Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes
Canada

Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage

December 12, 2023

REPORT SUBMITTED BY: Xona Partners Inc.

Xona Partners Inc.
2969 Sable Ridge Drive, Ottawa, Ontario K1T 3S3, Canada
www.xonapartners.com

ISBN: 978-0-660-69962-2
Catalogue number: BC92-130/1-2024E-PDF

XONA PARTNERS

Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage

A Report to the Canadian Radio-television and Telecommunications Commission

2023-12-12

This report was prepared by Xona Partners Inc. (Xona) in response to Request for Proposal #CRTC 23-0049: "Evaluation of Rogers' Network for resiliency related to 8 July 2022 outage."

The Canadian Radio-television and Telecommunications Commission (CRTC) has retained Xona to perform the tasks specified in the statement of work resulting from the aforementioned Request for Proposal.

Xona prepared the report based on information provided by Rogers Communications Inc. (Rogers), which is subject to Section 39 of the *Telecommunications Act*. While developing this report, Xona reviewed the Rogers responses to CRTC Request for Information dated 12 July 2022 and engaged with Rogers in a series of further questions and meetings to fulfill its mandate and obligations to the CRTC.

Table of contents

1. Glossary

9-1-1 Network Provider	The 9-1-1 Network Provider is the incumbent local exchange carrier that provides 9-1-1 emergency response service to the local authority pursuant to a tariff and/or agreement. The 9-1-1 network provider's tariff and/or agreement makes access to 9-1-1 emergency calling available to the end-users located within the serving area.
Access Control List policy filter	An Access Control List policy filter in a router is a table that provides the rules on how the router ought to manage the packet traffic. The Access Control List is described as a policy filter because it defines what traffic will pass through the router and how it will be directed based on the set of rules (filters).
Border Gateway Protocol (BGP)	Border Gateway Protocol is an exterior gateway routing protocol that enables the exchange of route information among routers in different autonomous systems, for the purpose of selecting the best path for data packets.
Core router	A core router is a router in the core network, or layer, of an IP network.
Change management process	Change management process is a systematic approach to managing network infrastructure and service changes. It is a process that is designed to minimize the risk of service disruptions and to ensure that changes are controlled and implemented efficiently.
Distribution router	A distribution router is a router in the distribution layer of a telecommunications service provider’s IP network. It sits between the access layer that connects end users to the network and the core layer that aggregates all the network traffic.
Domain name server	A domain name server is like an address book for the Internet. A domain name server translates user-friendly web addresses (like www.rogers.com) into numerical Internet Protocol addresses.

Incident management process	Incident management process is a systematic approach to identifying, responding to, and resolving incidents that affect network services. It is designed to minimize the impact of incidents on users by restoring normal service as quickly as possible.
Incumbent Local Exchange Carrier (ILEC)	The Incumbent Local Exchange Carrier is the 9-1-1 network provider in the context of this report.
Intermediate System to Intermediate System	Intermediate System to Intermediate System is an interior gateway routing protocol that enables the exchange of route information among routers within an operator's network for the purpose of selecting the best path for data packets. It is a similar type of protocol to OSPF.
National Alert Aggregation and Dissemination (NAAD) System	The National Alert Aggregation and Dissemination System accepts emergency alerts from authorized government agencies which are then made available to broadcasters and other media distributors who voluntarily distribute them to the Canadian public. Pelmorex Communications Inc. is designated as Canada's aggregator and disseminator of emergency public alert messages.
National Public Alerting System (NPAS)	The National Public Alerting System is a Federal, Provincial, and Territorial system that provides emergency management organizations throughout Canada with the capability to warn the public about imminent or unfolding hazards.
Open Shortest Path First (OSPF)	Open Shortest Path First is an interior gateway routing protocol that enables the exchange of route information among routers within an operator's network for the purpose of selecting the best path for forwarding data packets.
Originating Network Provider	The network which originates a 9-1-1 call. Includes the access network and the calling network. Typically operated by carriers or other service providers.
Over-the-top	Over-the-top messaging is a messaging service offered by an application that is typically agnostic to the telecom service

messaging	provider and runs independently from it. For example, services such as WhatsApp, Signal, Telegram, WeChat, and others are over-the-top messaging services, unlike short message service and multimedia messaging service, which are technologies built into the cellular technology (e.g., GSM, 3G, or LTE).
Production network	Production network is a common term used by service providers to distinguish active network elements from those used in a laboratory environment. Production, in this context, means processing customer traffic in a live environment.
Public Safety Answering Point (PSAP)	An answering location for 9-1-1 calls originating in a given area. A PSAP may be designed as Primary or Secondary, which refers to the order in which calls are directed for answering. Primary PSAPs respond first. This is a communications facility that is open 24 hours a day, 365 days a year, and is responsible for redirecting or transferring emergency calls to Secondary PSAPs that receive calls on a transfer basis only, and generally serve as a centralized answering location for a particular type of emergency call. Secondary PSAPs are staffed by employees of service agencies such as police, fire, or emergency medical agencies or by employees of a common bureau serving a group of such entities.
Routers	Routers are networking devices that receive and forward data packets in IP networks. Routers direct traffic within networks or between networks.
Routing protocol	A routing protocol specifies how routers forward packets from a source to a destination. Routing protocols are grouped into two major categories: interior gateway protocols and exterior gateway protocols. Interior gateway protocols are designed to work within an autonomous system—a network administratively controlled by a single organization. External gateway protocols are designed to manage the transfer of information between autonomous systems.

2. Acronyms

API	Application Programming Interface
BGP	Border Gateway Protocol
BRI	Base Risk Index
BSS	Business Support Systems
CRMS	Capacity, Reliability, Mandatory Safety and Service (Access Network)
CRTC	Canadian Radio-television and Telecommunications Commission
CSTAC	Canadian Security Telecommunications Advisory Committee
DGW	Distribution Gateway
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specifications
EDT	Eastern Daylight Time
FCC	Federal Communications Commission
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
ISED	Innovation Science and Economic Development (Ministry of)
ISP	Internet service providers
KPI	Key Performance Indicator
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
MVPN	Multicast Virtual Private Network
NAAD	National Alert Aggregation and Dissemination System
NCT	Network Change Ticket
NIST	National Institute of Standards and Technology
NOC	Network Operation Centre
NPAS	National Public Alerting System
NPI	New Product Introduction
NTI	New Technology Introduction
OSPF	Open Shortest Path First
OSS	Operational Support Systems
PKI	Public Key Infrastructure

PSAP	Public Safety Answering Point
RCMIN	Rogers Communications Management IP Network
RFC	Request for Comments
RFI	Request for Information
SD-WAN	Software-Defined Wide Area Network
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TSP	Telecommunications Service Provider
VPN	Virtual Private Network

3. Executive summary

3.1. Overview

In the early morning of 8 July 2022, Rogers Communications Inc. (Rogers) experienced a major service outage in its Internet Protocol (IP) core network that affected its wireless and wireline services across Canada (July 2022 outage). The July 2022 outage lasted from 4:58 EDT on 8 July 2022 to 7:00 EDT on 9 July 2022 as services were gradually restored. More than 12 million customers lost wireless and wireline services, including mobile subscribers, home Internet users, corporate customers, and institutional customers that provide critical services (e.g., Interac e-Transfer and electronic payment services).

This report details the results of an independent assessment of the Rogers network architecture for reliability and resiliency[1], as well as the processes in place at Rogers to manage network changes (change management process[2]) and respond to network incidents like outages (incident management process[3]) as these processes were central to the July 2022 outage.

In this report we detail the findings for the period before and during the outage and outline the measures that Rogers has since implemented to address deficiencies in its network design and processes. This report is primarily based on an extensive independent review of the Rogers responses to multiple rounds of questions and meetings with the Rogers technical and management staff during this assessment, as well as information Rogers provided in response to the CRTC's request for information (RFI) after the outage.

3.2. Description of the outage

Background. For context, Rogers operates wireless and wireline networks that share a common IP core network, as shown in a simplified form in Figure 1. The core network is part of the telecommunications network that is responsible for aggregating and routing data traffic both internally within the Rogers network and externally with the Internet and other service providers. Hence, for Rogers, both wireless and wireline data traffic is processed by the same IP core network. In the weeks leading to the day of the outage on 8 July 2022, Rogers was executing on a

[1] Reliability is a measure of the ability of the network to deliver services according to their design specifications. Resiliency is a measure of how the network responds to minimize the impact of failures and the speed at which it recovers from disruptions.
[2] Change management process is a systematic approach to managing network infrastructure and service changes. It is a process that is designed to minimize the risk of service disruptions and to ensure that changes are controlled and implemented efficiently.
[3] Incident management process is a systematic approach to identifying, responding to, and resolving incidents that affect network services. It is designed to minimize the impact of incidents on users by restoring normal service as quickly as possible.

seven-phase process to upgrade its IP core network. The outage occurred during the sixth phase of this upgrade process.

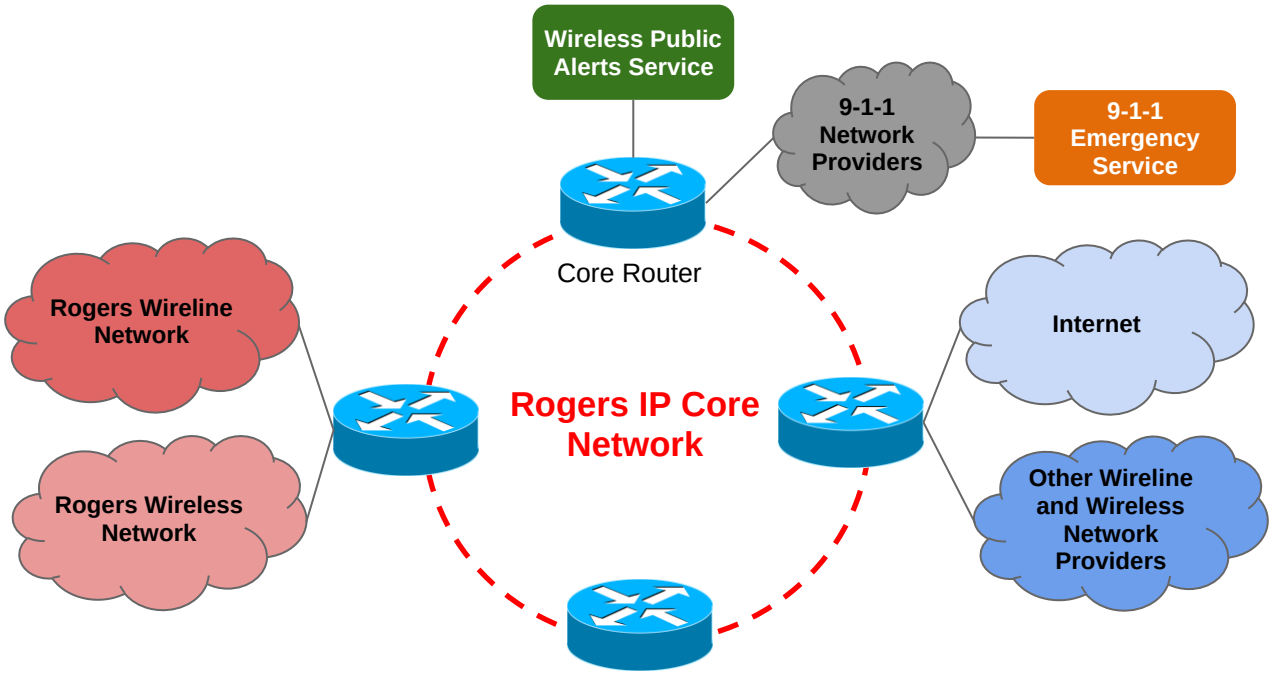

Figure 1 A simplified topology of Rogers' network architecture.

Root cause of the network failure. The July 2022 outage is attributed to an error in configuring the distribution routers[4] within the Rogers IP network. Rogers staff removed the Access Control List[5] policy filter from the configuration of the distribution routers. This consequently resulted in a flood of IP routing information into the core network routers, which triggered the outage. The core network routers allow Rogers wireline and wireless customers to access services such as voice and data. The flood of IP routing data from the distribution routers into the core routers exceeded their capacity to process the information[6]. The core routers crashed within minutes from the time the policy filter was removed from the distribution routers configuration. When the core network routers crashed, user traffic could no

[4] A distribution router is a router that directs traffic between the access layer which connects users to the network, and the core network which aggregates all the network traffic.

[5] An Access Control List in a router is a table that provides the rules on how the router ought to manage the packet traffic. The Access Control List is described as a policy filter because it defines what traffic will pass through the router and how it will be directed based on the set of rules (filters).

[6] Rogers stated that about 10,000 routes are advertised into the core router when the Access Control List policy filter is present on the distribution router. When this policy filter was removed, a single distribution router released over 900,000 route data into the core routers.

longer be routed to the appropriate destination. Consequently, services such as mobile, home phone, Internet, business wireline connectivity, and 9-1-1 calling ceased functioning.

Absence of router overload protection. The July 2022 outage exposed the absence of overload protection on the core network routers. The network failure could have been prevented had the core network routers been configured with an overload limit that specifies the maximum acceptable number of IP routing data the router can support. However, the Rogers core network routers were not configured with such overload protection mechanisms. Hence, when the policy filter was removed from the distribution router, an excessive amount of routing data flooded the core routers, which led them to crash.

Deficiency in the change management process. The configuration error, which led to the removal of the policy filter from the configuration of the distribution routers, is the result of a change management oversight by Rogers staff. Rogers staff deleted the policy filter that prevented IP route flooding in an effort to clean up the configuration files of the distribution routers. The change management process, which includes audits of change parameters, failed to flag the erroneous configuration change.

As stated above, this configuration change was the sixth phase of a seven-phase network upgrade process that had begun weeks earlier. Before this sixth phase configuration update, the previous configuration updates were completed successfully without any issue. Rogers had initially assessed the risk of this seven-phased process as "High." However, as changes in prior phases were completed successfully, the risk assessment algorithm downgraded the risk level for the sixth phase of the configuration change to "Low" risk, including the change that caused the July 2022 outage. The Low risk assessment resulted in Rogers staff not being required to conduct additional scrutiny, go through higher levels of approvals, and conduct laboratory testing for this configuration change. Downgrading the risk assessment to "Low" for changing the Access Control List filter in a routing policy contravenes industry norms, which require high scrutiny for such configuration changes, including laboratory testing before deploying in the production network.

