Auditor General
MANITOBA

Report to the Legislative Assembly

Cybersecurity Incident Response Process at Shared Health

Independent Assurance Report

WEBSITE VERSION

December 2024

This page is intentionally left blank.

Auditor General
MANITOBA

December 2024

Honourable Tom Lindsey
Speaker of the Legislative Assembly
Room 244, Legislative Building
450 Broadway
Winnipeg, Manitoba R3C 0V8

Dear Mr. Speaker:

It is an honour to submit my report, titled *Cybersecurity Incident Response Process at Shared Health*, to be laid before Members of the Legislative Assembly in accordance with the provisions of Section 28 of *The Auditor General Act*.

Respectfully submitted,

Original Signed by: Tyson Shtykalo

Tyson Shtykalo, FCPA, FCA
Auditor General

Office: 204.945.3790 | 500-330 Portage Avenue | Winnipeg, Manitoba R3C 0C4 | oag.mb.ca

This page is intentionally left blank.

Table of contents

This page is intentionally left blank.

Auditor General's comments

Public sector information systems are vital for delivering services to Manitobans. These systems hold a lot of data, including personal and other sensitive information. These systems are increasingly susceptible to cyberattacks, including ransomware and data theft.

We have released several IT audits in recent years, which identified the need to improve cybersecurity controls across the public sector. Improving these controls reduces the risk that bad actors will be able to access these information systems. However, even with the most robust controls in place, cyberattacks can still occur. Public sector organizations need to be prepared to respond when cybersecurity incidents happen, in order to minimize the impact to their operations and the potential loss of data.

In this audit, we determined that Shared Health has a plan and resources in place to respond to a successful cyberattack. However, there remains work to do. Shared Health must perform exercises to test its Cybersecurity Incident Response Plan, improve training, and complete its external communications plan.

This report includes 4 recommendations that will help Shared Health improve its readiness to respond to a cybersecurity attack. While these recommendations are specifically directed to Shared Health, all public sector organizations must take steps to prepare themselves for responding to cybersecurity incidents.

I would like to thank Shared Health's management and staff for their cooperation and assistance throughout this audit, and I extend my appreciation to my audit team for their efforts in completing this important work.

Original Signed by: Tyson Shtykalo

Tyson Shtykalo, FCPA, FCA
Auditor General

Recent audits where we discuss weaknesses in cybersecurity controls

- *Managing IT Security for Remote Access* (2024)
- *Information Systems – Privileged Access* (2022)
- *Aging Information Systems* (2022)
- *Vital Statistics Agency* (2020)
- *eChart Manitoba* (2018)

This page is intentionally left blank.

Report highlights

Why we did this audit

- Reliable and accessible information systems are vital for delivering public health-care services.
- These systems are susceptible to cyberattacks due to the criticality of the services they support and the wealth of personal information they hold.
- We wanted to determine if Shared Health has a process to promptly respond to cybersecurity incidents, minimizing the impact to health operations and loss of data.

Conclusion

Shared Health has a process to promptly respond to cybersecurity incidents, but regular testing and training can be improved.

This audit includes 4 RECOMMENDATIONS.

What we found

Cybersecurity Incident Response (CSIR) Plan

Shared Health has a plan for responding to cybersecurity incidents, but better training is required, and some supporting practices need to be documented.

- A security standard, plan, and supporting procedures have been developed, and Shared Health staff and external resources are ready to respond to cybersecurity incidents.
- Training sessions have not been held with all members of the CSIR team, which is responsible for responding to and managing cybersecurity incidents.
- A plan for communicating to external stakeholders during a cybersecurity attack has not been completed, and procedures for ransomware and extortion incidents are still under development.

Plan testing

Exercises are not being performed to test the CSIR Plan

- Testing the plan is important to ensure readiness for cybersecurity incidents.

Plan implementation

Processes are in place to activate the CSIR Plan when needed

- Cybersecurity incident detection and analysis are covered in Shared Health's incident management process.

This page is intentionally left blank.

