Viewpoint

International data breaches

Have you thought of everything?

Index - Navigation

Through the eyes of our expert international data breach team

Our frontline data breach team has spent more than 10 years dealing with a broad range of challenging data breach response scenarios. Through their expert eyes, here is a Viewpoint paper that talks about some of the considerations.

In the next few pages, we will shed some light on the unknown challenges and misconceptions surrounding cross-border data breaches.

Above all, we want to help reveal some of the practical points that organisations with international customers may never have considered. This knowledge could, however, make a big difference to the response quality, speed, and ultimately recovery. Directly linking back to financial and reputational impact from an international data breach.

Introducing

Jim Steven
Head of Data Breach Response Services, Experian Consumer Services

Ryan Bradshaw
Senior Data Breach Response Manager, Experian Consumer Services

Lauren Blackamore
Product Manager, Experian Consumer Services

Kharmen Ranson
Data Breach Response Manager, Experian Consumer Services

1) Data breaches don't have to be catastrophic

This may come as a surprise statement: even far-reaching international breaches can be mitigated against. If you are prepared, and have third-party advisers on hand, an international data breach is difficult, but manageable.

However, there is a lot of forethought and planning that needs to go into being prepared for every eventuality. And there does need to be a shift from an 'it'll never happen to us' mindset to a 'thinking ahead' strategy.

"The first call with the client is quite challenging, there is a lot of information for the client to digest. They believe at this time one letter template will be sufficient. However, when you start to talk through the considerations eg. language, different customer types, ex-customers, multiple brands they start to understand how this evolves from one letter template to multiple to ensure it's a personalised message."

Jim Steven

IBM/Ponemon institute: 2018 cost of a data breach study

$3.86 m

$3.86 million: average cost of a data breaches globally.

Incident response team: top cost saving factor.

Companies who contained a breach in less than 30 days saved over $1 million.

Healthcare organisations: highest costs associated with data breaches.

CONSIDERATIONS:

- Pre-plan: move away from an 'it'll never happen to us' mindset
- Turn to trusted partners and third-party advisers – ahead of time
- Through them, understand the practical flow of data breach response

2) Regulation, like GDPR, is not a pain point - it's a good thing

Embracing the EU General Data Protection Regulation (GDPR) has become a top priority for organisations. An important part of this means being fully prepared for an international data breach.

While getting to grips with GDPR may have been a headache for businesses, putting the customer first is a good thing. What's not, is a misinterpretation of the legislation, or a misunderstanding of the separate jurisdictional rules that apply in each country.

Those organisations who have engaged the right 3rd party experts, such as lawyers, insurers, forensics and response partners can really get to grips with the practical steps that will get them to the point of readiness for a data breach incident.

"You have to think about how to comply with regulation first and foremost. And then how to manage the fall-out in a way that helps you come across more positively in the eyes of your customers too. It's about your legacy."

Lauren Blackamore

"Looking at where you operate, where your consumers are, and where your employees are, is vital. And then you need to work out where all your data is held. Assessing in advance is where you can make headway."

Jim Steven

CONSIDERATIONS:

- With the rise of e-commerce, customers no longer see borders.
- GDPR works in conjunction with every EU country's data privacy law. You also need to be aware of country-specific legislation.
- Tailoring your response to the individuals affected is what's important. Talking to them in their language is the first step to simplify the experience from the individual affected.

3) Understand your customer data and where it is held

Despite the huge regulatory milestone that was the introduction of GDPR in May 2018, many organisations we speak to still don't know exactly where their data is – and therefore that of their customers. Most concerning is that they are still unclear about where the data of their international customers is held.

In the event of a data breach, this could slow the entire notification and recovery process down, and put an organisation in jeopardy of regulatory fines. Above all, additional delay in communication can further jeopardise a company's reputation.

"So many people still think that if you're a UK company you only lose UK people's data. And you just don't. So many of us now have international customers. If you think about e-commerce, we don't see borders within the digital environment any more. If there's a data loss, you need an international solution. And that becomes much more complicated, more quickly."

Jim Steven

"Where is your data? And it's not just your data. It's suppliers who have access to your data. And, also, how is that data networked? If a server is breached, it may not just be where that data is hosted. It could have penetrated elsewhere. Has it gone to local computers, throughout your network? Or is it isolated? This is where an IT forensics team can really support".

Lauren Blackamore

CONSIDERATIONS:

- Do you also know where the data of your international customers is held and can you access it quickly if you need to?
- What about third-party suppliers? Where do they hold your data?
- If a breach happens, how far down the supply chain will it go?

4) Understand how you would notify those affected

The first critical point organisations need to deal with – once the scope of the breach has been ascertained – is notifying their customers. But how? A letter, an email or even social media. There are many considerations that go into what method to use; those considerations also depend on where you and your customers are geographically.