3.3. Reliability of Rogers network architecture

The Rogers network is a national Tier 1 network and is architecturally designed for reliability; it is typical of what would be expected of such a Tier 1 service provider network. The July 2022 outage was not the result of a design flaw in the Rogers core network architecture. However, with both the wireless and wireline networks sharing a common IP core network, the scope of the outage was extreme in that it resulted in a catastrophic loss of all services. Such a network architecture is common to many service providers and is an example of the trend of converged wireline and wireless telecom networks. It is a design choice by service providers, including Rogers, that seeks to balance cost with performance.

3.4. Factors affecting network restoration

Network management infrastructure. A management network provides access to critical infrastructure sites or equipment in a network to enable troubleshooting and repair. At the time of the July 2022 outage, Rogers had a management network that relied on the Rogers IP core network. When the IP core network failed during the outage, remote Rogers employees were unable to access the management network. Moreover, Rogers did not provision its network operation centre and other critical remote infrastructure sites with redundant connectivity from alternative service providers for network management. This limited access to critical network equipment during the July 2022 outage for troubleshooting and root cause analysis. Rogers had to dispatch staff to remote sites to physically access the affected routers, which delayed network recovery efforts. In our assessment, network resiliency demands that telecom network operators have secure alternative access to crucial remote network elements that is not dependent on the data network. Both the inability of Rogers remote staff to access the management network and the absence of backup connectivity from alternative service providers to the network operation centre and other critical remote sites contributed to prolonging the July 2022 outage.

Limited communication among Rogers staff. Rogers staff relied on the company's own mobile and Internet services for connectivity to communicate among themselves. When both the wireless and wireline networks failed, Rogers staff, especially critical incident management staff, were not able to communicate effectively during the early hours of the outage. Rogers had to send Subscriber Identity Module (SIM) cards from other mobile network operators to its remote sites to enable its staff with wireless connectivity to communicate with each other. The absence of sufficient alternative means of communication slowed the Rogers response to the July 2022 outage.

Timely access to critical information for network recovery. A lack of information hampered the Rogers incident management process. Rogers staff did not initially have access to the error logs from the failed routers and could not pinpoint the root cause for about 14 hours from the start of the outage. Additionally, Rogers had completed multiple configuration changes during the maintenance window on the day of the outage. This adversely impacted outage recovery efforts, making it difficult to decide which network change ticket to roll back. These two factors contributed to misdiagnosing the root cause of the network failure in the initial hours of the July 2022 outage. However, once the root cause was identified, network restoration activities commenced methodically, and services were gradually restored.

3.5. Measures taken by Rogers to improve its network reliability and resiliency

Addressing the outage root cause and deficiencies in the management network architecture. In the months following the July 2022 outage, Rogers undertook a series of measures and initiatives to address the critical deficiencies that the outage exposed. Most importantly, Rogers implemented safeguards in the configuration of the routers in its core network to prevent the flooding of IP routing data, thus preventing a similar outage from happening in the future. Rogers also implemented a separate physical and logical management network to access network elements for troubleshooting and root cause analysis. Additionally, Rogers deployed backup connectivity from third party service providers to its network operation centre and other critical remote infrastructure sites, and invested in tools that would help validate router configuration changes.

Separate IP core for the wireless and wireline networks. Following the outage, Rogers announced it had decided to separate the IP core network for its wireless and wireline networks. This decision entails deploying a new IP core for the wireless network, while the existing IP core would remain to serve the wireline network. Therefore, if one IP core network were affected by an outage, the other IP core network would remain unaffected and operational.

Rogers has not yet finalized the implementation of the IP core network separation, which remains a work in progress. When implemented, separate IP core networks for the wireless and wireline networks will help to contain a failure to its respective access network and, therefore, avoid the type of catastrophic network failure experienced in the July 2022 outage, where both wireless and wireline services were unavailable due to the outage in the common core IP network. IP core network separation would improve the overall resiliency of the Rogers wireless and wireline networks.

Improving the change management process. Following the July 2022 outage, Rogers made several improvements to its change management process. These improvements included a new risk assessment algorithm; organizational changes to improve collaboration between network operations and engineering teams; an enhanced process for introducing new equipment and technology; improvements in implementing network changes such as introducing automation to streamline the change management process; and additional lab testing of planned network configuration changes.

Improving the incident management process. Following the July 2022 outage, Rogers made improvements to its incident management process, to include bolstering its incident management guidelines to encompass various outage scenarios; streamlining its incident response with well-defined leadership roles; implementing a solution for prioritization of alarms during outage; enhancing automated rollbacks to previous configurations when new changes are not successful; and implementing additional measures to improve its communication

protocols. Rogers has also equipped all incident response and crisis management team members with backup communications from third party service providers to maintain communication capabilities during outages.

3.6. Assessment and recommendations to Rogers

Our overall assessment is that the combination of measures that Rogers undertook after the July 2022 outage are satisfactory to improve the Rogers network resiliency and reliability as well as to address the root cause of the July 2022 outage.

Diligence in implementing the improved change management processes would be the most effective way to avoid a similar outage from occurring in the future. Enhancements to the incident response processes would improve the Rogers response to enable a faster service recovery if network failure occurs. We have several recommendations for additional measures that Rogers could undertake to further improve its network resiliency. These recommendations are:

1. Test emergency roaming with other mobile network operators and expand it to include a more comprehensive set of test scenarios. Rogers has signed the Memorandum of Understanding on Telecommunications Reliability, which includes emergency roaming with other mobile network operators to enable Rogers customers to access emergency services (e.g., 9-1-1 calls) during a major outage. This additional testing would ensure that emergency roaming is feasible under different network failure scenarios; specifically, the scenario observed during the July 2022 outage (wherein the radio network was up and the core network was down).

2. Develop a detailed root cause analysis for future major outages. This would benefit the process of assessing an outage and its impact, as well as identifying the appropriate mitigation measures.

3. Ensure wide coverage and rigor in testing configuration changes. This would help avoid errors leading to potential outages. Rogers would need to leverage new test tools for modeling test scenarios that replicate the production network, and to address the evolution of networking technologies.

4. Expand the scope of incident management drills. This would enhance staff and network's emergency preparedness and proactively uncover weaknesses.

5. Institutionalize learning from its own and other service providers' network failures to implement preventive actions, minimize the impact of network outages, and enhance quality of service.

6. Inform customers how to reach 9-1-1 services during an outage.

7. Share outage root cause and mitigation strategies with the broader Internet community (represented by bodies such as the North American Network Operator's Group), to help other telecom network operators prevent similar network failures.

3.7. Recommendations to telecom network operators

Lessons learned from the July 2022 outage. A summary of the important lessons learned from the July 2022 outage includes:

1. Implement router overload protection in the IP core and distribution networks.
2. Separate the network management layer physically and logically from the data network.
3. Provide the network operation centre and other critical remote sites with a secure backup connectivity from third-party telecom network operators.
4. Ensure that the audit process for network configuration changes is effective and involves different teams within the organization, such as engineering, operations, and project management. It is also advisable to involve equipment vendors where the configuration changes pertain to critical infrastructure, such as the IP core network.
5. Conduct lab tests of planned configuration changes and ensure that the lab equipment and test scenarios accurately reflect the production network.
6. Carefully manage the number of configuration changes completed in a single maintenance window and leverage tools and processes for automatic rollback of configuration parameters.
7. Implement an automated alarm prioritization solution to suppress unnecessary alarms for every type of change and to allow staff to focus on the important alarms.
8. Provide critical staff with secondary means to communicate, such as SIM cards from third-party network operators.
9. Simulate and practice network failure and outage scenarios to uncover deficiencies in the network architecture and the incident management process.

Evolving telecom network trends. There are evolving telecom network trends that impact network reliability and resiliency. These include the evolutions towards telecom public cloud platforms, network softwarization and virtualization, the increased use of Artificial Intelligence in network automation, readiness for post-quantum cybersecurity, and the convergence of terrestrial and non-terrestrial networks. Canadian telecom service providers are in the process of incorporating some of these trends into their network evolution. We highlight a few technological and process recommendations that would strengthen network resiliency in the face of such evolutionary network trends. These recommendations include:

1. Technological recommendations:

A. Leverage emerging non-geostationary orbit satellite constellations (e.g., low earth orbit satellite constellations) to provide remote sites with backup connectivity and consider emerging direct-to-cell constellations for emergency 9-1-1 calling.

B. Track and prepare to implement disaster roaming standards that are currently being planned in the 3rd Generation Partnership Project (3GPP) standard setting body.

C. Consider using over-the-top messaging applications as an alternative communication method, including emergency services. This would be useful in case of failures in some critical systems, such as the IP Multimedia System.

D. Leverage dynamic software-based SIM technologies, which provide various levels of programmability and allow new roaming models to alternative providers in case of major outages.

E. Consider and work towards the applicability of emergency spectrum and capacity-sharing techniques to mitigate the impact of network failures. These techniques temporarily and dynamically increase network capacity to accommodate roaming users.

F. Consider collaborating with content delivery networks and over-the-top application providers to define specific interaction models during emergencies. For example, dynamic traffic management allows content providers to adapt their behaviour based on feedback from telecom operators.

G. Consider offering critical infrastructure service providers secondary options for redundant connectivity services.

2. Process recommendations:

A. Implement incident response training and drills to uncover weaknesses in architecture, operations, and business processes that adversely impact outage recovery efforts.

B. Implement incident management response key performance indicators to benchmark the incident response effort and improve its effectiveness.

C. Designate clear roles and responsibilities for personnel to better respond to network outages.

D. Consider calculating the cost impact of a network outage to help mitigate the consequences of incidents through decision-making on resource allocation and communication with stakeholders to preserve brand-image and financial stability.

E. During an outage, service providers are advised to remind and inform the public on how to access emergency calling and public alerts services.

4. Introduction

Early on Friday, 8 July 2022, Rogers experienced a major outage on its wireless and wireline network that lasted for nearly 24 hours from inception until most customers regained their connectivity services. The outage, which was localized to the IP core network, affected all wireless and wireline connectivity services, for consumers and businesses alike. It also affected vital 9-1-1 calls and emergency or public alerts from the National Public Alerting System (NPAS).

The outage occurred in the process of upgrading some of the Rogers IP core network elements. An IP routing misconfiguration cascaded into a widespread outage that could be defined as catastrophic. All the Rogers wireless and wireline networks across all of Canada were out of service. This included vital connectivity to the Rogers NOC and other remote sites as well as among Rogers staff, which further delayed repair efforts.

In the immediate aftermath of the outage, the CRTC launched an inquiry to understand events leading to the outage and the Rogers incident management process. Following that inquiry, the CRTC determined the need to conduct a detailed technical review of Rogers wireless and wireline telecommunications networks for resiliency and reliability in all aspects that led to the 8 July 2022 outage, including network architecture; business management process and controls; change management processes; and incident management processes. This report presents results of the technical review and evaluation of whether changes Rogers made and proposed in response to the outage are sufficient to improve network resiliency.

This report is structured as follows:

- Section 5 describes the 8 July 2022 outage, primarily based on information provided by Rogers.
- Section 6 expands into our outage analysis; it presents conclusions based on synthesis of available outage data. To complete the analysis, we defined several areas for investigation, such as root cause, network architecture, and change and incident management processes. Most importantly, we focus on the effectiveness of execution compared to pre-outage processes and industry best practices.
- Section 7 presents the corrective actions Rogers undertook in the wake of the outage to improve network reliability and resiliency, as well as presents our assessment of these actions.
- Section 8 presents lessons learned and recommendations that we believe would be applicable to other telecommunications network operators in the broader context of improving telecommunications networks resiliency.

5. Incident description

5.1. Rogers network architecture

Rogers operates a national wireless network using GSM (2G), UMTS (3G), LTE (4G), and 5G technologies alongside Wi-Fi services. Rogers also operates a wireline network that includes Data-Over-Cable-Service-Interface-Specifications (DOCSIS) cable and fibre-based broadband Internet and telephony services.

[redacted]

The IP core network implements routers from two different major equipment vendors: [redacted] for the distribution routers and [redacted] for the core routers. The outage took the Rogers core routers out of service, thereby severing connectivity services to all Rogers customers. Connectivity was also severed with 9-1-1 network providers through the Rogers wireless and wireline networks. Emergency alerts disseminated by Pelmorex - the National Alert Aggregation and Dissemination (NAAD) System administrator in Canada[7] - could not reach Rogers wireless customers.

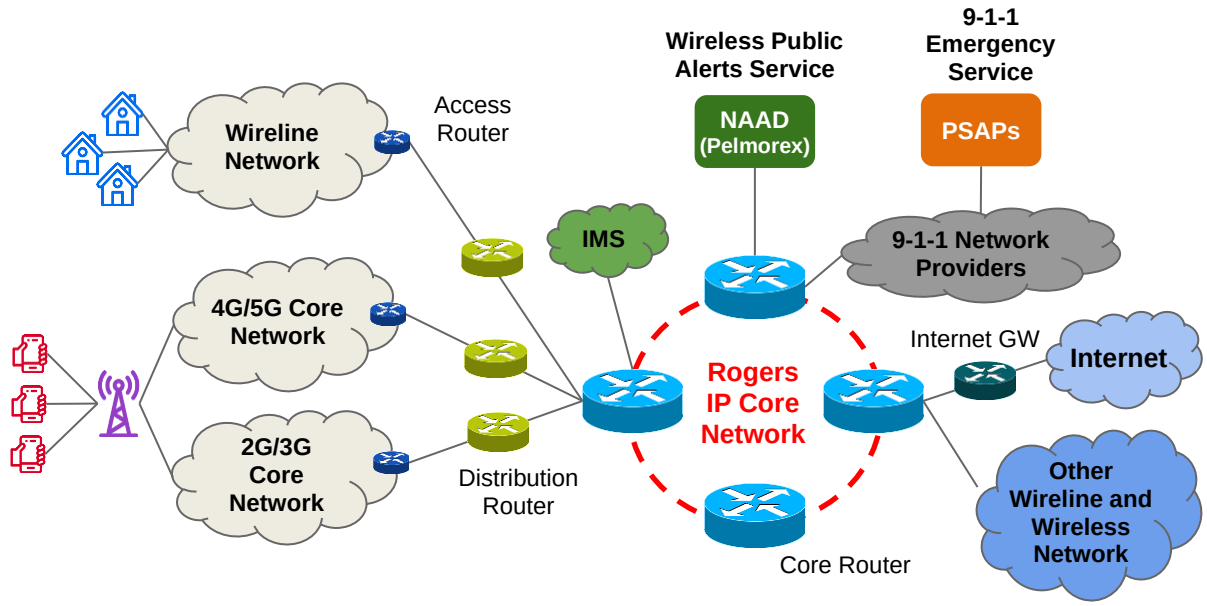

Figure 2 A simplified illustration of the Rogers network.

