PSBA
RHWYDWAITH SECTOR CYHOEDDUS CYMRU | THE PUBLIC SECTOR NETWORK FOR WALES

OFFICIAL

PSBA

Post Incident Review

BT Ref: CS0287201

Version: 3
Status: Issued
Date: 31/03/2026

PSBA
No3 Capital Quarter, Tyndall Street
Butetown, Cardiff
CF10 4BZ

BT

Gweithio mewn partneriaeth gyda Llywodraeth Cymru
Working in partnership with Welsh Government

Copyright

Confidentiality

All information in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without BT's prior permission in writing and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source other than BT.

Many of the product, service and company names referred to in this document are trademarks or registered trademarks.

They are all hereby acknowledged.

Information Notice

This document is not a contractual deliverable; therefore, the information provided within it is not to be relied upon and shall in no way impact the contractual requirements placed upon BT by the customer. This information is being shared on an 'as-is' basis, for information only, to facilitate closer co-operation between the parties. The information provided shall in no way be construed as BT providing representations, guarantees, assurances or making any other contractual commitment to the customer. It shall not be published or disclosed wholly or in part to any other party without BT's prior permission in writing and shall be held in safe custody

Document Control

Basic Information

This document is available in two forms, controlled and uncontrolled. The controlled variant is maintained electronically and accessed by authorised users. Uncontrolled variants are all other electronic and printed copies.

Title	CS0287201_Wales wide outage_PIR
Author	PSBA Client Service Managers

Review Date	
Last Review Date	Next Review Date
31/03/2026	

Change History				
Issue	Status	Date	Author / Editor	Details of Change
V.1	Draft	26/03/2026	Karen Newbold Kelly Bolderson Peter Wilson Laurence Spittle Matthew Higgon	1st Draft
V.2	Draft	29/03/2026	Karen Newbold Kelly Bolderson	Amendments
V.3	Issued	31/03/2026	Kelly Bolderson Karen Newbold	WG Approval

Table of contents

1. Introduction

This report has been produced by BT PSBA due to the problems and business impact experienced in relation to the incident detailed below:

Incident Reference	CS0287201
Incident Severity	Major Incident
Incident Created Date/Time	25/03/2026 16:58
Time of Initial Failure	25/03/2026 16:40
Resolution Date/Time	26/03/2026 01:15
Problem Reference	PRB0044713

A full investigation into this matter and the problems encountered has now taken place and this report provides a timeline of key actions, details of the root cause along with corrective actions and recommendations following the investigation.

2. Incident Management Summary

This incident occurred as a direct result of an unplanned configuration change undertaken to support the management of legacy Capita operated UPS devices, which are in the process of transitioning to BT/PSBA ownership and management.

It had been identified that the existing Capita UPS devices, addressed within a /16 subnet, required a modification to the routing configuration to enable effective management by BT/PSBA. This necessitated the controlled leaking of MPLS VPN routes.

To assess whether this approach could be implemented in a straightforward manner, a configuration change was applied to a PSBA core Provider Edge (PE) router. This change was implemented without being submitted through formal change control as it was considered non-service impacting.

No immediate impact was observed following the application of the route map. Once it was recognised that return traffic from the UPS devices would also require route import changes, the configuration was subsequently removed, as extending the change further was deemed inappropriate without formal change approval.

Approximately 20 - 30 minutes later, a broader management connectivity issue was identified. Initial investigations did not link the reported issues as connected to this earlier change as the two PSBA management links were observed to be flapping. The precise root cause of this instability

remains under investigation; however, the issue was resolved during subsequent remediation activities.

3. Resolving Activity and Root Cause

Once the management links were stabilised through Quality of Service (QoS) adjustments, which required a site visit, further troubleshooting was undertaken. This identified that a default route was being exported by the Vantage Data Centre Core Provider Edge (PE) router where the route map had previously been amended. This default route was subsequently imported into customer VPNs that contained legacy MPLS management configurations, contributing to the wider impact observed.

Specifically, the presence of a route target import of 64627:16 within a customer VRF could result in instability or service outage due to the customer default route being overridden. This would have manifested as loss or degradation of internet connectivity for affected customers.

Verification confirmed that the route map amendment had been removed. However, despite clearing routes and resetting inbound BGP advertisements, the default route continued to be incorrectly advertised. A controlled reload of the affected router was subsequently performed. This action successfully resolved the issue, restoring normal operation for both customer services and PSBA management connectivity.

