Does anyone really care about a data breach?

TalkTalk got hacked, sensitive info was stolen, customers were furious and shareholders fled to the hills. How bad will it turn out to be?

To the certainties in life of death and taxes, perhaps we should now add: getting hacked. Telecoms operator, TalkTalk, believe so. The established view is that the reputation of corporations that lose customer (or employee) data suffer immediate and long-term reputation damage. But to proffer a contrarian view – really?

Two of the biggest data breaches in 2014 in the USA were big name retail brands: Target and Home Depot. Between them they lost the credit-card and personal details of almost 100 million customers. And how did they fare in the 2015 Harris Reputation Poll of 27,000 members of the American public? They had nigh-on the same reputational scores as the year before. Their reputations were considered overall to be 'good' or 'very good'. So much for inevitable long-term damage (among consumers at least).

What of sophisticated financial audiences? Target suffered short-term damage and costs – a 46% fall in profits and it had to spend $236 million on software updates, legal fees, customer reimbursements and other costs related to the security breach; Home Depot incurred breach-related costs of $62 million. Yet while both companies saw their shares dip briefly, they swiftly rose again to levels well above the price before the hacks became public.

> "The public seems to have factored into its thinking that data breaches can and will take place. People just hope it won't happen to them"

The public and investors swiftly forgave and forgot. No long-term reputational damage. Can TalkTalk expect the same? The public seems to think that data breaches can and will take place. People just hope it won't happen to them. Cybercriminals (who in TalkTalk's case may even be as young as 14) are becoming ever more sophisticated and hacking is now an accepted fact of life. It's why most breaches barely make the news.

And the anecdotal evidence suggests that public trust – and corporate reputation – is affected less by the fact that a company was hacked than by what it does to deal with the crisis. So much like any crisis really.

TalkTalk has certainly followed the crisis rule book. It apologised, reassured and took action. The company has been open and very customer-focused to the point of overstating the number of customers potentially affected. It made its CEO available to media demonstrating both 'grip' and that it was taking responsibility. It set up a dedicated website for the incident and communicated directly and swiftly with every customer, offering free credit monitoring to all of its customers. The police made arrests, reinforcing – perhaps – that TalkTalk was a victim too.

So surely this is good news for TalkTalk? Maybe not. At the heart of reputation recovery surely lies what your reputation was before your crisis began.

YouGov's BrandIndex data five days into the story, demonstrated the impact the hacking was having on the public's perception of the company. TalkTalk's Buzz metric (measuring whether a respondent has heard something positive or negative about a brand in the past two weeks) had plummeted, falling from -1 to -50; its Reputation score had dropped from -10 to -34; its Recommend score – where respondents are asked whether they would recommend a brand to a friend - had plunged from -7 to -39. Essentially, TalkTalk's reputation was already poor and it just got worse.

The public presumes that companies have measures in place to protect their data (despite constant evidence to the contrary). TalkTalk portraying itself as a victim seemed less credible when people learnt that this was TalkTalk's third data breach in a year. Less victim, more a law breaker if it did not have the appropriate measures in place to safeguard its customers' data.

And what of investors? They hate surprises which is why they sell shares and share price falls when data breaches are announced. But they are fundamentally more interested in underlying performance, which is why Target and Home Deport shareprices recovered quickly. But TalkTalk's immediate shareprice fall merely compounded a 30% fall over the previous six months. Its existing reputation among some financial commentators and investors was of a financially fragile company run on a shoestring relative to its broadband rivals. That the company refused to waive contract break fees if customers wanted to leave played to this narrative.

Minimizing the impact of a data breach on public confidence requires transparency and swift, honest communication with customers. Just as in any crisis. The better your reputation before the breach, the faster you will recover. Whither TalkTalk?