Background

The Province of Manitoba's health-care system is delivered by a variety of organizations, including:

- Manitoba Health.
- Service Delivery Organizations.
  - Shared Health.
  - Five regional health authorities (including controlled organizations):
    - Interlake-Eastern Regional Health Authority
    - Northern Regional Health Authority
    - Prairie Mountain Health
    - Southern Health-Santé Sud
    - Winnipeg Regional Health Authority
  - CancerCare Manitoba.

Manitoba Health is the department within the Manitoba government that guides the planning and delivery of health-care services throughout the province. Manitoba Health operates under the provisions of the legislation and responsibilities of the Minister of Health.

Shared Health, established in 2018, serves as the provincial health authority. It provides province-wide services to streamline the delivery of health care and reduce duplication of support services, including managing information and communication technology for Service Delivery Organizations. This enables Service Delivery Organizations to focus on providing health services. Shared Health uses a shared services model to reduce complexity and improve efficiency within the health-care system in the province. Digital Shared Services is part of this shared service model. It provides technology services to Shared Health and other Service Delivery Organizations. Its duties include managing the cybersecurity program.

Digital Shared Services has a **Cybersecurity Incident** Response (CSIR) Standard that describes baseline security requirements, standards, and specifications to prepare for an effective response to an information security incident. It defines the critical administrative and technical control requirements to ensure that Digital Shared Services can detect, respond to, and manage cybersecurity incidents in a manner that would minimize impact and/or harm to IT assets and delivery of health-care services and patient needs.

A **cybersecurity incident** is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system.

Source: Shared Health Cybersecurity Incident Response Plan

The Cybersecurity Incident Response (CSIR) Plan supports the CSIR Standard by providing guidance for managing activities during high- or critical-priority cybersecurity incidents. Its objective is to ensure a consistent and effective response is made to contain and minimize the potential impact of these incidents. The CSIR Plan provides guidance on:

- Defining what a cybersecurity incident is and classifying incident priority.
- The roles and responsibilities required to effectively manage cybersecurity events, including defining the CSIR team.
- The process to respond to and effectively manage cybersecurity incidents.

A **firewall** is a device that has a network protection application installed to safeguard the network from intentional or unintentional intrusion. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

Source: NIST Special Publication 800-35

The CSIR Plan differentiates between an event and a security incident, ensuring that appropriate actions are taken based on the severity and potential impact. An event is any observable occurrent in a system or network. Events include a user sending an email or a **firewall** blocking a connection attempt. A security incident is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system.

The CSIR Plan outlines Shared Health's 7-stage process for managing cybersecurity incidents. This is illustrated in **FIGURE 1**.

Figure 1: Cybersecurity Incident Response process at Shared Health

A **Managed Security Service Provider** is a technology firm that provides cybersecurity services to companies and organizations.

Source: Canadian Centre for Cybersecurity

A **Security Operations Centre (or SOC)** is a team of cybersecurity professionals dedicated to monitoring an organization's IT infrastructure 24/7. The team is responsible for detecting, analyzing, and responding to security incidents in real time.

The CSIR Plan is activated when an event has been classified as high or critical priority cybersecurity incident. Initial event classification occurs during Shared Health's general incident management process, where all events are recorded in Shared Health's IT Service Management (ITSM) tool. These events are recorded by the Service Desk and may originate from Shared Health users or its **Managed Security Service Provider** (MSSP). The MSSP operates as **Security Operations Centre** (SOC), responsible for monitoring and protecting Shared Health's security devices and systems.

The Service Desk assigns the event to the appropriate support group for further investigation and diagnosis. The CSIR Plan provides security incident classification according to risk, which are as follows:

Critical

- Cybersecurity incident, such as a ransomware attack, that disrupts health-care services to a degree that prevents access to care (for example, cancellation of cancer treatments, routing patients to other jurisdictions, etc.) or health-care services OR in another manner that has a significant negative impact on patient outcomes.
- Cybersecurity incidents that impact health-care services on a provincial level.
- Unauthorized access to data or data exfiltration that could result in significant harm to an individual, members of the public, or health-care employees (for example, financial information).
- Unauthorized access to data or data exfiltration on a large scale (for example, systems with a million-plus unique patient records).
- Threat actors have compromised the environment to the degree where extreme measures (for example, take a data center offline, network isolation of a Service Delivery Organization, shutting down critical IT systems/service, etc.) are required to contain, eradicate, recover, and resolve the incident.

