Taking a customer-centric approach to a data breach

Insights from crisis response

July 2018

Crisis and Resilience

What's going to happen tomorrow? How will our organisation be tested?

At Deloitte we help our clients not just through the good times, but also in the toughest moments of crisis. We know what it is like to face a critical challenge – and meet it decisively.

Our crisis services are founded on trust. We build the relationships that make organisations all over the world place trust in us to prevent the avoidable and prepare for the truly unavoidable.

When things go wrong you may feel exposed to the fiercest scrutiny. But our unrivalled network including specialists from risk sensing, agile governance and critical communications, can help you turn the tide during a crisis.

Many of our clients have emerged from great challenges even stronger than before. Make our strength your strength.

To find out more contact
crisisandresilience@deloitte.co.uk

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

With reports of cyber incidents dominating our news with increasing regularity, few organisations would deny their growing concern that it may now be a case of when, not if the next data breach headline carries their name.

The new General Data Protection Regulation (GDPR) has shone a light on how businesses prepare for and respond to a data breach. But when faced with such an incident, many firms will instinctively focus their resource and efforts on containing the breach, rather than on their most important asset – their customers.

As the very visible outcome of the breach takes hold, organisations with significant customer databases that do not prioritise customer needs risk magnifying the crisis exponentially.

Failing to manage the customer impact is likely to not only trigger headline – grabbing regulatory fines but also customer loss – potentially impacting both the value and reputation of the brand, increasing the risk of executive resignations and accelerating the pace of a doubtless already plummeting share price.

So if the worst does occur, how can businesses ensure they are ready to respond and protect their customers?

As one of a series of crisis response insight articles from Deloitte, this paper looks at the customer-related challenges organisations now face in light of GDPR and identifies the factors which contribute to an effective, customer-centric response.

Over **2.5 billion** records were lost by global businesses in 2017 – a rise of

88%

on 2016[1]

[1] Gemalto Breach Level Index

Pre-breach: preparing for the inevitable

The GDPR states that firms are mandated to put in place appropriate "organisational measures" as part of their breach preparation activities. These measures require a response plan which includes amongst other factors, the notification to customers "without undue delay" of any breach which is likely to result in a high privacy risk for them.

To explore what this might mean in reality for most organisations, the following looks at the implications of a breach through the lens of the key **challenges** they are likely to present.

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

Customer impact: recognising 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 are not just using the stolen data to potentially access the customer's breached account but 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: mobilising a breach response capability

From the moment a business realises[2] it has fallen victim to a data breach, the clock starts ticking.

Inevitably the GDPR's 72-hour regulatory notification window is likely to compress the timelines for notifying customers, so mobilising 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 whilst maintaining operational continuity

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

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

[2]According to a 2017 IBM Security sponsored report on the cost of a Data Breach, it took on average **191 days** for businesses to realise they had suffered a breach

Expertise: 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 – ranging from customer communications experts, social media analysts and operational specialists, to ID protection and repair advisors and forensic investigators.

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 a critical dependency. Telephony capacity, enabling technology and a clear operational structure are all critical in the race to meet the inevitable spike in customer demand. Then there's the logistical back up required in key support areas such as a mass printing and mail-out capability and credit monitoring services – all need to be 'ready to go live' with supporting contracts already in place.

[2] 2017 Cost of Data Breach Study" Ponemon Institute Research Report. Sponsored by IBM Security

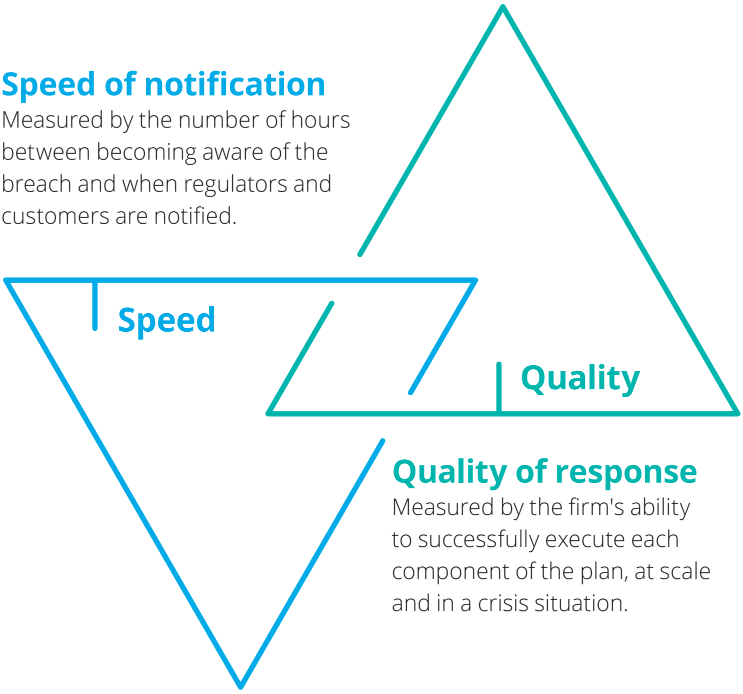
Post-breach: minimising the impact for customers

Critical response factors

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

Speed of notification

Measured by the number of hours between becoming aware of the breach and when regulators and customers are notified.



