Chapter 13
eHealth Saskatchewan—Maintaining Key Healthcare IT Servers

1.0 Main Points

eHealth Saskatchewan manages the health sector IT network including more than 5,000 servers and over 1,000 applications, with a significant amount of private and confidential data. These IT systems are essential to the timely management and delivery of health services by the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and 3sHealth.

Outdated IT infrastructure and software provide an opportunity for online attackers to breach IT networks and compromise data. Cyberattacks can take an IT system or entire organization offline, leading to patient care interruptions, privacy breaches, and expensive recovery costs.

We found eHealth had, for the period ending July 31, 2023, effective processes to maintain IT servers that host key healthcare systems and data to protect against known vulnerabilities other than the areas of our six recommendations. eHealth needs to:

- ➢ Track which IT systems are on what IT servers, along with their criticality rating, to support prioritization of server updates. Appropriate prioritization helps to quickly protect critical IT systems from known vulnerabilities.

- ➢ Detect and remove unauthorized IT servers, if any, on the network. Such servers increase the risk of unauthorized access or changes to sensitive health IT systems and data.

- ➢ Implement security measures for unsupported servers, which no longer receive regular updates from vendors for new security vulnerabilities (20 out of 341 servers we tested). Additional security layers (e.g., server isolation, increased intrusion monitoring) can help reduce risk for IT systems on unsupported servers and other connected servers, until the unsupported server is replaced.

- ➢ Periodically review users' privileged access to IT servers to ensure such access is only granted to appropriate users. Privileged accounts can bypass many security controls built into IT systems for other user accounts, so pose a greater security risk.

- ➢ Analyze security information to identify, mitigate, and report significant IT server maintenance risks to senior management and partners (e.g., Saskatchewan Health Authority).

Without proper maintenance of IT servers, there is increased risk of system failures and security breaches that negatively impact health service delivery (e.g., lab services, filling prescriptions) and public confidence in security of key healthcare systems and data. The availability and integrity of these systems is integral to healthcare providers making medical decisions for their patients.

2.0 Introduction

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 the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and 3sHealth.

eHealth provides IT equipment and support for over 430 healthcare facilities and more than 75,000 healthcare users across the province.[1] Since January 2017, eHealth has been working with others in the provincial healthcare system to consolidate IT services provided by the Saskatchewan Health Authority, Saskatchewan Cancer Agency, and 3sHealth into a single service provided by eHealth.

eHealth has over 750 full-time equivalent positions, including more than 360 positions in its technology area whose responsibilities include IT server maintenance. In 2022–23, eHealth spent $2.3 million (2021–22: $3.1 million) on hardware maintenance and $52.8 million (2021–22: $44.3 million) on software maintenance.[2]

We audited eHealth's processes to maintain IT servers that host key healthcare systems and data to protect against known vulnerabilities. Our audit focused on those servers hosting the Electronic Health Record (eHR) Viewer, as well as provincial lab, drug, medical imaging, and hospital clinical systems.[3]

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

2.1 eHealth's Management of Key Healthcare IT Systems

The use of IT in healthcare provides numerous benefits, such as more accurate information, customized patient care, improved communication between healthcare providers, and enhanced medication management.

eHealth is responsible for managing an IT network that supports more than 5,000 servers and over 1,000 applications.[4] eHealth has had some servers in place since about 2008 (i.e., in use for about 15 years).[5] The network, servers, and applications house critical IT health systems and data essential to the timely management and delivery of health services along with a significant amount of private and confidential data.

eHealth manages the Electronic Health Record (eHR) Viewer, used by authorized care providers to view a patient's provincial health record. The eHR Viewer accesses patient information from separate servers (for a variety of health-related IT systems) regardless of where a patient presents for care. The eHR Viewer IT systems include patient information such as:

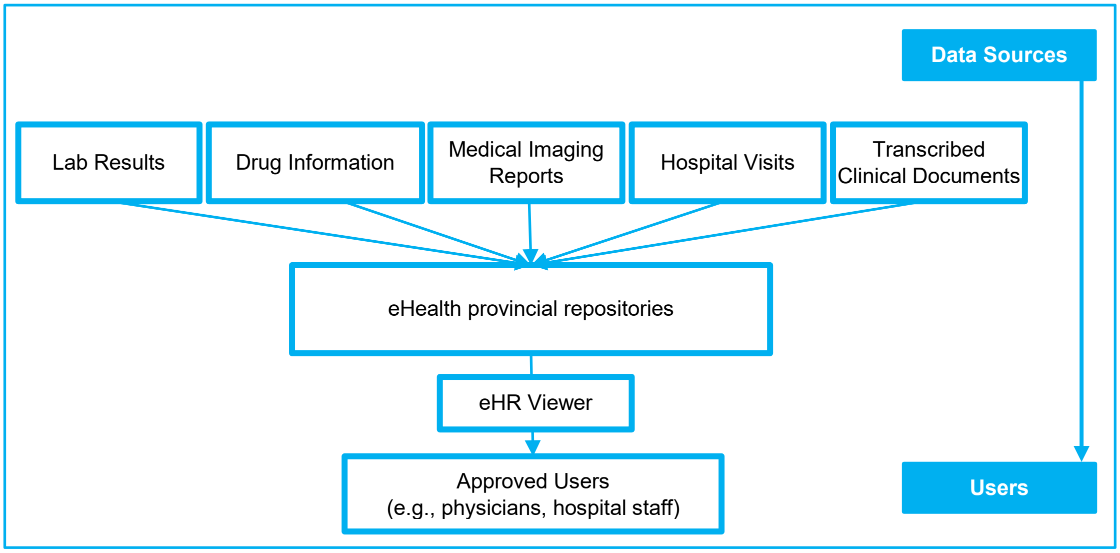
- Laboratory results

[1] eHealth Saskatchewan, *Annual Report 2022–23*, p. 3.
[2] Ibid., p. 29.
[3] The eHR Viewer is a secure, web-based portal providing real-time access to digital health records healthcare providers use to support patient care. Source: eHealth Saskatchewan Service Definition Sheet – Electronic Health Record (eHR) Viewer.
[4] eHealth Saskatchewan, *Annual Report 2022–23*, p. 9.
[5] eHealth server listings.

- Drug information
- Medical imaging reports
- Hospital visits
- Transcribed clinical documents

Figure 1 provides a simplified overview of electronic health record data paths.

Figure 1—Simplified Electronic Health Record Data Sources and Users (Data Paths)*


Data Sources
Lab Results
Drug Information
Medical Imaging Reports
Hospital Visits
Transcribed Clinical Documents
eHealth provincial repositories
eHR Viewer
Approved Users (e.g., physicians, hospital staff)
Users

Source: Adapted from information provided by eHealth Saskatchewan.
* A data path is the electronic flow of information between various sources and users.

2.2 Importance of IT Server Maintenance

Outdated IT infrastructure and software provide an opportunity for online attackers to breach an IT network. Well-managed preventative IT maintenance can help to reduce this risk.[6]

Aging IT infrastructure and software poses serious risks to an organization including, but not limited to:

- Frequent network outages resulting in performance issues (e.g., IT system not available to healthcare providers)
- Data corruption and loss
- Cyberattacks
- Considerably higher costs of repairing and maintaining outdated technology as older technology tends to break down frequently[7]

[6] Why Aging Infrastructure Is a Growing Problem. blogs.cisco.com/security/why-aging-infrastructure-is-a-growing-problem (5 September 2023).
[7] Nye Technical Services, LLC, 2019, *An aging IT infrastructure and the risks it poses to SMBs.*

In October 2021, a cyberattack on Newfoundland and Labrador's Eastern Health network paralyzed their provincial healthcare system, leading to patient care interruptions (e.g., delayed surgeries and medical procedures), privacy concerns, and expensive recovery costs (approaching almost $16 million). Significant deficiencies with IT system maintenance may have increased Eastern Health's network vulnerability. For example, reports state a number of potential issues related to outdated technology contributed to its vulnerability including an inadequate database for asset information and antiquated components in some IT systems in need of upgrade or decommissioning that Eastern Health could not appropriately manage or patch.[8]