High

- Cybersecurity incident disrupts health-care services to a degree that puts pressure on the health-care system by significantly impairing workflows for an extended period of time and/or delaying access to care (for example, cancellation of cancer treatments, routing patients to other jurisdictions, etc.) or health-care services OR in other manners that will have a negative impact on patient outcomes.
- Cybersecurity incidents that impact health-care services that are regional or site specific.
- Unauthorized access to data or data exfiltration could result in a publicly reported data breach that will likely not result in significant harm to an individual or members of the public.
- Threat actors have compromised the environment to the degree where measures are required to contain, remediate, and resolve. The incident requires taking non-critical systems or low impact network segments offline.

Medium

- Cybersecurity incident does not disrupt health-care services.
- Unauthorized access to data limited to user credentials (for example, through phishing) or other non-sensitive information.
- Event is contained, remediated, and resolved within the expected operating parameters of existing controls but suggestion that a threat actor or malware had infiltrated the environment.

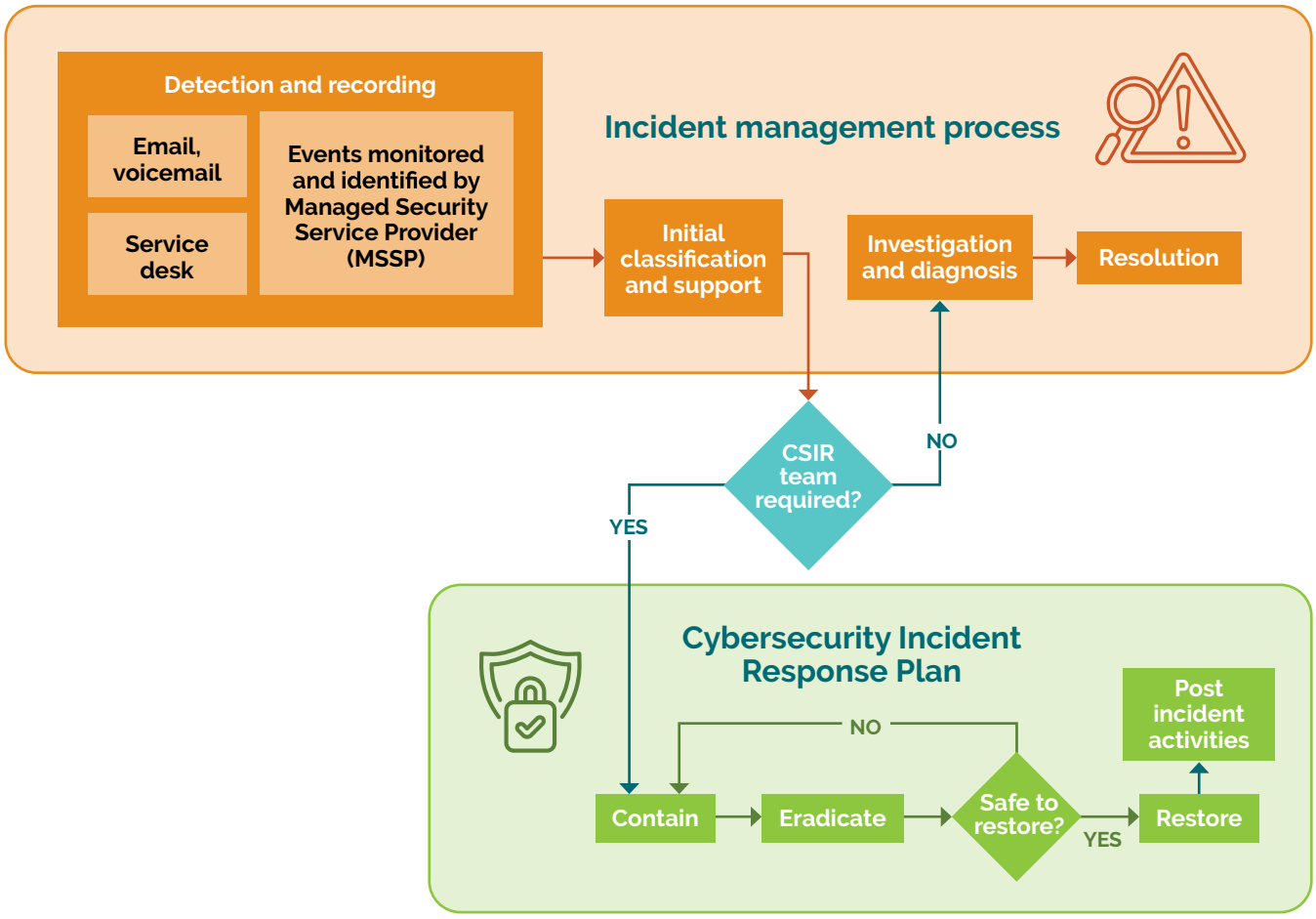
Low

- Incidents classified as low have no impact on access to care, patient outcomes, health-care services, organizational operations, organizational assets, or individuals. Event is contained, remediated, and resolved within the expected operating parameters of existing controls or standard operating procedures.

Source: Shared Health's Cybersecurity Incident Response Plan

When an event is classified as a high or critical priority cybersecurity incident, the CSIR Plan is activated and the CSIR team takes over the incident management process for resolution. The relationship between the 2 processes is depicted in **FIGURE 2**:

Figure 2: Relationship between cybersecurity incident response and incident management processes at Shared Health



The composition and responsibilities of the CSIR team are also defined in the CSIR Plan. The CSIR team is a cross-functional team that responds to cybersecurity incidents when they occur and are responsible for executing the incident response plan. The team not only includes technical people who will respond to the incident but also those who make business or legal decisions related to the incident. Further, the CSIR Plan references the Incident Management Guide to describe how meetings and communications will be conducted for cybersecurity incident response activities.

The Plan does not apply to adverse events caused by natural disasters. It is only applicable to information security-related events such as:

- **Denial of service** (DoS).
- Loss of sensitive information including Personal Health Information (PHI) and/or Personally Identifiable Information (PII).
- Suspicious computer or network activities, including email or **phishing** scams, **malicious code,** and **ransomware**.
