

Deloitte.

**Taking a customer-centric
approach to a data breach**
Insights from crisis response

Resilience under pressure	3
Once the data is gone, it's the customers who need protection	4
Pre-breach: preparing for the inevitable	7
Post-breach: minimizing the impact for customers	10
Speed of notification	11
Quality of response	12
Reducing the impact of a data breach	14
A customers-first breach strategy: worth planning for	16
Contacts	17

Resilience under pressure

Will tomorrow be your turn for a headline-making data breach?

We all know by now that just about every company will have a data breach at some point. That means most clients know it as well, and so they expect the companies they've entrusted their business to be thoroughly prepared to respond quickly and efficiently to the smallest slip through the tiniest crack in their cyber-secure fortress. And they want to know what's happening and whether their data has been affected—today, not in a month or more.

Tough recent privacy-related legislation in Canada and the European Union further pressures organizations to sufficiently protect their customers' data. Your clients trust you to prevent the avoidable and prepare for the unavoidable—and it's not an impossible task.

Read on to find out how you can validate your clients' confidence in you by putting them first in a data breach incident—from speedy notification to a quality response by way of sound infrastructure, effective processes and systems, and competent execution.

Once the data is gone, it's the customers who need protection

With reports of cyber incidents dominating the news with increasing regularity, few organizations would deny their growing concern they may be the next data-breach news story.

Recent data-protection laws and standards, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the European Union's General Data Protection Regulation (GDPR), which extends to countries outside Europe, have shed light on how businesses prepare for and respond to a data breach. But when faced with such an incident, many companies will instinctively focus their resources and efforts on containing the breach rather than on their most important asset: their customers.

As the extent of the breach becomes known publicly, organizations with significant customer databases that do not prioritize customer needs risk magnifying their crisis exponentially.

Failing to manage the impact to customers is likely to trigger headline-grabbing regulatory fines and customer loss, potentially affecting both the value and reputation of the brand, increasing the risk of executive resignations, and accelerating the plummet of a share price.

If the worst does occur, how can a business ensure it's ready to respond and protect its customers?

As one in a series of crisis response insights from Deloitte, this paper looks at the customer-related challenges Canadian organizations now face in light of PIPEDA and GDPR, and identifies the factors that contribute to an effective, customer-centric response to a data breach.



More than **2.5 billion** records were lost by global businesses in 2017—a rise of

88%

over 2016¹

¹Gemalto Breach Level Index



Pre-breach: preparing for the inevitable

The GDPR and PIPEDA mandate organizations to put in place appropriate measures as part of their breach-preparation activities and to keep a record of all breaches.

These measures require a response plan that includes, among other factors, the notification to customers without undue delay of any breach that is likely to result in a high privacy risk for them or present a real risk of significant harm.

To explore what this might mean for most organizations, the graphic on the next spread looks at the implications of a breach through the lens of the key **challenges** they're likely to present.

From the moment a business realizes it has fallen victim to a data breach, the clock starts ticking.

According to a 2018 Ponemon Institute report on the cost of a data breach, it took **197 days** on average for businesses to realize they had suffered a breach.²



Customer impact:
recognizing the real risk to customers

All too often, businesses struggle to grasp that the real risk for customers begins in the days and weeks after the breach, when the criminals may not only be using the stolen data to access customers' breached accounts but may also be looking to defraud them through ongoing phishing, email, and call scams.

So, notifying customers about the breach is only the first step on a much longer engagement journey. Supporting and protecting them in the days and weeks following the incident is what really counts.



Speed:
mobilizing a breach response capability

From the moment a business realizes² it has fallen victim to a data breach, the clock starts ticking.

Inevitably, expectations stemming from GDPR's 72-hour regulatory notification window is likely to compel companies to compress their timelines, so mobilizing an operation of the scale and capability required to provide an adequate customer response becomes a highly visible, high-risk race against time if a firm is unprepared.



Capacity:
delivering a breach response while maintaining operational continuity

A breach is likely to result in a near-vertical spike in demand on an organization's internal operations, so an early challenge will be having enough resources to continue business-as-usual operations alongside setting up an effective breach response operation.

One high-risk capacity issue will be coping with the likely surge of inbound communications from concerned customers. Long call-waiting queues will quickly transition to negative social media commentary and press coverage about frustrated customers.



Proficiency:
specialist breach experience and knowledge

More than any other crisis, a data breach requires an extensive range of specialists to support a successful customer response: customer communications experts, social media analysts, operational specialists, cyber response experts, and forensic investigators, to name a few.

And of course, this army of support must be coordinated and managed with military precision, ensuring the right support is delivered to the customer in the right way at the right time.



Infrastructure:
technical and logistical support

The availability of key infrastructure to support a fast breach response is critical. Telephony capacity, enabling technology, and a clear operational structure are all vital to meeting the inevitable spike in customer demand.

