How to communicate and manage your reputation with a data breach

Insights Paper
Reputation Management 2019

Written by: Stephanie Paul, Melanie Edgar and Samantha Townsend

Data breaches have become a global concern and risk for industry, with the number of reported breaches on the rise. Businesses impacted by data breaches are experiencing devastating consequences, including enormous financial losses, the erosion of customer and client confidence and the destruction of their brand and reputation.

Given the high level of public scrutiny and the increased regulatory environment, businesses have realised they can no longer bury their heads in the sand when it comes to cyber security. The issue has ignited a number of questions regarding industry readiness. How prepared are Australian businesses for a possible data breach? How do you communicate a data breach to your customers, clients, employees, vendors, suppliers and the public? How resilient is your organisation in the face of potential disaster?

Although there is no magic bullet for preventing a data breach (even global brands like Facebook and Yahoo have been exposed), businesses can take proactive steps to ensure they have a robust cyber security communications response plan in place.

Whether businesses are the subject of a data breach as the result of a cyber-attack or from human error, all data breaches pose a significant threat to business. The consequences can be significant and far-reaching and include financial loss, reputational damage, destruction or loss of data, risk of exposing intellectual property or trade secrets, and unplanned downtime.

Although 262 data breaches were reported to the Notifiable Breaches Scheme in Australia between October and December 2018 – with 64% of breaches caused by malicious or criminal attacks - most organisations are not taking proactive action when

it comes to cyber security. According to the 2018/2019 BDO and AusCERT Cyber Security Survey, only 43.20% of respondents have cyber insurance. With so much at stake, cyber security - including a comprehensive cyber security communications response plan – should be a top priority for all organisations.

So, the question is: *How ready is your business?*

Implementing a cyber security communication response plan

Managing reputational risk

All businesses should have a cyber security communication response plan in place to protect their brand and manage reputational risk in the event of a data breach.

Data breaches are often leaked to the media and general public before affected parties and employees can be informed, or an internal investigation completed. Due to the speed and ease that news can be reported on social media, information about a data breach can go viral - whether an organisation is ready or not.

Businesses are consequently placed under enormous pressure to respond quickly with the facts of what they know. Those that respond swiftly and effectively with robust communications that address their internal and external stakeholders' needs are more likely to mitigate any negative consequences, including incorrectly reported information. Over the lifecycle of the data breach, businesses may need to manage media interest on a daily to regular basis to alleviate reputational risks and nurture stakeholder relationships.

In advance of an incident, a good communications response plan will provide your business with the framework, tools and guidance to manage an extremely tough and challenging situation.

Determine roles and responsibilities

A communications response plan should clearly outline the steps required to manage a data breach, as well as the roles and responsibilities of each person in the internal and external incident response teams.

Consider who will represent the different areas of expertise in your business. Who will be the head contact in the leadership team, IT, legal, communications and marketing and digital media, just to name a few? Due to the sensitive nature of data breaches, the size of the internal team should be carefully considered to contain information and help prevent any unauthorised or inappropriate leaks.

Manage fatigue

The external team (where relevant) should be briefed and placed on standby to provide specialist support and surge capacity to manage this crisis situation. Specialist support could include a public relations firm (strategic communications advisors), legal advisor, financial forensics team, and cyber security advisors.

A communications chain of command should also be established for multiple scenarios, clearly outlining who will be the key decision makers.

Institute a clear and efficient approval process

To ensure all responses to the media and the general public are timely and efficient, the chain of command communication materials should be as streamlined as possible. If there are too many people involved in approving media statements or other important content (approval by 'committee'), the key messages can become convoluted from too many opinions and perspectives being voiced and critical timelines will be at risk of being missed for a business to provide its update.

Media train the company spokesperson

The plan should also nominate the business' key spokesperson. Ideally, they should be a senior figure in the business, are confident public speakers and have comprehensive knowledge of the business. One spokesperson (as opposed to nominating several spokespeople) will provide a sense of continuity and help build a stronger connection with the public during this sensitive and challenging period. The nominated spokesperson should also undertake regular media training (covering multiple scenarios) to ensure they are well-prepared for a data breach.

> "ONLY **43%** OF RESPONDENTS *have cyber* **insurance.**"

Prepare communications materials

A comprehensive suite of communication materials wil be required for communicating and managing a data breach.

Preparation is the key to not being overwhelmed in the middle of a crisis situation – make sure your business has a pre-approved toolkit containing a variety of communication templates. Materials in the tooklit will need to be mapped to different types of cyber risks.

Templates for media releases and holding statements will need to be prepared, as well as communications materials for stakeholders, staff and customers (scripts, emails, presentations, website content, hotlines, FAQs, fact sheets and more).

From a social media perspective, pre-approved social media posts and tweets will need to be developed, much in the same way as the holding statements and media releases, so your organisation can respond to the digital world in a timely manner.

Think ahead of the social media communities that would be vocal in the case of a cyber breach and the hashtags they may use to communicate their messages. Implement a social media listening service in the event of a breach and ensure these communities are monitored closely. Effective social media monitoring will be critical to successfully managing a cyber security breach.

Plan maintenance and training

Communications response plans must be easily accessible for all members of the business.

All relevant staff members should be trained and familiar with the plan so they understand the steps they will need to take in the event of a potential breach. Training exercises – such as a simulated data breach – will help staff intimately understand their role under the response plan.

Response plans should also be reviewed regularly – ideally three times per year when legislation is updated – to ensure they are up to date.

