NSW Department of Planning, Industry & Environment

Post-Flood Systems Debrief

Costa Zakis, Principal
costa.zakis@zakisadvisory.com.au

Version: 1.1 – 8 July 2021

ZAKIS
advisory

CONTENTS

EXECUTIVE SUMMARY

A major rain event affected significant areas of Australia in the second half of March 2021 with the week ending 24 March reported as the wettest week for the Sydney region since national daily records began in 1900. Flooding occurred in most coastal catchments in New South Wales with the Hawkesbury–Nepean catchment in Sydney experiencing its most significant flooding for more than 30 years.

The rain event on the weekend of 20 and 21 March 2021 placed a significant strain on some WaterNSW IT systems that were located within the NSW Department of Planning, Industry and Environment (DPIE) ICT environment. High traffic volumes in addition to some other network issues, resulted in intermittent outages and slow response times for users accessing the Real Time Data (RTD) and WaterLive applications. It was reported that internal operational systems were maintained near to real time with limited interruptions.

Three concurrent ICT related incidents occurred during the rainfall event which impacted web portals and water data systems:

1. Poor performance of website and WaterLive App which arose from automatic server re-starts when CPU load exceeded 90%. These restarts resulted in a 5-minute outage for customers and along with other forced outages, rendered the website and WaterLive app effectively unusable for customers.
2. An Amazon Web Services (AWS) Network Outage that prevented WaterNSW (WNSW) staff from accessing Hydstra and Hydrotel systems and removed the ability for all external users of the DPIE network to access the RTD. This issue also prevented transfer of data between internal systems.
3. Security Certificate expiry and WaterNSW network outage impacted internal and external accessibility to the web portal, WaterLive, RTD, WaterNSW Website and other internet facing systems.

A multi-agency debrief was held in May 2021 to understand the lessons that could be learnt from the response to the incidents so that the initiating issues could either be prevented to prevent reoccurrence or the response better managed.

The debrief identified that the IT teams from DPIE Water and WNSW, supported by DPIE's Digital Information Office (DIO) and Manly Hydraulics Laboratories (MHL), were able to implement a range of reactive solutions that ensured that operational data was made available to key internal users

within minimal interruption. Notwithstanding the technical response and camaraderie demonstrated by ICT staff, numerous lessons were learnt from the response. These included:

- There was a dependency on a small and critical group of ICT staff to monitor and respond to the network incidents.
- DPIE Water lacked an overarching incident management framework to coordinate all DPIE activities associated with the incident including the establishment of a common operating picture, management of communications and coordination of resources.
- The DPIE ICT network had several vulnerabilities due to hardware capacity restrictions and outdated architecture that did not meet the needs of users in periods of high demand.
- DPIE Water senior leadership were not aware that they had a responsibility for IT applications and hardware that supported the operational activities of other agencies. Similarly, ICT staff were not in roles that required them to provide 24/7 support to such systems.
- DPIE Water did not have a formalised practice of adopting a "forward posture" in preparation for anticipated events and incidents.
- MHL data services is currently operating separately from DPIE ICT operations. They should be considered in DPIE planning and preparedness activities.

Recommendations arising from this debrief are:

Reference	Recommendation	Responsible
R1	DPIE Water to develop an Incident Management Framework that caters for all forms of anticipated incidents that may affect the business. This framework should also apply to ICT incidents. The Incident Management Framework should include the following attributes and features: • Readily integrate with other incident management models used elsewhere within DPIE. • Nominate a standard management team structure that can expand and contract as required during the lifecycle of the incident. • Articulate standardised roles and responsibilities. • Include mechanisms for standardized briefing and situation updates. Include a series of checklists to guide the team before, during and after an incident. This will include the development and coordination of rosters for responses to prolonged incidents.	DPIE Water