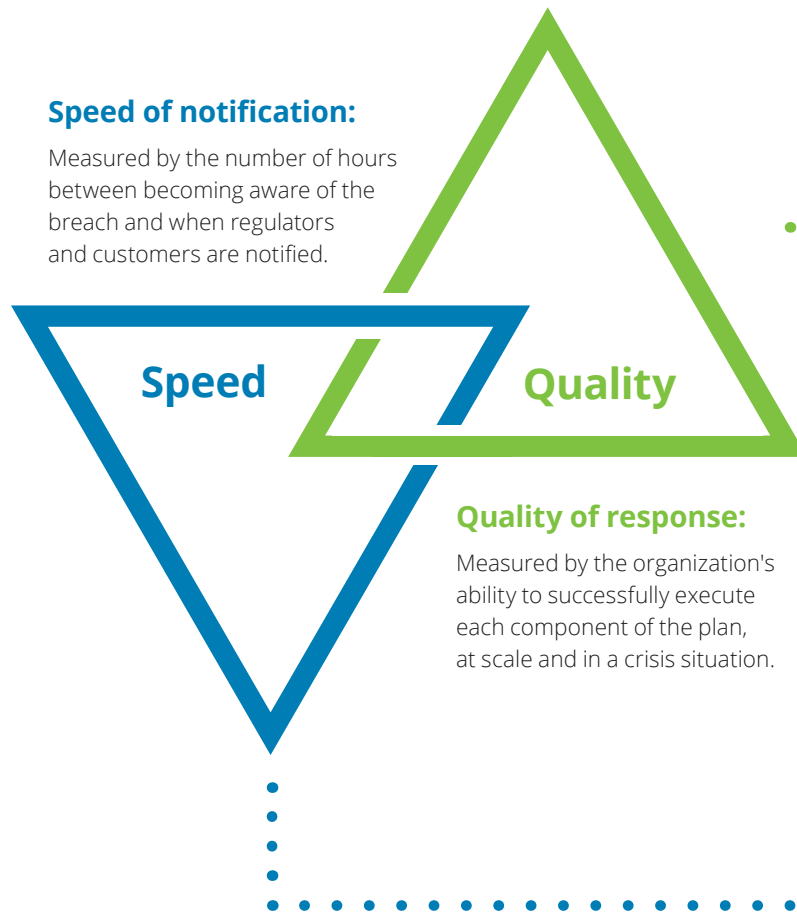
Logistical back-up is also necessary in key support areas. Mass printing and mail-out capability as well as credit-monitoring services, for example, all need to be ready to go live, with supporting contracts already in place.

²2018 Cost of a Data Breach Study, Ponemon Institute Research Report. Sponsored by IBM Security.

Post-breach: minimizing the impact for customers

Critical response factors

Ultimately, the outcome of a breach response is determined by two factors: the speed of notification and the quality of the response.



The critical component is staying focused on the customer during and after the breach.

Speed of notification

How quickly a business can inform customers of a breach and the accuracy of the details depends on the availability of scalable resources, the infrastructure in place to meet the subsequent spike in activity, and the quality of response.




In practical terms, this means:

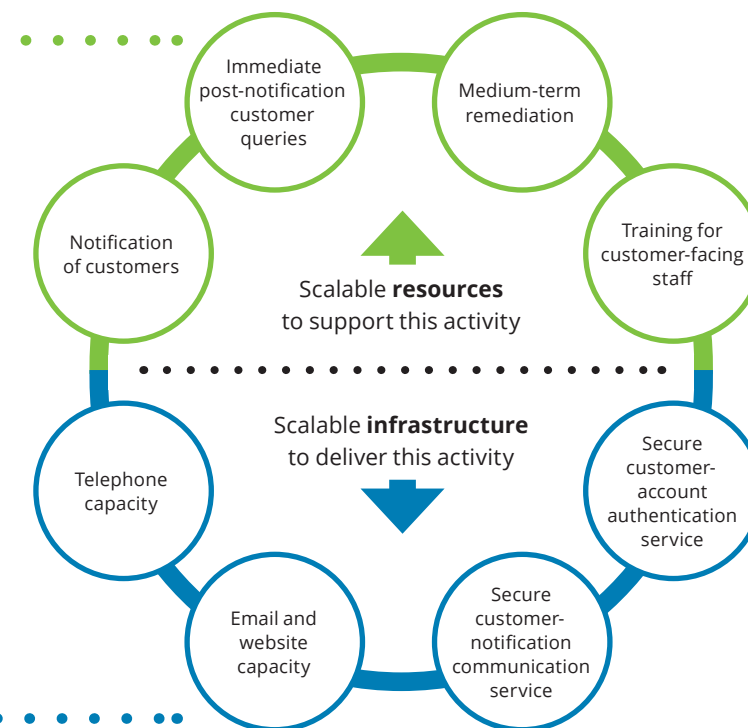
1. A scalable reserve team, guaranteed to mobilize immediately when a breach occurs to enable effective customer support.
2. The tools, processes, and systems to manage the customer engagement process in the days and weeks following the breach.