The outage also severed access to important systems that manage the Rogers wireless and wireline networks. This includes access to the NOC and to critical systems such as the Home Location Register, Home Subscriber Server, and Centralized User Database.

[7] The NAAD System administrator collects and validates emergency alerts from authorized government agencies throughout Canada and makes them available to the public through telecommunications service providers.

5.2. Incident trigger

The outage occurred during the execution of a broad process to change the [redacted]. To complete the process, Rogers determined it needed to delete a policy filter in the distribution routers. [redacted]

The change in the distributed router configuration enables direct distribution of wireless DNS addresses of the cloud infrastructure into the Open Shortest Path First (OSPF) protocol. The configuration change led to Border Gateway Protocol (BGP) redistribution of full routing tables into OSPF. This flood of updates overloaded the core routers and exhausted the central processing unit and memory resources, and ultimately, caused the core routers to crash which triggered the outage.

5.3. Incident timeline and restoration efforts

The policy filter was removed from [redacted] at 4:43 EDT on 8 July 2022 (the trigger event). **Error! Reference source not found.** shows key milestones in the i ncident timeline; additional details are available in Annex 1. Within two minutes, all the Rogers core gateways began failing; [redacted]. All Rogers wireless and wireline services ceased operating across Canada.

[redacted] Moreover, the failure of the wireless network hampered communication among the Rogers staff, who had limited access to wireless services from other mobile network operators (i.e., Rogers had a limited number of third-party SIMs).

[redacted]

Because of the outage, Rogers engineers lost access to network management [redacted] that Rogers engineers identified the distribution routers, which were flooding the core routers with route advertisements, as the root cause.

Once the root cause was identified, Rogers proceeded to restore the network, starting with the Central and East regions. Rogers had to take certain precautions for an orderly restoration of services. This included throttling the mobility management entity to prevent signaling storms resulting from large numbers of mobile phones attempting to register on the network.

Traffic was gradually restored through the evening of 8 July 2022 and into the morning of 9 July 2022. [redacted].

[redacted]

With all regions looking healthy, Rogers reversed the throttling that had been instituted on the wireless network mobility management entity in all regions. [redacted]

5.4. Impacted customers

All Rogers wireline and wireless customers, including those of flanker brands Fido and Chatr, were affected by the outage, in addition to wholesale and corporate customers who rely on services from Rogers. [redacted]

[redacted]

Rogers provides wholesale and roaming services to other telecommunications service providers (TSPs) as well as connectivity services to business enterprises, including financial institutions such as Interac, as well as to government organizations. Additionally, some Rogers Media broadcast stations use Rogers network services. In all, the following customers were affected by the outage:

- **TSPs**
  - TSPs who use the Rogers wireless network to communicate and operate their network
  - Wireless roaming partners
  - Third-party Internet service providers (ISPs) who primarily use the Rogers wireline network

- **Government**: Rogers provides wireline, wireless, voice over IP, long-distance, toll-free, and machine-to-machine services to different branches of government. [redacted] Different levels of governments were impacted:
  - Federal government
  - Provincial governments
  - Municipal governments

- **Critical infrastructure providers**: Organizations that primarily rely on wireline services such as Multiprotocol Label Switching (MPLS), Software-defined Wide Area Network (SD-WAN), Ethernet, and optical based communication protocols. These include:
  - Financial institutions [redacted]
  - Energy and utilities
  - Transportation services
  - Hospitals
- **Corporate enterprises**: Enterprises served by different Rogers wireless and wireline services including MPLS and SD-WAN services

- **Broadcasting clients**
  - Rogers Media broadcasting services primarily use wireline Internet connectivity with a few using wireless modems
  - Terrestrial relay distribution undertakings clients

- **Other Rogers companies**
  - Rogers Bank used the Rogers VPN and telephone services

5.5. Impact on emergency and alerting services

5.5.1. 9-1-1 emergency service

The IP core network outage severed the connectivity with 9-1-1 network providers and, consequently, with Public Safety Answering Points (PSAPs). As a result, a large proportion of Rogers wireless and wireline customers could not reach 9-1-1 emergency services during the outage. [redacted]

During the outage, the radio network remained operational while the core network was down, which led to a scenario where customer phones did not automatically roam onto alternate networks for 9-1-1 emergency calls. Some Rogers wireless customers were able to access 9-1-1 services in two cases. In the first case, some 9-1-1 calls were successful using the 2G/3G network, where traffic and signaling could reach Rogers' circuit-switched infrastructure when the IP core network was intermittently up. This was not possible using LTE, where the 4G mobile core is completely dependent on the IP core network. With the LTE core connectivity down, some phones attempted to use the 2G/3G network. Rogers confirmed seeing a higher call volume on its 2G/3G network.

In the second case, Rogers stated that some newer mobile phones are automatically programmed to search and use another service provider network to connect a 9-1-1 call when the home network is not available.

[redacted]

Focusing on the day of 8 July 2022, Rogers stated that it was able to connect [redacted] of the typical daily average of successful 9-1-1 calls over its wireless network. Adding Rogers customers who successfully completed 9-1-1 calls on Bell and TELUS networks, Rogers stated that the percentage was about [redacted].

Considering the wireless 9-1-1 call volume recorded on 8 July 2022, Rogers was able to successfully connect [redacted]of these calls. Rogers stated that it is not uncommon for customers to place additional calls to 9-1-1 to test their phone or request outage related information during an outage. Rogers added that a higher 9-1-1 call volume could have occurred due to wireless customers redialing 9-1-1 after having unsuccessful calls.

For the wireline network, [redacted] 9-1-1 calls were successful on 8 July 2022. This represents about [redacted] of the typical daily average. Rogers stated it had no statistics available for the total and unsuccessful wireline 9-1-1 calls.

For 9 July 2022, 9-1-1 call success rate improved, reaching [redacted] and [redacted] of the daily average for the wireless and wireline networks, respectively.

5.5.2. Public alerting service

Rogers wireless customers across its service area were not able to receive wireless public alerting service messages from Pelmorex, the public alerting service administrator, which aggregates alerts issued by the federal, provincial/territorial, or local government alerting authorities. The Rogers Broadcast Message centre platform was able to receive alerts from Pelmorex; however, Rogers could not deliver the alerts to its customers. [redacted]

Rogers cable TV service which uses Rogers IP core network was in outage and had no facility to send alerts.

Most Rogers TV and radio stations use Rogers IP network connectivity and were unable to receive alerts from Pelmorex. [redacted]

5.6. Communication and notifications

Communications with customers. Following the outage, the first Rogers customer communication was received via Twitter at 8:54 EDT, or 4h11m after the trigger event. The message was followed by similar messages over Facebook. Rogers, Fido, and Chatr social media accounts pushed updates periodically during the day.

Rogers and Fido call centres played an interactive voice response notification starting at 9:30 EDT. Both Rogers and Fido websites posted a banner message a few minutes afterwards, as well as virtual assistant banner updates. Some messages were also posted on community forums.

The Rogers Sports & Media radio stations and their websites issued a public service announcement starting around noon on 8 July 2022, to be repeated throughout the afternoon.

The messages advised customers of the outage impacting the wireless and wireline networks and indicated that Rogers staff were working to resolve the network issues as soon as possible. They provided no information on the expected time of service restoration. At 17:04 EDT Rogers staff first indicated that Rogers would credit customers for loss of service.

The Rogers Senior Vice President of Access Networks and Operations gave three television interviews in the afternoon and evening of 8 July 2022. At 22:48 EDT the Rogers Chief Executive Officer issued a message through a blog post stating that Rogers was working on identifying the root cause and confirmed that it would credit customers.

Communications with Pelmorex. Pelmorex contacted Rogers at 9:25 EDT (4h42m from outage onset) after hearing media reports of the outage. About 15 minutes later, Pelmorex disseminated an alert issued in Langham, Saskatchewan. Pelmorex contacted Rogers a second time at 9:54 EDT to inquire if the issuance of an alert had helped Rogers to determine whether alerts were reaching their

customers. Rogers confirmed that the alert was received by its Broadcast Message centre but that it was verifying distribution to wireless devices on the Rogers network.

At 11:19 EDT Rogers sent an email to Pelmorex advising of the national outage and cautioned that any agency attempting to broadcast emergency alerts to Rogers customers over the Rogers networks would be unsuccessful.

During the outage, Rogers sent two updates to Pelmorex. The first update was in the afternoon of 8 July 2022 to confirm that emergency alerts issued through the NAAD System would not be delivered to wireless users connected to the Rogers network. The second update was in the afternoon of 9 July 2022 to advise Pelmorex that the network had been restored.

Communications with 9-1-1 network providers. Rogers notified 9-1-1 network providers at 8:39 EDT on 8 July 2022 (3h56m from outage onset). The message advised that the Rogers network was unable to make and receive calls nationally including 9-1-1. The message requested the 9-1-1 network providers to notify the PSAPs.

At 17:01 EDT Rogers sent an update to 9-1-1 network providers advising of the continued outage.

At 10:51 EDT on 9 July 2022, Rogers notified the 9-1-1 network providers that its networks had been restored.

Communications with government authorities. Rogers notified the CRTC of the outage at 11:19 EDT on 8 July 2022. Rogers also notified Innovation Science and Economic Development (ISED) of the outage.

Communications with enterprise customers. Rogers for Business was unable to communicate with its customers directly. However, some employees with alternate telecommunications services were able to post an automatic reply using the cloud-based customer relationship management software application which is used by Rogers for Business clients. Clients who were able to access the application could have been notified accordingly.

Communications with other service providers. At 6:00 EDT on 8 July 2022, Rogers Chief Technology Officer (CTO) contacted his counterparts at Bell and TELUS advising them of the outage and warning against possible cyberattacks.

6. Outage cause and resolution analysis

This analysis assesses the root cause of the outage, the state of the network, and operational procedures in place before and during the outage. It also addresses the Rogers overall network architecture, as well as the change management and incident management processes (including communication with third parties). The various elements of the analysis apply to a broader set of outages.

6.1. Outage root cause analysis

The Rogers IP core network uses BGP as the exterior gateway protocol to advertise IP routes to other autonomous systems, and OSPF or Intermediate System to Intermediate System protocol as interior gateway protocol (IGP) to advertise IP routes within its own autonomous system. When the Access Control List policy filter was deleted from the distribution router configuration [redacted].

Rogers stated that the removal of the Access Control List policy filter that distributes the old DNS addresses from BGP into OSPF [redacted].

Over the years, TSPs have made errors in configuring BGP policy updates. As a result, the industry developed best practices to safeguard against route advertisement flooding resulting from incorrect BGP policy updates[8], such as:

A. Overload protection on the core routers [redacted].

B. Limiting the number of BGP routes advertised into OSPF by the distribution routers [redacted].

C. Manual and automated audits of the policy commands in relation with BGP route redistribution.

D. Automated rollback to a previous configuration, which helps limit the severity of the outage.

[redacted]

[redacted] The standard Rogers configuration for the [redacted] distribution routers allowed the distribution of Internet BGP routes into OSPF. Thus, when the policy filter was deleted from the policy statement, the standard configuration led to the distribution of an excessive number of BGP routes into OSPF. The OSPF link-state advertisements from the distribution router overloaded the core routers with data causing them to crash.

[8] As an example of industry best practices on this topic, we suggest referring to "Cisco IOS XR Deployment Best Practices for OSPF/IS-IS and BGP Routing" available at: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xr-software/IOS-XR-Best-Practices/IOSXR-Deployment-BestPractices.html

Failing to implement the above safeguards was an oversight by Rogers and did not [redacted]

[redacted]

[redacted]

6.2. Network architecture and resiliency

The following is our assessment of various network architecture and design dimensions in relation to the Rogers July 2022 outage and underlying root cause, with applicability to a broader set of network resiliency aspects.

IP core network redundancy. Rogers has a redundant transport network connecting the different sites of the IP core network that forms the backbone of the wireline and wireless networks. [redacted]

In our assessment, the Rogers network architecture is designed for reliability and follows industry best practices. [redacted] Models to ensure logical routing separation for better isolation of faulty nodes do exist as design choices.

Wireless packet core network redundancy. The national wireless core network comprising the mobile packet core (mobile data) and service core network (voice, short message service, multimedia message service, [redacted] Each region has physical and logical redundancy, with [redacted] sites per region for inter-region redundancy. The wireless core network depends on the IP core network, which rendered it un-operational during the IP core network outage.

Converged wireline/wireless IP core network design. The IP core network supports both the wireline and wireless networks. The July 2022 outage was localized to the common IP core network, which led to wide impact as it affected both wireless and wireline services. In our assessment, this is not a design flaw, but rather a network design choice that Rogers has made, which is similar in topology to that adopted by many other Tier 1 service providers worldwide. However, separate wireless and wireline IP core networks can help to contain a fault to one network without affecting both the wireless and wireline core networks at the same time.

Multi-vendor IP core network design. The Rogers explanation on the difference between how [redacted] routers manage link-state advertisements should not be misconstrued as an interoperability issue between the two routers [7:Q5, Q6; 13:Q40]. [redacted]

Service providers worldwide deploy systems from multiple vendors for various reasons including avoiding vendor lock-in or for specific differentiating features and performance. [redacted] routers are among the most common routers in telecommunications networks. Their operating systems [redacted] are among the most well known in the industry. Both solutions offer robust OSPF implementation: routing interoperability is not an issue. However, there are differences in the

configuration structures[9], automation, command line interface syntax, and some default behaviour between the two vendors' solutions. Engineers working on one vendor's routers in a multi-vendor network would need to be familiar with the other vendor's routers to configure and troubleshoot effectively.

Specifically, deploying [redacted] at the edge and [redacted] at the core is a common deployment model across various telecom operators, with well-documented best practices.

Emergency service architecture. 9-1-1 service delivery shares common physical and logical paths with the public wireline and fixed wireless networks. In the Rogers network configuration, we infer that no additional resiliency mechanisms have been implemented to specifically route 9-1-1 data traffic over alternative paths at the edge and the core of the network. We note that some telecom network operators do provide for dedicated backup infrastructure to cater to emergency traffic, in addition to specific prioritization mechanisms.