Quality of response

Measured by the firm's ability to successfully execute each component of the plan, at scale and in a crisis situation.

And of course the critical component is staying focused on the customer during and after the breach.

Speed of notification

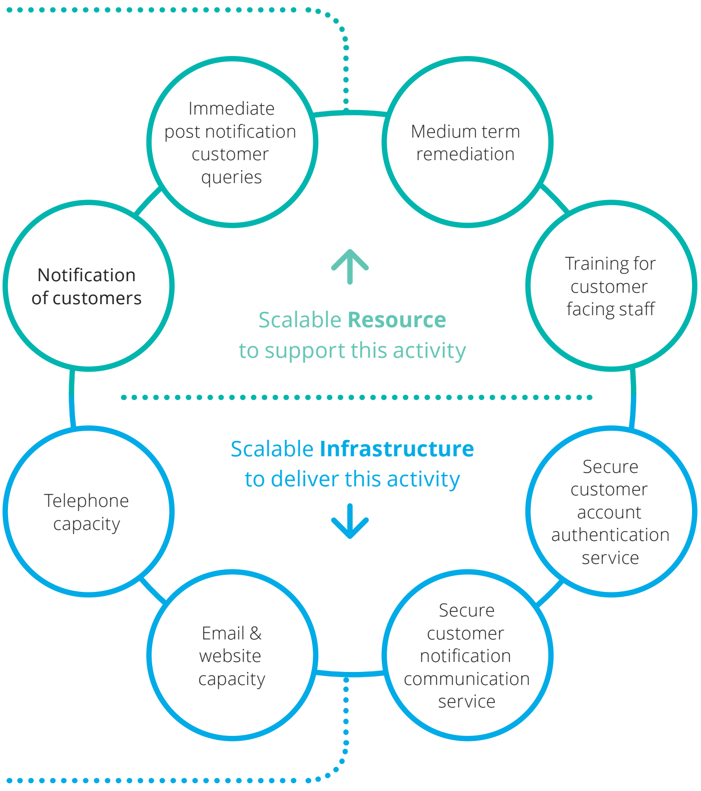
Looking specifically at the notification of customers, how quickly a business can inform them of a breach depends on the availability of scalable resource and infrastructure to meet the subsequent spike in activity.
So that means:

1. A reserve, scalable army of resource, guaranteed to mobilise immediately when a breach occurs and 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 supporting infrastructure to execute it.

Successful, customer-centric plans recognise the volume of **trained resource** required to be in place to enable every one of the firm's 'at risk' customers to be notified, their questions and concerns addressed and any suspected fraudulent activity remediated.

Successful plans also recognise the **scale of the infrastructure** required to support this, including:


Notification of customers
Immediate post notification customer queries
Medium term remediation
Training for customer facing staff
Scalable **Resource** to support this activity
Scalable **Infrastructure** to deliver this activity
Telephone capacity
Email & website capacity
Secure customer notification communication service
Secure customer account authentication service

Outbound notification systems 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 dependency for success - the quality of the customer notification response – is unsurprisingly determined by the level of **specialist skills** and **experience** of the customer response team.

Many firms may be under the mistaken assumption - in the idealistic days before their data breach - that the customer notification process is a 'one off' activity, so straightforward it can be delivered by existing customer support staff with no specialist knowledge or experience of such a crisis.