Even the most effective breach response plan will fail to meet the speed-of-notification race without adequate capacity and the supporting infrastructure to execute it.

Successful customer-centric plans recognize the volume of **trained resources** required to be in place to enable every one of the firm's at-risk customers to be notified, to address these customers' questions and concerns, and to remediate any suspected fraudulent activity.

Effective plans also recognize the **scale of the infrastructure** required to support breach notification, including:

-  **Outbound notification systems** with high-volume first-class mail capabilities and high-capacity incident-response website hosting
-  **Inbound communications tools** with a high-capacity phone system to quickly and securely direct customer calls and emails
-  **Identity-protection platform** that provides customer identity repair, monitoring systems, and insurance



Quality of response

The second requirement for success is determined by the level of **specialist skills** and **experience** of the response team.

PIPEDA and GDPR requirements are primarily concerned with data privacy and timely notification of breaches. However, timely notification without the proper level of detail can actually amplify customer frustration, fuelling scathing social media posts, media visibility, and litigation. Furthermore, notifying without the proper detail will likely force an organization to issue further notifications as the incident details become known, thereby keeping its name in the news for all the wrong reasons and frustrating clients. The quality of response is influenced by an organization's ability to investigate large volumes of data efficiently and effectively. Most data that is breached resides in databases, and is intermixed with sensitive personally identifiable information, health care information, financial data, loyalty rewards, social media accounts, usernames, and passwords.

Increasingly, media stories about data breaches indicate that an "unknown" number of records were involved or that information "may have been" accessed. These statements are examples of breaches in which the number of records affected could not be determined. When an organization cannot prove otherwise, they are often forced to assume that all information may have been accessed during the breach. This complicates clear messaging to customers and increases the impact associated with the breach.

Fortunately, there's an advanced investigation method that can help organizations pinpoint breaches to specific customer records, thereby allowing them to limit the impact of the breach and provide accurate messaging to customers. This method, called database forensics, is the focused investigation of database technology. Database forensics can qualify and precisely scope breaches, allowing companies to act to reduce the breach's size and impact. In some cases, it can prove that information governed by notification requirements was not accessed, which would release organizations from having to publicly disclose the incident.

The graphic on page 14 highlights both the more obvious impact factors associated with a data breach—for example, technical investigation and customer notification—and those that are commonly overlooked, which result in hidden costs.

Advanced investigation can help reduce the size and impact of a breach. In some cases, it can release organizations from having to publicly disclose the incident.