- Unauthorized access to any Shared Health managed data or system including improper or inappropriate use of systems or network resources.

Denial of service is a cyberattack that directs a large volume of malicious Internet traffic at a target, often a website or any Internet-connected service, aiming to overwhelm and disable it.
Source: Canadian Centre for Cybersecurity

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain.
Source: Canadian Centre for Cybersecurity

Malicious code is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
Source: NIST Special Publication 1800-10B

Ransomware is a type of malware (malicious software) that denies a user's access to files or systems until a sum of money is paid.
Source: Canadian Centre for Cybersecurity

This page is intentionally left blank.

Objective, scope and approach, and audit criteria

Objective

To determine whether Shared Health has a process to promptly respond to cybersecurity incidents and minimize the impact to health operations and loss of data.

Scope and approach

The audit included the inspection of documents, procedures, standards, reports, and other documentation relevant to the process implemented by Shared Health to manage cybersecurity incidents of Manitoba's provincial health care system. We interviewed key process owners and stakeholders within Shared Health's Digital Shared Services to understand the processes and activities in place to manage and respond to cybersecurity incidents.

Audit criteria

To determine whether Shared Health has a process to promptly respond to cybersecurity incidents and minimize the impact on health operations and loss of data, we used the following criteria:

Criteria	Sources
Criteria 1: Incident response policy, plans, and procedures should be developed to detect, analyze, prioritize, contain, mitigate, and recover from cybersecurity incidents.	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61r2: Computer Security Incident Handling Guide
Criteria 2: Exercises are performed to test security incident response plans and to provide staff training on their responsibilities for security incident management.	
Criteria 3: Security incidents are managed according to incident response policy, plans, and procedures.	

This page is intentionally left blank.

Shared Health has a process to promptly respond to cybersecurity incidents, but regular testing and training can be improved

Reliable and accessible provincial health information systems are essential for delivering health-care services that directly impact people's lives. However, these systems are highly vulnerable to cyberattacks—including ransomware and data theft—due to the wealth of sensitive personal and health-related information they store. Attackers know that any disruption could jeopardize patient care, and health-care organizations may feel compelled to pay the cybercriminals to ensure the continued delivery of life-saving services and prevent the sale or exposure of sensitive information.

