OPTUS

24 November 2023

The Secretariat
Senate Environment and Communications References Committee
Parliament House
Canberra ACT 2600

Via email: ec.sen@aph.gov.au

To Whom It May Concern,

Thank you for the opportunity to address Questions on Notice from the committee's hearing on Friday 17 November.

Our responses to Senators' questions can be found in the attached document. These include both the questions taken on notice during the hearing itself and the supplementary questions that were received in writing on Monday 20 November.

In addition, Optus wishes to clarify the record about its crisis management preparedness, which has been the subject of both questions from Senators at this inquiry and broader public commentary.

First and foremost, Optus has an established, comprehensive risk management framework and supporting processes which aligns to the ISO 31000 industry standard. This framework and supporting processes ensure Optus maintains a sound understanding of the nature and extent of its material risks and maintains effective internal controls to manage these risks.

In doing this, Optus has taken a systematic approach through its risk management processes and systems for continuous identification, quantification, monitoring and control of risks, which is further enabled by robust risk governance, risk capability and risk culture. This includes the following measures:

1. Conducting annual risk profiling exercises to determine the nature and extent of material risks to Optus and ensure appropriate control measures are in place;
2. Performing issue management processes to ensure control gaps are tracked and remediated;
3. Enacting overarching governance and oversight processes through business unit/operational level risk committees and the executive-level risk committee (ERC).

Through the annual risk profiling exercise, Optus identifies the risk of business and service disruption due to network failure as a material risk for ongoing management and monitoring by the ERC. The governance provided by the ERC includes ensuring that key and effective controls are in place to manage this risk. These controls include:

- **Network architecture:** Designing and maintaining a network architecture that has multiple layers of redundancy in place to work to reduce the risk of an outage occurring.

- **Scenario identification, planning, and testing:** Performing exercises to identify possible scenarios that could lead to this risk materialising. In the unfortunate circumstance that an outage does occur, there are a number of scenario-based response plans and procedures in place that would be activated and used by the response teams to diagnose the problem and prioritise the restoration of services to customers. These plans are also reviewed and tested to ensure they are up-to-date and relevant.

- **Incident management:** Maintaining processes and systems to proactively identify network issues and remediate them as quickly and effectively as possible, including ensuring root causes are identified and addressed.

- **Crisis management procedures:** In the highly unlikely event of a full outage, an incident would be escalated into a crisis and Optus will activate its Crisis Management Procedures (CMP). The objective of the Optus CMP is to mitigate the effects of a crisis, minimise disruption to operations and recover operations. The overall priorities include:
    - Prioritise supporting customers by minimising the impact of the outage.
    - Restoration of customer services.
    - Ensuring the safety of people, including customers and staff.
- **Crisis management exercises:** The crisis management procedures are continuously reviewed, tested, and practised through scenario-based incident response exercises. These exercises include testing of our infrastructure, systems, and customer support functions such as call centres. We do this to make sure our processes are up to date, the right capabilities are in place, and roles and responsibilities to take appropriate actions are clear, so that our response to a crisis event is effective.

Yours sincerely,

Andrew Sheridan
Vice President, Regulatory and Public Affairs

OPTUS

Question	Answer
What time was the first technician on site to deal with the outage?	The most critical Optus exchanges have an engineer on site 24 hours a day. The Networks Operation Centre (NOC) is monitored 24 hours, and the first Optus engineer was physically present in the NOC at 04:45am.
How big is Optus's communications team? How many people work in your communications team?	Nine
Do you have a plan in place for a full outage like you had the other day?	Optus confirms that the outage did trigger the crisis management procedures, and the crisis plan operated as planned. Details are provided in the cover letter.
Under the Telecommunications (Emergency Call Services) Determination ruling, you are required to do a welfare check on people wo tried to call during the large network outage. You are saying you've done that for 228 people?	Welfare checks were undertaken for 229 people
Why does the government not have in place a backup contingency plan should some pretty significant departments experience this sort of outage?	This is a question for Government.
How many senior network engineers does Optus employ? [Brief exchange] I'm not asking that question. I am asking about network engineers at the CIO sort of level – the technical side	Optus employs 120 senior engineers within the networks business unit. Optus employs a further 200 engineers across our IT, enterprise, TV and product divisions.
When was your network architecture last reviewed? When was the last major review?	The Optus network has undergone several reviews for different aspects, such as resiliency and configuration, in the last year. The most recent review was completed in October 2023.
Is there any legislation that is needed for you to do a better job or any legislation that is currently impeding you and needs to be removed?	Optus is not aware of any changes that are required.
How often do you get cyber-attacks and what size are they?	There is no universally agreed formula for calculating this across industry. To provide a response, we have collated events from relevant cyber security controls which indicate around 17M attacks per day on average.
Do you know how many small businesses were impacted by the outage in terms of payments?	We are not in a position to fully determine this yet.
Confirm that you have paid out cash and not just in-kind services	Optus has paid out both cash and account credits.