Attackers exploit vulnerabilities within servers to breach networks and compromise data, which may take an entire organization offline. IT maintenance ensures that IT systems remain operational and secure to help prevent such breaches. IT maintenance includes:

- Installing regular manufacturer-issued updates to fix security issues and bugs
- Removing unwanted or unused IT systems
- Upgrading or replacing IT system components (e.g., servers)[9,10]

Also, knowing what IT assets you have, where they are, and who is responsible for them, can help to effectively protect and manage IT servers.[11,12]

Without proper maintenance of IT servers, organizations may be at risk of system failures and security breaches. This can lead to unavailable servers, data loss, or compromised personal health information—negatively impacting health service delivery (e.g., lab services, filling prescriptions) and affecting the organization's reputation.

3.0 Audit Conclusion

We concluded, for the period ended July 31, 2023, eHealth Saskatchewan had effective processes, except in the following areas, to maintain IT servers that host key healthcare systems and data to protect against known vulnerabilities. In relation to key healthcare IT servers, eHealth needs to:

- **Track which IT systems are on what IT servers, along with their criticality rating**
- **Detect and remove any unauthorized IT servers on the network**
- **Implement security measures for unsupported servers**
- **Periodically review users' privileged access to IT servers**

[8] P-2023-001/PH-2023-002, May 23, 2023, privacy incident report of the Office of the Information and Privacy Commissioner of Newfoundland and Labrador. www.oipc.nl.ca/pdfs/P-2023-001-PH-2023-002.pdf (15 September 2023).

[9] IT Maintenance: Taking the right approach for maintaining your IT Systems. www.businesstechweekly.com/operational-efficiency/outsourcing-and-supplier-management/it-maintenance/ (5 September 2023).

[10] Why Aging Infrastructure Is a Growing Problem. blogs.cisco.com/security/why-aging-infrastructure-is-a-growing-problem (5 September 2023).

[11] CIS Critical Security Control 1: Inventory and Control of Enterprise Assets. www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets (5 September 2023).

[12] CIS Critical Security Control 2: Inventory and Control of Software Assets. www.cisecurity.org/controls/inventory-and-control-of-software-assets (5 September 2023).

- **Analyze security information to report significant IT server maintenance risks and mitigation plans to senior management and partners (e.g., Saskatchewan Health Authority)**

Figure 2—Audit Objective, Criteria, and Approach

Audit Objective:

The objective of this audit was to assess whether eHealth Saskatchewan had effective processes, for the period ended July 31, 2023, to maintain IT servers that host key healthcare systems and data to protect against known vulnerabilities.

For the purposes of this audit, IT servers include the related operating systems that support communication with critical healthcare systems and data. Our audit focused on servers hosting key healthcare systems and data including the Electronic Health Record (eHR) Viewer, as well as provincial lab, drug, medical imaging, and hospital clinical systems (over 300 out of 5,000 servers).

Audit Criteria:

Processes to:

1. **Keep reliable information about IT servers**
   - Track IT servers
   - Maintain sufficient information about IT servers (e.g., operating system version, business criticality)
2. **Regularly update IT servers**
   - Use risk-informed plans for upgrading and updating (patching) IT servers
   - Define roles and responsibilities (including for suppliers and partners) for IT server maintenance activities
   - Complete scheduled upgrades and updates to IT servers
   - Implement alternate security controls (e.g., system isolation) if upgrades or updates cannot be completed
3. **Monitor IT server maintenance**
   - Verify upgrades and updates to IT servers are completed as expected
   - Analyze effectiveness of maintenance processes by examining incident trends (e.g., server downtime)
   - Periodically report on server maintenance to senior management and partners

Audit Approach:

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

We examined eHealth's policies, procedures, and reports relating to maintaining IT servers to protect against known vulnerabilities. We interviewed key staff responsible for IT server maintenance. We hired an external consultant to analyze the timeliness of updates applied to IT servers and to help assess eHealth's processes against good practice.

