White Paper

Data breach response: readiness vs the reality

The growing trend of plans that don't safeguard businesses or their customers

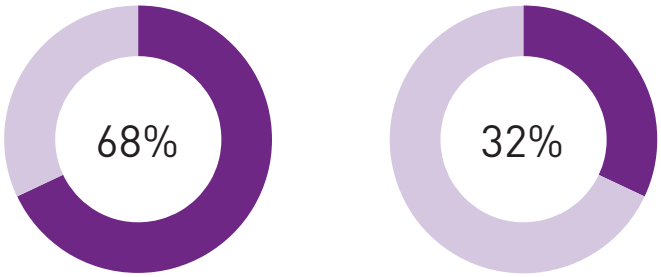
Contents

Introduction

Data breach: the digital dilemma

The world in which we live in 2017 is more interconnected and integrated than ever before. More personal information is being stored online and UK businesses are growing more technologically efficient by the day. Data is central to how we live; it is realising opportunities that were never possible before. Yet, while our digital knowledge and capabilities are expanding at a phenomenal speed, the sophistication of cybercriminals who target businesses of all sizes, is continuing to evolve - and they are often succeeding. This is the digital dilemma we face both as businesses and as individuals.

2016 data breach threats



Virus / spyware / malware

Impersonation of the organisation[i]

Research

i. HM GOVERNMENT 2016 Cyber Security Breaches Survey

Awareness vs action

Businesses today are more aware of data breaches than before and realise that cyber security needs to be part of their company's DNA. Yet many companies are still falling victim to data breaches which can have a devastating impact – particularly on smaller organisations. Response plans that aren't watertight and all-encompassing can cost a company great financial and reputational damage. According to HM Government statistics, the most common data breaches are happening to businesses that have already been attacked previously and have survived. Put simply: no one is immune.

2016

MOST COMMON breaches on businesses that have **already** been attacked[ii]

ii. HM GOVERNMENT 2016 Cyber Security Breaches Survey

2016

ONLY 29% of businesses have formal written cyber security policies[iii]

iii. HM GOVERNMENT 2016 Cyber Security Breaches Survey

Our research

Experian commissioned research consultancy ComRes to shed new light on this constantly evolving topic, backed up by new statistics. ComRes is a member of the British Polling Council.

On behalf of Experian, ComRes conducted an online survey of IT business decision-makers at small, medium and large businesses in Great Britain (Online) in January 2017, across a variety of sectors (including manufacturing, arts and recreation, business and finance). Respondents were either: involved in the decision-making of their company's data breach management, or were aware of data breach management if they were not directly involved. All respondents work for businesses that hold personally identifiable information (PII) data for 100 or more customers or employees.

The 200 professionals questioned were from the following sized companies: 50 from small businesses (1-49); 50 from medium-small businesses (50-100); 50 from medium-large businesses (101-250); and 50 from large businesses (250 or more).

It is important to note that when comparing figures from the business survey this year with 2016 findings, only SMEs were questioned last year, and not large businesses.

At the same time, ComRes also surveyed 2,001 British adults to obtain a wide and varied comparison of what business decision-makers think in contrast to the public – or, in other words, their (potential) customers.

To review the full ComRes research and questions visit: www.comresglobal.com

Our investigation

In this whitepaper, we will dissect and investigate the following findings:

- **Response plan effectiveness:** While many businesses have plans in place, we analyse if their plans are rigorous enough and if businesses really are as ready as they claim.
- **Customer confidence:** Maintaining customer trust is of paramount importance to businesses. Many businesses acknowledge this, but do they really take steps to prioritise this? We look at the reputational damage that's at stake.
- **Who's ultimately responsible?:** Increasingly it's IT business decision-makers who are chosen to lead the organisation's breach plans - but are they the right people and ultimately do they understand what this evolving responsibility really entails?
- **Across international borders:** We assess the state of play of current regulations – and what it means for businesses trading with customers in Europe, and further afield.

"We can see businesses are still trying to work out who is ultimately responsible for driving data breach readiness plans across the organisation. If businesses really are set on putting customers at the heart of their response, getting into the detail of what a response really entails is now a critical component of any business' DNA."

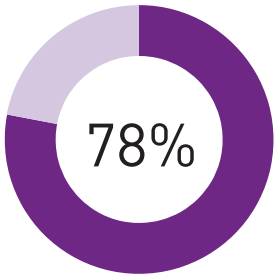
Jim Steven, Head of Data Breach Response, Experian

Data breach readiness and response

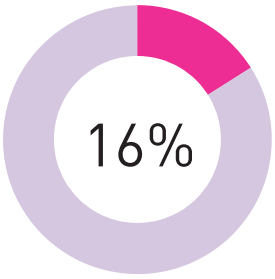
Is your business really ready?
According to our extensive analysis, one in five businesses across different sectors (21%) has experienced a data breach in the past two years, with loss or theft of records containing sensitive or confidential information. This statistic is similar to last year's findings (23%). Although this may not sound like a hefty figure, the reality is cybercriminals are becoming nimbler by the day. Data breach readiness is therefore a sensible business decision that, as we will discover, is a lot more cost effective than waiting for the worst to happen.