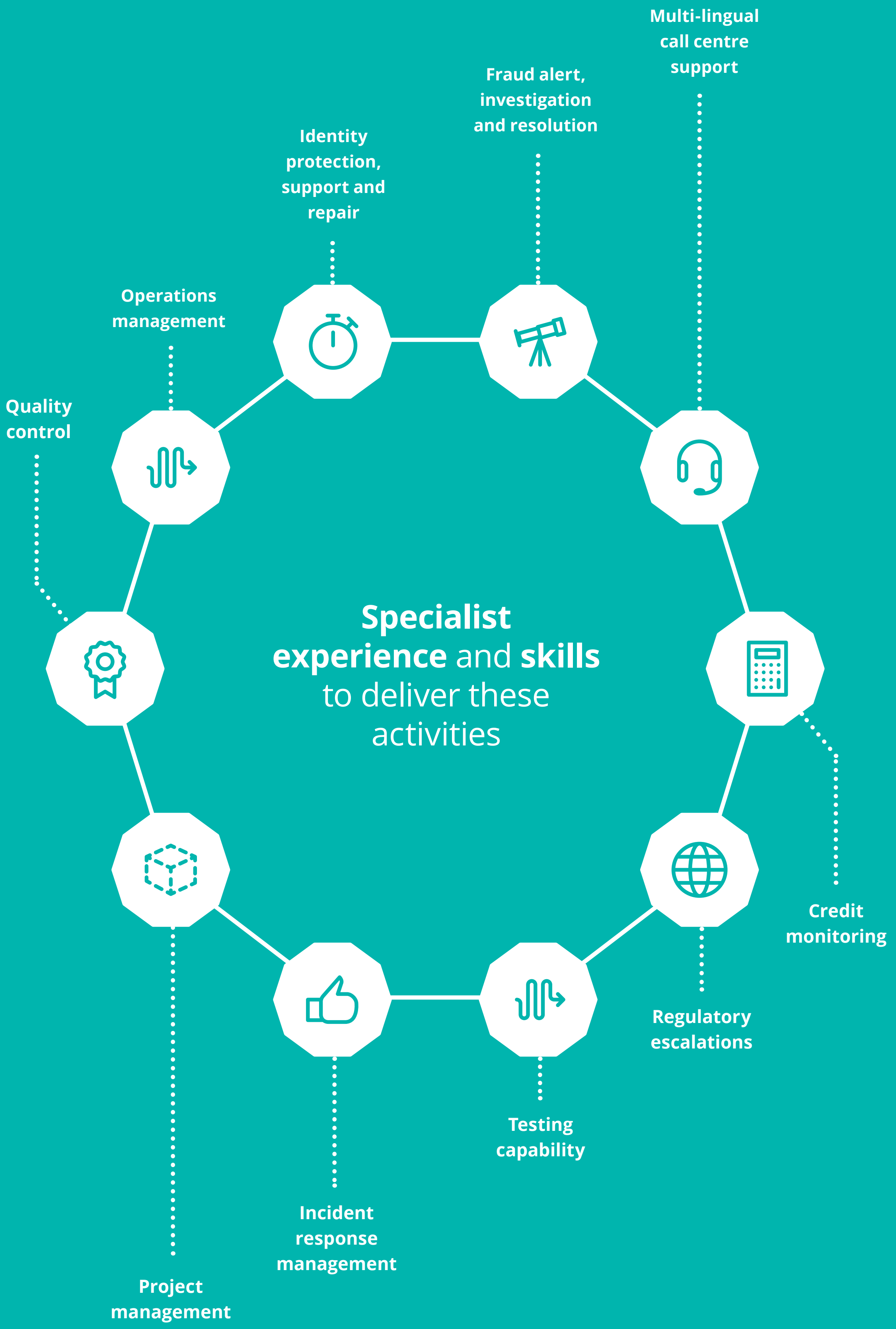
In fact the opposite is true. The graphic on the following page outlines the activities involved in a best practice response program. It highlights both the more obvious requirements – for example incident response management and regulatory escalation – and those activities which could mean the difference between a positive and negative customer experience, or between retaining their loyalty and a reputation damaging customer loss headline.