Then there are the different templates that are used to notify customers of a breach. If an organisation has different branding for different sections of the business, that needs to be incorporated into the correspondence accurately. Not to mention different domains and languages – which we will expand on next.

"Letters are more expensive and take longer, but more trustworthy – in many customers' eyes. Email is far faster and cheaper, but it may not be seen or believed. Organisations need to understand the consequences. If I am sending it out to French customers, it needs to come from an email with a French domain. And if you're using third parties, do they have access to your domain? It's complex and it can add days to your notification timeline, if a plan is not in place in advance."

Ryan Bradshaw

CONSIDERATIONS:

- Email notification may be cheaper, but how can you be sure it's been read?
- A letter may be costlier for an organisation to send out, but in some people's eyes it's more trustworthy and believable.
- It's important to note that whatever channel you decide on, all communication with customers may be used in future litigation. So, it pays to get it right from the get-go.

5) Pre-determine what resources and expertise you need to respond

The set-up of phone lines to help customers in the event of a data breach is one of the most intricate and important steps in the response process. Customers value speaking to someone for reassurance. Therefore, it needs to be organised quickly, and accurately.

Conversely, organisations we speak to often think it's something that's easy and straightforward. Far from it. Readiness planning regarding call centre services (post notification) can make the difference between a five day and a three-week turnaround. And that changes the scope of impact on the business.

"The set-up of phone lines is one of the most complicated aspects when responding to an international data breach. You may have to provide a local number and preferably a Freefone in the local country. We may need to set-up multiple lines in different countries and languages to accommodate customer needs."

Ryan Bradshaw

"The whole point of regulation is to protect the customer. If you aren't providing the right language and phone number – or charging someone £1.50 a minute to call an international number to find out what's happened - that is not customer-focussed. It's actually to the detriment of the customer."

Kharmen Ranson

CONSIDERATIONS:

- Will you use a local, international or Freefone number for your post-notification call centre? They're all achievable, but come with different set-up times and costs.
- You will need calm, consistent and informed experts to answer the calls. Will you use a third party?
- Every country comes with its own time zones and languages. This all needs to be taken into account and takes time if it's not pre-planned.

6) Understand what language requirements may be needed

Setting up a phone line is just part of the battle. Once an organisation works out where the customers that have been affected by the data breach are, they'll have to think about their native tongue.

Simply setting up one generic English line is not consumer-centric and could potentially lead to confusion and a lack of reassurance to customers. If handled incorrectly, this may have an adverse effect on how people view an organisation's brand in the future. Conversely, if handled well, organisations go a long way to keeping their reputation intact.

"When dealing with data breaches outside the UK/EU it is also important to consider the time zones. Finding native speaking experts is one challenge, the other is ensuring you can provide a call centre which is open at the right time for each country in which your customers reside. Having the capability to provide a call centre service that considers a potential time zone difference of 8-12 hours really demonstrates how seriously the organisation has put each individual's needs at the centre of the response."

Ryan Bradshaw

"The Chinese are an important consumer base for many. But what language would you use? There are 15 dialects of Cantonese to work with in the Chinese market. Then there's Mandarin. This is where planning ahead makes things so much easier. This can all be pre-prepared and you can hit the ground running."

Jim Steven

CONSIDERATIONS:

- During a data breach is not the time to put up a language barrier. Native speakers need to be on the phone lines to convey vital information - clearly.
- Once the languages are decided, call centre speakers need to have pre-approved, scripts and FAQs to work from.
- Understand where your markets are and what the corresponding languages are beforehand to save time.

7) Consider what remediation you might offer to those affected

Identity monitoring services are an extremely important part of helping mitigate risk of identity theft following a data breach. In the United States and the United Kingdom credit monitoring offers the an opportunity to keep a check on changes to their report.

One consideration thought is that depending on local laws it may be deemed inappropriate or even illegal to monitor people's identity. So assessing this in advance is important.

"Outside the UK and the USA, there's a number of countries that don't have mature credit monitoring services. So, you turn to identity monitoring. But then you've got the added complexity that not all countries will allow you to offer identity monitoring in their jurisdiction. In Sweden, for example, you are not allowed to scan and search for people's national insurance or identity number. It's illegal. It's far from generic. So we're tailoring our services to provide help that is relevant and appropriate."

Jim Steven

"Internally it's difficult to organise all these conversations about how to tackle notification, languages, identity monitoring rules, regulation etc. Even the starting point of getting your team rallied and talking it through is tricky across time zones and that's why conversations in advance around these practicalities can save time and unnecessary pressure in the heat of the moment."

Lauren Blackamore

CONSIDERATIONS:

- Some countries have identity monitoring, some credit monitoring, but in some it's illegal?
- It's complicated, therefore you need experts to guide you through jurisdiction-specific compliance, preferably in advance.
- Consider investing in identity theft and credit monitoring services.