21% of UK businesses have been breached in the past 2 years

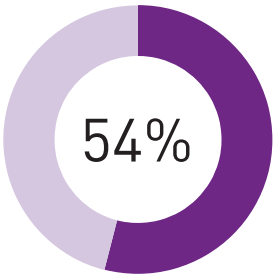
UK businesses in 2017



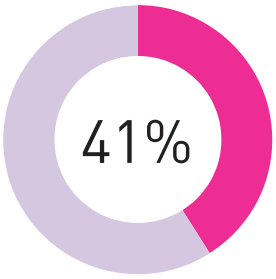
Have data breach plans



Do NOT have data breach plans

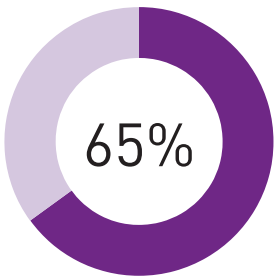


Have data breach teams

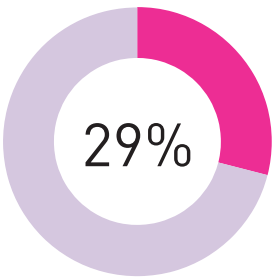


Do NOT have data breach teams

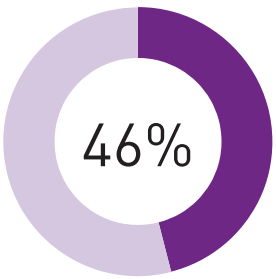
UK SMEs in 2016



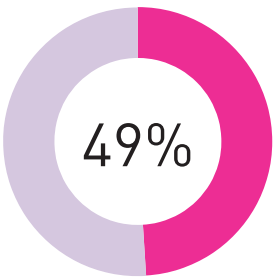
Have data breach plans



Do NOT have data breach plans



Have data breach teams



Do NOT have data breach teams

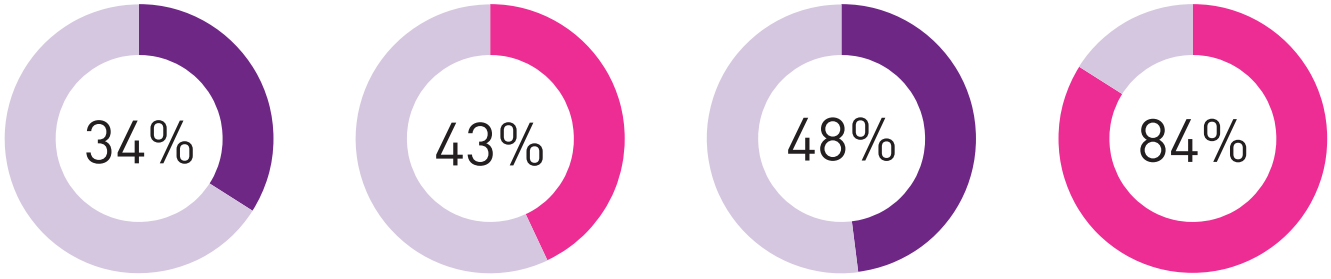
Response plans, effectiveness and reality

At first glance, businesses of all sizes have upped their game in protecting themselves, with a significant rise in businesses having data breach plans, and an increase in the number of allocated response teams. But what about the 16% of businesses that don't have any plans, or the 41% that haven't allocated specific people to deal with the fallout of a breach?

Essential components of a plan

For those who have data breach plans, when you scratch beneath the surface, and invert the ostensibly positive statistics, we can also reveal that the effectiveness of these plans is questionable. Many are far from watertight and are leaving businesses and their customers and employees open to fraud.

2017 data breach: the first steps



Customer notification - Meeting expectations

Of all of our far-reaching analysis on this subject, the most striking findings revolve around the finer detail of the response strategies to individuals. Firstly, a surprising 34% do not include customer notification. This is at odds with what customers expect.

Legal considerations - Minimising risk

When a data breach occurs, legal counsel is of paramount importance to ensure the right steps are taken. And yet, 43% of businesses say they do not have any legal cover for data breaches. This means they may be in danger of falling short of regulatory requirements. Additionally, without the right legal counsel, timely and adequate customer notification may become an unachievable step. The EU General Data Protection Regulation (GDPR) outlines that if the risk is high for those affected, notification is a key action businesses need to take. Essentially, to protect the business any information sent out to customers' needs a legal seal of approval.