Reference	Recommendation	Responsible
R2	Enable a cross agency ICT expert group that can convene during incidents to work on problems and expedite solutions.	DPIE Water
R3	DPIE Water should adopt a philosophy and standard operating practice of activating a suitably sized and resourced incident management team to adopt a "forward posture" for predicated or proximate events that could bring about the need for a coordinated response within DPIE Water because of an event of incident. The purpose of this "forward posture" would be to collect, collate, interpret, and disseminate information that will then allow DPIE Water to prepare for a potential incident, activate pre-event checklists and shorten the response time to any incident.	DPIE Water
R4	DPIE's ICT environment does not appear to have a robust and tested IT Disaster Recovery Plan for the relevant water systems that includes a system of classifying network incidents and specifying the level of response required. DPIE Water should work with DPIE ICT using DPIE's risk framework & tools, to develop this network incident classification system and link it to the DPIE Water Incident Management Framework.	DPIE Water / DPIE ICT
R5	DPIE ICT needs to develop a common understanding of the customers that are dependent on its ICT network and their vulnerabilities to disruptions. This information needs to be integrated within the new network incident classification system and link to the DPIE Water Incident Management Framework.	DPIE ICT
R6	DPIE Management need to be briefed on the status and vulnerabilities of the DPIE ICT network including critical customers and third parties that may be reliant on the network.	DPIE Water / DPIE ICT
R7	DPIE ICT need to resolve how they will provide ICT network response support after hours for systems where there are customers who have a high reliance on the availability and performance of DPIE Water hosted IT infrastructure and applications to undertake operational activities and reporting.	DPIE ICT
R8	MHL data services should be considered in the above activities, planning, and preparedness, noting they are currently operating separately from DPIE ICT operations (mix of AWS and dependency on Department of Customer Service (DCS) ICT).	MHL / DPIE Water

BACKGROUND

Weather event

A major rain event affected significant areas of Australia in the second half of March 2021. The highest rainfall totals occurred in eastern New South Wales, with the coastal areas, including Sydney, experienced multiple days of heavy rainfall. The week ending 24 March 2021 was the wettest week for the region since national daily records began in 1900. Flooding occurred in most coastal catchments in New South Wales with the Hawkesbury–Nepean catchment in Sydney experiencing its most significant flooding for more than 30 years. New South Wales had its second-wettest day, third-wettest week, and second-wettest March on record since 1900 (Bureau of Meteorology, 19 April 2021).

Systems Incidents

The WaterNSW Real-time Data Website (RTD), WaterInsights portal, WaterLive Application and Hydstra platform provide access to information and data from over 5,000 monitoring stations in NSW which measure meteorological parameters and the quality and quantity of water in NSW rivers, streams, groundwater bores and dams. Over 1,400 of these stations continuously monitor water sources and the environment delivering real-time data through the WaterNSW telemetry and remote data capture networks (Water NSW, 2021).

Internet users can view current and historic data including latest values, data plots and associated metadata regarding the monitoring sites. In addition to public facing websites and applications, the Water Data Systems provide automated data delivery to third-party stakeholders such as SES, BoM and DPIE and internal operations teams (Water NSW, 2021).

While the RTD and website are owned and operated by WaterNSW, they reside within the infrastructure of DPIE ICT network. DPIE ICT staff generally have a 24/7 response to critical incidents, but they do not provide 24/7 support. They assist WaterNSW and call upon staff from the Digital Information Office (DIO) to assist with problem resolution during critical incidents. Following a recent restructure, senior leadership within DPIE were not aware that they had a responsibility for operational systems for another agency prior to this event.

The rain event on the weekend of 20 and 21 March 2021 placed a significant strain on the RTD system and portals. WaterNSW reported that web analytics processes recorded an increase in usage of over 300% while their Web Analytics showed approximately 85,000 corporate website hits on the Dam

Level page per day with 74% of website hits made by new users who had not accessed WaterNSW URLs previously (Water NSW, 2021).

The high traffic volumes, in addition to some other network issues, resulted in intermittent outages and slow response times for users accessing the RTD and WaterLive applications. It was reported that internal operational systems were maintained near to real time with limited interruptions.

