Online Crisis Communication: An Australian Case Study

Matthew Warren[1,2] and Shona Leitch[1]
[1]RMIT University, Australia
[2]University of Johannesburg, South Africa

Matthew.warren2@rmit.edu.au
shona.leitch@rmit.edu.au

Abstract: In contemporary organisational crisis management, real-time digital communication has become essential for protecting corporate reputation and maintaining stakeholder trust. This paper examines the strategic role of social media in crisis communication through an analysis of a significant cyber security incident. On 2 July 2025, Qantas Airways, Australia's flag carrier, experienced a major cyber attack that compromised an offshore system containing personal data of approximately six million customers. This paper investigates the airline's crisis communication response across multiple digital platforms, including Twitter, Facebook, and other online channels, while also examining the communication activities of additional stakeholders involved in the incident. This study critically evaluates Qantas Airways' management of the cyber security breach in relation to crisis communications. The analysis identifies both effective strategies and areas of weakness in the airline's approach to managing public sentiment, disseminating incident updates, and engaging with affected stakeholders through social media channels. The findings contribute to understanding best practices in digital crisis communication and offer practical insights applicable to organisations navigating similar security incidents in an increasingly connected environment.

Keywords: Cyber Security, Crisis Communications, Social Media and Australia.

1. Introduction

Kaplan and Haenlein (2010) defined social media as “a group of internet based applications that build on the ideological and technological foundations of Web 2.0 and that allow the creation and exchange of User Generated Content”. In this paper we focus on one Australian case study and the use of social media, namely how it can be used in an incident/crisis situation relating to Qanas, Australia’s leading airline.

In 2010, a Qantas flight made an emergency landing in Singapore due to an engine problem. In the key ‘golden hours’ after the incident Qantas were using traditional media to combat inaccurate media reports that reported that the plane had actually crashed. At the same time, passengers were tweeting pictures of the damage as their plane sat on the tarmac and a photo from an island showing locals holding a large piece of debris circulated around Twitter with the hashtag #QF32 that intensified spreading the false rumours of a plane crash (Roshan et el, 2013). However, the Qantas Twitter account remained strangely silent on the issue (Days later), Alan Joyce, Qantas CEO, said: "We were ready for traditional media we had our press statement out within half an hour of us knowing the issue. But we had missed this whole social media end of communication" (Bailey 2013).

This example describes the role social media can play in a crisis, and illustrates that organisations, even large ones such as Qantas, may be unprepared to manage the additional communications challenges presented by the widespread use of social media (Roshan et el, 2013). In the paper we address two main questions

- How did Qantas communicate with their audience in social media during an incident/crisis?
- How did Qantas use different social media applications in incident/crisis communication?

This paper is structured in terms of describing the key terms, the presentation of the Qantas 2025 case study and then discussing the outcomes of the case study.

2. Social Media: Key Terms

In this section we discuss some of the key terms that relate to the paper.

2.1 Social Media

"Social media" has never had clear boundaries. When someone warns about the dangers of social media, they might mean Instagram, WhatsApp, YouTube, or TikTok or all of them at once. The term became has a buzzword applied so broadly that its meaning eroded. Researchers from different fields (psychology, computer science, economics, communication) each emphasise different aspects, and the platforms themselves keep changing (Wolfers et al, 2025).

An example of different social media definitions include:

- Carr & Hayes (2015) — internet-based channels of mass-personal communication where value comes primarily from user-generated content;
- Obar & Wildman (2015) — Web 2.0 platforms built around user-generated content, personal profiles, and social networks;
- Kaplan & Haenlein (2010) — internet applications built on Web 2.0 that allow users to create and exchange content.

Earlier research described that for social networking sites, they are a subform of social media. Platforms when they allow users to (Boyd & Ellison (2007)):

- Construct a public or semi-public profile;
- Articulate a list of connections to other users;
- View and navigate their connections and those of others.

2.2 Incident / Crisis Management and Communication

The communication between the organisation and its audiences as a negative occurrence happens. The reason why crisis communication is important is that an incident/crisis can occur to any small or large corporation (Roshan et al, 2016). What is key is that corporate reputation is more affected by corporate response rather than the event that caused the incident/crisis (Roshan et al, 2016). You also have the situation that organisations with poor communication during an incident/crisis often make the situations worse (Marra 1999). Coombs and Holladay (2004) defined crises as unpredictable events that can disrupt an organisation's operations, threaten to damage organisational reputations However, this definition can be divided into an incident and crisis.

