In partnership with:

Communications Case Study

LinkedIn, leaking out

Which is more important in crisis communications – speed or accuracy? The answer is that speed is desirable and accuracy essential. If you communicate facts that are wrong, it is more damaging to your credibility than being slow.

Ideally of course, you want your crisis communication response to be both speedy and accurate but in the real world there often isn’t enough clear information about the incident for swift dissemination; we never have all the facts we want.

Many a crisis team has been bypassed by the media because journalists can find other sources of comment – possibly uninformed and speculative as may be – that nonetheless moves the story on. Prevarication can be the enemy of effective crisis communication.

But there are many things the lateral-thinking PRO can communicate early in a crisis that are 100% correct and worthy of media coverage.

On the morning of 6th June 2012, news broke that 6.5 million of LinkedIn’s user passwords had been stolen and posted on a Russian hacker website to be cracked. LinkedIn, immediately took to Twitter and its blog. It said that it was investigating the breach reports but could not confirm that hackers had accessed the site.

Essentially, they had nothing to go on. But that morning, LinkedIn Director, Vicente Silveira, took the opportunity to communicate that “while our investigation continues, we thought it would be a good idea to remind our members that one of the best ways to protect your privacy and security online is to craft a strong password, to change it frequently (at least once a quarter or every few months) and to not use the same password on multiple sites. Use this as an opportunity to review all of your account settings on LinkedIn and on other sites too. Remember, no matter what website you’re on, it’s important for you to make sure that you protect your account security and privacy.”

The media reported this sage advice. LinkedIn was controlling the narrative.

By the afternoon LinkedIn confirmed that some of the passwords were from LinkedIn accounts. It apologized and outlined how, while its investigations proceeded, affected members would be contacted so they could reset their passwords. Again, worthy of media reporting and the views of LinkedIn were still being sought by the media and prioritised over those of its critics.

It had taken LinkedIn seven hours to confirm that it had been hacked – a long time for a technology sector company with a technology issue. But they had nonetheless successfully communicated enough relevant and useful information to control the media narrative and give them time to ensure absolute accuracy about what had happened.

LinkedIn understood the fundamentals of what makes news during a crisis. The mainstream media has three stages of inquiry during a crisis: The first stage, establish what has happened and what action has been taken as a result. The second stage, explain how it happened. The third stage, ascertain who is to blame

Specialist press websites and tech bloggers rushed ahead to the third stage. They questioned the speed and clarity of elements of LinkedIn’s response and its security. But unless they have a ‘smoking gun’, they will usually be too far ahead for the public and mainstream media who want to process what’s happened.

By the following day, 7th June, LinkedIn confirmed all 6.5 million passwords were from LinkedIn accounts. But it could still offer no explanation as to how the passwords had been obtained or what other data might have been compromised.

LinkedIn reiterated their apology and advice about password protection, assured members that the company was working hard to protect their personal data.

Pre-empting the second stage of the mainstream media investigation, it offered new information – that they were working with the FBI to investigate the matter. Implicit in this to the media is “hold off to second stage inquiry until the FBI professionals have got to the bottom of it”.

By 9th June, LinkedIn was actively pushing the line that it was a victim of “criminal activity” and were “working closely with the FBI as they aggressively pursue the perpetrators of this crime”. And for good measure added that “as you may have heard, there have been reports of other websites that have suffered similar thefts” (music site Last.fm and dating site eHarmony had also suffered password breaches at the same time).

And then it dropped off the media’s radar.

Journalists abhor an information vacuum. Communicate fast and accurately to control the narrative and prevent journalists from needing to find other sources of comment who may be unkind to you.