Singtel Optus Pty Ltd
ABN 90 052 833 208
1 Lyonpark Road, Macquarie Park,
NSW 2113 Australia
PO Box 888 North Ryde,
NSW 1670 Australia
T +61 2 8082 7800
F +61 2 8082 7100

Who from your team [first contacted the Minister for Communications?	Contact was made with the Senior Advisor in the Minister's Office by Andrew Sheridan. The CEO first contacted the Minister.
Details of the government services impacted.	Optus provides connectivity to government agencies. Optus cannot provide insight into question about services provided by third parties.
Did Minister Rowland ask for assistance in helping deal with outages of government services to the extent they were impacted?	Optus' discussion with the Minister and Government on the day focused on restoring Optus services.
What time did KBR contact Minister O'Neil?	It was approximately 9.30 am.
Whether you've received any notice of any legal claims or are there any proceedings which have been instituted?	No.
What has been the cost of that PR and strategy advice?	Optus' commercial terms are confidential.
provide on notice to the committee a copy of all the advice and recommendations you've received from your PR and strategy team and your government relations team in relation to today's hearing	Ms Bayer Rosmarin did not receive written advice -or recommendations.
You said earlier that you have had small businesses lodge complaints. What do I tell small businesses?	If a business has an Optus Account Manager please contact them, or contact the nearest Optus Business Centre, Monday to Friday, 9am to 5pm.
Do you support the government mandating critical infrastructure to include established fail-over paths to prevent outages like this in the future while ensuring all providers are operating on a level playing field in terms of redundancy requirements?	Optus cannot comment on possible future regulations.
Do you support the government mandating industry-wide security and redundancy standards to ensure all companies must make the same preparations rather than risking cost competition resulting in the emergence of lower standards across industry?	Optus cannot comment on possible future standards.
What is your view on the viability of customers of one mobile network roaming onto other networks when it is impacted by a natural disaster or other network outage? Is this something being actively considered and/or pursued?	Optus is working with the other MNOs to assess the viability of temporary disaster roaming. If a roaming solution was in place, it would have likely resulted in other mobile networks being unable to accommodate the extra traffic given the number of users trying to roam. If the capacity issue could have been addressed, roaming would likely not have worked as the Optus core network was down and Optus subscribers would not have been able to be authenticated for roaming.

During the hearing, you referenced the issue being a result of a sort of cascade failure triggered by a routine Singtel upgrade that caused your normal defences to shut themselves down. Given the fact you have claimed it is indeed a somewhat routine upgrade, what confidence can consumers and the millions reliant on your service, that this issue won't happen again?	Optus is fully confident that this type of failure cannot occur again.
Is it a standard industry practice - if the network is partnered internationally - for these sorts of routine data exchanges to occur? Do these other telcos run the same risk of an anomalous cascade occurring?	It is standard industry practice.
What is now being done by Optus to ensure these routers aren't overloaded again, given this practice of upgrading is routine?	Optus has adjusted its configurations on all the international gateway routers and the routers that connect our Business and Consumer networks to prevent the propagation of large routing information changes.
Does this issue highlight that Optus had inadequate infrastructure implemented to begin with? Or was this a failure in employee competencies or resourcing?	This issue does not highlight inadequate infrastructure or resourcing or skill competencies.
Does Optus have the means and capability to provide meaningful services to a customer base as large as the one it has? Why or why not?	Yes we do. Optus has been providing services for more than 30 years. This is the first outage of this kind.
Did Minister Rowland ever notify you of a government contingency plan in place to deal with the loss of essential services? Did any government department you were in contact with?	Optus' discussion with the Minister and Government on the day focused on restoring Optus services.
What substantive action, if any, did the government take to assist you in the restoration of services?	Optus was the party responsible for restoring services.

During the hearing it was put to the Committee that Optus takes the blame for the issue, but simultaneously, it was pointed out that Singtel initiated the process and has carriage of the process that led to the outage. You also claim that you had defences in place designed to mitigate this very issue, but Singtel's initiation of the procedure saw a spike that effectively shorted out your routers. So is this a shared problem? Do you still maintain Optus was at fault? Or is Singtel correct in denying responsibility?	The cause of the outage was that Optus' Cisco routers hit a fail-safe mechanism which meant that each one of them independently shut down.
Is it known what the cause of the surge was? You have put it to us, a routine data transfer as a result of a standard upgrade initiated by Singtel led to this cascade failure of your routers and the defences you had in place designed to mitigate issues of this nature, so is there any clarity through the investigation process what caused the additional output that led to the failure? Can you unequivocally rule out foreign actors or sabotage?	The cause of the outage was that Optus' Cisco routers hit a fail-safe mechanism which meant that each one of them independently shut down. There is no evidence to suggest influence by any foreign actor or sabotage.
What levers does Singtel have at its disposal to ensure this kind of issue doesn't occur again? Have they offered any assistance?	The network issue occurred within Optus' network and it is Optus' responsibility to take measures to ensure the event cannot occur again.
Please provide the basis for your answer to Senator Roberts that there was no backbone connection between the Australian East and West Coast. In your answer please include nature of connection (T1, T2), network map, and ownership of this connection.	Optus' network is connected by multiple physically redundant fibre links between the East and West coasts. Optus uses self-owned fibre links, leases on third-party fibre links and utilises the Indigo Central subsea cable.
Please provide information on the percentage of east coast to west coast traffic which is carried on this connection.	100% of Optus traffic between the east and west coast of Australia is carried on the links above.
Please provide detail of the percentage of east coast to west coast traffic that is carried via Asia, and via the pacific connection.	No Optus traffic between the east and west coast of Australia is carried via Asia. It is not clear what is meant by pacific connection.