Customer Breach Support
How to deliver a good customer experience in a data breach
Customer Breach Support | How to deliver a good customer experience in a data breach
Introduction

The General Data Protection Regulation (GDPR) has landed in Europe and organisations wait with baited breath to see how the various regulators across the EU will deal with the breaches we have seen over the last few months. Just how big are the penalties going to be? How tough are the authorities going to be when defending the new regulations to improve the protection of citizens’ data?

While large fines will demonstrate how severe a breach can be and send a shiver through the business community (possibly resetting the risk barometer), the real issue is reputation—in the market, with customers and under the glare of the media.
The customer challenge

In Europe we are in new territory—navigating how to effectively manage the response to a data breach, under the eye of the newly empowered regulators. In the USA the data breach response market is mature and comprehensive, having been regulated for many years, albeit more loosely.

American companies have led the way in the delivery of comprehensive customer notification and support programmes, as well as providing protection via identity protection programmes, credit monitoring and dark web analysis. Extending, in the best cases, to full customer support if they feel they have suffered fraud or stolen identity.

In the USA, these services are expected and businesses that do not offer a detailed and well-executed customer experience are scorned. In Europe, we are seeing a wide range of response strategies employed by companies as they struggle to deal with the fall out of a data breach. Some provide scant details to their customers or direct them to their bank for help. Few organisations proactively provide a substantial support service. A multilingual response is provided in some cases but not many and certainly not on a comprehensive basis.

It is clear that there is no established standard and that most businesses have little understanding of the considerable complexity involved in supporting customers through a data breach.

The challenge is responding and engaging with your customers, against significant time pressures, whilst battling the breach crisis environment—lack of information, complexity, uncertainty, huge risks and lack of time. This is the world of crisis management and the normal mantra applies.

"By failing to prepare, you are preparing to fail"

Benjamin Franklin
Many of the breached organisations featured in the press will have had an incident or crisis response plan in place—for business continuity, cyber attack generally or for other crises they may expect to befall them. Some of these may even cover aspects of data breaches. However, few, if any, will have had a specific customer breach support plan in place. As a result, businesses struggle to provide a coherent response against the clock for their customers after data has been lost.

In many ways this is an extraordinary failure. Businesses put immense effort into securing their customers who are the lifeblood of most businesses in the B2C world, with a whole industry recently grown around customer experience or “CX” as it is known. Yet when a breach occurs and the organisation loses sensitive information belonging to its customers, they appear unprepared. This is when they need to demonstrate care and respect for their customers through a well-oiled response that has clear strategies, resources and infrastructure in place.
When a data breach occurs and is confirmed—in itself not necessarily a simple activity—the business must consider several stakeholder groups. There are two key parties at the forefront: customers and regulators. Notifying the regulator is relatively straightforward as long as you have built your strategy to do so. However, notifying customers immediately opens an arena of considerable risk and complexity.

Do you use email to notify customers, running the risk of being seen as a phishing attack? Do you send a letter by post which guarantees the highest readership and attention—but is more costly? Or do you send a website notification that, in reality, few will probably see and will drive a very low response?

Then there are the promises that this notification will commit to; the level of detail and the immediate scope of support you can offer. The ‘customer notification’ may generate huge call volumes way beyond the call handling capacity a business has at its fingertips. Understanding how to estimate this level of attention and assure the resource availability is critical, failing to do so could lead to long wait times and the risk of a social media storm.

Can you manage it well, keeping call waiting time down and customers satisfied—while also continuing business as usual with your call centre? All whilst customers begin to complain publicly on the Internet, leading to the media taking note of the breach. When it comes to the customers (or employees, patients etc.) there may be a need to operate a customer facing service in multiple languages at scale and within a short time frame. Providing support, reassurance and engagement to ensure that customers feel you care about
the risks they now face from the criminals who seek to use their data. This can be a huge challenge across several geographies and takes considerable organisation to establish, integrate and manage.

Identity monitoring and repair is another key area in both mitigating the risk to the customer and in supporting customers to respond to identify theft or fraud. Few know just what to do when this happens and there is little help available elsewhere unless you provide it.

A data breach is a hugely complex event on so many levels; technically, strategically and operationally. We see time and again, that those who have taken the time to prepare and put in place the key areas of support, will benefit from a quicker, better, more customer centric response when the chips are down.
The key areas to encompass

**Resources**
Internal and external resources (on call and retained) with expertise to respond, meet the surge and deliver

**Infrastructure**
The systems and capacity to cleanse data, route significant call volumes and keep websites up

**Notification**
The pre-established strategy as to how you plan to reach out ‘without undue delay’

**Engagement**
A clear approach for engaging with customers and meeting their needs

**ID Protection**
Strategies that outline what support your business is prepared to offer and under what circumstances (all of which carries cost)

**ID Repair**
The ability to help your customers pick up the pieces if they have been successfully attacked

**Insurance**
Clear understanding of exactly what your cyber, or other, insurance covers and what you can/cannot do as a result of those limitations—how fast can you reach your insurer or broker?

**Training and Exercising**
Being prepared goes beyond having a customer breach notification plan; your business requires an ongoing programme of scenario based training to build your capacity to protect your customer’s information
Conclusion

While GDPR has provided a focus and for good reason—it is only the first step to meeting the expectation of your customers and employees (as employee data is likely to be lost as well). Breaches will continue to happen, by hacking or more mundane reasons of misdirected email or lost laptop. Every business needs to be ready to respond in a timely fashion in order to manage the issue and provide high levels of customer service to maintain brand reputation. Failing to do so may cause damage to brand and business that could be catastrophic.
Get in touch

---

**Dominic Cockram**  
Partner  
Risk Advisory  
dcockram@deloitte.co.uk

---

**Hugo Morris**  
Partner  
Risk Advisory  
hmorris@deloitte.co.uk

---

**Mark Whitehead**  
Director  
Risk Advisory  
marwhitehead@deloitte.co.uk
Customer Breach Support | How to deliver a good customer experience in a data breach