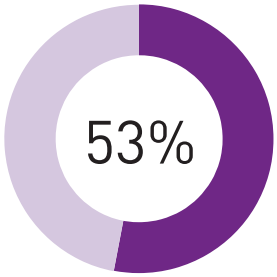
Crisis management – Reputation

It's the job of a communications team to effectively communicate what's happened and this will support the company's efforts in managing reputation – whether that's by controlling what goes out to the media, or to the public. Its role in a time of crisis should not be underestimated, and yet only 52% of businesses have a data breach crisis or communications plan in place. There are a number of high profile data breaches which illustrate clearly how important this element of planning is.

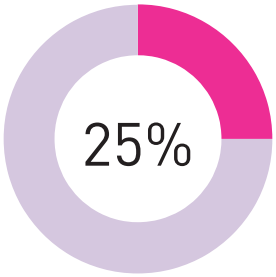
Forensics – Assessment

84% of businesses do not have forensic analysis included within their data breach response plan. Without detailed forensics, an organisation won't be in a position to ascertain how at risk it is. When looking at a live breach scenario, EU GDPR demands that there's a clear understanding of what data has been lost. Not having concrete facts can delay the time it takes to respond adequately to customers.

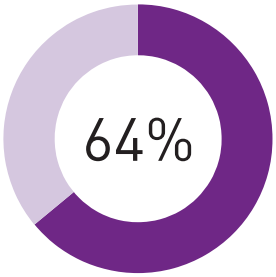
Customer data



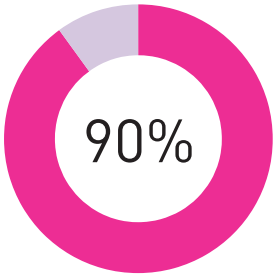
Do NOT have clean customer / employee data



Review once a month



Review once a quarter (NET)

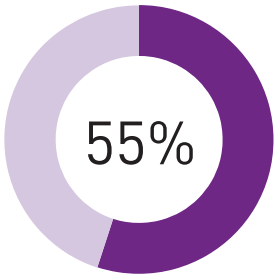


Review once a year (NET)

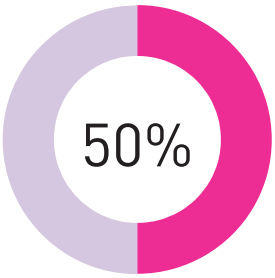
Accurate customer data

Data that is uncleansed or hasn't been deduped in some time could hamper the business' ability to contact customers or employees as quickly as planned. Simply, those who have moved house could be left uninformed. However, while figures are better this year than last, 90% of companies review customer data at least once a year, with 11% of businesses saying they do this just once a year. It's perhaps not surprising then, that more than half admit they do not possess clean customer and employee data.