This debrief covers three concurrent ICT related incidents that occurred during the rainfall event which impacted web portals and water data systems:

1. *Poor performance of website and WaterLive App*. The RTD server would automatically restart due to excessive CPU load (>90%). Additional manual restarts were also undertaken to ensure that platforms were at full capacity during scheduled data loads. Each restart resulted in a 5-minute outage for customers. Although the portal remained available, the website and WaterLive app became effectively unusable for customers due to the long load times and system unavailability.
2. *Amazon Web Services (AWS) Network Outage*. This outage prevented WaterNSW staff from accessing Hydstra and Hydrotel systems and removed the ability for all external users of the DPIE network to access the RTD. This issue also prevented transfer of data between internal systems such as data delivery to CARM. The RTD, WaterLive, Hydstra and Hydrotel were not accessible for several hours until interim solutions were put in place. Full-service restoration was at 8am on Monday 22 March.
3. *Security Certificate expiry and WaterNSW network outage*. A WaterInsights outage was identified due to an expired webservice authentication certificate. A separate and concurrent internet service failure at the Unanderra Data Centre led to an outage that impacted internal and external accessibility to the web portal, WaterLive, RTD, WaterNSW Website and other internet facing systems.

Separate post-incident technical investigations have been undertaken by WaterNSW. The outcomes of these investigations and proposed solutions are outlined in a separate WaterNSW Report (Water NSW, 2021).

DEBRIEF DETAILS

The Post-flood systems debrief was facilitated by Costa Zakis of Zakis Advisory on 7 May 2021. Owing to COVID-19 related restrictions, the debrief was conducted remotely as a Microsoft Teams meeting.

Participants

The following participated in the debrief:

Danielle Baker	Director Water Analytics	DPIE Water
Peter Rosa	Principal Water Information Officer	DPIE Water
Micah Starkis	Director Data and Information	DPIE Water
Tony Caine	Senior Developer	DPIE Water
Mitchell Isaacs	Chief Knowledge Officer	DPIE Water
Bronson McPherson	Director Engineering	Manly Hydraulic Laboratories
Galen Lewis	Data Cloud Manager	Water Infrastructure NSW
Michael Galloway	Team Leader Hydrometrics	Manly Hydraulic Laboratories
Madeleine Mispel	Director Policy, Water Sector Reform	DPIE Water
Rina Solomon	IT Business Partner	DPIE Corporate Services - DIO
Joan Gilbert	Director of the Office of Group Deputy Secretary - Corporate Services	DPIE Corporate Services
Phil Glastonbury	Manager Assets and Water Data Systems	Water NSW
Dan Berry	Manager Water Systems Operations	Water NSW
Paul Roche		Bureau of Meteorology
Ben Xu	Director Digital Acceleration	Department of Customer Service

Definitions

The following definitions and abbreviations are used within this report:

Bureau of Meteorology	BoM
Department of Planning Industry and Environment	DPIE
Manly Hydraulics Laboratory	MHL
NSW State Emergency Service	SES

DEBRIEF OUTCOMES

This debrief focused on understanding

- What occurred with the IT systems during the incident window,
- What could be done to prevent re-occurrence of the IT performance issues until such time as long-term solutions are put in place, and
- How the overall management and response to the incident could be improved.

Debrief outcomes are presented from two perspectives:

1. Activities within the response that worked well
2. Opportunities for Improvement.

Activities that worked well

These identified elements were considered to be effective in responding to the incident. Therefore, it is desirable that the processes or behaviours that contributed to this outcome should be incorporated into any incident response in the future.

Aspect / Element	Description
Active communications between agencies	Communications between WNSW and DPIE teams was very responsive and collaborative. WNSW provided status updates on some of the difficulties they had with data including when some monitoring stations were offline. WNSW had sound communications with SES to understand their needs and any issues. MHL proactively contacted the BoM to understand their data priorities and needs to prioritise their activities.
Planned WNSW system outages were kept to a minimum and to small time windows	WNSW Operations teams and the BoM were obtaining the data they needed but there were a small number of instances where data was delayed, or an issue could not be resolved quickly.
Coordination of WNSW outwards communications	Outward communications within WNSW was managed through its corporate incident management team. This freed up ICT resources to focus on their technical activities.