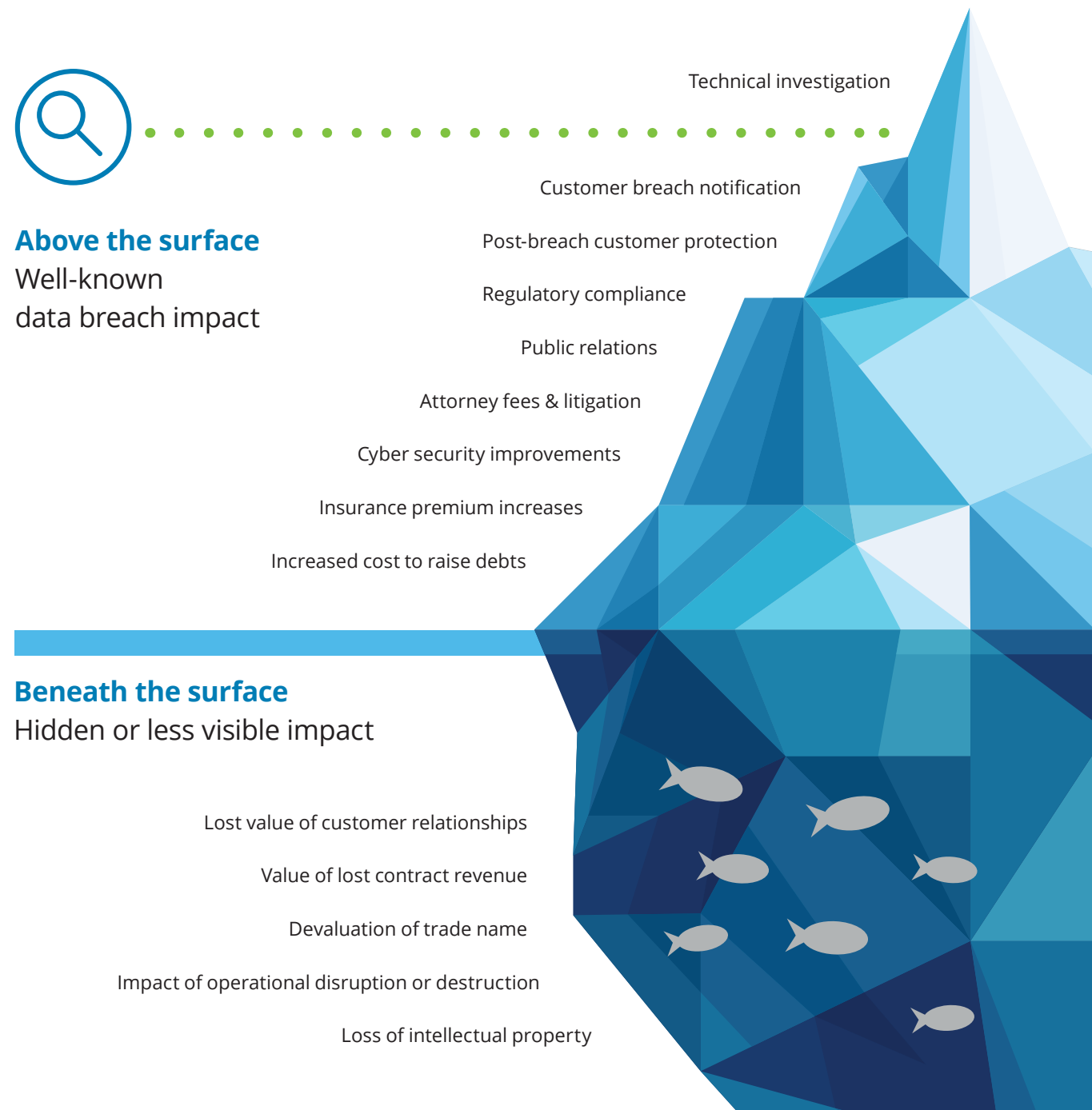
Organizations seeking database forensic expertise should ensure prospective providers have advanced tooling, skills, and credible experts who can defend findings in legal proceedings. Not all providers and experts are equally experienced in this advanced investigation field, and organizations should do their homework before selecting a provider.

In addition to gathering the right information to develop breach notification messaging, organizations need to have a full identity-protection strategy that encompasses everything from access to credit monitoring and fraud alerts to specialist identity-repair support services. Such support can do much to alleviate customers' concerns, reassuring them that everything is being done to support and protect them at this vulnerable time.

In short, a carefully managed customer engagement strategy is critical to an effective data breach response. The quality and awareness of a company's customer-handling staff in the contact centres, therefore, is also crucial—their ability to triage the needs of different customers, provide identity protection advice and support, and help with identity repair is key to the success of the customer engagement implementation. In many cases, this responsibility is outsourced to professionals to speed action and improve the customer care of those who routinely perform this work. A failure to manage and care for the customer is a failure to manage the organization's reputation.

Reducing the impact of a data breach

Specialized database and big data forensics can help organizations better discount, or pinpoint, breaches to specific customer data. This can limit breach impact to just the cost of technical investigation, or reduce it across all elements outlined in the infographic.



It's almost inevitable that organizations will find themselves facing a data breach, but it's not inevitable that the consequences include customer loss and reputation-damaging headlines.

A customers-first breach strategy: worth planning for

Large-scale customer breach response is more complex than most businesses realize, and few organizations have the infrastructure, resources, and specialist knowledge required to deal with the fallout on their own.

A best-practice customer-centric response protects customers, minimizes regulatory and reputational risk, and reduces the overall financial impact of a data breach. Deploying this at the pace dictated by Canadian and European legislation is only possible with effective planning before any breach occurs. Organizations need to ensure they have the right resources to cope with the volume of customer queries, and that they have the secure and scalable infrastructure that delivers the best service to those who own the future of the business: the customers.

During a data breach, support for customers is critical, complex, and significantly undervalued. High-performing customer support services minimize the potential for damage to customers from any subsequent criminal activity and help mitigate fines under PIPEDA and GDPR.

Such support services also reduce the possibility of reputational damage and improve customer retention—because well-supported customers are less likely to migrate to other organizations.

It's almost inevitable that organizations will find themselves facing a data breach, but it's not inevitable that the consequences include customer loss and reputation-damaging headlines.

Taking a customer-centric approach to planning for and responding to a data breach is the key to unlocking a positive outcome from an otherwise potentially catastrophic event.

Contacts

To find out more, contact:



Kevvie Fowler
Partner, Global Incident Response Leader and Canadian Resilient Practice Leader
905-767-8067
kfowler@deloitte.ca



Robert Masse
Partner
514-393-7003
rmasse@deloitte.ca

Cyber incident?

Call our incident response hotline:

1 833 DELOITTE (335-6488)

Deloitte.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private companies limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.