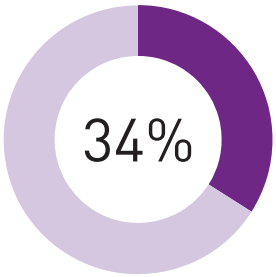
Transparency and openeness



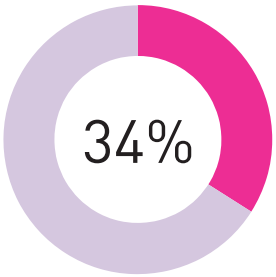
Would NOT be open and transparent



Would NOT provide a quick & appropriate response



Would notify customers by telephone



Would send a notification letter

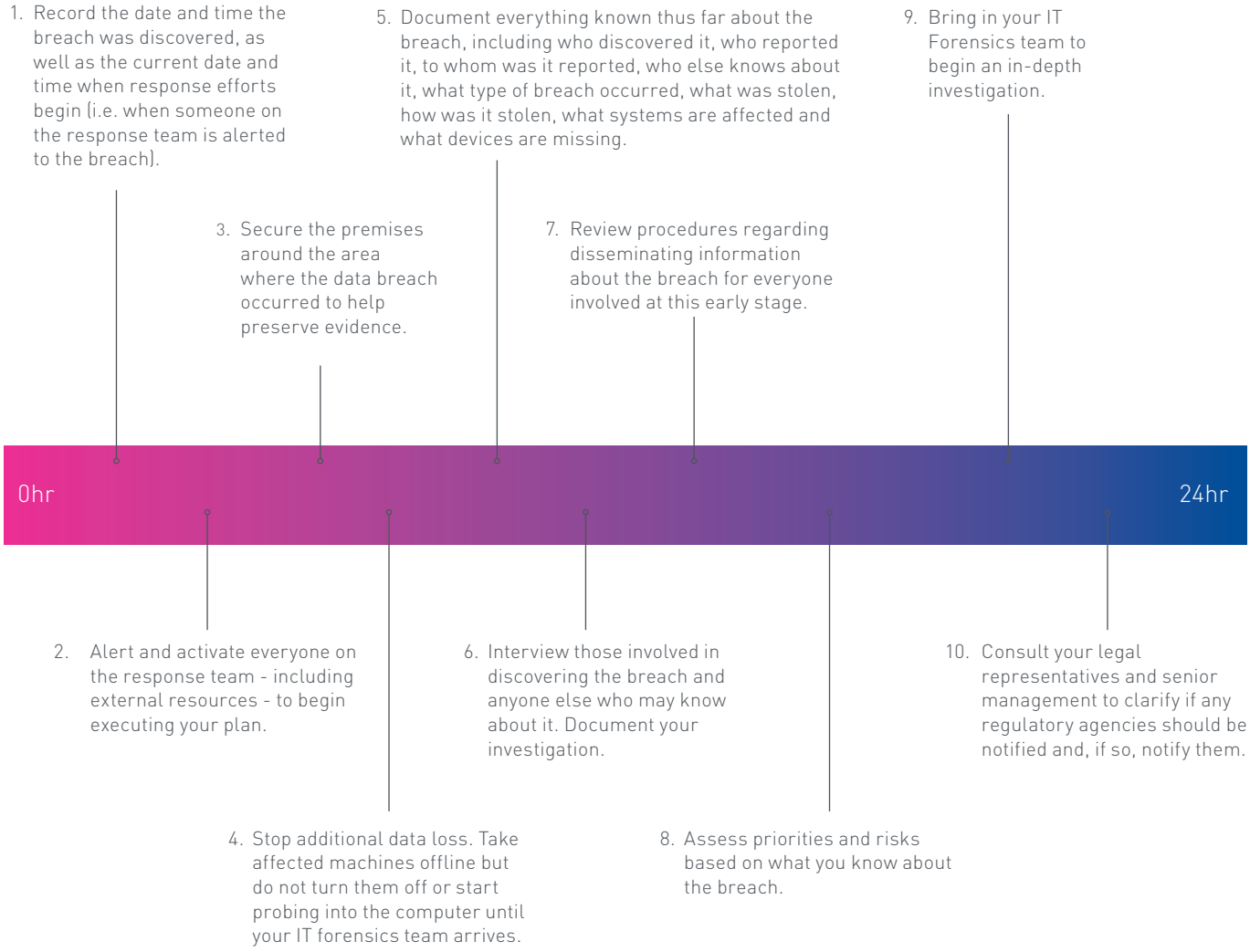
Putting customers at the heart of the response

While it's worrying that less than half (45%) of businesses admit they would share the details about a data breach with their customers, the fact that half (50%) would not provide a quick and appropriate response is surprising, and puts customers at even greater risk. Interestingly, the 34% that said they would notify customers reported that they would do so by phone in the first instance – this can create a dilemma for both the business and the individual. How can individuals assess if a phone call is authentic? The 34% of businesses who would send a notification letter are engaging in best practice, and yet less than a quarter of businesses (23%) have a notification letter template at the ready. When the pressure is on, a legally reviewed letter allows an organisation to respond quickly and accurately, while also offering a moment to reflect and forensically analyse the details.

Misjudged plans

Our research has shown that vital pieces of the jigsaw are still missing when it comes to response plans and readiness. And while businesses may be doing this unwittingly, the breadth of the plan, development of the strategy and team could be preventing businesses from putting the customer front and centre.

Key steps that can be taken in the first 24 hours of a data breach



Customers first

Reputation and trust

Our research about businesses' attitudes has revealed a paradigm: having a data breach response plan in place doesn't mean customers are adequately protected. Yet, perhaps the most conflicting research we've unveiled revolves around the differences that exist between how organisations treat their customers, in relation to how customers expect to be treated.

Opinion matters

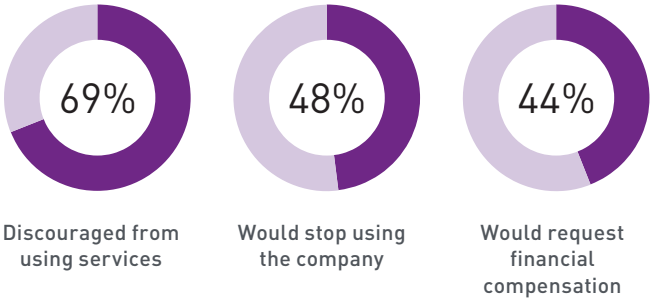
Nearly seven in ten customers (69%) would be discouraged from using the services of a business that had experienced a data breach, while nearly half (48%) say they would stop using the company altogether. What's more, over two in five (44%) say they would request financial compensation. This is in stark contrast to only 17% of businesses saying they'd be likely to offer any compensation to customers affected by a breach. The questions here are: can businesses, especially smaller ones, afford to lose customers, or provide expected compensation to important customers or employees?