4. Follow-on Actions

Lesson Identified	Unplanned change implemented outside of agreed PSBA change control processes
Improvement Action	Reinforce change control requirements through an internal briefing, highlighting: The importance of formal change submission and approval The risks of unplanned changes to service stability and customer impact Roles and responsibilities during planned and emergency changes
Lesson Identified	Ineffective internal communication during P1 / Major Incidents, resulting in delays and fragmented updates
Improvement Action	Create a dedicated P1 / Major Incident Microsoft Teams channel to be used for all live Major Incidents. The channel will act as the single point of real-time communication for: Service Desk, 2nd / 3rd line teams, Incident Manager and relevant Stakeholders

Lesson Identified	Readiness to respond to a major network-wide incident.
Improvement Action	Explore the introduction of disaster recovery and business continuity test exercises to strengthen organisational readiness for major or P1 incidents. These exercises will help validate existing processes, identify gaps, and improve confidence and consistency in incident response.
Lesson Identified	Loss of management access prevented resolver groups from fully troubleshooting the incident, limiting visibility of network state and customer impact.
Improvement Action	During periods of management blindness, all engaged technical teams must actively assess customer impact based on information provided by reporting Organisations. Service Desk and Incident Management to ensure: Impact details from customers (sites affected, symptoms, timelines) are captured, validated, and shared in real time with all resolver groups. Customer-reported impact is used to guide troubleshooting and decision making when tooling or management access is unavailable. To mitigate this problem in future, we are investigating to possibility of installing a fixed link between Capital Quarter and PBSA management racks within Vantage Data Centre at Newport. With the installation of dedicated management terminals and a robust dual factor Authentication system, this will allow access to the network outside of SSP (secure management platform) and verify status accordingly. Given the right security design and sign off, these terminals could be made available to remote operatives.
Lesson Identified	Insufficient understanding of customer impact in detail resulted in resolver groups not being fully informed, reducing the effectiveness of troubleshooting and delaying root cause identification.
Improvement Action	Improve initial triage by strengthening probing questions at the point of incident reporting and reinforce the importance of continuous impact reassessment and communication throughout the incident lifecycle to support accurate and timely root cause analysis.
Lesson Identified	Speed of which incident was escalated to PSBA management
Improvement Action	Review P1 / Major Incident process to ensure escalation criteria and timeframes are clearly defined. Service Desk training will be delivered to reinforce early recognition of P1 / Major Incident conditions and to ensure escalations are implemented promptly and consistently in line with the defined process.

Lesson Identified	Legacy configuration within the Network.
Improvement Action	A review of the PSBA estate will be undertaken to identify and assess legacy configuration across the network. Clear processes and timeframes will be established for the removal of legacy configuration, alongside the introduction of robust controls to ensure legacy configurations are not introduced in future and are proactively prevented from remaining within the estate.
Lesson Identified	Communications during the incident, including the distribution of both email and SMS messages, were not fully effective, resulting in some customers not receiving timely or appropriate updates.
Improvement Action	A review of communication distribution lists and processes will be undertaken to ensure accuracy and completeness for both email and SMS notifications. Service Desk training will be reinforced to improve consistency, clarity, and timeliness of customer communications during P1 and Major Incidents, ensuring messages are appropriately targeted and effectively conveyed.

5. Timeline of Key Events

25/03/2026

16:30 A network change was implemented to support the transition and ongoing management of former Capita-operated UPS devices into BT/PSBA management

16:40 The network change was subsequently rolled back

16:57 Inbound call from Mid Wales Fire & Rescue Service (MWFRS) reporting loss of connectivity at the Presteigne site. Slow connectivity observed by the Service Desk. Case CS0290435 auto-created at 18:29 against PSB00016850

16:58 A case was opened in Service Now (the incident management system) for a group of alerts (CS0287201). Approximately 400+ alerts were observed at this time. A Major Incident (MI) was declared

17:00 Inbound call from Carmarthen Council reporting multiple sites down. The Service Desk advised of a high volume of alerts indicating a potential Major Incident. The customer could not provide a PSB reference due to loss of connectivity and instead provided postcode SA15 2EZ for PENTRE AWEL-LLANELLI-CRM-UA, which was confirmed as one of the alerts received. The customer was advised that MI communications would follow

17:04 The Service Desk engaged with 3rd line technical team to advise that 409 alerts were observed in the monitoring system; cause unknown at this time

17:05 3rd line now engaged and investigating

17:05 The Service Desk received a second call from Carmarthen Council reporting additional sites down. Approximately 1,500 alerts were observed within the monitoring system. This information was relayed to the 3rd line technical team

17:06 3rd line indicated that the issue was believed to be a management related issue

17:06 An overflow call was taken. Natural Resources Wales, reporting two sites down.