Financial incentives aside, an inadequate cybersecurity incident response process and poorly designed controls can leave organizations unable to effectively manage and recover from security incidents. This can result in prolonged downtime, affecting multiple systems and leading to severe consequences such as the inability to deliver critical medical services, exposure of personal health information, forced reliance on manual processes, and significant reputational damage.

In this audit, we found Shared Health has processes in place to promptly respond to cybersecurity incidents and minimize the impact to health operations and loss of data. However, there is room for improvement, especially around regular testing and training.

We based this conclusion on the following findings:

- The Cybersecurity Incident Response (CSIR) Standard and Plan are in place, but they lack comprehensive training, and some supporting practices to respond to cybersecurity incidents are not yet documented. (**SECTION 1**)
- Exercises to test the cybersecurity incident response plan have not been conducted. (**SECTION 2**)
- Processes are in place to activate the CSIR Plan when needed. (**SECTION 3**)

1 Cybersecurity Incident Response Plan in place, but better training required, and some supporting practices need to be documented

The Cybersecurity Incident Response (CSIR) Security Standard at Shared Health requires a cybersecurity incident response plan that is documented, communicated, and approved. In February 2024, Shared Health approved its CSIR Plan which details the process for responding to and managing cybersecurity incidents. It was prepared by the cybersecurity team at Digital Shared Services and defines cybersecurity incidents.

Cybersecurity incidents are handled based on their classification. Low- and medium-priority incidents are managed by the internal cybersecurity team, while high- and critical-priority incidents are addressed by the CSIR team. The CSIR team is a cross-functional team within Shared Health that is responsible for executing the CSIR Plan when cybersecurity incidents occur. Some of the members of this team are:

- Senior leadership (such as Chief Operating Officer and executives from Digital Shared Services and Service Delivery Organizations)
- Chief Information Security Officer
- Digital Shared Services management
- Information Security
- Technical subject matter experts (such as application and server support)
- Human resources
- Legal

Shared Health also leverages external resources when responding to cybersecurity incidents, including a Managed Security Service Provider (MSSP), which offers security event detection and analysis. In addition, Shared Health's cybersecurity insurance policy also provides access to further resources, such as breach coaches, digital forensics experts, and legal counsel, ensuring comprehensive support in the event of a cybersecurity incident.

The CSIR Standard also requires Shared Health to record cybersecurity incidents throughout their lifecycle. To comply with this requirement, Shared Health uses an IT Service Management (ITSM) tool. The ITSM tool documents key details such as ticket numbers, contact information, incident descriptions, prioritization, actions taken, and resolution details.

We found Shared Health has made progress in developing and documenting its Cybersecurity Incident Response (CSIR) Plan. However, the following are still in progress or not yet implemented:

- The responsibilities of the CSIR team were not communicated to the entire response team.
- The external communication plan and Executive Ransomware and Extortion Playbook were still in progress.
- The evidence retention policy was not defined.

1.1 Cybersecurity Incident Response Plan responsibilities not communicated to entire response team

Shared Health has a Cybersecurity Incident Response Standard, which sets baseline security requirements, standards, and specifications to ensure an effective response to information security incidents. This standard also defines critical administrative and technical control requirements for detecting, responding to, and managing cybersecurity incidents.

A requirement of this standard is the documentation, communication, and approval of a Cybersecurity Incident Response (CSIR) Plan. Although a documented CSIR Plan was approved in February 2024, only select members of the Cybersecurity Incident Response (CSIR) team, who were also part of the leadership team, were informed of their responsibilities. No dedicated sessions—either via training or plan testing—were conducted to thoroughly review the CSIR Plan with the entire CSIR team. As a result, unique roles and specific expectations that differ from the more widely known Incident Management Guide were not shared.

Without formally communicating existing plans and procedures to the CSIR team and providing members with necessary training on their roles and responsibilities, there could be delays in responding to cybersecurity incidents at Shared Health.