Time is of the essence

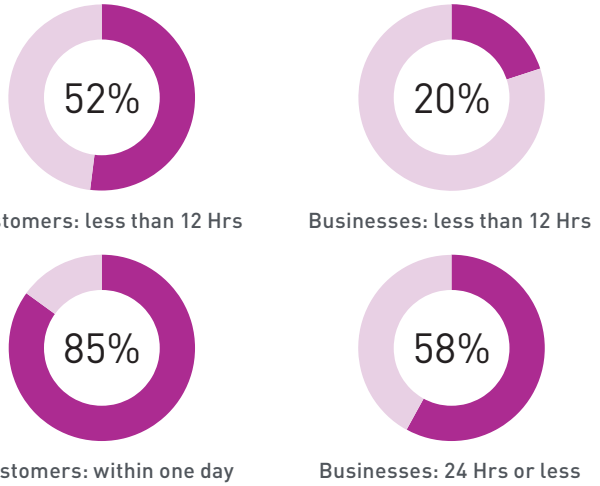
It's also important to highlight how quickly customers expect to be contacted in the event of a breach, compared to what organisations feel is necessary. A pattern is certainly emerging once again, with customer expectation in relation to speed of notification being far greater than what businesses feel is an adequate timeframe.

17% of businesses say it's the customer's responsibility to protect themselves from online theft.

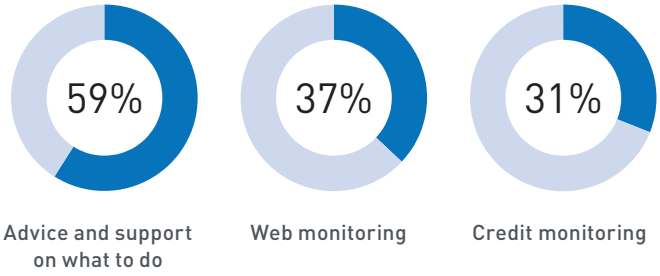
Post breach customer sentiment



Speed of response: Customer expectation vs business

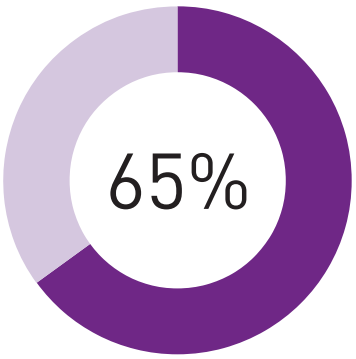


What customers expect

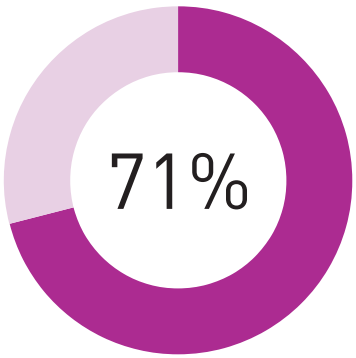


Alignment of expectations

When we surveyed the public, three in five (59%) assume organisations will provide advice and support on what to do, while significant proportions (37%) would also expect web monitoring services (alerts served to them directly when personal data is found online) and alerts about changes to their credit report (31%). Yet only 15% of businesses say they'd offer a free credit monitoring service. However, the greatest – and yet often overlooked - challenge for businesses is yet to come: the woefully inadequate lack of facilities that could make contacting customers in an emergency challenging and call centre services inadequately prepared to receive calls from those who have been affected.



Customers would contact the organisation if personal details stolen



Businesses may NOT have call centre capacity

Misalignment of resources

Just these two statistics alone show that there is a clear misunderstanding by businesses on how their customers would react to such a situation. With little or no call centre resources catered for within the data breach response plan, organisations will find themselves in the situation where they do not have the ability to reassure customers and employees, which is a key component of the response. We would argue that effectively managing enquiries in the time of crisis, with pre-determined FAQs for call centre staff, is key to providing an efficient and effective response.

Reputational impact

Being kept in the loop is high on the list of priorities for customers. Far from a deliberate attempt at sabotage, our research shows that organisations seem unaware of the reputational damage that's at stake. This is a dangerous oversight, and when it comes to accountability and responsibility within organisations, there's also confusion as to who is ultimately accountable.

Accountability:

who is ultimately responsible?

While more than half (51%) of customers say it's the organisation's obligation to keep their identity and information safe, within an organisation there needs to be an unequivocal leader at the helm in the event of a data breach.

51% of customers say the organisation is responsible for protecting them from online theft

Who's in charge?