Network management infrastructure. A management network provides access to critical infrastructure sites or equipment in a network to enable troubleshooting and repair. During the July 2022 outage, Rogers lost access to network elements for several hours, and had to physically dispatch technicians to sites for recovery. [redacted]

Network monitoring and troubleshooting. [redacted]

Lab test and validation. It is typical when making planned configuration changes on core network elements to test the new configuration and validate it in a lab setting, especially for access control list and filter changes. This is a precautionary process given the dire consequences of potential failures in the core network.

Rogers classified the overall process – of which the policy filter configuration is only one of many parts – as "high risk". However, as some earlier parts of the process were completed successfully, the risk level was reduced to "low". This is an oversight in risk management as it took no consideration of the high-risk associated with BGP policy changes that had been implemented at the edge and affected the core.

[redacted]

Network stress scenario handling design. Network stress testing addresses multiple components of the network, including routing stress scenarios and signaling storm scenarios. Rogers actions during outage resolution shows good planning to address signaling storms (primarily those affecting the IP Multimedia System and mobile packet core). [redacted]

[9] For example, [redacted].

6.3. Business management processes

Business management processes include change management processes and incident management processes. Below is our assessment of activities pertaining to these two processes as related to the July 2022 outage. The assessment focuses on processes for operating and managing the network and processes that manage interactions with customers and partners.

6.3.1. Change management process

Change management is a systematic approach to managing network infrastructure and service changes. It is a process that is designed to minimize the risk of service disruptions and to ensure that changes are controlled and implemented efficiently. Below is our assessment of Rogers change management processes as related to the activities pertinent to the July 2022 outage. [redacted]

Risk assessment in change management. Rogers stated that the configuration change on the core and distribution routers specified by [redacted] which subsequently caused the outage, was the sixth phase of a seven-phase network upgrade process that had begun weeks earlier. This configuration update belonged to a series of changes required by business and network architecture design requirements.

Before this configuration update was implemented, there was a different configuration update for the [redacted] which was "Completed – No Issues" before the execution of [redacted]. Both NCTs were identified by the Rogers incident management team as potential causes for the outage. Initial recovery efforts focused on rollback of [redacted]

Rogers had assessed the risk for the initial change of this seven-phased process as "High". Subsequent changes in the series were listed as "Medium." [redacted] was "Low" risk based on the Rogers algorithm that weighs prior success into the risk assessment value. Thus, the risk value for [redacted] was reduced to "Low" based on successful completion of prior changes.

The risk assessment rated as "Low" is not aligned with industry best practices for routing protocol configuration changes, especially when it is related to BGP routes distribution into the OSPF protocol in the IP core network. Such a configuration change should be considered as high risk and tested in the laboratory before deployment in the production network.

Audit of configuration changes. Best practices call for specific manual and automated audits of configuration changes. [redacted].

Prioritization of upgrade-related alarms. [redacted]

Automatic configuration rollback. Automatic configuration rollback was not configured on both the core and distribution routers[10]. Such a mechanism would return the router to a previous configuration in case the engineer who is performing the upgrades loses access to the router prior to confirming the upgrades, and after a certain time-lapse from entering the commands. For the July 2022 outage, it is unclear if automatic configuration rollback would have helped in the case of the distribution routers.

Limited access to vendor support. Presence and direct involvement of [redacted] routing expert engineers would have been key in auditing configuration changes and troubleshooting. The vendors were not actively involved in the early stages of the outage. [redacted]

[redacted]

Effect of implementing multiple changes. Multiple configuration changes were planned during the same maintenance window[11]. This adversely impacted outage recovery efforts as it made it difficult to decide which NCT to rollback. Multiple configuration changes contributed to misdiagnosing the root cause in the initial hours of the outage. Thus, technicians initially focused on the core routers rather than taking a holistic view that considers the distribution routers given the context of the changes.

6.3.2. Incident management process

Incident management is a systematic approach to identifying, responding to, and resolving incidents that affect network services. It is designed to minimize the impact of incidents on users by restoring normal service as quickly as possible. Below is our assessment of the Rogers incident management processes and how Rogers responded to the incident once the outage occurred. Specifically, the speed of identifying the outage root cause and time required to restore services indicates the effectiveness and efficiency of the relevant incident management processes.

Business continuity processes – execution. Rogers has a disaster recovery and a Business Continuity Program that encompasses a range of policies, protocols, and procedures backed by "a diverse team." The Business Continuity Program is supported by a centralized dedicated Business Continuity Team, a governing body, and localized departmental resources. According to Rogers, the Business Continuity Team undergoes annual training, continuous development, regular assessments, and formal incident response practices [10:Q54]. However, the July 2022 outage exposed deficiencies in the execution of business continuity processes (e.g., limited number of SIMs for communication and lack of backup connectivity). [redacted]

[10] As informed by Rogers in a call on 1 September 2023.
[11] These changes were not detailed by Rogers, but could be inferred from the timeline and Rogers' responses.

Business continuity processes – incident management. Rogers has stated that it has a comprehensive incident response process for the NOC. Rogers classifies incidents into three levels based on specific criteria, such as disruption to infrastructure, financial impact, risk to the safety of employees, customer impact, and estimated impact duration [12:Q68].

Each incident level leads to a predefined response and team. Rogers has stated it follows a structured approach that directs tactical and operational responses by activating the appropriate crisis management team, cross-functional incident management team, and departmental incident management teams based on the incident's classification.

Incidents classified as Levels 2 and 3 are considered particularly disruptive and classified as "critical." In such incidents, the Network Operations incident management team is convened under the command of the NOC National Network Management Director, who will activate the Emergency Operations Centre (also known as the "war room") and launch the critical incident management plan.

Rogers appropriately classified the July 2022 outage as Level 3. Such classification requires full staffing of the Emergency Operations Centre and the involvement of outside stakeholders (e.g., vendor assistance, 911 ecosystem partners, etc.). However, the process of calling and assembling staff at predefined points was hampered since most Rogers staff were relying on Rogers wireless and wireline networks that were in outage.

Emergency preparedness. [redacted]

Decision making and interdepartmental workflow. During the early hours of the outage there were certain deficiencies in how different departments within Rogers interacted. While this may be due to limited communication among staff, it could point to other deficiencies in how different departments interact with each other.

The incident management team identified two network change tickets as the possible root cause of the outage:

[redacted]

Backup connectivity to remote locations. There was no backup connectivity link to the NOC and to other remote locations. This delayed access to critical network elements that had to be physically accessed by dispatching personnel to specific sites. The lack of backup network access to the NOC and remote locations indicates that the disaster recovery plan had not been thoroughly practiced and tested.

Limited communication among Rogers staff. The outage hampered communication among Rogers technical staff who were not equipped with an adequate number of mobile network access lines from another service provider to use in the case of such a network failure. Rogers obtained SIM cards from other mobile network operators and physically dispatched them to locations to allow

Rogers staff to communicate with the war room a few hours after the start of the outage. Even late on 8 July 2022, staff were being dispatched to bring in the necessary resources.

[redacted]

Delayed or lack of vendor engagement. [redacted]

Root cause analysis report. [redacted]

Physical access to data centres and infrastructure nodes. Rogers staff reached the NOC 2h7m from the outage start. It is not clear when staff arrived at other remote sites and data centres; however, Rogers stated that it dispatched alternate carriers' SIMs to remote sites close to five hours from the start of the outage. This is a relatively long time, given the criticality of the outage. Best practices require physical presence in proximity of remote sites if they are deemed critical for the overall infrastructure.

Prioritization of service restoration. Rogers assigned the highest priority to restoring wireless services according to the following priority order:

1. Wireless service
2. Wireline services
   [redacted]

With over 10 million wireless subscribers, Rogers was justified in focusing first on restoring wireless services to enable the largest number of customers to access 9-1-1 services.

Wireline services were next on the priority list followed by [redacted]

Rogers noted that many critical care services and major infrastructure customers have backup connectivity. Provisioning such backup is always part of good operational practices for such a category of organizations.

6.3.3. Communication with external parties

Effective external communication - timely, accurate, clear and concise, consistent, and empathetic - is essential for a successful incident response. Customers and partners need to be kept informed of the situation so that they can take appropriate action. The section below evaluates Rogers communication with customers and partners during the July 2022 outage.

Notifications related to emergency services and alerts. Rogers notified the 9-1-1 network providers four hours after the outage start. Rogers sent one update message to 9-1-1 network providers before service was restored on 9 July 2022. Rogers argued that the NOC did not have any connectivity, which precluded earlier notification. As such, 9-1-1 network providers were notified "as soon as Rogers NOC was able to establish communications and identify the specific impacts." [7:Q11]

Regulatory Policy CRTC 2016-165 does not directly address 9-1-1 outages that are caused by a failure at the originating network. Telecom Decision CRTC 2017-389 [3] excludes the recommendations of the Emergency Services Working Group related to origination network outage notifications [4]. While there was no mandatory requirement for Rogers to notify 9-1-1 network providers, there are calls by different industry forums for originating network providers, such as Rogers in this case, to notify 9-1-1 network providers in a timely manner. For instance, the Emergency Services Working Group recommends that [4]:

1. The originating network provider(s) must notify the 9-1-1 network provider as soon as possible.
2. The notifying originating network provider(s) should provide any material updates to the 9-1-1 network provider as soon as they are available.
3. The notifying originating network provider(s) should communicate to the 9-1-1 network provider the resolution of any reported originating network 9-1-1 trouble.

Additionally, we point to the Federal Communications Commission's (FCC) Second Report and Order on Improving 9-1-1 Reliability of 18 November 2022 [5]. The FCC requires originating network providers to "notify 9-1-1 special facilities[12] of outages as soon as possible, but no later than within 30 minutes of when the outage that potentially affects 9-1-1 service is discovered." The FCC sets additional requirements on the means of communications: dual requirement by phone and by email as well as the content and frequency of the updates (two hours).

Rogers took even longer to notify Pelmorex of the outage. In fact, it was Pelmorex who first reached out to Rogers following a media report of the outage. Here also there are no mandatory requirements by the CRTC for Rogers or other originating network providers to notify the NAAD administrator.

The lengthy time that elapsed before notifying 9-1-1 network providers and the NAAD administrator, as well as the way notifications happened, indicates that a well-thought-out communication plan with these external parties was either missing in the Rogers incident management plan or not followed. Notification to 9-1-1 network providers and the NAAD administrator does not have to come from the NOC, but from a person designated by Rogers for such practices. While the outage was severe and required much attention from Rogers to restore its services, access to alternative means of communication as well as practicing different outage scenarios would have been helpful to ensure a timely notification of 9-1-1 network providers, and, correspondingly, the PSAPs and the NAAD administrator.

[12] Any entity that provides 911, E911, or NG911 capabilities such as call routing, automatic location information, automatic number identification, or the functional equivalent of those capabilities, directly to a PSAP.

Customer communication. Rogers first notified its customers of the outage through a post on Twitter at 8:54 EDT, [redacted]

Additional messages to Rogers, Fido, and Chatr customers followed over the course of the day using different channels including:

- Social media: Twitter, Facebook, and Instagram
- Customer support through interactive voice response to Rogers and Fido customers
- Rogers, Fido and Chatr homepage, support, and outage hub banners
- Community forums
- Technical support live chat
- Public service announcements through Rogers Sports & Media radio stations and their websites.

The messages were general in nature and did not provide any detail related to the nature and severity of the outage. More importantly, Rogers did not communicate how customers could access emergency services during the outage (e.g., not to disconnect the call early, or to remove SIM cards from customer cell phones to access a third-party network).

Business customer communications. Rogers for Business was not able to communicate directly with business customers. Some employees with alternate home connectivity were able to set up an automatic reply [redacted]

Delayed coordination with third-party operators. [redacted]

Communication with the telecom/Internet community at large. Rogers shared some information about the causes of the outage with other telecom operators at the Canadian Security Telecommunications Advisory Committee (CSTAC). We also note that many telecom operators who experienced major outages have made detailed explanations to the wider Internet community via specific forums, such as the North American Network Operator's Group (NANOG) or the Internet Engineering Task Force (IETF), with the goal of sharing insights and helping other network operators avoid similar outages.

7. Post-outage improvement decisions analysis

Following the outage, Rogers undertook several measures to improve its business and operational processes and to make changes to its network architecture. Some of these network resiliency improvements are directly related to addressing the causes of the July 2022 outage and to prevent similar contributing factors from causing a service outage in the future. Others are driven by corporate business and technology strategy such as the evolution of the wireless network to 5G technology. This section outlines and assesses the potential merits of the improvements Rogers has made to enhance network resiliency.

7.1. Network architecture and resiliency improvements

Public wireless and wireline networks are designed with specific resiliency objectives. Achieving such objectives requires a continuous assessment of all the architectural dimensions that do impact resiliency, including technology choices, solution providers selection and operational deployment and support. This has a direct impact on capital and operational costs. Deciding on what to implement leads to specific trade-offs that need to be analyzed. Rogers has decided to implement several architectural changes to address the root causes of the outage as well as prevent broader outages. They are described below, along with our assessment of their effectiveness.

Routing overload protection. The overload of routers in the Rogers network resulting from a router misconfiguration is the root cause of the July 2022 outage. Routing overload is the sudden flooding of routing data sent to the router that exceeds a router's capabilities to process. This generally leads to the router failing and being unable to route any traffic. [redacted]

Our assessment is that the routing overload protection mechanisms that Rogers has implemented are fundamental to preventing a similar outage from occurring in the future. A continuous audit of such mechanisms by Rogers, along with their vendors, is required, as technology and corresponding network architectures evolve.

Signaling storms overload management. A signaling storm within a mobile network refers to a sudden and unanticipated increase in signaling traffic. Signaling storms occur for various reasons, such as when many devices simultaneously attempt to connect to the network following a network outage. During the July 2022 outage recovery process, Rogers implemented one of the most important lessons from its April 2021 outage - that of pre-emptive throttling or the gradual adding of subscribers to avoid signaling storms as the mobile network recovers from outage. This led to a smoother progressive recovery of network services during the July 2022 outage. Signaling storm management is a critical aspect of recovery from outages that should be part of any network traffic management.

Our assessment is that Rogers has put in place appropriate signaling storms protection mechanisms and deployed them successfully during the outage. Such

mechanisms need to be continuously tested and evaluated, as this is one of the most common root causes of outages for mobile network operators.