8) Cyber Liability insurance covers the financial burden, but not the potential reputation damage

If a data breach has occurred and you have cyber liability cover, chances are you'll have this financially covered from an insurance point of view. Although, you may be covered financially there is still the challenge of understanding what needs they have and finding the right resources when an incident occurs.

A lot of organisations Experian advises find themselves in an ambulance-chasing scenario. But it really doesn't need to be this way. By partnering up with third party experts ahead of a data breach, a pre-planned strategy can make you look slick and professional, even in a time of crisis.

"There's a mindset that the insurance company will pay. Which it will, to a certain extent. But that doesn't protect reputational damage due to delays or mishandling of the situation. And it doesn't solve the issue. Whether you have 10 customers or 2 million, you need to find a way to work with third party partners to get yourself in a strong position, regardless of insurance."

Jim Steven

CONSIDERATIONS:

- Credible, trusted third-party support will lead to greater efficiency in responding to the situation and keeping the costs down.
- The insurers may pay, but consider will this manage the potential risk of reputational damage?
- Pre-preparation with the help of expert advisers, means the consumer is kept calm, and the media headlines will be more contained.

9) Business as usual is challenging when a data breach happens

Data breaches can be so all-consuming for an organisation, during a breach it's very hard – nearly impossible – for a business to operate as normal. Especially when a breach is international in scope.

First there is finding out what the breach actually looks like, then how far it's spread, whose data has been compromised, instruction of legal teams and insurers, then notification of customers. And that's just the start. Organisations that think they can continue to run under these challenging circumstances are misguided. The question is: for how long can you afford to stop operating as usual? The quicker the breach is managed, the quicker normal office hours can be resumed.

"If you speak to anyone who's suffered a breach, they'll say they've done nothing but breach for the past three weeks, day and night. Recently I was on the phone to a company's legal counsel at 03:00 in the morning and they had not slept for 27 hours, because they had to go live that next morning. Add international into the mix, and it's worse because of the time-zones and customers."

Jim Steven

CONSIDERATIONS:

- Everything will need to be evaluated and this means a lot of business as usual activity just has to go on hold.
- Having a data breach team pre-versed in how to respond to a crisis will mean you are clear about who your trusted partners are and that the key steps are taken.
- It doesn't make good business sense to go searching for a data breach response team in the heat of the moment.

10) Finding the right experts is key to a successful response

Just as you probably wouldn't move house without consulting an estate agent or a solicitor, you shouldn't try and navigate a complex field far from your own expertise without third-party help. In the immediate aftermath of a data breach – and beyond - specialist advisers will be your lifeline. It's vital that you are guided through some very practical, but essential steps that need to be taken to keep your customers reassured, and the regulators happy.

However, there is no need to be in a panic-stricken situation. By partnering up with response experts well ahead of a data breach happening, it is a manageable scenario during which you can lean on others for support and gain valuable knowledge. By saving time recovering from a breach, you will also save money and your reputation.

"You start with: we've got a problem, but we don't quite know what that is yet. If it is a breach, what do we do? You engage legal communities to assess the lay of the land. If it's a cyber event, you instruct an IT forensics company to check if you've actually had a data loss. Has someone got into your systems? When did they get in and what did they take? The notification regulations start to kick in. Yes, we've found a hole, yes someone has extracted information. But what information and who is it? At that point you're standing up crisis PR, thinking about what you're going to tell your external and internal community and you're trying to block the hole. This happens whether it's international or domestic. Then there's remediation."

Jim Steven

CONSIDERATIONS:

- The practical – and legal steps - that need to be taken following a breach are not obvious. Expert guidance will be needed to avoid fines and reputational damage.
- The speed in which you recover will dictate how much money it will cost you, and how you are viewed in the eyes of your customers.
- Preparing a thorough data breach response plan ahead of time makes good business sense.

About Experian

About Experian Data Breach Response Services

Know your

Threats | Vulnerabilities
Our proven business consultants will work with you to determine the right approach and help you to prepare a tailored consumer data breach response plan.

Prepare your

Plan | Resources | Processes | Data
Our proven experts will align the right resources tailored to your business scenario and create pre-determined communications which are stored ready for a live incident.

Recover your

Reputation | Trust
When a live incident occurs we work with you to finalise and activate the notification fulfilment, call centre support and web/credit monitoring services to affected individuals.

About Experian IdentityWorks Global

Our global dark web monitoring service enables you to provide a remediation service to your customers/employees following the theft, loss or disclosure of their personally identifiable information (PII). This is an important step in illustrating the importance the organisation places on such an incident and its commitment to taking reassuring action.

Contact us

www.experian.co.uk/databreach

breachresponse@experian.com

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk/databreach