from the IT Help Desk, Security Team, Network Administrators, IT Operations, Human Resources, Executive Management, and Legal. The Response Plan also has processes for notifying external parties such as clients, legal advisors, and law enforcement officials.

From September 2022 to August 2023, we found the Ministry appropriately utilized its CSIRT for one incident described in **Section 4.4**.

Having comprehensive, up-to-date response plans allows agencies to respond effectively to a cyberattack or security incident. This decreases the risk of systems being unavailable when needed and the potential loss of data. In addition, appropriate response plans can help reduce the total time required to recover from a cyberattack and the associated costs.

4.3 Security Assessments and Response Plan Testing Needs Improvement

While the Ministry of SaskBuilds and Procurement performs periodic vulnerability scans of its network and has documented cyber response plans, it has not yet sufficiently tested its plans. It also needs to include periodic penetration testing within its security assessment plans.

We found the Ministry's service provider performs monthly vulnerability scans. These scans focus on the Ministry's network including servers, workstations, and firewalls by examining the security of these devices for known vulnerabilities. The Ministry assesses any identified issues to determine whether it needs to make any configuration changes to improve security and address vulnerabilities. Vulnerability scanning is an important part of testing any cyber incident response plan because it helps to identify which parts of the network are most likely to be targeted by hackers. Vulnerability scanning is also part of the Ministry's continuous efforts to enhance oversight and security as part of its security assessment plans.

> Penetration testing discovers real security weaknesses, while vulnerability assessments are good for security maintenance.

[13] *Framework for* Improving *Critical Infrastructure Cybersecurity*. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (4 March 2024).

Another good technique to test response plans and assess the operation of network security is to perform periodic penetration tests.[14]

Penetration testing is a crucial part of an organization's cybersecurity strategy. It involves simulating cyberattacks to identify vulnerabilities in computer systems or networks. 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.

The Ministry does not perform penetration testing to help assess the security of its network and systems. At August 2023, the Ministry only performs penetration testing when requested by its clients for specific applications the Ministry hosts in its data centre. From September 2022 to August 2023, its clients did not request the Ministry to perform any penetration tests.

Regular penetration tests can help to identify such deficiencies to better support cyber risk assessments. Without robust security assessments about the effectiveness of implemented IT security controls, the Ministry increases the risk that it will not identify and adequately address new and evolving cybersecurity threats in a timely manner.

2. **We recommend the Ministry of SaskBuilds and Procurement undertake penetration testing on a periodic basis to identify and address cybersecurity threats.**

One of the most important good practices for incident response testing is to conduct periodic 'fire drills' (e.g., simulations, tabletop exercises) that simulates a cyber incident. Organizations conduct these fire drills to spot any weak links in their response plans, ensure that all personnel know exactly what to do, and refine the response plans based on any shortcomings observed in the fire drill.

The Ministry's latest test of its cyber response plans occurred as a tabletop exercise in August 2023. This exercise tested the processes in the Ministry's ransomware playbook. We observed this test and found it aligned with the Response Plan and playbooks. We found the participants understood their roles in the response. However, this was the Ministry's only test of its plans since its initial response plans were first developed in January 2022.

While the Ministry has set the expected frequency (i.e., annually) of testing its response plans, the plans only specify the use of tabletop exercises. Good practice includes frequently testing response plans with a variety of techniques (e.g., walkthroughs, tabletop exercises, simulations).[15,16]

Without periodically (i.e., at least annually) testing its response plans, there is increased risk staff of the Ministry's response team (including backup personnel) may not fully understand their roles and responsibilities when a cyber incident occurs. This could result in the Ministry not appropriately responding to incidents timely. In addition, fully tested

[14] docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf, p. 245 (7 December 2023).
[15] nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, p.151 (7 December 2023).
[16] The frequency of the testing would be affected by a variety of factors including criticality of the system or application. For example, the standard for agencies that store credit card information is that penetration testing should be conducted annually or whenever there is a significant system or application change. docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf, p. 247 (7 December 2023).

response plans can give the Ministry assurance that its plans will be effective when cyber incidents occur.

3. **We recommend the Ministry of SaskBuilds and Procurement expand its testing techniques and continuously test its cyber incident response plans.**

4.4 Recovery Plans Documented

The Ministry of SaskBuilds and Procurement has adequate documentation to assist with recovery in the event of a cyber incident.

The Ministry's incident response playbooks include general information on its processes to recover from various cyber threats. Also, the Ministry's Disaster Recovery Plan contains information and details the Ministry would need to recover eight out of its 14 key client systems (e.g., MIDAS) in the event of loss.[17] The Ministry tests its Disaster Recovery Plan for these key systems once a year and restores them at an alternate site. We found these processes reasonable.

We reviewed the Ministry's playbooks and found they contained information related to recovery processes. As each cyber incident is unique, we found the Ministry documented recovery processes in its playbooks at a high level—enabling flexibility in its responses to cyber incidents. However, the Ministry has not fully tested its recovery processes. See **Recommendation 3**.

We also reviewed the detailed recovery processes outlined in the Ministry's Disaster Recovery Plan. The Recovery Plan included key information such as server names, location of backup information, and location of recovery scripts used to restore systems and data.

Between September 2022 and August 2023, management indicated it experienced one significant cyber incident. The incident did not cause any system outages or data loss, therefore no recovery processes were required. We reviewed the Ministry's response to the incident and found it responded appropriately, including amending its firewall rules to block suspect internet addresses and also preventing unauthorized access during the attack. The Ministry detected the threat and implemented mitigation measures on the same day.