Wireline-wireless IP core network separation. Rogers wireless and wireline networks share a common IP core network that acts as a conduit for user traffic to the Internet and network services. Implementing separate IP core networks for the wireless and wireline networks helps to contain an outage to its respective access network and, therefore, avoids the type of catastrophic network failure experienced on 8 July 2022, where both wireless and wireline services were unavailable due to the outage in the common core IP network. The underlying assumption for avoiding a common outage in both the wireless and wireline networks with separate IP core networks is that specific upgrades to the wireline and wireless network are not occurring simultaneously with the same effects. Therefore, if one IP core network were affected by an outage, the other IP core network would remain unaffected and operational.

IP core network separation is a strategic decision that should be viewed in context of Rogers overall business objectives and not solely from the perspective of the July 2022 outage. It is first and foremost a trade-off decision among costs, resiliency, and operational complexity. We note that multiple large telecom operators have converged wireline and wireless cores.

Rogers states that an independent wireless IP core network would improve its wireless network performance and resiliency. According to Rogers, the benefits of the new wireless IP core network include [12:Q70]:

A. Provide new wireless experiences with improved quality of service.

B. Support mobility features such as seamless handover and session continuity across regions to enhance customer experience and reduce latency.

C. Leverage modern automation workflow tools to build out the dedicated IP network and data centre.

D. Streamline maintenance window work activities with operational governance dashboards.

E. Provide end-to-end automation and orchestration functions.

Our assessment is that the split of wireline and wireless core networks has benefits in terms of fault isolation and resiliency but comes at the expense of an increase in management functions and network costs. The separation would help Rogers avoid a simultaneous wireless and wireline IP core outage as experienced in July 2022.

Mutual redundancy between the wireless and wireline core networks. Rogers has decided to both physically and logically separate the wireless and wireline IP cores. Rogers is in the process of assessing the potential where the IP core of one access network would serve as a backup for the other access network in case its IP core network fails. For example, the IP core for the wireless network

would act as a backup for the wireline network in case its IP core fails, and vice versa. Rogers mentioned that it is in process of evaluating network designs, and that there is no timeline for the implementation of this redundancy model.

Our assessment is that a mutual redundancy between the wireless and wireline IP core networks would increase resiliency and would better address some failure scenarios. However, mutual redundancy requires careful designs, and comes with increased implementation complexity in terms of redundancy, network capacity engineering and traffic management.

Increased resiliency of the management network. [redacted] As a result, Rogers staff were unable to remotely access network elements during the outage. This hampered their efforts to identify the root cause of the outage and to quickly take recovery and service restoration measures. Post-outage, Rogers introduced the following improvements to remediate this deficiency:

1. Implemented a separate physical and logical management IP network called the [redacted] which is used to connect to all network elements for in-band and out-of-band management. [redacted] has its own core, distribution, and access layers. [redacted] which has diverse and redundant connectivity [redacted] network elements can be accessed both in-band and out-of-band, like production network elements [9:Q8].
2. Upgraded the [redacted] improve redundancy, resiliency, regional failover, and latency [13:Q67, 12:Q77].
3. For the [redacted] locations, Rogers implemented an out-of-band management network with connectivity sourced from third-party service providers. Specifically, this connectivity extends to the console infrastructure interfacing with the network elements.

A management network with dedicated data path infrastructure offers several benefits, including:

A. **Traffic isolation**: A separate management network isolates low-bandwidth management traffic from high-bandwidth user traffic and ensures that the types of traffic do not compete for bandwidth.

B. **Security and access control**: It is easier to secure a separate management network than the transport network (data plane) because the management network is not typically accessible to users or applications in the transport network. This could help reduce the risk of a security breach affecting critical network devices and services.

C. **Simplified troubleshooting**: A separate management network, both in-band and out-of-band, allows network administrators to continue monitoring, diagnosing, and troubleshooting the network in the event of an outage without being dependent on the production network.

Our assessment is that the use of the redundancy models is mandatory for network management as described above. These redundancy models shall ensure a rapid and efficient access to the NOC and network elements in case of outages. Our recommendation is to further enhance the redundancy with additional network access technologies, such as the use of non-terrestrial networks.

Network partitioning. Network partitioning is an approach that segregates, or partitions, the network into multiple regions to enhance network resiliency. Each partition operates as an independent unit, which helps to isolate faults and failures to a specific region, thus preventing them from affecting the entire network. Rogers networks are partitioned into multiple regions as would be expected to enhance network resiliency (isolate faults) and improve user experience (optimize traffic flow, reduce congestion).

[redacted]

A further differentiator from the pre-outage architecture is in the design of the service delivery core (e.g., IP Multimedia System, short message service, Internet gateway). Rogers has strengthened the resiliency of the service delivery core by implementing:

1. Per-region mobile core with physical and geographical redundancy within and between each region [9:Q7].
2. Per-region key IP elements such as route reflectors, network-to-network interconnects at the interface of wireline and wireless service networks, and Internet gateways dedicated to both wireline and wireless networks.

Our assessment is that this architecture would improve resiliency through better isolation of potential failures within a region and reduce the risk of other regions being affected [7:Q2c]. We note that Rogers already had several logical partitioning mechanisms during the July 2022 outage, but the nature of the outage limited their effectiveness. We suggest that, over time, Rogers carefully analyze and assess the implementation of other ways of logically partitioning the network such as introducing routing hierarchies.

Other network resiliency improvement. Post July 2022 outage internal assessment and engagement with its vendors, Rogers undertook additional measures and planned to introduce additional features in the IP network to enhance network resiliency [9:Q16, 13:Q66]:

1. Features and measures that were implemented or are in process of being deployed:

    [redacted]

Our assessment is that the resiliency enhancements proposed above have a direct impact on enhancing not only resiliency, but also cybersecurity and network scaling. More importantly, the process with which these enhancements have been

decided, including working closely with network vendors, should be a continuous improvement process within Rogers, especially as network technologies are rapidly evolving which require prompt adaptations of network resiliency mechanisms.

Network monitoring. [redacted] Fault events and alarms assist engineers with troubleshooting and identifying the root cause of failures. Rogers has upgraded its current suite of network management tools to: 1. expand the scope of network event monitoring and system event logging; and 2. make network management tools available to a larger number of users. Rogers also acquired a new capability to correlate and monitor in real-time routing telemetry, traffic, and performance analytics [12:Q63].

A summary of network monitoring adaptations includes:

[redacted]

Our assessment is that the newly acquired tool and enhanced existing monitoring tools would improve Rogers ability to prevent outages and to better identify causes of errors in network operations. However, we suggest that Rogers progressively evolve the tools it uses to address ongoing network trends such as softwarization and virtualization which are top priorities for telecom operators.

Alternate carrier access for network management and operations. Rogers relied on its core network to connect its remote sites including its NOC, corporate offices, and broadcast centres. The July 2022 outage in Rogers IP core network had paralyzed Rogers internal and external communication, and hampered Rogers efforts to effectively and timely respond to the outage in its early hours. In response, Rogers deployed Internet connectivity from third-party ISPs at its sites to address the loss of communication in case its networks suffer an outage. This includes the following facilities:

[redacted]

Rogers is also in the process of evaluating the use of backup satellite connectivity for strategic locations [10:Q73].

Our assessment is that provisioning the NOC and other remote sites with connectivity from third-party telecom network operators provides an adequate level of network management redundancy and will increase network resiliency. We suggest that Rogers augment this with satellite connectivity for network locations that are deemed most strategic.

MoU on Telecommunications Reliability. Rogers cited being a signatory to the September 2022 Memorandum of Understanding (MoU) on Telecommunications Reliability. The MoU was completed at CSTAC at the request of ISED following the July 2022 outage. It represents a framework agreement among 12 major TSPs[13] on

[13] 11 service providers following the merger of Rogers and Shaw, and the acquisition of Freedom Mobile by Videotron.

emergency roaming, mutual assistance, and emergency network outage communications protocols for advising the public and government during major outages and emergencies.

1. **Emergency roaming**: Rogers established bilateral emergency roaming agreements with Bell, TELUS, SaskTel, Eastlink, and Videotron/Freedom covering 9-1-1 emergency services and voice roaming [10:Q65]. These agreements would have detailed the emergency roaming mechanics, type, and quantity (i.e., number of subscribers, sessions, or amount of traffic). Emergency roaming is subject to approval of the counterparty service providers and the available capacity on their networks for roaming customers. With over 10 million Rogers wireless subscribers being out-of-service nationwide during the July 2022 outage, it is unknown whether the other service providers would have been able to accommodate the Rogers request for emergency roaming given the large influx of users, even if data services are not enabled and service is restricted to 9-1–1 and voice only. While the concept of emergency roaming is rather simple, its implementation could prove challenging in emergencies and outages. This would be an area that the wireless ecosystem including operators, vendors and regulators could collaborate on its effective implementation. We note that a few regulators around the world have been calling for disaster roaming[14], and that the 3GPP standard setting body began working on it in Release 17[15] [17].

2. **Mutual assistance**: The Mutual Assistance Protocol allows a service provider to extend assistance to another service provider that is experiencing an outage or emergency. This includes, for example, sharing physical assets, equipment, or human resources among other assets. The benefits of mutual assistance in the context of the July 2022 outage are largely out-of-scope, although there could have been small niches of benefits that could not be assessed due to myriad technical, procedural, and business considerations into which there is no visibility.

3. **Emergency network outage communication protocol**: This protocol sets guidelines for communicating network outage information to the public and to government authorities (e.g., CRTC, ISED, and Ministries of Emergency Preparedness and Public Safety). The guidelines include:

[14] South Korean operators enabled disaster roaming in 2020 based on a pre-standard implementation. The agreement stipulates disaster roaming service availability within 1 hour of an outage. Users of 4G and 5G networks would automatically roam on another service provider network.

[15] 3GPP calls the feature Disaster Roaming, which, as defined in Release 17, applies to radio access network nodes being in outage while other parts of the network are functional. The standard covers roaming for emergency services and broader subscriber voice and data services. We expect future releases to broaden the outage scenarios to consider other types of failures.

A. Informing the public of network outage with information that must include the impact on 9-1-1 services: this aspect was missing from the Rogers July 2022 outage communications.

B. Setting a target of two hours to inform the public from the time a service provider invokes the state of a critical outage. In our opinion, this is a relatively long time since one needs to add the time between the inception of the outage and the declaration of a critical outage. In the July 2022 outage, there was no official time for the declaration of a critical outage. We do note that the Rogers incident manager initiated a conference call 47 minutes after the outage trigger point; and the Rogers CTO reached out to his counterpart 1h17m from inception. Hence, it could have taken about 3 hours from inception to send the first public notification. Furthermore, we note that the MoU provides no specifics on the frequency of outage status updates.

C. Inform government authorities within 2 hours of "becoming aware" of the outage.

The MoU does not include any guidelines on communicating with other stakeholders such as PSAPs and the NAAD administrator. It outlines a set of broad commitments that are subject to each service provider's outage response plan.

Our assessment is that the MoU is a good first step to ensure adequate roaming during disasters and emergency situations, and that Rogers has successfully put in place agreements with specific third-party roaming operators. However, network failures vary in nature, including the type of elements that fail and the scope of the failure (e.g., failures in the access network or in some elements of the core network). This necessitates different technical requirements on the network infrastructure and user devices to enable emergency roaming. Specifically, it is necessary to validate scenarios that require user devices compliance with end-to-end roaming specifications under specific failure scenarios. For example, if the radio access network is operational whereas the core network is down, which requires end-user devices to support specific signaling messages that force the devices to scan alternate networks for roaming and complete emergency calls. It is also important to audit emergency roaming implementations to ensure that it would be effective.

7.2. Change management improvements

Rogers enhanced its change management to address deficiencies in risk management, planning, processes, and organization. Following is our assessment of the change management improvements that Rogers has made.

New risk assessment algorithm. Rogers developed a new algorithm to assess and classify the risk associated with a change in network elements, software

upgrades, or configuration [11:Q53]. The new risk assessment method comprises two steps:

[redacted]

The new risk assessment algorithm would have identified the classification of the NCT that led to the July 2022 outage as "High risk" as the change would have been of "restricted" type, which requires more stringent audit and approvals from the Rogers technical hierarchy. Thus, the new risk assessment algorithm is more comprehensive in that it considers additional parameters that affect network change risk. However, this is a complex algorithm that could only be judged when put to the test.

Our assessment is that the new risk assessment algorithm would help increase the level of diligence when applying specific network changes. Our suggestion is to continuously monitor and adapt the algorithm to address changes in network technologies and new deployment models.

Organizational improvements. Rogers made the following improvements:

[redacted]

Enhanced collaboration between operations and engineering teams would help in identifying potential faults prior to committing configuration changes, as well as in improving potential problem resolution. Vendor resident engineers would help reduce the time to engage vendors to provide support to Rogers staff in case of network failures [12:Q68] [redacted]

Our assessment is that a close interaction with vendors is fundamental to improving network resiliency at the design and deployment stages. The remaining organizational changes are also positive; however, their impact would depend on how well they are implemented. For instance, it is important to ensure that communication overhead between the different teams is efficient to not slow down the execution of tasks.

New product introduction process. Rogers follows a standard process for new product introduction/new technology introduction (NPI/NTI) in its wireless and wireline networks. The process, which is based on a stage gate framework, is typical and common to large telecom operators.

Rogers includes network software upgrades and configuration changes into the stage gate framework. For configuration management, which is part of the root cause of the July 2022 outage, Rogers follows a [redacted] framework spanning concept and definition through solutioning, testing, and deployment [11:Q46, 13:Q72].

The NPI/NTI framework that Rogers presented as governing configuration management is a high-level process that leaves many details of the actual configuration management process specific to the July 2022 outage undisclosed.

For example, the framework process presented by Rogers includes testing. However, the actual configuration process may not deem testing necessary if the change is low risk, which, incidentally, was the case for the July 2022 outage, where the configuration change responsible for the outage was assessed as low risk. As another example, configuration changes would require audits and approvals at various levels and functions within the Rogers organization. This varies depending on the nature of the change, something that the framework does not identify. In short, the NPI/NTI framework is valid, but it is the processes within the framework, and the execution of these processes, that are critical.

Our assessment is that incrementally evolving the new product introduction processes based on learnings from this and previous outages is positive in increasing network resiliency. However, this will depend on how these processes are implemented given that their description remains at a high level.