4.0 Key Findings and Recommendations

4.1 Accurate Tracking of IT Systems Hosted on IT Servers Needed

eHealth Saskatchewan tracked some key information about its IT servers, but did not accurately track IT systems hosted on the servers or their related criticality (including data classification). In addition, eHealth did not have a way to identify all new servers connected to the network.

Although eHealth does not have written policies and guidance for tracking information about its IT servers, we found it manually tracked physical servers it manages using spreadsheets and asset tags. eHealth kept information about virtual servers using an electronic server management system. Information tracked included:

- Server name and logical location (i.e., IP address)
- Information about the physical server running the virtual server (e.g., server name, physical location, asset tag, IP address, vendor)
- Operating system and version

The information tracked in the server management system did not include details about the applications or databases hosted by the server, or how critical these systems and their data are for delivering health services. Instead, eHealth used network diagrams of IT systems (i.e., applications and databases) that show server names and network locations to trace to information in the server management system.

During our server testing, we found eHealth's network diagrams were not up-to-date (e.g., referred to incorrect or replaced servers)—making it difficult to determine specific servers related to each key healthcare IT system and the related criticality. Without this information, eHealth cannot efficiently consider IT system criticality to help prioritize when it applies updates to each server. eHealth updated its diagrams during the audit to clarify the specific servers related to the Electronic Health Record (eHR) Viewer, as well as provincial lab, drug, medical imaging, and hospital clinical systems. After updating, it determined a total of 341 servers related to these IT systems.

We also found eHealth did not have a way, such as an automatic discovery system, to alert its staff when new servers connect to the network. These discovery systems help to quickly identify and remove any unauthorized (rogue) servers that can introduce vulnerabilities. A rogue server is simply a server, created through employee error or by an attacker, of which network staff are not aware. A rogue server can not only be a target for attackers, but also can create performance issues such as slowing down a network. As explained in **Section 4.3**, multiple layers of security (e.g., firewalls) can exist around servers to reduce the risk of a rogue server connecting to a network, although they cannot eliminate this risk.

Exploited vulnerabilities through an unauthorized server can lead to unauthorized access or changes to sensitive health systems and data. Unauthorized changes to healthcare data could impact medical decisions, potentially resulting in harm to patients. In addition, patients may be at risk of identity theft from any compromised personal health data.

1. **We recommend eHealth Saskatchewan regularly detect and quickly remove unauthorized IT servers, if any, on the network.**

By March 31, 2024, eHealth plans to implement an asset management system to track information about servers, including hosted IT systems, and to automatically identify any unauthorized servers connected to the network.

Without sufficient tracking of IT systems hosted on key healthcare IT servers, and their related criticality, eHealth may not appropriately prioritize updates to efficiently maintain all servers to protect them from known vulnerabilities. For example, eHealth can use this information to prioritize updates for critical IT systems.

2. **We recommend eHealth Saskatchewan track the IT systems, and their criticality, hosted on key healthcare IT servers to support maintenance decisions.**

4.2 Supported IT Servers Regularly Updated

eHealth Saskatchewan updated its supported IT servers, where vendors provided periodic security updates, on a regular basis.

eHealth receives notifications from server operating system vendors (e.g., Microsoft) about server security updates (i.e., patches), indicating the related risks of vulnerabilities addressed in the updates. Some vendors release updates more frequently than others (e.g., Microsoft monthly, some other vendors semi-annually). Vendors rate vulnerabilities from critical to low risk, depending on how much harm they may cause if exploited and how easy (i.e., likelihood) they are to exploit. Vendors may recommend immediate updates on an emergency basis for a critical vulnerability being actively exploited around the world.

Verifying (e.g., checking reliable websites for further details) and testing updates before applying them to servers helps ensure they are legitimate and are not expected to create operational issues.