Recommendation 1

We recommend Shared Health implement training programs to ensure Cybersecurity Incident Response team members are fully aware of their specific roles and responsibilities outlined in the Cybersecurity Incident Response Plan.

1.2 Some supporting practices for cybersecurity incident response still being documented

Shared Health's Cybersecurity Incident Response (CSIR) Standard requires that the CSIR Plan includes communication considerations, particularly for high and critical-priority incidents where security controls have been bypassed or failed. Currently, the Incident Management Guide provides internal communication protocols and processes for managing these incidents. We found an external communication plan was still under development. Once completed, this external communication plan will outline how to communicate with external stakeholders, such as customers, vendors, law enforcement and the media, during and after a cybersecurity incident.

The CSIR Standard also requires the CSIR Plan be supported by runbooks, providing guidelines for high-risk events such as ransomware and denial of service attacks. Many of these runbooks were in place. In addition, we observed that playbooks have also been prepared. Runbooks and playbooks provide structured, documented instructions to guide teams in responding to incidents, ensuring

consistency and efficiency in execution. However, the Executive Ransomware and Extortion Playbook was still being developed. An Executive Ransomware and Extortion Playbook is essential because it is intended for senior leadership and executives, such as CEOs, CFOs, and legal teams. While a Ransomware playbook is already in place, it focuses more on technical guidance and is geared for information security and incident response teams. In contrast, a separate Executive Ransomware and Extortion playbook would equip Shared Health's leadership with the information needed to handle these disruptive extortion cases and help them prepare to make decisions in such high-pressure situations.

While Shared Health has some mitigating measures in place, including the Incident Management Guide, existing runbooks, and breach coaches available through their cybersecurity insurance policy, the absence of a fully developed external communication plan and the incomplete Executive Ransomware and Extortion Playbook pose risks to the organization's ability to respond effectively to high and critical-priority incidents. Without a dedicated external communication plan, there is a risk of delays, miscommunication, and inadequate stakeholder engagement during cybersecurity incidents, which could impede response efforts and result in reputational consequences. Additionally, relying solely on the Ransomware playbook can leave Shared Health vulnerable to strategic, reputational, and financial risks that a purely technical response would not be able to address. Having a separate Executive Ransomware and Extortion playbook ensures that leadership is prepared to make informed decisions while maintaining operational continuity and stakeholder confidence.

Recommendation 2

We recommend Shared Health finalize the Cybersecurity Incident Response external communication plan and the Executive Ransomware and Extortion Playbook. Once completed, these documents should be reviewed with relevant stakeholders.

1.3 Evidence retention policy not defined

According to the National Institute of Standards and Technology (NIST) Special Publication 800-61r2, *Computer Security Incident Handling Guide*, it is important that all facts regarding an incident be immediately recorded. Shared Health uses its IT Service Management (ITSM) tool to document critical incident details including ticket number, contact details of the person reporting the incident, incident description, prioritization, actions taken, and resolution details.

The same NIST standard also requires organizations to establish policies for how long evidence from an incident should be retained. We found that existing Cybersecurity Incident Response (CSIR) documents at Shared Health, including the CSIR Standard, CSIR Plan, and Incident Management Guide, did not include specific requirements for data and evidence retention related to cybersecurity incidents.

Without clearly defined data and evidence retention requirements for cybersecurity incidents, Shared Health may face challenges in preserving critical information needed for forensic analysis,

legal proceedings, or regulatory compliance. This lack of guidance could result in the loss or mishandling of important incident-related data, potentially hindering investigations, weakening the organization's ability to respond to future incidents, and exposing Shared Health to legal and regulatory risks.

Recommendation 3

We recommend Shared Health establish a data and evidence retention policy for cybersecurity incidents. This policy should define the retention period, considering legal requirements, potential for prosecution, and organizational needs.

2 Exercises not performed to test Cybersecurity Incident Response Plan

Maintaining readiness for cybersecurity incidents requires not just having a response plan, but also ensuring it is tested regularly. Testing different types of cybersecurity incidents—using a variety of testing methods such as tabletop and functional tests—validates the effectiveness of incident response procedures and prepares teams for real-world scenarios.