Improvements in implementing network changes. Rogers introduced two improvements to how it executes network changes during the maintenance windows to minimize risk [12:Q68]:

1. Introduced a new classification for the type of changes:

[redacted]

We note that during the July 2022 outage, there were multiple changes (an unknown number, as no confirmation of the details of all the changes was provided by Rogers). [redacted]

Our assessment is that the above improvements help to ensure that the riskiest network changes would undergo a more in-depth review. The decision on what changes would be subjected to closer scrutiny depends on the risk assessment procedures. Hence, it is suggested that a continuous audit and update of the risk assessment procedures be implemented.

Automation. Rogers has introduced automation to streamline the change management process to eliminate potential manual procedure related errors and speed up the process, such as:

[redacted]

[redacted]

Our assessment is that automation will play an increasingly important role in improving network resiliency. The actions taken by Rogers to leverage specific automation tools are positive and would help prevent possible future outages. We suggest that Rogers continuously audit these automation tools to ensure they do not become the root cause of possible outages due to automation errors or automation based on non-optimal data.

Lab testing in configuration change management. The change management Risk Index that Rogers implemented after the July 2022 outage includes lab testing as a measure to reduce the risk level of the change [11:Q53].

Rogers indicated the following types of testing:

[redacted]

Following the April 2021 outage, Rogers worked to ensure that the lab replicates the wireless network production environment and adopted continuous deployment processes for software solutions [12:Q61]. [redacted]

Lab tests would help to reduce the risk of introducing new elements, software, and configurations into the network. The effectiveness of lab tests would depend on their scope, i.e., the breadth (or coverage) and depth (or rigor) of the tests, as well as the ability to reproduce the production environment in a lab setting. Rogers would be able to avoid future outages from similar types of configuration changes provided the test regime in its laboratories is comprehensive, which is not possible to assess for this report.

Our assessment is that evolving the test methodologies, tools, and equipment is a positive step to prevent future network failures. However, the complexity in achieving optimal testing is in replicating the production network in a lab environment and in simulating a large set of possible fault scenarios. Our suggestion to Rogers is to focus on solutions that address these two challenges.

7.3. Incident management improvements

Preparedness. Rogers stated that it bolstered its incident management guidelines to encompass various outage scenarios such as voice outage/call delivery failures, wireless 9-1-1 call failures, wireline Cable Modem Termination System outages, fibre cuts, severe weather, broadcast/channel outages, Ignite TV streaming outage, third party service outage, switch control provisioning outage, and call centre connectivity/offline outage [12:Q68]

Additionally, Rogers stated that it carried out several tabletop drills involving speculative situations. During these drills, team members rehearsed incident response actions, role-played communication procedures amidst an incident, and verified the improved response strategies and manuals [12: Q68].

The above activities, if carried out diligently, should enable Rogers to proactively identify gaps in procedures and tools before outages occur, and to consequently implement the necessary corrective actions. For instance, Rogers incident management guidelines prior to the outage included drills, but the drills failed at identifying critical shortcomings such as lacking communication methods among personnel and for NOC backup connectivity. Hence, it is imperative that the scope of emergency training be encompassing, and that exercises and drills be an integral part of emergency preparedness to fully test the performance of the incidence

response. It is also imperative to have an exhaustive categorization of potential outage root causes, with well-defined impacts, driving the structure of the drills.

Our assessment is that improving preparedness to address outages is positive and would ensure better incident management when outages occur. It is important to ensure that the drill scenarios are broad enough to cover a large set of potential outage root causes, especially considering the fast-evolving network technologies and deployment models.

Protocols and organization. Following the July 2022 outage, Rogers has made several enhancements to streamline the incident response effort, primarily:

1. Using fewer conference bridges;
2. Assigning well-defined leadership roles; and
3. Creating new guidelines for the nomination and election of incident manager and technical prime roles during incidents.

Our assessment is that these new protocols are positive and provide an efficient mode of accountability during emergency situations. However, their effectiveness will depend on how they are implemented in real-world scenarios.

Prioritization of alarms during outage. [redacted]

Our assessment is that alarm prioritization is an important step in speeding up the diagnosis of network faults and helps with improving overall network resiliency. We suggest that Rogers continuously audit the type of alarms, their prioritization, the corresponding alarm data aggregation, and insight techniques for optimal effectiveness.

Data centres related resiliency. [redacted]

Our assessment is that the data centre redundancy design is adequate and positively affects network resiliency. We suggest that Rogers complement such designs with the relevant data centre resiliency audits using the appropriate standards to avoid single points of failures that could adversely affect network operations.

9-1-1 incident management enhancements. Rogers has enhanced its 9-1-1 incident management along two dimensions. The first dimension includes [redacted]. The second dimension includes emergency roaming agreements with mobile network operator signatories to the ISED MoU on Telecommunications Reliability [16]. These agreements allow Rogers to conditionally transfer customers to an alternative operator in qualified critical emergencies (i.e., the nature of the outage impacts the implementation of these agreements). Emergency roaming is a best effort service subject to acceptance of the alternative operator based on available network capacity among other factors. Emergency roaming requires a technical implementation that may or may not have been completed by Rogers and its partners [19]. An illustrative example of that would be the validation of handsets

and end-user device behaviour in situations where the radio network is operational but the mobile core network is not. In such a case, user devices would need to support signaling messages that inform the devices of the unavailability of emergency calling to trigger the devices to scan for alternative networks to complete roaming emergency calls.

Rogers has provided its recommendations for measures to improve network resiliency and reduce the impacts of outages in relation to 9-1-1 and public alerting in response to CRTC Network Working Group Task Identification Form NTFF044 [20]. In its response, Rogers highlighted improvements to enhance the reliability and resiliency of its emergency services, of which the most relevant include implementing default routing to third-party call centres and establishing new broadcast centres and alert system connections to NAAD for better public alerting. Rogers also suggested additional measures, including mandating the support of non-service initialized 9-1-1 by all TSPs, implementing 9-1-1 calling over satellite as backup option, enabling voice over Wi-Fi calling by default, notifying customers using various communication channels during an outage, and mandating wireless service providers to maintain dedicated webpages on 9-1-1 access and public alerts.

Our assessment is that these 9-1-1 enhancements are positive to improve the resiliency of emergency services. However, the various enhancements are still at the analysis stage (e.g., ensuring that the handsets already in use would be able to roam in the case where the radio network is up and the core network is down). Decisions need to be made as far as what to implement and deploy and, more importantly, how to audit such implementations.

Automated rollbacks. Rogers implemented automated rollback to previous configurations when new changes were not successful on the core routers. Automated rollback is an important tool for the incident management process that was missing in the July 2022 outage. Rogers deployed new tools to assess whether rollbacks are required [15:Q14]. [redacted]

Our assessment is that implementing appropriate configurations rollbacks does improve network resiliency. [redacted]

Communication protocols. Rogers stated that it enhanced and implemented new measures to improve its communication protocols. Primarily, Rogers stated that it has implemented a "specialized Corporate Communication playbook" that addresses [10:Q73]:

- Ownership and responsibilities;
- Use of various communication channels;
- Communication cadence (frequency) across channels; and
- Communication content based on timing and severity of the outage.

The communication playbook applies to different segments [10:Q54, 15:Q2], including:

- **Internal communications**
- **Retail customers**: Rogers created new templates for consistent communication; increased staffing and enhanced guidelines; integrated a list of Rogers, Fido and Chatr customers into its CRM and third-party messaging platforms; invested in the [redacted] dashboard to track impacted wireline home service; implemented real-time online outage maps; and enhanced self-service options.

  In its response to a 22 August 2022 RFI, Rogers proposed making changes to its emergency service webpage[16] (Q14.A) [7]. The proposed changes provide information to customers on how to access 9-1-1 services during an outage. Rogers implemented these changes on its website sometime between 21 June 2023 and 30 August 2023.
- **Business customers**: Rogers extended Salesforce Customer Communities Portal to all its business customers. Rogers Business Major Incident Playbook, defined where the incident impacts over [redacted] customers, now includes communication via email and [redacted] online ticketing systems.
- **Government stakeholders**: Rogers implemented an interim notification process with the CRTC by email and through GCKey within two hours of being aware of a "major service outage." This measure is required on an interim basis according to Telecom Notice of Consultation CRTC 2023-39 [21].
- **Pelmorex**: Rogers initiated a voluntary notification process to promptly notify Pelmorex by email in case of an incident of the highest severity (i.e., an incident that is expected to result in long-term impact to Rogers customers, brand, or reputation).
- **9-1-1 network providers**: Per Rogers criteria, high-severity incidents that impact 9-1-1 services would trigger a notification to 9-1-1 network providers. The notification is by email with specific guidelines (e.g., high importance with read receipt confirmation). Rogers would request the ILECs to relay the message to PSAPs. Rogers would update the ILECs regularly at hourly or mutually agreed upon times.
- **TSPs and EMOs**: Rogers notifies TSPs of an outage on an as-needed basis at its discretion. Rogers notifies EMOs of an incident of the highest severity using a predefined template like that for 9-1-1 network providers.

[16] Rogers emergency services webpage is available at: https://www.rogers.com/support/mobility/911-emergency-service#tips-%26-reminders-for-calling-9-1-1-in-the-event-of-a-network-outage

To maintain communication capabilities during outages, Rogers has taken/is undertaking the following measures [10:Q55]:

1. Broadened the distribution of third-party SIM cards to all incident response and crisis management team members for backup communications.
2. Established redundant Internet access through third-party ISPs to its different sites [redacted]
3. In process of evaluating the viability of satellite connectivity for critical strategic locations across Canada, as an additional backup option to guarantee communication availability.

The above measures should help Rogers be more responsive in informing the different stakeholders.

Our assessment is that the various improvements in communication guidelines are sufficient. We suggest that Rogers continuously test and audit these communication models for continuous improvement. This is particularly important as the type, scale, and impact of network outages vary.

7.4. Capital expenditures

Following the outage, Rogers stated that the split of the wireless and wireline IP core network would cost $261 million, and that it would spend an additional $11 billion over three years to build out and strengthen its network[17].

It is important to note that the Rogers capital expenditures currently are highly influenced by two factors:

[redacted]

7.4.1. Wireless-wireline network separation

Rogers planned to spend $261 million to physically separate the wireless IP core network. A new IP core would be architected and built for the wireless network, while the current IP core would remain for the wireline network. The project includes purchasing and deploying new gateways in different Rogers data centres. Rogers will provision redundant fibre optical transport between these locations. Additional expenses would be for new tools and automation in addition to design services, project management and other professional services.

[17] The original number is $10 billion stated by Tony Staffieri, Rogers' CEO, at Rogers' appearance before the Standing Committee on Industry and Technology on 25 July 2022. In its 22 August 2022 response to the CRTC's RFI [7] Rogers stated the amount is $10.905 billion. In this report, we round up to $11 billion when making a reference to this amount.

The separation of the two IP core networks would help contain an outage like that of 8 July 2022 to part of the network where the error originates. This would prevent a complete loss of services and reduce the impact on customers.

Rogers' IP core network, in its pre-outage architecture, is a conventional architecture that is typical of many service providers, including mobile network operators, fixed access, or converged fixed-mobile access service providers.

[redacted]

The separation of the wireless network is a strategic decision by Rogers that should be considered in broader terms than the July 2022 outage. Specifically, Rogers is in the process of deploying a 5G core and upgrading its cloud infrastructure to provide new services at higher levels of performance, such as lower latency. A separate wireless IP core network better positions Rogers to offer additional resiliency, albeit at an additional cost and complexity that results from operating two IP core networks, including the edge, core, Internet gateways and the various service and network layer interfaces between them.

7.4.2. Infrastructure expansion

Following the July 2022 outage, Rogers stated its plan to make over $11 billion investment in capital expenditures over the following 3 years to build out and strengthen the network. Table 3 shows the capital expenditures allocated to the wireless and wireline networks which is a slightly different representation of the information presented by Rogers where expenditures were allocated to the access and core networks.

[redacted]

The capital expenditures announced by Rogers would be incurred in the general context of business operations, network upgrades and improved resiliency. Some of these costs could be attributed directly to the July 2022 outage and improving network resiliency. This includes the $261 million for the cost of the wireline-wireless network separation and the tools to improve network monitoring and operational efficiency.

Access network expenditures. Rogers plans to expand the coverage footprint and upgrade the access technology for both its wireline and wireless access network for a total cost of [redacted] over three years. These expenditures would not help in mitigating the type of outage experienced on 8 July 2022. The access network equipment typically needs to meet minimum requirements set out by service providers in terms of availability (e.g., carrier-grade availability, mean time-to-failure). Hence, they do not represent a step beyond what is considered as part of normal operating procedures for service providers, Rogers included.

Core network expenditures. Rogers allocated [redacted] to wireline and wireless core network evolution. [redacted]

Parts of the core network upgrades contribute to enhancing network resiliency. However, it would be difficult to isolate these upgrades strictly in the context of the July 2022 outage.

Spectrum expenditures. [redacted] It remains that both diligence in implementing industry best practices for the change management process is critical in minimizing the likelihood of a similar critical outage and proficiency in executing the incidence response process is critical to minimizing the outage duration and extent.

Tooling. Rogers acquired new tools and additional licences to existing tools to improve network monitoring and operations management [12:Q63]. Following the July 2022 outage, Rogers acquired [redacted]. It also expanded the availability of several other tools it already uses to a larger number of staff to help with network monitoring and troubleshooting. Additionally, Rogers is setting up and validating a lab for the wireless IP core [redacted]. These tools and labs come at a cost for both software and hardware. These costs, which would be directly attributed to the July 2022 outage, were not explicitly disclosed by Rogers.

7.5. Summary of assessment and recommendations to Rogers

The July 2022 outage is not the result of a design flaw in the Rogers core network architecture. Architecturally, Rogers wireless and wireline networks are designed for expected Tier 1 service provide reliability and resiliency. [redacted]

The July 2022 outage uncovered deficiencies in Rogers change management processes and incident management processes. The error in configuring the distribution router, which caused a flood of route advertisements that crashed the core routers, is a failure in the change management process. [redacted] These network design choices include the architecture of the network management, which relied on the Rogers data network, the lack of backup connectivity solutions to access remote sites, and the specific router configuration in use to prevent routing traffic overload.