Aspect / Element	Description
DPIE did not experience any external pressure	Due to proactive briefing to senior management, DPIE staff did not experience any external pressure regarding issues arising from the systems outages. This allowed resources to maintain their focus on issue resolution.
Real time workarounds identified	The ICT teams were able to identify real time workarounds for issues so that data could be provided e.g., static data made available when RTD was not available. Realtime load balancing was able to be achieved within the ICT environment to create capacity and manage performance. Solutions and limitations were communicated to WNSW in a timely manner to allow for adjustments on their side.
Auto messaging and alarms for system issues	Internal alarms across all key systems to provide early warning at an internal ICT and telemetry levels.
Staff were committed to the resolution of the issues	The DPIE ICT team do not provide 24/7 support. Accordingly, formal after hours or incident rosters were not in place. Therefore, there was a reliance on the good will and best efforts of staff to resolve the issues over the weekend. Resources were able to scale up as needed.
Fatigue monitoring	Fatigue monitoring was well managed to help staff and manage the prolonged event.
Informal updates	Informal updates were provided amongst teams to allow for the timely sharing of information, rather than waiting for formal meetings.

Opportunities for Improvement

Opportunities for Improvement were identified for aspects of the response that were less than optimal or for clear deficiencies. Each identified opportunity is not necessarily a standalone action item and may form part of an integrated set of initiatives that will improve overall responses to incidents.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Incident team or call list was not established within DPIE Water	A formal management structure and team for the DPIE response was not established.	There was a high reliance on individuals and the good-will of staff to be available and responsive to the needs and issues arising from the incident. It was difficult to coordinate rostering, the sharing of information, status updates and consistency of upwards reporting to senior management and Ministers.	DPIE Water to develop a preliminary protocol to activate an incident management team for ICT incidents. The scale of activation may be linked to the severity of the ICT issue (e.g., internal/external users, system criticality, weather profile).	DPIE Water to develop and incident framework that activates a formal incident team proactively for anticipated and actual issues. Incident team should cover ICT and other possible incidents across DPIE Water. The formal incident management team is to include resources beyond technical specialists (e.g., include senior leadership, legal etc.). Ensure that WNSW, BoM and other key stakeholders are aware of the DPIE Water incident team to enable cross agency collaboration and information sharing.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Need to agree incident severity	The scale and degree of incidents needs to be documented so that a proportionate management and organisational response can be delivered.	DPIE runs the risk that it will under or over respond to a broad range of incidents and in doing so not meet the expectations of stakeholders, fail to support other agencies or waste resources.	A rudimentary ICT incident classification model needs to be developed to manage the response of technical and management resources. This can ultimately be linked to a DPIE incident management framework.	A DPIE Water Incident framework should include incident categories and escalation descriptions matched to incident levels.
Need to build common picture of the DPIE "customer"	For DPIE to manage its incident response by setting clear operational objectives, it is important to have a clear understanding of the DPIE customer.	Failing to have clarity of who the DPIE customer is will limit the ability of DPIE to meet stakeholder expectations during incidents.	Identify key dependencies and relationships within the DPIE ICT architecture.	Document a customer relationship model linked to the DPIE ICT architecture. This will feed into a document ICT incident response framework.