Shared Health's Cybersecurity Incident Response (CSIR) Standard mandates that security incident response plans be reviewed and/or tested annually with a tabletop exercise. We found Shared Health had not conducted a review or tabletop exercise of the CSIR Plan during the audit period.

2.1 Cybersecurity Incident Response Plan not tested

According to the National Institute of Standards and Technology (NIST) Special Publication 800-84, *Guide to Test, Training and Exercise Programs for IT Plans and Capabilities*, although it is important to have plans in place to help organizations respond to and manage various situations involving information technology (IT), it is equally important to maintain these plans in a state of readiness. Therefore, it is important to test the readiness of the CSIR Plan. This can be done by having the CSIR Plan tested to validate procedures can be carried out efficiently and effectively.

Testing can be conducted through:

- Tabletop test: This is a discussion-based test where participants review and discuss their roles and responses to a hypothetical cybersecurity scenario. IT assets such as hardware or system logs are not used. This test helps organizations initiate discussion of roles, responsibilities, coordination, and decision-making among participants.
- Functional test: This test involves simulating a real cybersecurity scenario, allowing participants to execute their response roles using procedures and IT assets as they would in an actual cybersecurity incident.

Both types of exercises are crucial for ensuring that response plans are practical, comprehensive, and ready to address real-world cybersecurity challenges.

We found that the Cybersecurity Incident Response (CSIR) Standard requires Shared Health to review and/or test the CSIR Plan annually with a tabletop exercise. There is no requirement to do functional test of the CSIR Plan. We further found that Shared Health had not conducted any tests for any incident scenarios including ransomware, data theft, or denial of service attacks.

Since no tests were performed, the effectiveness of the CSIR Plan cannot be evaluated to ensure that Shared Health is prepared to promptly respond to a major cybersecurity event.

Recommendation 4

We recommend Shared Health conduct annual tests of the Cybersecurity Incident Response Plan. A testing strategy should be developed to include various test methods and incident types to strengthen response capabilities.

3 Processes in place to activate the Cybersecurity Incident Response Plan when needed

We evaluated how Shared Health manages cybersecurity incident response, recognizing that only high and critical incidents are managed under the Cybersecurity Incident Response (CSIR) Plan.

We observed that the broader incident management process covers detection, recording, and classification of all security events. The classification is critical in determining whether an incident will be managed by the CSIR Plan and CSIR team. Between April 2022 and April 2024, no high or critical cybersecurity incidents were reported.

Since no high or critical incidents occurred during the audit period, we assessed the practices and controls for detecting, recording, and classifying medium and low priority security events using the incident management process. All events go through this process with their risk classification determining whether they escalate to a high or critical priority cybersecurity incident requiring Cybersecurity Incident Response team involvement. We found that incident management and cybersecurity response processes are aligned. Shared Health's cybersecurity response phases like detection and analysis are integrated into Shared Health's incident management process, providing a clear approach to classifying and managing incidents, minimizing potential risks to Manitoba's health-care system and facilitating timely service restoration.

Additional information about the audit

This independent assurance report was prepared by the Office of the Auditor General of Manitoba (the Office) on Shared Health's process of responding to and managing cybersecurity incidents. Our responsibility was to provide objective information, advice, and assurance to assist the Legislature in its scrutiny of the government's management of resources and programs, and to conclude on whether Shared Health complies in all significant respects with the applicable criteria.

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements set out by the Chartered Professional Accountants of Canada (CPA Canada) in the CPA Canada Handbook—Assurance.

The Office applies Canadian Standard on Quality Management 1, which requires the Office to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the Code of Professional Conduct of the Chartered Professional Accountants of Manitoba, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

In accordance with our regular audit process, we obtained the following from management:

- Confirmation of management's responsibility for the subject under audit.
- Acknowledgement of the suitability of the criteria used in the audit.
- Confirmation that all known information that has been requested, or that could affect the findings or audit conclusion, has been provided.

Period covered by the audit

The audit covered the period between April 2022 and March 2024. This is the period to which the audit conclusion applies.

Date of the audit report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on November 29, 2024, in Winnipeg, Manitoba.

This page is intentionally left blank.

