VOL 40, SEPTEMBER 2023

TESTING TIMES

Crisis communication strategies and responses in the spotlight

KEY LEARNING POINTS

- MANAGING DATA MATTERS
- HAVE MORE THAN AN APOLOGY
- MOVE QUICKLY
- PRIORITISE THOSE AFFECTED
- UNDERSTAND THE IMPACT

Amanda Coleman
COMMUNICATION

WHAT HAPPENED?

Managing personal data may feel like a dull subject but it is a significant risk to every business and being ready to manage any issue is vital. The loss of data can damage a business' reputation, lead to a costly fine and may be your next crisis.

Last month the Police Service of Northern Ireland (PSNI) mistakenly released details of all of its almost 10,000 police officers and staff. The information was shared in error linked to a Freedom of Information (FOI) request. Details were available on the PSNI website for some time. It is one of three data breaches linked to PSNI that are being examined. The release of personal details of officers and staff was a significant security issue and dissident republicans has, as was feared, accessed the data.

At the same time Norfolk and Suffolk police identified an issue with a 'very small percentage' of FOI responses. The technical issue led to raw data being provided that included 1,230 people's information and it was feared this included the data of victims and witnesses.

And the end of August saw South Yorkshire Police apologise for losing data including body worn camera footage in a 'significant and unexplained' situation. It was stated that 69 cases could be affected by the loss.

In addition a quick check identified further data breaches from Christies, Seiko, National Grid in America, University of Minnesota and the language app Duolingo. There was also a situation where the A level results of all students at John Taylor High School in Staffordshire were shared with parents due to 'human error'.

What was the communication response and what could it have been?

In all of the police cases they issued apologies for the situation. The PSNI put the Chief Constable to front a press conference after he returned from holiday to face the media and the Northern Ireland Policing Board. The police explained that they realised the seriousness of the situation and highlighted the actions that they were taking.

The Northern Ireland Policing Board have announced an independent 'end to end' review of all the data breaches. The Chair said it had 'damaged the reputation of the service and impacted the confidence of officers…'.

The details of the review will be vital reading for all managing data and preparing to respond to any breaches.

Norfolk and Suffolk police released the information linked to the notification that they had made to the UK Information Commissioner. The information about the situation was released publicly as they started to contact the people affected which could take until the end of September.

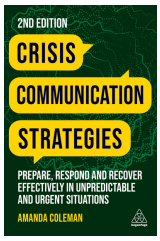
An internal investigation and an apology was central to the communication from South Yorkshire Police. They explained that the data had been deleted rather than moved. But the impact of this may become clear as it potentially impacts on civil and criminal court cases. At a time when policing is under significant pressure, it is questionable whether an apology is going to be enough, and more action and a demonstration of changes may be needed.

Subscribe to my crisis comms newsletter https://underpressure.substack.com/

What do we need to remember in this situation?

- Prioritise management of data – the area of data management and dealing with Freedom of Information requests is a high-risk area and needs to have appropriate staffing and management in place
- Have a data breach communication plan – know what you would do to communicate if there is a serious loss of data, this can work side-by-side with a cyber-attack communication plan
- Be open about the situation – don't attempt to hide the problem, be open and share the details of what has happened at the earliest opportunity
- Prioritise speaking to those affected – don't wait for them to hear from the media or via staff, put resources into speaking to those affected so they learn from you and quickly
- Be ready to move quickly – having a plan will help you to operate at speed but with data losses and cyber threats speed is essential
- Stakeholder communication is essential – there is a requirement to alert regulatory bodies but make sure other stakeholders learn about the situation and what you are doing before it becomes public
- Apologise but have more to say – an apology is important but there has to be more that supports it. Explain what you are doing, how you are supporting those affected and be clear changes to how data is managed will happen
- Recognise the reputational damage – data losses can have a significant impact on the reputation of an organisation. Recognise that it may take some time before you can repair the damage done

For advice on issues management get a copy of Everyday Communication Strategies



For more case studies and crisis communication tips get a copy of Crisis Communication Strategies by Amanda Coleman available at book stores and on Amazon.