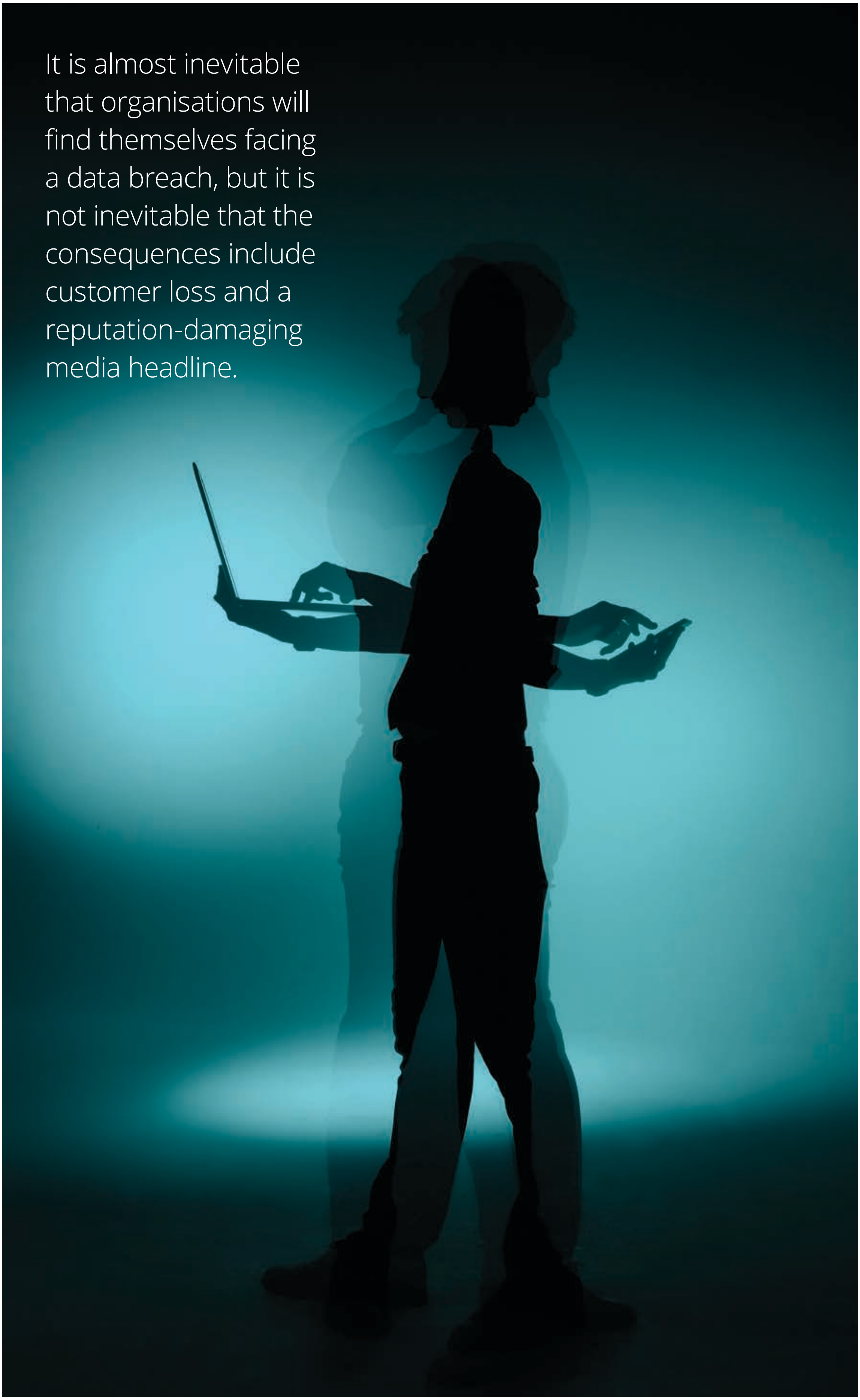
While some customers will simply want to know what has happened and why, others may believe they have been personally attacked or have other worries about their online identity. The scope of concerns will be wide across an audience with significantly different levels of understanding of the digital world and the realities of cyber risk; all require a relevant answer. There are indeed many risks they face, including identity theft, individual phishing attacks using their data to seek additional information, and many more. It is a dangerous time.

"While some customers will simply want to know what has happened and why, others may believe they have been personally attacked or have other worries about their online identity."

To address this it is important to have a full identity protection strategy, encompassing everything from access to credit monitoring and fraud alerts to specialist identity repair support services. Such support can do much to alleviate the customer's concerns and reassure them that everything is being done to support and protect them at this vulnerable time.

So a customer engagement strategy, and its closely managed implementation is critical. The quality and awareness of a firm's customer handling staff in the contact centres is key. Their ability to triage the needs of different customers, provide identity protection advice and support, as well as help with identity repair will become the central tenet of this customer engagement. In many cases this is outsourced to professionals to speed action and improve customer care of those who do this work all the time – failure to manage and care for the customer is failure to manage the reputation.


Specialist experience and **skills** to deliver these activities
Multi-lingual call centre support
Fraud alert, investigation and resolution
Identity protection, support and repair
Operations management
Quality control
Credit monitoring
Regulatory escalations
Testing capability
Incident response management
Project management



It is almost inevitable that organisations will find themselves facing a data breach, but it is not inevitable that the consequences include customer loss and a reputation-damaging media headline.

Conclusion

Large scale customer breach response is more complex than most businesses realise and few organisations have the infrastructure, resource and specialist knowledge required to deal with the fallout alone.

Best practice customer breach support protects customers, minimises regulatory and reputational risk and reduces the overall financial impact of a data breach. Deploying this at the pace dictated by the GDPR is only possible with effective planning before any breach occurs – ensuring that the right expertise is available to cope with the volume of customer queries, and that secure and scalable infrastructure 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 minimise the potential for damage to customers from subsequent criminal activity and help mitigate regulatory fines under GDPR. They also reduce the possibility of reputational damage and improve customer retention – because well-supported customers are less likely to migrate to other organisations.

It is almost inevitable that organisations will find themselves facing a data breach, but it is not inevitable that the consequences include customer loss and a reputation damaging media headline.

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

To discuss any of the issues raised, please contact:

Hugo Morris
Partner
Deloitte Managed Services
+44 (0) 20 7303 5985
hmorris@deloitte.co.uk

Mark Whitehead
Director
Deloitte Managed Services
+44 (0) 20 7303 0698
marwhitehead@deloitte.co.uk

Notes

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.