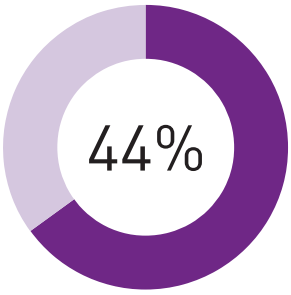
These statistics are fairly consistent. Around two in five senior IT business decision makers think their senior level management should be accountable in the event of a data breach (44%), whilst a similar proportion (41%) put the responsibility in the hands of the IT department. In fact, large businesses specifically are most likely to place accountability with IT professionals (50%).

Burden of responsibility

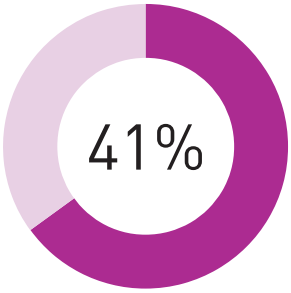
Interestingly, rather than it being on the to-do list of CEOs or senior executives as it has in the past, the burden of huge responsibility is now falling increasingly on the shoulders of IT business decision-makers. But do IT experts realise the enormity of this task? A data breach would not only require a technological assessment of what's happened and how to rectify it, but also a leader who can navigate and fulfil a broader set of skills and expertise.

If we briefly recap on what either a CEO or an IT professional would have to do in the event of a breach, it quickly becomes apparent a full team of experts need to be in place to deliver what's essential:
And this is just the tip of the iceberg.

Breach responsibility: business perspective



CEO / Board of Directors



IT Department

Immediate data breach responses

- Customer notification
- Customer communication
- Customer contact centre
- Briefing crisis & comms teams
- Liaison with lawyers
- Ready the insurers
- Forensic analysis
- Credit & web monitoring

At the helm

For anyone tasked with navigating their company through a data breach storm, only 33% of businesses have experts in place to help them respond to the incident. In simple terms, if the IT department is expected to see a response plan put into action, who is looking after investigating what's happened and who has been compromised? There appears to be a mismatch in ownership. A pre-planned, proactive stance needs to be taken by a clear leader, ahead of time. Whether that designated person is from senior management, or the IT department, they need vital support from both internal and third parties that are in place well in advance of a crisis. This becomes even more important when companies are trading across international boundaries.

33% have experts at the ready to respond to a data breach

The international playing field

Global Data Protection Regulation is coming
The General Data Protection Regulation is a new EU legal framework intended to strengthen and unify data protection for individuals within the European Union. And with nearly half (47%) of businesses saying they hold personal data overseas, it should not be overlooked. If you hold personal data of customers in Europe, you need to be fully *au fait* with the laws and comply.

47% businesses say they hold data of customers or employees who live overseas

EU GDPR LAWS: BREACH PREPARATION

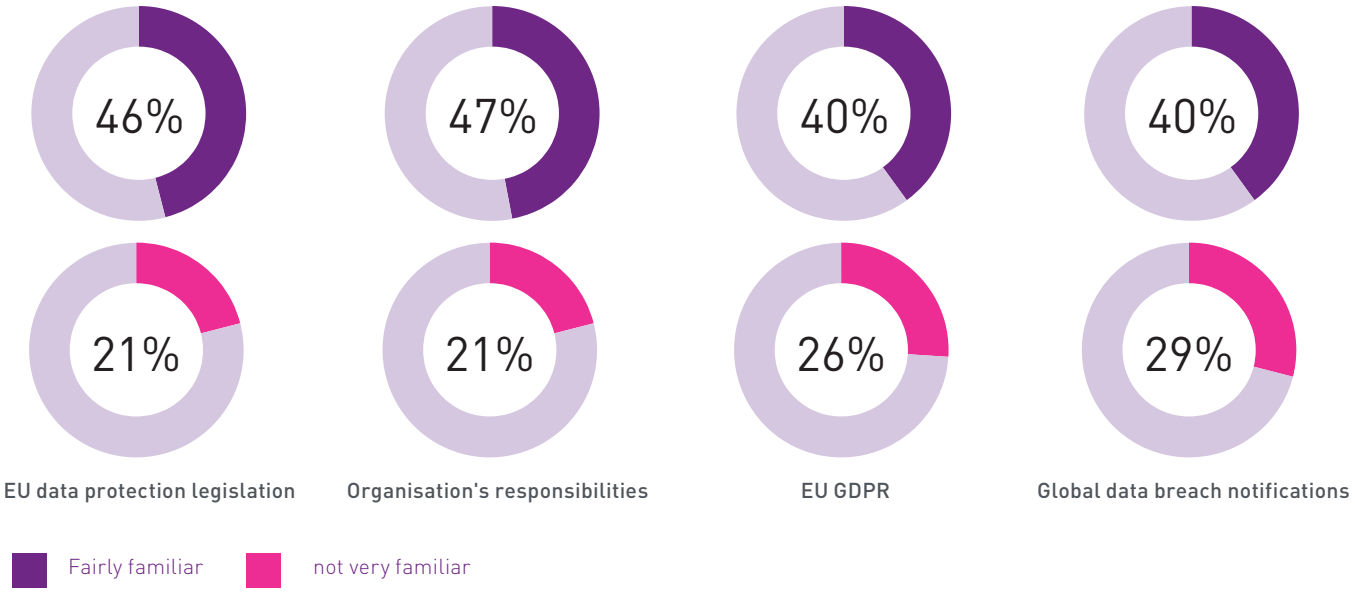
- Educate staff
- Internal breach reporting procedure
- Robust breach detection and investigation procedures