We found eHealth documented its processes for updating IT servers, which involves applying all relevant security patches to all servers.

eHealth expects staff to test and apply all emergency updates (e.g., to address vulnerabilities attackers are known to be actively exploiting) as soon as reasonably possible (e.g., within 48 hours), following an emergency change process.[13] For two emergency changes tested, we found eHealth tested and applied both changes timely (i.e., within 24 hours).

eHealth tests and applies all non-emergency updates to groups of servers based on a schedule. eHealth did not use vulnerability risk-ratings (e.g., high to low) to determine when to apply these updates to each server group. eHealth management did not think the additional time to apply all non-emergency updates to servers each update cycle created significant delays in addressing high-risk vulnerabilities. We found eHealth's justification reasonable given it applies the non-emergency updates timely after release by a vendor (e.g., about a month after Microsoft releases patches).

A separate IT system tracks approvals and workflow tasks related to server updates. A change advisory committee reviews and approves all changes to servers before staff implement them. We found eHealth followed its processes to test and approve all 13 non-emergency server updates we tested.

Our analysis found over 90% of servers related to the key healthcare systems we tested received automatic updates, with the remaining requiring some manual intervention to complete the update.

[13] Emergency changes require less extensive testing and approvals before implementation. This approach results in faster server patching and helps mitigate risks introduced by the longer change management processes used for non-emergency changes.

eHealth contracted a service provider to host and manage the medical imaging IT system. As part of the contract, the service provider is responsible for identifying and applying updates for medical imaging IT servers using the same processes eHealth's staff follow (e.g., testing before applying updates, within the same timeframes). We reviewed the two monthly reports from the service provider and found the service provider updated medical imaging IT servers as expected.

As of July 2023, we found 97% of servers we tested that receive ongoing updates from vendors were up-to-date. We found about 3% of servers were missing the most recent non-emergency update, which eHealth expected to be applied in the next update cycle (i.e., within the next month or six months depending on what type of operating system the server was running). There may be circumstances (e.g., server is powered down) where servers are unavailable when eHealth rolls out updates. However, eHealth did not assess the risk of waiting until the next cycle to apply the updates to these severs. In **Section 4.1**, we describe that eHealth does not sufficiently track information about hosted IT systems, and their criticality, to support efficient maintenance decisions.

Timely updates of IT servers to protect against known vulnerabilities helps to reduce the risk of unauthorized access to or loss of availability of key healthcare IT systems and data.

4.3 Need to Manage Unsupported IT Server Risks

eHealth Saskatchewan does not have a plan to implement security measures for unsupported IT servers to protect key healthcare systems and data from new vulnerabilities that arise.

Of the 341 key healthcare IT servers we tested, we found 20 servers were running unsupported operating systems where vendors no longer supply updates for new vulnerabilities identified.

Servers may become unsupported when the hosted IT system is not able to run on newer, supported servers, and an agency is not ready or has not planned to replace a hosted IT system. Operating system vendors identify new vulnerabilities daily, so the longer servers are unsupported, the greater the risk an attacker may identify and exploit an unpatched vulnerability. Agencies should carefully evaluate risks of delaying IT system and related server upgrades (e.g., additional costs to address a successful cyberattack, significant server downtime, risks to the agency's reputation, compromised patient data).

Organizations can use multiple layers of security (i.e., defence-in-depth) around servers to reduce risk based on business criticality of the IT systems and the sensitivity of related healthcare data. **Figure 3** explains how organizations can use defence-in-depth to reduce risk. Since defence-in-depth cannot eliminate all risk, risk assessments are needed to support security decisions.

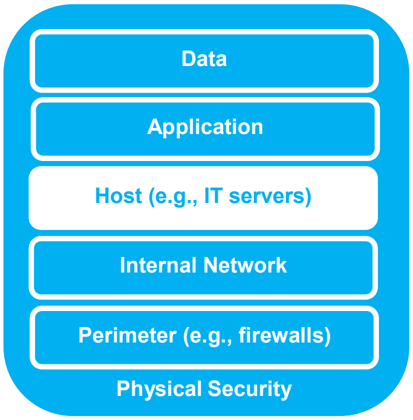
We found eHealth did not have a plan to address risks of unsupported servers timely. In one case, it planned a project in 2021 to upgrade unsupported servers and described related risks to its partners in the project plan. However, eHealth and its partner delayed the project with no clear timeline set for completion and did not add mitigating controls in the interim (e.g., additional intrusion monitoring, isolating unsupported servers on the network).