Communications materials and services checklist

What communications materials and services in the following list have you prepared in anticipation of a cyber breach? Remember to map all items to each cyber risk.

1. A dark website that can be quickly activated as a central repository
2. Website banners to direct people to incident portal/webpage
3. 1800 customer line
4. Call centre scripts
5. Holding statement
6. Media releases
7. Media monitoring service to activate
8. Staff communications materials – emails, letters, scripts
9. Stakeholder checklists
10. Stakeholder communications materials – emails, letters, scripts
11. Fact sheet
12. FAQs
13. Pre-approved social media content
14. Social media listening and monitoring service to activate
15. Translation services for materials required for other countries

> “RESPONSE PLANS SHOULD *be reviewed* **regularly**”

Considerations for a successful cyber security communications response plan

A cyber security communications response plan should allow businesses to:

- Provide timely, factual and clear communication to affected parties;
- Outline the course of action being pursued by the business and steps for affected parties to follow to help mitigate the situation; and
- Direct people to where they can access more information from the business once available.

Apologise

The power of an early apology cannot be overstated. A communications response plan should acknowledge the gravity of the breach, and provide a sincere apology and a commitment to maintain open and transparent communications while the situation is rectified.

Ensure the apology is genuine and does not blame the situation on other parties, faulty systems or circumstances 'out of your control'. A genuine apology will help repair damaged relationships with affected parties; foster good will and potentially reduce any anger or bitterness. The customer, client and or employees should always be front and centre of any apology – after all, it is their data that has been breached and their personal security compromised.

All communications materials that include apologies should be developed in tandem with the legal team and mapped to different cyber breach scenarios.

How not to apologise

US consumer credit reporting agency Equifax's apology for a data breach in 2017 which compromised the personal information of up to 143 million Americans – one of the biggest breaches in the world - is a good example of how not to apologise.

CEO Richard Smith's media statement said the breach was "clearly disappointing for our company" and he apologised to "consumers and our business customers for the concern and frustration this causes".

Equifax's description of the breach as "clearly disappointing for our company" deflected the focus away from the customer and made Equifax the 'victim'. Also describing the data breach as a "concern" for customers also diminished the seriousness of the situation.

Respond swiftly

Responding quickly, frequently and honestly tells the general public that you are working 24/7 to address the situation and repair any damage that has been created. It also demonstrates that you genuinely care for your customers.

Be transparent

Businesses should be as transparent with their customers as legally possible.

Of course, this does not mean you should reveal all your company's decisions or steps to be taken in order to be perceived as being transparent. However, you should share all relevant facts and information with customers and the general public. Make sure your team understands just how much information can be shared in various situations (always refer to your legal advisor if unsure and the Notifiable Data Breaches Scheme under the Office of the Australian Information Commission (OAIC)).

Although it might be tempting to omit information from statements to protect your organisation's reputation, being dishonest in this situation will most definitely backfire and pose a greater risk to your brand and reputation than the original breach. Being vague or omitting details from official statements will look like you are deliberately hiding information and you cannot be trusted. Omissions may also land your organisation in a difficult position with the relevant regulatory bodies, such as the OAIC and Cyber Emergency Response Team.

Positive action

Delivering a heartfelt apology doesn't mean much if you can't back it up with meaningful action. An organisation needs to clearly outline the steps they will be taking to rectify the situation, including any mandatory reporting requirements, and action to prevent future similar breaches or cyber-attacks from occurring. Possible steps might include removing people responsible for the breach, restructuring the business to prevent further breaches or hiring new staff or advisors who are data breach specialists.

Provide support and information

Businesses should provide regular updates to customers, clients, key stakeholders and key media.

These updates should also direct customers and journalists to a place where they can access any relevant information on the breach including media statements, fact sheets, FAQs and instructions. This could be a webpage that links back to the main homepage on the business's website. This web page should provide information on the breach, how it happened, who has been affected and what course of action the business is taking. The business should also clearly outline how affected customers can either register their interest for regular updates; register for compensation (if any is being offered) or contact the business for further information.

When it comes to successfully managing a data breach, the size and the reputation of the affected business does not matter. All data breaches wreak havoc - no matter whether the business is an ASX-listed corporation or a suburban store. What does matter is how prepared your business is, and how well-developed your communication materials are.

When transparency matters

Yahoo – now known as Altaba - experienced a data breach in 2014 where 500 million accounts were compromised. The business stayed quiet on the matter, even while it was in negotiations to sell its core internet business to Verizon in the (Northern Hemisphere) summer of 2016. The business only disclosed the matter to the public and Verizon in September 2016.

The consequences were dramatic. The following day, Yahoo's stock price dropped 3% and as Verizon declared the breach a "material adverse event" under the Stock Purchase Agreement, Yahoo agreed to reduce the purchase price by US $350 million. The US Securities and Exchange Commission (SEC) later issued Yahoo with a US$35 million fine for failing to disclose the breach in its public filings.

Businesses that have developed a cyber security communication response plan are more likely to stay focused in an extraordinarily high pressure situation. They will have a clear course of action to follow in the event of a data breach, and, as a result, are more likely to emerge with significantly more of their customers retained and their reputations intact.

In today's digital era, where businesses have become increasingly more vulnerable to data breaches, being prepared could be the difference between sinking or swimming.

Level 17, 100 Edward Street,
Brisbane QLD 4000
GPO Box 1564, Brisbane 4001
P +61 7 3230 5000
W www.phillipsgroup.com.au