17:08 The Service Desk observed approximately 5,000 alerts across Wales within the monitoring system

17:10 3rd line advised that while CORE devices were accessible, management access to both NAT devices were unstable due to BGP peering loss to the secure management platform. This prevented further troubleshooting as the devices were continually flapping. A request was raised to fault out the management links

17:10 Inbound call from DHCW reporting loss of default route from the data centre and VPN issues. Case CS0287465 was raised at 17:16 and assigned to 2nd line. At this stage, the issue was not assumed to be related to the Major Incident

17:25 An outbound call was made by the Service Desk to MWFRS, confirming a major outage impacting the customer site. The customer was advised that Major Incident communications would be issued and the previous incident linked to the MI

17:27 An initial communication was issued; however, at the time it was difficult to determine which organisations were impacted. As a result, the communication was sent via distribution lists that did not include all organisations. No customer text message was sent

17:28 3rd line advised the issue was believed to be management related; however, unstable access to the management devices (less than 30 seconds at a time) prevented further troubleshooting

17:29 The Service Desk confirmed inbound customer calls and shared example details with 3rd line. 3rd line confirmed devices were up and provided uptime detail

17:45 3rd line advised they were unable to confirm customer reported issues, as the PSBA network appeared stable, although management links were unstable and under investigation, they were waiting for the outcome of the management links to troubleshoot further

17:52 Inbound call from Neath Port Talbot Council querying the Major Incident notification received and reporting one site down, with uncertainty as to whether the issue was related to the ongoing Major Incident

18.06 3rd line reported continued instability on the Cardiff and Bangor management links, which remained flapping

18:15 Inbound call from Wrexham Council querying the status of Major Incident communications. The Service Desk advised that a further update would be issued shortly. Impact to customer service was not clarified

18:19 Inbound call from Carmarthen Council requesting an update on the ongoing outage affecting Carmarthenshire. The Service Desk advised that a further update would be provided shortly

18:20 The Service Desk relayed customer reported site outages in Carmarthen to 3rd line; no specific details were provided in relation to Wrexham. 3rd line advised that management link restoration was required to continue troubleshooting

18:21 Inbound call from HMP Parc reporting service issues. The caller advised of internet connectivity problems. The Service Desk confirmed that an ongoing issue was under investigation and advised the caller to contact the DCHW National Service Desk for further updates as this site is covered by the health shared services

18:25 Message from Caerphilly Council confirming MI comms received, schools appear to be unaffected. Asking for clarification on incident details.

18:26 3rd line confirmed Carmarthen (UA06) HQ passing plenty of traffic. Service Desk tried to call customer. Went to voicemail, no message left.

18:32 Inbound call from MWFRS querying whether the ongoing outage was local or Wales-wide. The customer advised that other sites were affected, reporting intermittent connectivity, loss of network access, and issues signing in. The Service Desk advised that the outage was Wales wide. The customer confirmed multiple sites impacted across different areas of Wales and advised of intermittent and complete loss of internet service at some locations. Impacted site details were shared with the Service Desk and escalated to 3rd line

18:36 Second MI communications email, investigations remain ongoing

18:39 MWFRS reported all services down following previous report of intermittent loss of service

18:40 3rd line advised that only limited checks could be completed during brief access windows before sessions dropped, with no issues identified. Carmarthen was noted to have lost

default routing at approximately 17:00 but had since stabilised. Three MWFRS devices were unreachable from management and could not be checked further

18:45 Management link circuit checks completed; no faults found

18:49 Inbound call from DHCW requesting a ticket update. The Service Desk advised of link to the ongoing Major Incident

18:53 Service Desk contacted Major Incident Management (MIM) duty manager for further support

18:54 PSBA Account Director received message from Betsi Cadwalader Health Board

18:55 Following advice from 2nd and 3rd line, the Service Desk re-engaged the management link circuit supplier; no issues or alerts were identified on their system

18:57 MIM confirmed BT Networks not aware of any Wales specific issue or related major service outages (MSO) in the region. There was an ongoing MSO in London area

19.03 PSBA Account Director contacts the Service Desk

19:03 Wrexham Council called Service Desk requesting a call back

19:10 Service Desk notified Client Service Managers Teams chat of ongoing incident

19:17 Service Desk engaged 3rd line to advise on ongoing outage and potential correlation with London MSO. Advised contacting the MSO team for clarification of impact

19:20 Contacted MSO team who confirmed Wales sites are not impacted by the MSO

19:28 Client Service Managers enquire to Service Desk whether further assistance was required

19:36 Inbound call from Cwm Taff HB regarding PSB00023094, which was answered by the overflow team