- Incident: an unpredictable event that resembles a crisis since it threatens organisational reputation. Still, an incident needs attention and if it is neglected or mismanaged it can escalate into a crisis (Roshan et al, 2015).
- Crisis: "a crisis is the perception of an unpredictable event that threatens important expectancies of stakeholders and can seriously impact an organisation's performance and generate negative outcomes (Coombs 2011)

Public communications activities focused on supporting communication to the public about the impacts of a cyber incident. This includes public information about the impact of incidents and actions that can be taken, and government and industry actions to support responses to these incidents (Roshan et al, 2016).

2.3 Cyber Security Incident

As cited by Roshan et al (2013. Incidents and crises, are common occurrences (Schultz et al. 2011). If an incident or crisis is not handled appropriately they can result in reputational damage to an organisation, bring financial loss, cause injuries or death to stakeholders or cause environmental harm (Heath and Millar 2004). Poor communication during an incident/crisis could even make the situations worse (Marra 1999).

A Cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations (ACSC, ND). In the context of this paper, a Cyber Security Incident in relation to QANTAS is the case study of the paper.

3. Qantas Case Study

On the 30th June, 2025 Qantas admitted that they had been a victim of a cyber incident (ABC, 2025a, BBC, 2025). The incident took the form of:

- 5.7 million unique Qantas customers data records were compromised at a third party call site in the Philippines;
- 4 million records were disclosed including names, email addresses and Qantas Frequent Flyer details;
- A further 1.7 million records impacting included the above information but also additional personal information such as phone numbers, date of birth, addresses, etc.

On the 18th July, 2025, Qantas sought to limit the spread of personal information of the Quantas customers information on the internet and the dark web. Qantas said it has obtained an interim injunction "to prevent the stolen data from being accessed, viewed, released, used, transmitted or published by anyone, including by any third parties" (ABC, 2025b).

Qantas use the following platforms to engage with their customers and their stakeholders.

Table 1: Qantas Information Platforms

Platform	*Crisis Information Shared*
Email	Yes
Web Site	Yes
Facebook	Yes
X	Yes
LinkedIn	Yes
Instagram	No
YouTube	No
TikTok	No

The data collection took the form of analysing the different information platforms and determing how messages that had been shared about the cyber incident. The following we describe discuss how the different official Qantas information platforms were used to shared information about the cyber incident.

3.1 Emails

Three emails were sent directly to Qantas customers:

- 2nd July – Describing that a cyber incident occurred on the 30th June and the scope of the incident;
- 2nd July – Telling members how they were impacted and the type of data that they had lost;
- 10th July – Telling members exactly the data about them that had been lost in the cyber incident and the steps that customers could take to protect their online identity.

*Official Qantas Website (*www.qantas.com.au)

The Qantas website was a focal point of distributing information related to the cyber incidents, they had dedicated webpages related to the incident. Specifics events related to:

- 2nd July – Describing that a cyber incident occurred on the 30th July and the scope of the incident;
- Updated 1st– 2nd July – describing how data had been lost and the type of data involved;
- During the period 2nd July and the 23rd July the website was updated seven times– sharing updates on the cyber incident situation, what to do next, contact points for customer, FAQ (Frequently asked Questions) about the incident.

The website became the focal point as single source of information from Qantas relating to the cyber incident.

*Facebook (*https://www.facebook.com/Qantas/)

During the period 2nd – 9th July, 2025 there were three Facebook posts about the cyber incident. In terms of interaction:

1877 people interacted with the post, e.g. thumbs up, loved the posts.

3576 comments were left to the posts;

161 individuals shared the posts with their Facebook network.

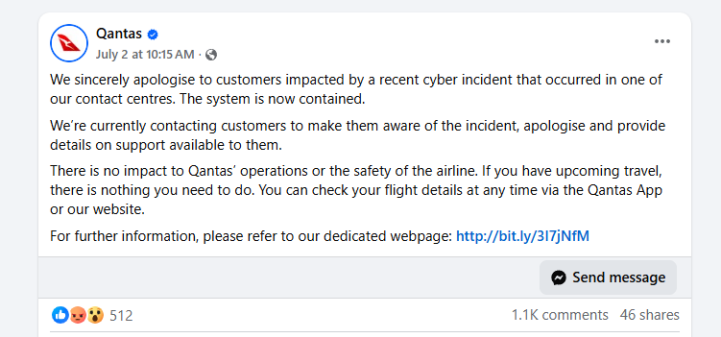

Figure 1: Qantas July 2 Facebook Page Post

The posts shared updates about the incident but always directed to the Qantas webpage as the source of truth.

X (formally Twitter) (https://x.com/Qantas)

During the period 2nd – 9th July, 2025 there were four x posts about the cyber incident. In terms of interaction:

199 Interactions with the post, e.g. thumbs up, loved the posts;

248 comments with left to the posts;

76 individuals shared the post within their X network;

There were 83000 views of the X posts.

The posts shared updates about the incident but always directed to the Qantas webpage as the source of truth.