Table 4 summarizes the identified deficiencies that led or contributed to the July 2022 outage. The deficiencies are classified into the following categories:

- **Architecture**: Items related to Rogers' network architecture.
- **Change management**: Items related to the change management process.
- **Incident management**: Items related to the incident management process.
- **Operations**: Items related to network operations.
- **Other**: Items that are not in any of the above categories.

Table 4 Summary of identified deficiencies and corrective actions by Rogers.

#	Category	Description of identified deficiency	Corrective action by Rogers
1	**Architecture**	Resiliency of the management network; [redacted]	• Implemented [redacted] - a separate physical and logical management IP network. • Upgraded the network-to-network interconnect for [redacted].
2	**Architecture**	Lack of alternative connectivity to critical infrastructure sites including the NOC	• Deployed Internet connectivity from multiple third-party ISPs to the [redacted]. • Provisioned other key network sites, broadcasting service locations and corporate offices with connectivity from third-party providers.
3	**Change Management**	No adequate routing overload protection on core routers	• Implemented a limit for BGP redistribution into OSPF (core router configuration parameter). • Implemented a limit for the number of entries in the OSPF database.
4	**Change Management**	Ineffective audit and validation of new configuration parameters	• Engage operations team with engineering earlier in the design cycle. • Created a core engineering team to peer review configurations or software changes. • New classification of type network changes (“automated”, “restricted”) which would draw additional scrutiny. • New risk assessment algorithm could contribute to additional scrutiny.
5	**Change Management**	Limited systemic lab testing of configuration parameters prior to committing changes into production network	Revised the risk assessment algorithm for network changes. The new risk assessment algorithm includes lab testing and introduces a new change type [redacted] for more stringent reviews as a measure to reduce the risk level.
6	**Change Management**	[redacted]	[redacted]
7	**Change Management**	Inappropriate classification of the risk associated with the configuration change/network configuration ticket	Developed a new risk assessment algorithm to assess and classify risk of network changes. The new algorithm is fairly comprehensive; however, its viability could only be qualified when tested.
8	**Change**	Many simultaneous	• Implemented a limit on the volume of

#	Category	Description of identified deficiency	Corrective action by Rogers
	Management	changes in the same maintenance window without an accommodative rollback plan	change activities during the maintenance window. • Introduced a new classification for the type of changes.
9	**Change and Incident management**	[redacted]	[redacted]
10	**Incident Management**	[redacted]	Implemented an automated alarm prioritization solution to suppress unnecessary alarms for every type of change and allow staff to focus on important ones.
11	**Incident Management**	Limited number of third-party SIMs for key personnel	Broadened the distribution of third-party SIM cards to all incident response and crisis management team members.
12	**Incident Management**	Limited or ineffective training and drills for the incident management process (emergency preparedness in particular)	Carried-out tabletop drills involving speculative situations.
13	**Incident Management**	Automated rollback (specifically in situations when access to the network elements is lost)	Router automatic configuration rollback under investigation.
14	**Incident Management**	Communication protocols	Updated communication guidelines with defined ownership and responsibilities, communication channels, content and cadence for retail and business customers, government stakeholders, NAAD, and 9-1-1 network providers.
15	**Incident Management**	Comprehensive implementation of emergency roaming to address specific outage root causes	Rogers placed emergency roaming agreements with other mobile network operators. However, it is necessary to validate scenarios that require compliance of user devices with end-to-end roaming specifications under specific failure scenarios. It is also important to audit emergency roaming implementations to ensure that they would be effective.
16	**Operations**	[redacted]	• Acquired and deployed [redacted] tool which will help address this deficiency.

#	Category	Description of identified deficiency	Corrective action by Rogers
			• Purchased additional licences for other tools it already uses in network monitoring.

In the months since the outage, Rogers undertook several measures to address these deficiencies. One of the most critical deficiencies is the absence of router overload protection, which is at the root cause of the outage. Rogers has addressed this deficiency by implementing overload protection on its distribution and core network routers, which should prevent a similar outage from happening in the future provided these protection safeguards remain in place.

Architecturally, Rogers implemented a separate management network that improves the resiliency of its overall network. Together with backup connectivity to remote sites from third-party providers, Rogers would be able to access remote sites to respond to a similar type of outage more quickly than in July 2022.

Shortly following the July 2022 outage, Rogers announced that it will separate the IP core network for the wireless and wireline networks. This measure would help isolate a similar fault to the one that occurred in July 2022 to its respective access network. From that perspective, it would improve the network resiliency since the fault would not simultaneously impact the wireless and wireline networks. However, this measure is a design choice by Rogers that comes at an additional cost in both equipment and management.

Rogers enhanced its configuration management process by implementing several measures, including an improved change risk assessment algorithm, additional layers of audits and approval of configuration changes, improvements to its labs with new tools and expansion of licences of existing tools, and new SLAs with vendors to receive support from vendor resident engineers. These and additional change management measures are summarized in Tables 5 and 6 below.

Rogers also made enhancements to its incident management process to improve its response time to network failures. Enhancements include implementing an alarm prioritization solution to help staff focus on important network alarms, partial implementation of automatic configuration rollbacks for network routers, expanding the use of network routing monitoring tools, network data analysis tools and making available third-party SIM cards to a larger number of staff.

Table 5 summarizes additional measures made or announced by Rogers following the July 2022 outage. The measures are classified into the same categories as described for deficiencies above.

Table 5 Additional post-outage measures.

#	Category	Additional measures implemented post-outage	Assessment
1	**Architecture**	Wireline-wireless core IP network separation and network partitioning	A design choice that improves network resiliency by isolating faults to their respective access network, which precludes the catastrophic loss of both wireless and wireline networks as occurred in July 2022.
2	**Architecture**	Implemented/plans to implement features to improve resiliency: [redacted]	These enhancements help improve network resiliency and cybersecurity.
3	**Architecture**	Mutual redundancy between the wireline and wireless IP core networks, where the wireline IP core would act as backup for the wireless core and vice versa	Increases the level of redundancy of both the wireline and wireless networks and addresses specific failure scenarios (e.g., the wireless core down while the wireline core is operational). [redacted]
4	**Change Management**	Automation in parts of the change management process to translate Method of Procedures activity into an NCT	Automation could help reduce errors provided the right audits are implemented and followed.
5	**Incident Management**	Incident management response improvements: • Use fewer conference bridges • Assigned well-defined leadership roles • Created new guidelines for assigning key leadership roles during incidents	The measures would improve the coordination of resources and the corresponding response to resolve an outage.
6	**Incident Management**	Signed the MoU on Telecommunications Reliability	Emergency roaming agreements, mutual assistance and outage communication protocol contribute to streamlining collaboration among service providers during outages. However, since the MoU is non-binding and several of its measures are subject to bilateral agreements among the service providers, its effectiveness would have to be validated in an actual outage or stress scenario. Also, several technical implementations and corresponding validations need to be done.

#	Category	Additional measures implemented post-outage	Assessment
7	**Incident Management**	9-1-1 service access during outage	Rogers updated its Emergency Services webpage to include tips on how to access 9-1-1 services during an outage.
8	**Other**	Capital expenditures of $11.166 billion over the next 3 years	Largely unrelated to the July 2022 outage. A fraction of this amount could be attributed directly to improving reliability and resiliency. This includes $261 million for core network separation plus additional cost for tools and additional labs.

The combination of measures that Rogers undertook after the July 2022 outage is satisfactory to improve overall network resiliency and addresses the specific root cause of this outage. However, the severity of the 2022 network outage is primarily a combination of configuration faults and failure in processes. Hence, diligence in implementing existing or improved processes would be the most effective way to avoid a similar outage from occurring in the future and to improve the response to recover services when a failure does occur. In this spirit, Table 6 summarizes several recommendations that Rogers would benefit from to further improve its processes.

Table 6 Recommendations to Rogers.

#	Recommendation	Rationale
1	Develop a detailed root cause analysis document following network failures and outages	Root cause analysis document would help develop the appropriate contingency plans aside from the original purpose of the document of identifying the reason for the failure. Note that Rogers had provided a comprehensive root cause analysis report for the April 2021 outage, but not for the 2022 outage.
2	Ensure wide coverage and rigor in testing change configurations related to IP, wireless and wireline core networks	Lab tests help to reduce the risk of introducing new elements, software, and configurations into the network. The effectiveness of lab tests would depend on their scope, i.e., the breadth (or coverage) and depth (or rigor) of the tests, as well as the ability to reproduce the production environment in a lab setting. Rogers would be able to avoid future outages from similar types of configuration changes provided the test regime in its laboratories is comprehensive, which is not possible to assess for this report.

#	Recommendation	Rationale
3	Inform customers how to reach 9-1-1 and public alerts services during outage	Customers receiving specific information on how to access 9-1-1 and public alerts services during outages would help in mitigating the impact of the outage.
4	Institutionalize learning from own and other service providers' network failures to implement preventive actions, minimize network outages and enhance quality of service	It helps Rogers identify vulnerabilities and weak points within its networks to mitigate future risks and prevent similar incidents proactively. After the April 2021 outage, Rogers made considerable improvements to its change and incident management processes and hardened the mobile network, but these were not fully extended to the IP core network. The root cause of many infamous prolonged outages in communication networks worldwide was the lack of immediate access to failed network elements, and deficiencies in hardening systems to protect them from overload and congestion.
5	Expand the scope of incident management drills wherever possible to a level that is more comprehensive than "tabletop drills"	Including specific drills to address broad outages impacting major network services, as in the case of routing failures or DNS failures, would help prepare for these scenarios and ensures readiness if such outages occur.
6	Test emergency roaming with other operators to make sure the process is efficient - this is not only technical testing, but procedural as well	Defining specific test plans to address emergency roaming will ensure that the specified fault scenarios are handled correctly during outages and provide a platform to improve responses as technology and services evolve.
7	Share outage root cause and mitigation strategies with the wider Internet community represented by bodies such as NANOG	In addition to sharing lessons learned with Canadian telecom industry forums such as CSTAC, this recommendation highlights contributing to a broader Internet community of forums, with the goal of helping other operators prevent similar network failures.

8. Network resiliency recommendations for all carriers

In this section, we present a list of the key lessons learned from the July 2022 outage for the benefit of TSPs. We then provide a brief overview of key telecommunications network evolution trends that impact network resiliency. We conclude by outlining a few recommendations to further improve the reliability and resiliency of telecommunications networks in Canada in the context of evolving technology trends. These recommendations are not specifically addressed to Rogers, rather, they are meant to inform all service providers on means to improve network resiliency and reduce the probability of future outages and their corresponding impact on Canadians. Some of these recommendations are applicable immediately while others would need to be developed over the short-term horizon.

8.1. Lesson learned from the July 2022 Rogers outage

The important lessons learned from the July 2022 outage include the following:

1. Implement router overload protection in the IP core and distribution networks.
2. Separate the network management layer physically and logically from the data network.
3. Provision the network operation centre and other critical remote sites with a secure backup connectivity from third-party telecom network operators.
4. Ensure that the audit process for network configuration changes is effective and involves different teams within the organization, such as engineering, operations, and project management. It is also advisable to involve equipment vendors where the configuration changes pertain to critical infrastructure, such as the IP core network.
5. Conduct lab tests of planned configuration changes and ensure that the lab equipment and test scenarios accurately reflect the production network.
6. Carefully manage the number of configuration changes completed in a single maintenance window and leverage tools and processes for automatic rollback of configuration parameters.
7. Implement an automated alarm prioritization solution to suppress unnecessary alarms for every type of change and to allow staff to focus on the important alarms.
8. Provide critical staff with secondary means to communicate, such as SIM cards from third-party network operators.

9. Simulate and practice network failure and outage scenarios to uncover deficiencies in the network architecture and the incident management process.

8.2. Network technology evolution trends

Telecommunications networks are increasing in complexity over time as new technologies must coexist with legacy ones. The number of functions, or network elements, as well as the interfaces between them, is increasing. Moreover, the implementation of network functions is changing with consequences on the entire network lifecycle from planning and design to procurement, testing, operation, and maintenance. We present a few of the most significant developments that directly impact network and service resiliency. These developments must be carefully considered as telecommunications networks evolve over the coming few years.

Softwarization, virtualization, and workload distribution. Over the last decade, we have witnessed a rapid evolution in the design and implementation of telecom network functions. Hardware-based models have progressively evolved into software-based implementations for specific telecom network elements, which in some cases run over virtualized environments primarily in private clouds hosted by the telecom network operators themselves. This allowed the distribution of some network workloads in contrast with the traditional centralized deployment model (e.g., distributed virtual network functions for 4G and 5G packet core networks). Service providers had to balance trade-offs in performance, cost, functionality, and vendor readiness in deciding which network functions to virtualize and distribute. We are now witnessing a rapid deployment of such virtualized networking functions at scale[18]. Consequently, service providers need to manage and operate primarily software-based systems. This entails adopting techniques and processes such as continuous integration continuous delivery - a software development approach to optimize the software delivery and deployment process, making it faster and more reliable, via more frequent and automated testing, integration and deployment - and development, security, and operations models, which integrate security at every stage of the software development and deployment process, with the goal of increasing application security and deployment agility. Network virtualization also affects the network architecture and the distribution of network workloads, requiring specific approaches to monitor and address potential faults to ensure resiliency across distributed software environments.

Migration to telecom cloud platforms. Following the first wave of virtualization and cloudification of telecom network functions, we are now witnessing a migration of certain network functions to run on cloud platforms that could remain at the premise of the telecom service provider as private clouds, run on public cloud providers' infrastructure, or run on hybrid private/public clouds. This started with the OSS and BSS and was followed with the mobile core networks for some Tier 1

[18] Network function virtualization helps telecom network operators deploy and scale services with more agility, and provides higher flexibility for network deployment models.

mobile operators in addition to experimentation with radio network components running on cloud platforms. Given the increased dependency of telecom operators on cloud platforms, this trend, and specifically the leverage of public cloud providers' infrastructure, will have direct consequences on redundancy, availability, and resiliency.

Integration of artificial intelligence (AI) data models. Telecom network operators have traditionally deployed data lakes across multiple platforms and used various solutions to gain insights into different use cases such as customer management, network diagnostics and security enforcement. Data management in telecom networks, including data capture, ingest and storage, continue to evolve. In recent years, different AI techniques were introduced in various applications to improve the efficiency, reliability and predictability of networks; to optimize traffic management (e.g., identify and mitigate network congestion, and predict future traffic patterns); to detect and prevent cybersecurity attacks; to interact with end users (e.g., large language models for customer experience management); and to automate network maintenance tasks (e.g., configuration, provisioning and troubleshooting). The use of AI in telecom networks raises questions about how AI systems are used for automation and decision making including how AI interference and learning models are built, the integrity of the data used for learning and the knowledge base used for reasoning.