EU GDPR LAWS: BREACH NOTIFICATION

- Notify customers directly if at high risk
- Report to authorities within 72 hours
- Fines up to 10 million euros (2% of company's global turnover

While GDPR will not formally apply until May 2018, it was adopted in April 2016 and businesses need to prepare and make the necessary adjustments now, so they can ready themselves in time.

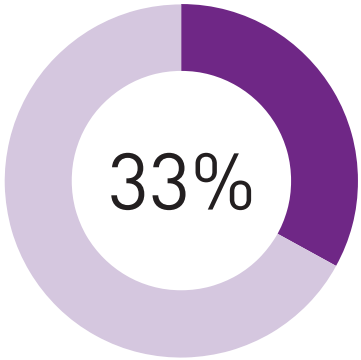
Business knowledge of legislation



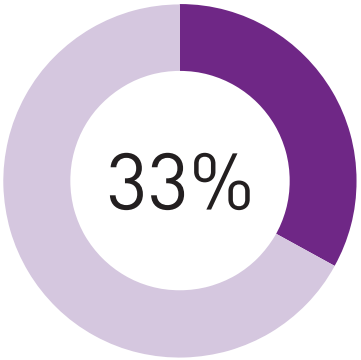
Overseas legislation

Our statistics show that a worrying number of businesses which hold personal customer data abroad are not familiar enough with EU legislation. Nearly half admit they are only 'fairly familiar' with the laws, its responsibilities, while two in five say the same about their global notification procedures. While quite a large proportion are not familiar with any of the required procedures a worryingly high proportion are also not bearing in mind the varied preparation they need in place with legal, insurers, multilingual expertise aligned to the jurisdiction in which they are trading, ranging from a quarter (25%) to a third (33%). This exposes businesses to fines of 2% of their global turnover, not to mention the potential loss of customers through reputational damage.

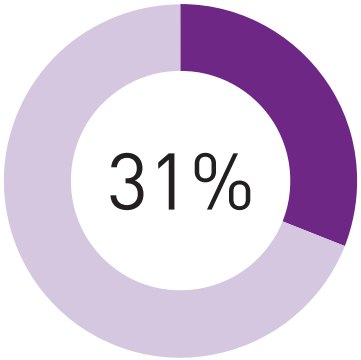
Business overseas response plans



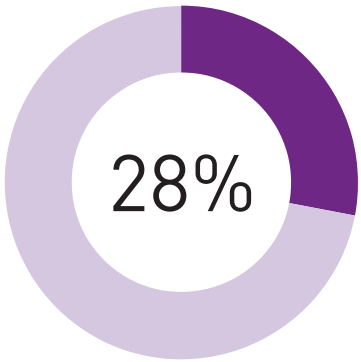
Legal counsel to support jurisdictional law



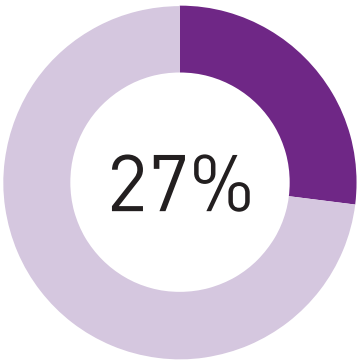
Insurance to cover financial cost to customers



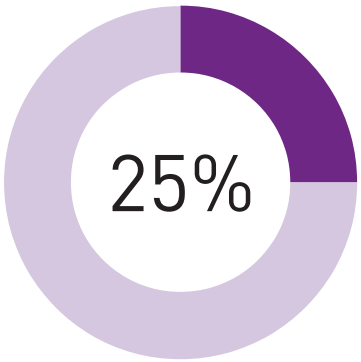
Prepared notification letters in relevant language(s)



Prepared crisis communications in relevant language(s)



Defined breach response teams across different areas



Call centres with multilingual support

Conclusion:

Investigation analysis

"With individuals expecting the very best experiences and reassurances there is no room for misplaced sentiments. As we move towards May 2018 and GDPR regulation, those who prepare now will be confident that they have the ability to reassure and respond competently and continue to maintain fruitful relationships with their customers."