19:37 MIM duty manager confirmed Wales wide issue was not related to wider MSO

19:38 Third MI communications email, investigations remain ongoing, PSBA management engaged

19:38 PSBA Account Director engages with Technical Design Architect team for assistance

19:43 Client Service Managers contacted and on-line to provide additional support

19:44 Advised by MIM to contact OOH 3rd line and check the ICUK management circuits

19:46 The Service Desk requested that MIM check whether any planned work or Major Service Outages (MSOs) were linked to the two ICUK management link circuits

19:48 Inbound call from DHCW, which was answered by the overflow team

20:17 Inbound call from Wrexham Council, which was answered by the overflow team

20:20 An internal bridge call was convened with 3rd line, the Technical Design Architect, Service Desk support, and Account Management teams to review triage activities and determine next steps. The Technical Design Architect confirmed plans to attend Cardiff Stadium House to continue the investigation

20:33 Internal PSBA Teams call initiated between Service Desk and PSBA Management

20:33 Caerphilly confirming corporate are affected by MI, Client Service manager details passed by customer to Caerphilly IT engineer

20:41 PSBA Account Director received message from DHCW

20:43 Inbound call from DHCW, which was answered by the overflow team

20:54 Client Service Managers followed up on previous customer calls and messages to provide updates and gather further impact information

20:57 Service Desk requested emergency access to the Vantage Data Centre, so access would be available if required

21:09 Inbound call from JISC regarding email sent to Service Desk. Customer advised they have not received MI notification; Customer shared having issues with slowness across one site and a couple of sites hard down. Customer requested to share previous communications which was actioned

21:14 Service Desk outbound call chasing Vantage Data Centre for access

21:30 Teams call with DHCW, Health Boards across Wales and PSBA management team

21:33 Inbound call from National Resources Wales following up from previous call at 17:06. No MI communications had been received, two sites down. Requested comms to be forwarded

21:36 Inbound call from MWFRS, requesting update

21:48 Fourth MI communications email, asking customers to make contact if experiencing network issue, all technical teams engaged. Contact list updated to include all customers across the PSBA estate, and an email update sent. SMS increased to include customers across PSBA

21:57 Inbound call from Cardiff Council experiencing issues, calling in on the back of comms update

22:00 TDA makes changes to QoS on the BGP to return management and alarms start to clear, management restored

22:03 An internal bridge call was convened with Service Desk and PSBA Management to review situation and next steps

22:04 Service Desk outbound call to TDA to confirm Vantage access available. TDA confirmed his location at Cardiff Stadium site. TDA heading to Vantage Data Centre to continue fault investigation

22:27 Following changes to QoS on the BGP to return management alarms clearing, now down to single figures

22:27 Inbound call from NWFRS requesting incident update. Advised Engineer on site, awaiting update

22:42 Caerphilly Council on call engineer provides impacted site list

22:44 An internal update bridge call was convened with Service Desk and PSBA Management

22:45 Teams call with DHCW, Health Boards across Wales and PSBA management team, advising that alarms are now clearing from Service Desk perspective. Health boards not seeing any improvement

22:48 TDA confirmed his direction to Vantage Data Centre for further investigation

22:55 An internal update bridge call was convened with Service Desk and PSBA Management

23:15 Teams call with DHCW, Health Boards across Wales and PSBA management team, no improvement seen. Technical call to be arranged between PSBA TDA and DHCW technical

23:17 Fifth MI communications email, investigations remain ongoing, issue identified, network alarms starting to clear

23:17 Inbound call from Carmarthen Council, requesting further update. Advised alarms clearing, unable to advise RCA at this time

26/03/2026

00:02 An internal update bridge call was convened with Service Desk and PSBA Management

00:25 TDA continuing investigation in Vantage Data Centre data centre

00:40 Teams call arranged between TDA, Client Services and DHCW Health board engineers to assist with further triaging

01:00 An internal update bridge call was convened with Service Desk and PSBA Management

01:02 A configuration issue affecting the internet learned route was identified and corrected

01:10 A controlled router reload was undertaken by the Technical Design Architect to ensure correct routing was applied

01:26 Sixth MI communications email, Technical Design Architect at Vantage Data Centre and engaging directly with DHCW

01:30 Teams call with DHCW, Health Boards across Wales and PSBA management team now seeing service restored

01:43 Health Board customers reported that services were beginning to restore

02:08 Health Boards confirmed services restored

02:19 Seventh MI communications email, following collaboration between Technical Design Architect and DHCW, services are restored, monitoring will continue

10:15 Final MI communications email issued to resolve incident. Network stable since 01:15 Cause identified as a network change