*LinkedIn (*https://www.linkedin.com/company/qantas)

During the period 2nd – 9th July, 2025 there were three LinkedIn posts about the cyber incident. In terms of interaction:

1177 Interactions with the posts, e.g. thumbs up, loved the posts;

123 comments with left to the posts;

39 individuals shared the post with their LinkedIn network.

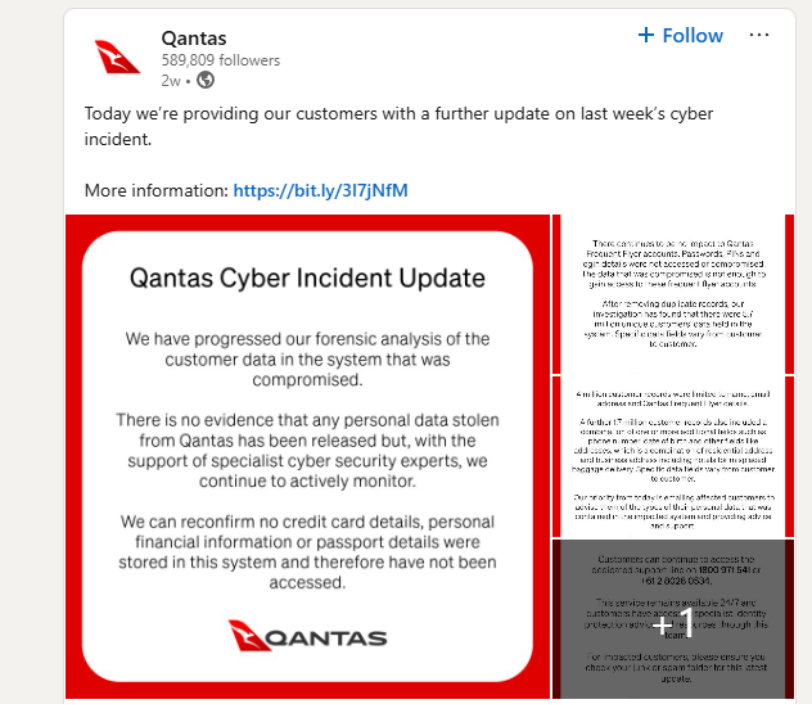

Figure 2: Qantas July 2 LinkedIn Post

The posts shared updates about the incident but always directed to the Qantas webpage as the source of truth. The use of the LinkedIn platform could relate to its professional nature and that some Qantas customers would be LinkedIn users rather than Facebook users.

There was no information about the cyber incident shared on the official Qantas social media channels for Instagram, YouTube or TikTok.

4. Discussion

In Australia a key cyber security concept is Critical infrastructure (CI). These are Physical facilities, supply chains, information technologies and communication networks which if destroyed, degraded or rendered unavailable for an extended period would significantly impact on the social or economic wellbeing of the nation, or affect a nation's ability to conduct national defence and ensure national security (ACSC, ND). In Australia the Aviation Sector is considered a key Australian CI domain.

From 2025 every Australian CI sector needs to develop Cyber Response Plan, including a communication strategy, in order to control the narrative of a cyber incident (Australian Government, 2025). In order to comply with the Australian Government directive Qantas would have had to developed a formalised Cyber Response Plan.

The Qantas Cyber Incident (June / July 2025) showed that Qantas follow a defined incident communication plan in place especially regarding the use of social media and online information channels. Qantas have a number of platforms to engage with customers. They chose their website as the source of incident information as well as three other Qantas social media platforms accounts reinforcing the same messaging as well as directing customers to the website as single source of truth.

One observation especially on Facebook was that Qantas did not interact with any of the user comments or questions about the incident. Qantas were using the social media platforms of as way of sharing information in an outwards direction. This could be for a number of reasons such as lack of resources during the incident to respond to every question that was posed or the communication aspect of the Qantas Cyber Response Plan did not include customer interaction.

What was also observed was that the official Qantas Instagram, YouTube or TikTok accounts were not used to share any information about the incident. The visual nature of these social media platforms may make it harder to share appropriate crisis incident information and Qantas discounted these platforms for their formalised plan.

In terms of the paper research question, the paper has highlighted

- In 2025 how did Qantas communicate with their audience in social media during an incident/crisis?

  Qantas has a formalised Cyber Response Plan including a crisis communication component. Qantas repeated the same messages across a number of platforms but directed customers to the official Qantas webpage as the single source of truth.

- How did Qantas use different social media applications in incident/crisis communication?

  In terms of the use of social media platforms Qantas avoid of use of image based social media platforms to share information even thought they may be more popular platforms.

5. Future Research

In October, 2025 the personal data of Qantas customers were released on the dark net. Up to 6 million Qantas customer records were exposed in July during a cyber attack on a third-party platform used by Qantas (ABC, 2025c).