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Management awareness	Due to a recent restructure, DPIE Water management were not aware of the criticality of DPIE hosted applications or architecture during floods. They were also unaware of known deficiencies or anticipated issues of the ICT environment.	The weather event was predictable and the anticipation of traffic foreseeable, but DPIE senior leadership was not informed or prepared in advance. As a result, they were reactive and not able to proactively provide additional resources or manage upwards.	DPIE management need a briefing on the DPIE ICT environment, criticality of systems and obligations to third parties.	Identify the ICT critical control points to understand possible points of failure and exposure. Management briefing on the above. Pre-event (incident) considerations and planning (ICT and DPIE Mgt) for anticipated high traffic, usage or vulnerabilities.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Forward posture standup for DPIE	DPIE was not well prepared for the anticipated rainfall event and the associated demand that would be experienced for data by members of the community and other agencies.	DPIE was reactive to the resulting ICT incidents and had not pre-prepared its response for any ICT related issues including the establishment of rosters etc. to manage any potential issues. DPIE ICT had not pre-identified system vulnerabilities in advance of the rain event and it had not initiated pre-event activities to reduce system load, remove unnecessary applications or pause any network upgrades, tests or activities that may have been scheduled to run.	Proactively standup relevant technical and management resources when information or briefings suggest that there may be heightened reliance or sensitivities on DPIE infrastructure. Initiate activities to promote favourable system performance during periods of anticipated high network usage.	DPIE to establish an incident management protocol that allows for situational monitoring and the ability to take a forward position or early activation of incident management team to expedite responses. Include senior management briefings. Include DPIE IT on DPIE forecast / forward posture notifications. Establish ICT protocols to be activated during periods of anticipated high network traffic to proactively monitor performance and ensure system stability and reliability.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Pre-event checklist	The absence of a forward posture prevented pre-event actions to be implemented. Actions undertaken were dependent on the experience of individuals.	The absence of checklists removed the ability to be comprehensive, predictable or have a reliable audit trail.	Develop pre-event checklist for implementation in forward posture. WNSW have this in their Operations response but not their IT responses.	Incident management framework to be developed and include pre-event incident checklists.
Status updates	Ongoing status updates were ad hoc during the response.	It became difficult to conduct upwards briefings when the timing of status updates was not known.	The responsibilities for status updates and upwards briefings are to be established at the initiation of any ICT incident response.	A DPIE Water Incident management framework should make provision for incident briefings at specific times or under certain circumstances. Status updates and tracing of performance improvements to be included.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Formalise regular ICT incident team updates across agency ICT teams	Situation updates amongst ICT technical staff across WNSW/DPIE/MHL was ad hoc and not formalized.	Opportunity was lost to share information to promote situational awareness and collaborate on solutions.	Continue with ad hoc approach through informal meetings.	Formalise ICT incident response framework. Initiate formal ICT status updates at defined frequencies during incidents to facilitate cross team information sharing and communications.
High reliance on single resources within DPIE	The DPIE response had a high dependency on specific individuals to diagnose issues and implement solutions.	High workload on individuals. This would have introduced additional issues if the incident had continued longer than the weekend concerned, or if those individuals had been unavailable.	Pre-establish formal rosters. Identify back-ups / succession.	DPIE should activate a formal incident team for identified incidents. One of the roles of this team would be to oversee resource rosters for incidents