Convergence of terrestrial and satellite networks. The integration of non-terrestrial networks, specifically low earth orbit satellite constellations, into 5G and future 6G networks is one of the most significant developments in the evolution of telecom networks. Several mobile network operators are in the process of evaluating satellite to device connectivity. Different models are emerging including ones that support tight integration at both the network and service levels. This raises opportunities for building additional resiliency in telecom networks, especially for use in emergencies.

API models in telecom networks. New application programming interface (API) models have emerged to allow end users and application providers to interact directly with the network and service infrastructure. The GSMA Open API launched at the Mobile World Congress conference in 2023 is one example. API models are not a new development; however, the type of APIs, the services and scale of interaction and the level of interoperability raises challenges as to how API models will be managed, secured, and deployed at scale. Telecom network operators have the added responsibility of ensuring these models are deployed with the required service level resiliency and security requirements.

Network Automation and Orchestration. Network automation aims to enhance network agility, reliability, and efficiency while reducing operational costs and the potential for human errors. Automation applies to different tasks such as configuration management, change management, fault management, performance monitoring and security. Automation technology is rapidly evolving and is applied to different parts of the network, including API-driven application delivery automation,

orchestration of network services, and network provisioning automation. Ensuring the resiliency of automation systems and processes should be a priority for telecom network operators. This requires specific audits of the automation systems and the interaction models between the different network elements to ensure interoperability, SLAs satisfaction, and secure interaction.

Advent of quantum safe networking technologies. Quantum computer capabilities have been rapidly evolving, increasing the prospects of breaking public key infrastructure-based cryptography algorithms (PKI). Telecom network operators face a potential challenge to their security systems since they rely on PKI for a large variety of functions, including user authentication, data security, and routing protocols security. Quantum-safe technologies address the growing risk that existing encryption algorithms would be compromised by quantum computers. Several solutions are advanced to harden the security of telecom networks. For instance, Quantum Key Distribution addresses the exchange of encryption keys using interception-resistant quantum-based techniques. Another example includes post-quantum, or quantum-resistant, encryption and key exchange mechanisms such as the algorithms that the National Institute of Standards and Technology (NIST) is in the process of standardizing (NIST has selected four such algorithms by 2023). A few leading telecom operators have been conducting trials of quantum-based solutions in live commercial deployments. Some regulators are looking to mandate post-quantum security for sensitive communications. The evolution towards quantum-based security architecture would be a key component of network resiliency requirements over the next few years. Failing to address cybersecurity threats and evolving both security protocols and processes in the face of quantum computing threats would put the resiliency of telecom networks at risk in the case of security attacks.

8.3. Recommendations for enhanced resiliency

The aforementioned technological trends impact telecom network architecture, design, implementation, and operation. Accordingly, network operators would have to evolve their processes and technical capabilities. Regulators as well would have to evolve the regulatory landscape to accommodate such trends over the coming years.

Below, we highlight additional forward-looking recommendations considering state-of-the-art evolution of telecom networks and services. These recommendations are broad in nature and apply to all network operators. We structure them into technological and process recommendations. However, we don’t describe the specifics in this report given the complex implications of such technological evolutions.

8.3.1. Technological recommendations for TSPs

Non-geostationary orbit satellite networks. The recent developments in low earth orbit and medium earth orbit satellite constellations, and their respective

device ecosystem, augment geosynchronous orbit satellites for connectivity and provide a good complement to connect support teams during major outages in addition to providing additional redundancy for out-of-band management.

Direct-to-device satellite connectivity. The emergence of global-scale, low-earth orbit satellite constellation operators prompted device vendors and service providers to develop solutions to connect mobile phones directly to satellites. One example is Apple's emergency SOS service introduced on the iPhone 14 in 2022, which provides low-bit rate, low-capacity bidirectional text messaging service for emergencies. Other direct-to-device models are more ambitious, seeking to provide a few Mbps-grade throughput. Such solutions would complement terrestrial 9-1-1 calling and emergency alerts services in certain outage situations.

Future 3GPP disaster roaming standards. Regulators around the world are beginning to call for wider implementation of disaster roaming[19] among service providers due to the pervasive nature of telecommunications networks and the potential for more frequent and widespread outages. The mobile industry is cognizant of the importance of emergency roaming for disaster recovery and major outages situations. The 3GPP standard setting body began work on disaster roaming in Release 17, with further updates and expansion of roaming scenarios promised in future releases [17]. Mobile network operators should consider such new solutions for future network upgrades. Mobile network operators shall work closely with their vendors to ensure compliance, plan for the potential implementation of these new specifications in their 5G networks, and align with their roaming network partners accordingly.

Over-the-top messaging. Failures in some critical systems, such as the IP Multimedia System, led to outages in voice, messaging, and video while Internet services remain available. In such cases, over-the-top messaging applications provide an alternative way for communication, including emergency services.

Dynamic software-based SIM technologies. Software-based SIM technologies feature various levels of programmability and allow new roaming models to alternative providers in case of major outages. This would require agreements between operators on appropriate dynamic roaming solutions that leverage dynamic SIM programmability.

Emergency spectrum and capacity sharing. Various models for spectrum assignment are possible that could have direct benefits during major outages, for instance, in the case where users from an operator are moved to other service providers during an outage. Spectrum sharing is an example of such mechanisms, where operators would dynamically share spectrum to temporarily increase network capacity to accommodate the roaming users. Enabling such techniques requires commercial and technical agreements among operators, and potentially

[19] Disaster roaming in this case includes emergency roaming (e.g. ability to dial 9-1-1 using the services of a third-party mobile network roaming operator) as well as other roaming services, including voice, data and text.

standardizing specific mechanisms. Capacity sharing also applies to wireline operators for dynamic bandwidth and capacity sharing across the access, backhaul and core networks. Operators would need to standardize the mechanisms and interactions including clear identification of fault scenarios and the process to address them.

Interaction with content delivery networks and over-the-top applications. Telecom service providers could collaborate with over-the-top application and content providers to define specific interaction models during emergencies. For example, dynamic traffic management (e.g., throttling, policing, shaping, etc.) allows the egress traffic from caches and servers of content providers and over-the-top application providers to adapt dynamically based on feedback from telecom network operators.

Redundant connectivity for critical infrastructure service providers. The July 2022 outage highlighted the importance of having secondary or backup connectivity to maintain critical infrastructure services operational (e.g., public safety, health care, financial services, utilities, etc.). TSPs would better serve this class of customers by advising them to consider secondary connectivity options from alternate providers to enhance their own service availability. TSPs could offer leased third-party services from a different service provider with an independent network infrastructure to reduce the probability of service outage.

8.3.2. Process recommendations

Incident response training and drills. It is critical that service providers conduct regular training and conduct drills that simulate different outage scenarios and emergencies. Training will make staff more comfortable and ready to deal with emergencies and outages, and to have an unambiguous knowledge of their role and responsibilities. Drills will help the service provider uncover deficiencies in the outage response process, network architecture and general preparedness.

Incident management response KPIs. Key performance indicators for incident response help organizations assess the effectiveness of their processes and ensure that incidents, such as network or service outages, are handled efficiently. Setting KPIs for incident management offers several benefits: enhanced accountability, effective resource allocation, data-driven decision making and reduced risk. Common KPIs could be aligned with those defined by the Information Technology Infrastructure Library and by the Control Objectives for Information Technologies frameworks for incident/problem management. Specifically, we note that the evolution of network technologies and deployment models calls for the adaptation of existing KPIs to include new aspects such as virtualization, telecom cloud models, automation, use of AI learning models, etc.

Designated roles and responsibilities. Service providers would benefit from having certain personnel with clear roles and responsibilities during emergencies and outages. One such responsibility would be to notify ILECs and NAAD, among

other parties of the outage. Such roles should not conflict with roles related to resolving the outage (e.g., an engineering role in troubleshooting outage root cause).

Outage cost calculation. Operators would benefit from calculating the cost impact of a network outage, which is a vital component in risk management and business continuity planning. Outage cost calculation provides actionable insights to support financial decision-making. It helps the service provider mitigate the consequences of incidents through decision-making related to resource allocation and communication with stakeholders to preserve brand-image and financial stability.

Emergency service communication. Service providers should remind the public on how to access emergency calling and public alerts services during an outage. Service providers would be advised to maintain an online webpage with up-to-date relevant information on accessing emergency services during outages.

9. References

[1] Cloudflare Blog, "Cloudflare's view of the Rogers Communications outage in Canada," 8 July 2022, https://blog.cloudflare.com/cloudflares-view-of-the-rogers-communications-outage-in-canada/ (Last accessed: 1 August 2023).

[2] Rogers Communications Inc., Second Quarter 2022 Results, 27 July 27 2022, https://investors.rogers.com/wp-content/uploads/2022/08/Rogers-Q2-2022-Press-Release-AODA.pdf (Last accessed: 1 August 2023).

[3] CRTC Interconnection Steering Committee - Emergency Services Working Group, "*Consensus report ESRE0076: 9-1-1 Service Outage Notification Processes*," Telecom Decision CRTC 2017-389, 27 October 2017.

[4] CRTC Interconnection Steering Committee - Emergency Services Working Group, "*9-1-1 Service Outage Notification Processes*," Report Number: ESRE0076, 25 May 2017.

[5] Federal Communications Commission, "*Improving 911 Reliability*," FCC 22-88, 18 November 2022.

[6] Rogers Communications, "*Response to RFI: Rogers Canada-wide service outage of July 2022*," DOCS#4215437, July 22, 2022.

[7] Rogers Communications, "*Response to RFI: Rogers Canada-wide service outage of July 2022*," DOCS#4229639, August 22, 2022.

[8] Rogers Communications, CRTC RFI Responses, "*Submission Group 1: July 8 Events, RCA & Contributing Factors*," July 17, 2023.

[9] Rogers Communications, CRTC RFI Responses, "*Submission Group 2: Architecture & Business Management*," July 18, 2023.

[10] Rogers Communications, CRTC RFI Responses, "*Submission Group 4: July 8 Events, RCA & Contributing Factors*," July 14, 2023.

[11] Rogers Communications, CRTC RFI Responses, "*Submission Group 5: July 8 Events, RCA & Contributing Factors*," July 20, 2023.

[12] Rogers Communications, CRTC RFI Responses, "*Submission Group 6*," July 31, 2023.

[13] Rogers Communications, CRTC RFI Responses, "*Submission Group 7*," August 4, 2023.

[14] Rogers Communications, "*Response to RFI: Rogers Canada-wide service outage of July 2022*," DOCS#4215439, CONFIDENTIAL Rogers (CRTC) 11 July 2022-1_ix_Appendix.

[15] Rogers Communications, CRTC RFI Responses, "*Submission Group 8*," August 30, 2023.

[16] Innovation, Science and Economic Development Canada, "*Memorandum of Understanding on Telecommunications Reliability*," 9 September 2022, https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability (last accessed: 23 August 2023).

[17] 3GPP TS 23.501, "*System architecture for the 5G System*," v18.2.2, July 2023.

[18] Rogers Communications, CRTC RFI Responses, "*Submission Group 9*," September 13, 2023.

[19] Rogers Communications, CRTC RFI Responses, "*Submission Group 10*," October 6, 2023.

[20] Rogers Communications, "*Rogers Responses to CRTC Questions dated 22 February 2023*," Contribution #NTCO0746 prepared in response to task #NTFF044 for discussion in the Network Working Group, Task Identification Forms 44 Sub Working Group, August 11, 2023.

[21] CRTC, "*Telecom Notice of Consultation CRTC 2023-39*", 22 February 2023.

Annex 1: Outage timeline

The following timeline captures critical milestones in the July 2022 outage timeline that are material to this report.

2022 Date	Time (EDT)	Elapsed time from inception (hr:min)	Detail
8 July	2:27		[redacted]
8 July	4:43	0:00	Rogers committed the first change to the first impacted distribution router, deleting a policy filter, which is now known to be the event trigger. [redacted]
8 July	4:58	0:15	The distribution routers flooded all core routers with routes that exceeded their memory limit and consequently prevented them from processing traffic. [redacted]
8 July	6:28	1:45	[redacted]
8 July	8:39	3:56	Rogers notified the 9-1-1 network providers [also referred to as ILECs: Bell, TELUS, SaskTel] of network-wide outage, and requests they cascade the message to the PSAPs.
8 July	8:54	4:11	Rogers sent the first message to customers over Twitter advising of network-wide outage. Rogers followed up with similar messages across different platforms (interactive voice response, social media).
8 July	9:25	4:42	Pelmorex, which operates the NAAD, first contacted Rogers seeking any information on the impact of the outage on the distribution of emergency alerts after becoming aware of the service outage from media reports and personal disruptions.
8 July	9:38	4:55	[redacted]
8 July	10:21	5:38	[redacted]
8 July	11:10	6:27	[redacted]
8 July	11:19	6:36	Rogers sent notification to the CRTC and Pelmorex advising them of the national outage and cautioning that any agency attempting to broadcast emergency alerts to Rogers customers over the Rogers networks would be unsuccessful.
8 July	17:01	12:18	[redacted]

2022 Date	Time (EDT)	Elapsed time from inception (hr:min)	Detail
8 July	17:45	13:02	[redacted]
8 July	18:48	14:05	[redacted]
8 July	19:00	14:17	[redacted]
8 July	20:32	15:49	Rogers restored services to just over [redacted] subscribers in the [redacted] regions.
8 July	21:50	17:07	[redacted]
8 July	22:03	17:20	Rogers restored services to over [redacted]subscribers in all regions [redacted]
8 July	23:13	18:30	[redacted]
8 July	23:43	19:00	Rogers wireline corporate VPN access was restored.
9 July	0:50	20:07	[redacted]
9 July	1:34	20:51	Across Canada, about [redacted]subscribers were successfully registered. [redacted]
9 July	3:00	22:17	[redacted]
9 July	4:50	24:07	[redacted] About [redacted] subscribers were successfully registered. [redacted]
9 July	7:00	26:17	[redacted]
9 July	10:51	30:08	Rogers notified 9-1-1 network providers that the network has been restored.
9 July	16:25	36:42	Rogers successfully broadcasted the first alert issued from Pelmorex since the start of the outage.