This formed a second stage of the Qantas Cyber incident, when data was collected about Qantas use of social media as part of their incident plan. The next stage will be to formalised analysed the two parts of the Qantas Cyber Incident is a single more in depth study.

6. Conclusion

The study reported in this paper explored the use of social media for organisational crisis communication by a qualitative content analysis of social media platform during the Qantas 2025 incident.

The paper provides detailed analyses that led to support for existing understandings and important new

understandings on how organisations use social media for crisis communication based on the Qantas experience as well as describing the next stage of the research in relation to this incident and other related incidents.

Ethics Declaration

The paper does not require ethical clearance for the research.

AI Declaration

While preparing this work, the author(s) used Grammarly Pro for grammar correction. After using the tool, they reviewed and made necessary edits to the content, taking full responsibility for the final text.

References

ABC (Australian Broadcasting Company) (2025a) Qantas cyber attack victims say the airline is failing to protect data, URL: https://www.abc.net.au/news/2025-07-09/qantas-customers-let-down-by-cyber-attack/105507176, accessed 2/4/2026.

ABC (2025b) Qantas says 'legal protections in place' as cyber hacking group threatens to release personal data, URL: https://www.abc.net.au/news/2025-10-08/qantas-responds-to-cyber-hacker-threat-to-release-data/105866656, accessed 2/4/2026.

ABC (2025c) Hackers release Qantas customers' data on dark web URL: https://www.abc.net.au/news/2025-10-11/hackers-release-qantas-customers-data-on-dark-web/105881266, accessed 2/4/2026.

ACSC (Australian Cyber Security Centre) (ND) Glossary Term C's. https://www.cyber.gov.au/learn-basics/view-resources/glossary/c, accessed 2/4/2026.

Australian Government (2025) Australian Cyber Response Plan (AUSCYBERPLAN), URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/australian-cyber-response-plan.pdf, accessed 2/4/2026.

BBC (British Broadcasting Company) (2025) Qantas data breach exposes up to six million customer profiles, URL: https://www.bbc.com/news/articles/cd6gnyl9923o, accessed 2/4/2026.

Bailey, J. (2013). Crisis Communications in the Age of Social Media: How the Aviation Industry Woke up to the Power of Citizen Journalists., URL: http://www.ipra.org/itl/04/2013/crisis- communications-in-the-age-of-social-media-how-the-aviation-industry-woke-up-to-the-power-of-citizen-journalists, accessed 2/4/2026.

Boyd, D., & Ellison, N. B. (2007) Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communications,* (13), 210–230.

Carr, C. T., & Hayes, R. A. (2015) Social media: Defining, developing and divining. *Atlantic Journal of Communication,* (23), 46–65.

Coombs, W.T. (2004) Impact of Past Crises on Current Crisis Communication Insights from Situational Crisis Communication Theory, *Journal of Business Communication* (41:3), pp 265-289.

Coombs, W.T. (2011) Ongoing Crisis Communication: Planning, Managing, and Responding. SAGE Publications.

Heath, R., and Millar, D. (eds.). (2004). A Rhetorical Approach to Crisis Communication: Management, Communication Processes, and Strategic Responses. Hillsdale, NJ: Lawrence Erlbaum Associates.

Kaplan, A., and Haenlein, M. (2010) "Users of the World, Unite! The Challenges and Opportunities of Social Media" *Business Horizons* (53:1), pp 59-68.

Marra, F.J. (1999) Crisis Communication Plans: Poor Predictors of Excellent Crisis Public Relations, *Public Relations Review* (24:4), pp 461-474.

Roshan, M, Warren, M, Carr, R (2013) 'Understanding the role of social media in incident/crisis communication', 24th Australasian Conference on Information Systems (ACIS). 4-6 December, Melbourne, Australia.

Obar, J. A., & Wildman, S. S. (2015) Social media definition and the governance challenge, An introduction to the special issue. *Telecommunications Policy*, (9), 745–750

Schultz, F., Utz, S., and Göritz, A. (2011). Is the Medium the Message? Perceptions of and Reactions to Crisis Communication Via Twitter, Blogs and Traditional Media" *Public Relations Review* (37:1), pp 20-27.

Roshan, M, Warren, M, Carr, R (2015) 'Understanding stakeholders' expectations of organisational crisis communication by social media', in proceedings of the 2nd European Conference on Social Media (ECSM).

Roshan, M, Warren, M, Carr, R (2016) 'Understanding the use of social media by organisations for crisis communication', *Journal of Computers in Human Behavior,* (63) (October).

Wolfers, L, Neumann, D, Klein, S, Gaiser F, Anderl C and Utz S (2025) What do you mean by "social media"?, *Annals of the International Communication Association*, (49), 192–204, Oxford Academic, UK.