Risks associated with unsupported servers may be mitigated by additional security layers (e.g., server isolation) or performing IT system and related server upgrades (i.e., replacements).

Figure 3—Defence-in-Depth

This diagram illustrates the common layers where security may be implemented. The white box indicates the layer that includes IT servers. 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 that 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).

Without effective and timely plans to protect unsupported servers from new vulnerabilities, there is increased risk of unauthorized access or changes to, or downtime of, key healthcare systems and data. Healthcare providers rely on data in these systems to deliver time-sensitive health services.

3. **We recommend eHealth Saskatchewan implement security measures to address the risks introduced by having unsupported servers hosting key healthcare systems and data.**

4.4 Insufficient Monitoring of Privileged Access to IT Servers

eHealth Saskatchewan did not periodically (e.g., quarterly, annually) review all users granted privileged access to IT server administrative functions. We found users with privileged access to servers who no longer needed it.

Restricting privileged access to only those users who require access to conduct their jobs reduces the risk of unauthorized access or changes to sensitive IT systems and data hosted on the servers.

During our testing of 87 users with access to make changes to IT servers, we found one user who left eHealth in November 2022, but whose access eHealth had yet to remove at July 2023. We found eHealth used controls to prevent this user from logging into the privileged account after leaving eHealth. Additionally, we found nine users where eHealth was uncertain of the continued appropriateness of their level of access granted.

Without a process to periodically (e.g., quarterly) review privileged server access, there is increased risk of unauthorized individuals inappropriately accessing and making changes to sensitive healthcare systems and data. Privileged accounts pose a greater security risk, as these users can bypass security controls built into an IT system by accessing the system directly through the servers instead of logging into a user account in the IT system.

4. **We recommend eHealth Saskatchewan periodically review whether appropriate individuals have privileged access to key healthcare IT servers.**

4.5 Better Analysis Needed to Support Effective IT Server Maintenance

eHealth Saskatchewan did not scan all key healthcare IT servers for vulnerabilities and sufficiently analyze security information to support vulnerability remediation and process improvement.

eHealth used server vulnerability scans to identify missing security updates. When eHealth's scanning tool identifies potential vulnerabilities, it automatically creates security tickets in an IT system which then notifies eHealth staff for further investigation and action, if needed. eHealth did not have a way to know whether all servers were included in the scans.

We found 16 of the 341 servers we tested were not included in the vulnerability scans. This means eHealth did not have all possible information to help protect the servers against potential security vulnerabilities.

During 2023, eHealth was transitioning from a monthly scanning process to a continuous scanning process for each server. Management advised us its vulnerability scans missed these 16 servers due to implementation issues during this transition period.

eHealth also did not analyze security information (i.e., trends) from scans over time, network incidents, or problems reported through security tickets to identify potential risks for maintenance processes. For example, analysis of logged security information could include:

- Scans that identify trends related to improperly applied server updates
- Security tickets related to server downtime problems to help identify whether maintenance processes, or lack thereof, impact server availability
- Attempted security incidents to help determine whether timeframes to complete updates or upgrades are sufficient

At July 2023, eHealth was transitioning operation of its vulnerability management processes to an external service provider. It expects this service provider will help to verify whether it scans all servers, as well as help it analyze security information to identify potential risks related to maintenance processes.

Without analyzing security information for all key healthcare IT servers, eHealth may not identify servers it is not updating as expected. The risk of an attacker exploiting a vulnerability increases the longer eHealth takes to update servers, as more attackers become aware of the vulnerability and build cyberattack methods.

5. **We recommend eHealth Saskatchewan regularly analyze security information logged for key healthcare IT servers to support timely server updates for identified security vulnerabilities.**

4.6 Reporting of IT Server Maintenance Risks Needed

As of July 2023, eHealth Saskatchewan had not sufficiently defined reporting requirements about IT server maintenance risks to share with its senior management or partners.

eHealth signed a master service agreement in 2022 with its key partner, the Saskatchewan Health Authority. The agreement did not set out reporting requirements or agreed upon service targets (e.g., IT server update and availability levels).