Having adequate documentation of processes to recover from a cyber incident helps agencies to recover systems and data timely.

4.5 Incident Communication Strategies Reasonable

The Ministry of SaskBuilds and Procurement communicates with its clients and service providers in the event of breach(es) due to a cyber incident consistent with its Cyber Incident Response Plan.

[17] MIDAS includes modules for general ledger, cash management, accounts payable, accounts receivable, purchasing (including tendering management, requisitions and receiving), payments, public sector forecasting, capital assets, inventory and human resources/payroll used by all the ministries.

The Response Plan details processes to inform affected clients and service providers when a cyber incident occurs, as well as requires the Ministry to consult with its legal team and Privacy Officer to determine who to notify based on the circumstances of the incident.

The Response Plan sets out responsibilities of the response team—the Chief Information Security Officer is responsible for communicating the cyber incident to affected parties, including the Ministry's executives, and clients' ministers, deputy ministers, and management. We found the Ministry also maintains an updated client contact list. (e.g., the list included 42 contacts at 29 clients of the Ministry).

We found the Ministry developed email templates to communicate cyber incidents to its clients. We found the templates appropriately set out required information to communicate such as:

- Assessed severity of the incident
- Status of incident response
- Expected date of resolution

For the incident described in **Section 4.4**, we found the Ministry appropriately communicated with the affected clients and service providers. For this incident, the Ministry worked with two of its service providers to assist in the analysis and the response.

Having adequate communication steps helps the Ministry to provide affected parties with transparent and timely information about cyber incidents. Increasing awareness of a cyber incident as it occurs can assist in providing a more effective response.

4.6 Post-Incident Analysis Appropriate

The Ministry of SaskBuilds and Procurement's Cyber Incident Response Plan includes steps to review the Ministry's response to an incident once it has been resolved.

We reviewed the Ministry's Response Plan and found it includes reasonable steps for the Ministry to review its response to cyber incidents following their resolution. Based on the severity of the cyber incident, these steps could include post-incident analysis, meetings to discuss lessons learned, and assessing the need to revise its response plan. Meetings are expected to be held with staff directly involved in the response.

We found the Ministry developed guidance for documenting its post-incident reviews. The Ministry expects its post-incident reviews to determine whether:

- Staff followed documented processes
- The response involved the appropriate staff, including consideration of additional resources, such as tools and external experts
- Communications to affected parties (e.g., clients) were appropriate
- Staff took appropriate actions to prevent similar future incidents

For the cyber incident described in **Section 4.4**, the Ministry appropriately documented and analyzed the response to the incident. Its review included a summary of actions taken to resolve the incident and recommendations for improvement to further increase security. The Ministry did not identify any required changes to its response plans.

Subsequently reviewing responses to cyber incidents allows the Ministry to improve its response plans. Improvements can also lead to increased security over the systems and data the Ministry manages and can help reduce the total time an agency requires to recover from a cyberattack and the associated costs.

5.0 GLOSSARY

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

Denial of Service Attack – This is a type of cyberattack where an attacker attempts to slow or stop applications or network services using non-legitimate connection requests. This prevents legitimate connections.

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 allow only certain types of data through.

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

Penetration test – A simulation of a real-world cyberattack to find vulnerabilities in a computer system.

Ransomware attack – An individual gains access to a computer system, encrypts data and system files rendering them unusable. The individual demands a ransom in exchange for the encryption key.

Security event – An observable occurrence that could affect your information security (e.g., an unsuccessful log in attempt).

Security incident – One or more security events that actually or potentially jeopardizes the confidentiality, integrity or availability of an IT system.

Security vulnerability – An unintended weakness in a computer system exposing it to 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.

Tabletop exercise – A simulation exercise where participants discuss the steps they would take in the event of a cyberattack. The participants would follow the entity's documented response plans and procedures. This allows the entity to assess their documented response plans.

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

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 SaskBuilds and Procurement's Clients at August 31, 2023

Ministries:	
Executive Council Ministry of Advanced Education Ministry of Agriculture Ministry of Corrections, Policing and Public Safety Ministry of Education Ministry of Energy and Resources Ministry of Environment Ministry of Finance Ministry of Government Relations	Ministry of Highways Ministry of Immigration and Career Training Ministry of Justice and Attorney General Ministry of Labour Relations and Workplace Safety Ministry of Parks, Culture and Sport Ministry of SaskBuilds and Procurement Ministry of Social Services Ministry of Trade and Export Development Public Service Commission
Agencies:	
Apprenticeship and Trade Certification Commission Financial and Consumer Affairs Authority of Saskatchewan Global Transportation Hub Authority Public Guardian and Trustee of Saskatchewan Provincial Capital Commission	Saskatchewan Housing Corporation Saskatchewan Legal Aid Commission Saskatchewan Liquor and Gaming Authority Saskatchewan Municipal Board Saskatchewan Public Safety Agency Water Security Agency

7.0 Selected References

Auditor General of British Columbia. (2021). *Management of Medical Device Cybersecurity at the Provincial Health Services Authority*. Victoria: Author.

Auditor General of British Columbia. (2019). *Detection and Response to Cybersecurity Threats on BC Hydro's Industrial Control System*. Victoria: Author.

Auditor General of Canada. (2022). *Cybersecurity of Personal Information in the Cloud*. Ottawa: Author.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg: Author. nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (8 November 2023).

Provincial Auditor Saskatchewan, (2021). *2021 Report – Volume 2*, Chapter 17, *Saskatchewan Gaming Corporation—Preventing Cyberattacks*. Regina: Author.