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Architecture design	Manage data and information delivery in a form that better manages the overhead of systems (e.g., real-time critical information is delivered in a pre-defined form to reduce overhead on internal systems). Some metadata is kept static and API calls reduced to priority information on Real Time Data.	The current system design rebuilds data and analysis (plots etc.) dynamically for every user call. This uses significant system resources and slows down system performance.	Have Water Insights on a re-implementation of RTD box that will deliver static content that would be an hour old. This will remove dynamic rebuilding and improve system performance.	RTD will be decommissioned and all data will be housed in an Azure data lake as opposed to servers. Public will get their information from Water Insights as part of the Wave program.
Server capacity	IT servers reaching capacity.	Public API traffic taking servers were operating at capacity affecting external and internal users.	Relocate internal and external services onto different servers to better manage traffic load.	Move all WNSW applications (Hydrastra and Hydrotel) off existing servers to a more readily expandable platform.

Opportunity	Experience / Description	Impact	Short term Solution	Long term Solution
Share lessons learnt across agencies (in and out of NSW)	ICT teams duplicate effort in resolving system deficiencies and limitations. A shared understanding of solutions to problems with commonly used applications or infrastructure is not generally available.	The identification of solutions is delayed while fault finding and solution trials are undertaken, the opportunity to leverage past experience or solutions is lost, technical expertise is not always leveraged, adverse outcomes may be repeated.	Share to lessons learnt from the IT "failures" across agencies so that system deficiencies / learnings are shared – fast track, reduce effort e.g., MHL have learnt about Wiski and can share learnings. BoM run a cross agency / jurisdiction working group to share learning journeys and thinking.	Formalise a standing working group across DPIE, WNSW, BoM and other related parties within NSW and other jurisdictions to share knowledge of ICT vulnerabilities and solutions. Enable a cross agency ICT expert group that can convene during incidents to work on problems and expedite solutions.
Incorporation of MHL data services in planning and preparedness	MHL are currently operating separately from DPIE ICT operations (mix of AWS and dependency on Department of Customer Service (DCS) ICT).	MHL systems worked well in all recent events. However, opportunities exist to reduce DCS ICT dependency, and incorporate best practice learnings from broader DPIE activities.	Consider MHL data services in planning and preparedness activities.	Review remaining DCS ICT dependencies and incorporate best practice learnings from broader DPIE activities.

RECOMMENDATIONS

Reference	Recommendation	Responsible
R1	DPIE Water to develop an Incident Management Framework that caters for all forms of anticipated incidents that may affect the business. This framework should also apply to ICT incidents. The Incident Management Framework should include the following attributes and features: • Readily integrate with other incident management models used elsewhere within DPIE. • Nominate a standard management team structure that can expand and contract as required during the lifecycle of the incident. • Articulate standardised roles and responsibilities • Include mechanisms for standardized briefing and situation updates. Include a series of checklists to guide the team before, during and after an incident. This will include the development and coordination of rosters for responses to prolonged incidents.	DPIE Water
R2	Enable a cross agency ICT expert group that can convene during incidents to work on problems and expedite solutions.	DPIE Water
R3	DPIE Water should adopt a philosophy and standard operating practice of activating a suitably sized and resourced incident management team to adopt a "forward posture" for predicated or proximate events that could bring about the need for a coordinated response within DPIE Water because of an event or incident. The purpose of this "forward posture" would be to collect, collate, interpret, and disseminate information that will then allow DPIE Water to prepare for a potential incident, activate pre-event checklists and shorten the response time to any incident.	DPIE Water

Reference	Recommendation	Responsible
R4	DPIE's ICT environment does not appear to have a robust and tested IT Disaster Recovery Plan for the relevant water systems that includes a system of classifying network incidents and specifying the level of response required. DPIE Water should work with DPIE ICT using DPIE's risk framework & tools, to develop this network incident classification system and link it to the DPIE Water Incident Management Framework.	DPIE Water / DPIE ICT
R5	DPIE Water ICT needs to develop a common understanding of the customers that are dependent on its ICT network and their vulnerabilities to disruptions. This information needs to be integrated within the new network incident classification system and link to the DPIE Water Incident Management Framework.	DPIE ICT
R6	DPIE Management need to be briefed on the status and vulnerabilities of the DPIE ICT network including critical customers and third parties that may be reliant on the network.	DPIE Water / DPIE ICT
R7	DPIE ICT need to resolve how they will provide ICT network response support after hours for systems where there are customers who have a high reliance on the availability and performance of DPIE Water hosted IT infrastructure and applications to undertake operational activities and reporting.	DPIE ICT
R8	MHL data services should be considered in the above activities, planning, and preparedness, noting they are currently operating separately from DPIE ICT operations (mix of AWS and dependency on DCS ICT).	MHL / DPIE Water

REFERENCES

Bureau of Meteorology, 19 April 2021. *Special Climate Statement 74 - extreme rainfall and flooding in easternand central Australia in March 2021,* s.l.: Commonwealth of Australia.

NSW Department of Planning, Industry and Environment, 2016. *Functional Mapping to Existing Application Environment for Water Resource Management - Final Deed,* s.l.: Unpublished.

NSW Department of Planning, Industry and Environment, 2021. *DRAFT - Notes on Hydstra realtime data as context for incident on 21-03-2021 v0.02,* s.l.: unpublished.

NSW Department of Planning, Industry and Environment, 2021. *PIR - Water outage event 19-21 Mar 2021,* s.l.: Unpublished.

Water NSW, 2021. *Waterinsights and RTD Webservices Outage,* s.l.: Water NSW.