In June 2023, eHealth prepared a preliminary report for the Authority as part of its work to define reporting requirements. The report did not include targets or results specific to IT server maintenance (e.g., unplanned outages due to IT server maintenance issues). Management advised us it continues to work with its partners to expand reporting to include service targets and additional information about server maintenance risk areas.

Establishment of key service targets can also help eHealth to define reporting requirements to its senior management—such reporting may help eHealth identify potential risks early and avoid missing certain service expectations. Reporting could include actual results compared to service targets such as patch compliance levels, service outages related to maintenance activities or incidents, or security trends related to maintenance. Reports could also explain why actual results did not achieve service targets, along with recommended corrective actions.

Management advised us that eHealth used an informal, internally set target that at least 80% of servers have all current patches applied. At the end of each update cycle (e.g., monthly), managers review reports and/or discuss the level of update compliance with their staff or service providers. These results are not formally shared with senior management, although they may be discussed at meetings.

If less then 80% of servers did not successfully receive updates, eHealth staff investigate and take action to improve compliance. Compliance can vary due to ongoing maintenance projects or business use of servers interfering with the update process. Also, reports could include servers that are not correctly reflected in the reporting tool (e.g., not actually in production yet, decommissioned) and should be removed from reporting.

As described in **Section 4.3**, we found eHealth had a plan with its partner to upgrade certain unsupported servers. The plan described risks (e.g., lack of availability) associated with these unsupported servers. However, eHealth and its partner did not set a timeline for completion and did not implement mitigating controls in the interim.

Figure 4 sets out possible risks related to the untimely maintenance of IT servers that could be relevant to eHealth and its partners.

Figure 4—Risks Associated with Untimely Maintenance of IT Servers

Risk	Impact
Security breach	Inappropriate changes to data that could impact healthcare decisions, resulting in patient harm, or even death Unauthorized access to data, violating patient privacy and creating exposure to identity theft IT systems unavailable when needed to support timely care of patients Higher costs to address the security breach and implement controls to prevent future breaches
IT system slowdown or breakdown	IT systems unavailable when needed to support timely care of patients Higher costs to keep IT systems operating efficiently
Data loss or corruption	Data unavailable when needed to support timely care of patients Higher costs to recover or reproduce data

Source: Nye Technical Services, LLC, 2019, *An aging IT infrastructure and the risks it poses to SMBs*.

Without sufficient formal reporting, senior management and eHealth's partners may not sufficiently understand existing risks that could prevent timely provision of healthcare services or that could compromise the security of patient data. Healthcare providers need timely access to accurate and complete patient information to support quality healthcare.

6. **We recommend eHealth Saskatchewan regularly report to its senior management and partners about significant risks and mitigation plans related to maintenance of key healthcare IT servers.**

5.0 GLOSSARY

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

Defence-in-depth – The practice of using layered security mechanisms to increase security of the IT 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.

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.

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

Security vulnerability – An unintended weakness exposing a computer system 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.

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

Virtual server – A virtual server re-creates the functionality of a dedicated physical server, allowing efficient sharing of hardware and software resources.

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. (2020). *IT Asset Management in B.C. Government*. Victoria: Author.

National Institute of Standards and Technology. *Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology.* Gaithersburg, MD*:* Author. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4-draft.pdf (6 September 2023).

Provincial Auditor of Saskatchewan. (2020). *2020 Report – Volume 1*, Chapter 8, *Horizon School Division No. 205—Maintaining Facilities*. Regina: Author.

Provincial Auditor of Saskatchewan. (2015). *2015 Report – Volume 2*, Chapter 32, *Advanced Education—Managing Risks to Post-Secondary Service from its Unsupported Critical IT System*. Regina: Author.

The Information Systems Audit and Control Association. (2012). *COBIT 5*. Rolling Meadows, IL: Author.