VOL 58, MARCH 2025

TESTING TIMES

Crisis communication strategies and responses in the spotlight

KEY LEARNING POINTS

- BE OPEN
- CHECK REPORTING ABOUT INCIDENTS
- EXPLAIN THE IMPACT
- ENSURE YOU UNDERSTAND
- GO WHERE PEOPLE ARE

WHAT HAPPENED?

Cyber threats need to be at the top of everyone's risk register. In the latest attacks during February a health provider, a book publisher and a talent agency were all targeted. In the UK, private health company HCRG Care Group, previously Virgin Care, was affected by a Medusa ransomware breach. Posts were identified on the dark web from a group claiming responsibility and threatening to expose more than 2TB of stolen data if the company refused to pay a $2 million demand. The situation emerged in late February, when there were problems accessing the website and patient information. The Medusa attack is known to exploit remote desktop vulnerabilities. The company alerted the Information Commissioner and regulators.

During February, the UK book publisher CPI was the subject of a ransomware attack and explained that action was being taken to recover systems following the attack. The Information Commissioner also said they had been contacted by talent agency The Agency about an issue. From information seen by publication The Bookseller, The Agency was linked to a Rhysida ransomware attack which had also targeted the British Library.

Technology issues have also been in the headlines as Apple removed the Advanced Data Protection feature, following issues raised by the UK Government. The ADP ensured only account holders could view photos and documents stored online. It means that not all iCloud data will be fully encrypted. Apple said it was 'gravely disappointed' that the system was no longer available.

Finally, the Cyber Monitoring Centre has started to rate cyber incidents in the UK. Incidents that have a potential financial impact of more than £100m, affect multiple organisations, and where data and information are available, will be rated from 1 (least severe) to 5 (most severe). Events will be categorised and ratings published alongside a report, which it is hoped will help organisations to protect themselves.

What can communication and business learn from the situation?

The health company HCRG Care Group gave some detailed information about the action that had been taken and the nature of the incident. They explained that forensic specialists were brought in to investigate and offered reassurance about operational activity being able to continue. However, in statements, they were not able to quantify the numbers that had been affected or say what data had been compromised. It is known that employees' personal data, financial records, medical information and government identity documents have been taken previously. It is surprising to see that the Head of Communication was quoted in some of the articles, which could mean that advice given early in the discussion was attributed to them.

In a positive step, HCRG Care Group did make an apology to those patients whose appointments had been affected and needed to be rescheduled due to the attack. But none of this information about the incident was available on the company's website.

CPI provided an explanation about the situation, including that they already had significant protection in place and that action was being taken. The statement explained that they were talking to customers and stakeholders. In contrast, The Agency refused to comment on the attack and The Bookseller provided some details from an internal email that had been seen. The Information Commissioner's Office confirmed the situation.

All the incidents were heavily covered in the technology media and by those monitoring cyber-related issues.

What do we need to remember in this situation?

- Be open and provide information to help those affected – both HCRG Care Group and CPI provided details to explain what was happening and the action that was being taken.
- Be aware of reporting on incidents – there are a number of regulators and bodies that are reviewing attacks and will be commenting on yours, even when you may not want to.
- Expect that staff will be discussing the situation – provide them with relevant information that will support what you say publicly.
- Alert those who are likely to be affected – this means both customers and staff, depending on the nature of the attack.
- Consider what support people may need – your customers may not understand the implications of a cyber-attack, data loss or a ransomware incident, so be clear in your communication. If they need to monitor or act, explain that.
- Provide information through a range of channels – don't just expect that if you tell the technology media everybody will know about the situation and what they may need to do. Consider website updates, social media and direct communication.
- As a communicator, ensure you understand enough details about the nature of cyber-attacks and what response different incidents may require.
- Ensure that cyber attacks are planned for and exercised – it is clear from the documents and reports that are available that all organisations are at risk.

New book Strategic Reputation Management published available now.

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.