Summary of recommendations and responses from officials

Recommendation 1

We recommend Shared Health implement training programs to ensure Cybersecurity Incident Response team members are fully aware of their specific roles and responsibilities outlined in the Cybersecurity Incident Response Plan.

Response of officials:

Shared Health agrees with the opportunity to improve our current practices identified in the Recommendation. In response to this Recommendation, we are currently:

- Reviewing this version of the Cybersecurity Incident Response (CSIR) Plan with key members of the CSIR team to ensure they are aware of the plan, and that they are clear on their roles and responsibilities.
- Working with our Corporate Training Solutions (CTS) team to build a CSIR Plan training course to be published on our online learning management system (LMS) for ongoing training.

With regards to concerns that unique roles and specific expectations differ from the more widely known Incident Management Guide, we have addressed these concerns through the development of our Cybersecurity Incident Response external communication plan and the Executive Ransomware and Extortion Playbook as identified in Recommendation 2.

Recommendation 2

We recommend Shared Health finalize the Cybersecurity Incident Response external communication plan and the Executive Ransomware and Extortion Playbook. Once completed, these documents should be reviewed with relevant stakeholders.

Response of officials:

Shared Health agrees with the Recommendation and both documents associated with this Finding have been finalized. Key stakeholders were engaged throughout the development of the external communications plan and ransomware playbook.

While the external communications plan and ransomware playbook will assist with our planning and preparation activities, we believe our strategy of engaging a breach coach service available through our cyberinsurance as part of our incident response efforts remains a reasonable mitigation to all risks associated with this Finding.

Recommendation 3

We recommend Shared Health establish a data and evidence retention policy for cybersecurity incidents. This policy should define the retention period, considering legal requirements, potential for prosecution, and organizational needs.

Response of officials:

Digital Shared Services agrees with the opportunity to improve our practices identified in the Recommendation and has updated our cybersecurity incident response standard with retention requirements to align with the Limitations Act.

Recommendation 4

We recommend Shared Health conduct annual tests of the Cybersecurity Incident Response Plan. A testing strategy should be developed to include various test methods and incident types to strengthen response capabilities.

Response of officials:

Digital Shared Services agrees with the opportunity to improve our practices identified in the Recommendation and we plan to develop a strategy for reviewing and testing our incident response plan as well as supporting documentation. Upon completion of the strategy, we will establish a regular schedule of activities (e.g., walkthroughs and tabletop exercises) to test the Cybersecurity Incident Response Plan.

Vision
Government accountability and public administration excellence for Manitobans.

Mission
To provide independent information, advice and assurance on government operations and the management of public funds.

Values
Independence – We are independent from government and our work is objective and unbiased.
Integrity – We act with honesty and uphold high ethical standards.
Innovation – We promote innovation and creativity in what we do and how we do it.
Teamwork – We work as a team by sharing each other's knowledge and skills to reach our goals.

Auditor General
Tyson Shtykalo, FCPA, FCA

Assistant Auditor General
Wade Bo-Maguire

Principal, IT Audit
Ian Montefrio

Manager, IT Audit
Arlene Nebrida

Senior IT Auditor
Tony Chu

Manager, Data Analysis
Gabriel Nazario

Communications Manager
Frank Landry

Admin Support
Tara MacKay
Alex Dela Cruz
Ivanna Romero

Graphic Design
Waterloo Design House

The Office of the Auditor General of Manitoba acknowledges with respect that we conduct our work on the ancestral lands of Anishinaabeg, Anishininewuk, Dakota Oyate, Denesuline, and Nehethowuk Nations, and on the National Homeland of the Red River Métis. We respect the Treaties that were made on these territories, we acknowledge the harms and mistakes of the past, and we dedicate ourselves to move forward in partnership with Indigenous communities in a spirit of reconciliation and collaboration.

WEBSITE VERSION

Auditor General
MANITOBA

For more information, please contact our office at:

Office of the Auditor General
500-330 Portage Avenue
Winnipeg, Manitoba R3C 0C4
Phone: 204-945-3790
contact@oag.mb.ca | www.oag.mb.ca

@AuditorGenMB
@AuditorGenMB
@AuditorGenMB
company/manitoba-auditor-general