Jim Steven, Head of Data Breach Services, Experian

- Readiness and response:
  - While our new figures reveal a higher number of businesses that have data breach response plans and teams in place this year, the lack of 360* watertight strategies also shows significant swathes of businesses are waiting and testing the 'it won't happen to us' theory.
  - Response plans still lack thoroughness with key elements not prepared for, including: uncleansed data, legal, forensic, call centre and communications support. These plans could unintentionally put the business and customers at risk.

- Customers first:
  - Our research has unearthed a contrast between how customers expect organisations to behave in the event of a data breach, versus what businesses believe they should do. This runs the risk of reputational damage.
  - The missing details of many response plans, such as web and credit monitoring, advice and customer contact services, means businesses are not putting customers at the heart of their response.

- Accountability:
  - There's a distinct lack of clarity within organisations as to who is in charge in the event of a data breach. This will only lead to confusion, delays and further costs if a crisis happens.
  - While traditionally this responsibility would be the Board's or a CEO, increasingly IT management is being tasked with it. However, many are unaware of what's involved in a foolproof breach response plan and the support they would need.

- International playing field:
  - The EU legal landscape is changing, and businesses with customers in Europe appear to be lagging behind in understanding what's required of them by law. This could expose businesses to hefty fines – as much as 2% of global turnover.
  - A thorough data breach response plan is therefore even more important, as it will cover the nuances of dealing with different jurisdictions and languages.

About Experian's Data Breach Response Services
Helping organisations to prepare and respond in the event of a data breach

We understand your primary concern at the time of a data breach incident will be the people affected. Having the ability to notify, provide reassurance and offer remediation at this critical time will help you to maintain trust, reduce reputational impact or financial loss.

Immediate or pre-readiness response assistance:
We have more than 10 years' experience supporting thousands of organisations of all sizes to respond, reassure, and recover in the event where personally identifiable information has become compromised.

When you need immediate assistance to support a live incident we are here to help you. Or we can work with you proactively to put a pre-breach readiness plan in place, ensuring you are prepared for the future with increased confidence.

Do you have a question?

If you have any questions relating to this whitepaper or Experian's Data Breach Response services the team are always here to answer your questions in complete confidence.

Jim Steven
Head of Data Breach Response

Experian Affinity Partnerships
jim.steven@experian.com

Sarah Longstaff
Senior Marketing Manager

Experian Affinity Partnerships
sarah.longstaff@uk.experian.com

Email: breachresponse@experian.com
www.experian.co.uk/databreach
Call us on 0844 4815 888
Outside UK +44 844 4815 888

Other helpful resources:
Data Breach Response step by step guide (2017)
SMEs Under Threat whitepaper (2016)
Data Breach Whitepaper 2.0: Data Breach Readiness (2015)
www.experian.co.uk/databreach

ComRes

BUSINESS SURVEY

ComRes interviewed 200 Business IT decision-makers in Great Britain (Online) between 9th – 16th January 2017. Respondents were surveyed across a variety of sectors and business sizes, ensuring good representation from all business types. All were screened to ensure they were involved in or aware of data breach management at their organisation, and all organisations had to be responsible for at least 100 Personally Identfiable Information (PII) records. Given the subject of the survey, respondents in the IT and Financial sectors are over-represented. ComRes also conducted similar research in 2016 with SMEs.

CONSUMER SURVEY

ComRes interviewed 2,001 British adults online between 13th and 15th January 2017. Data was weighted by age, gender, region and social grade to be representative of all British adults aged 18+. ComRes also conducted similar research among British adults in 2016 and 2015.

ComRes is a member of the British Polling Council and abides by its rules. Data tables are available on the ComRes website, www.comresglobal.com.

Unless otherwise stated, all statistical references within this paper relate to ComRes research.

To review the tables and full set of research visit: www.comresglobal.com

About Experian

Experian® is the world's leading global information services company. During life's big moments – from buying a home or a car, to sending a child to college, to growing a business by connecting with new customers – we empower consumers and our clients to manage their data with confidence. We help individuals to take financial control and access financial services, businesses to make smarter decisions and thrive, lenders to lend more responsibly, and organisations to prevent identity fraud and crime.

We have 17,000 people operating across 37 countries and every day we're investing in new technologies, talented people and innovation to help all our clients maximise every opportunity. We are listed on the London Stock Exchange (EXPN) and are a constituent of the FTSE 100 Index. Learn more at www.experianplc.com or visit our global content hub at our global news blog for the latest news and insights from the company.

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

T: +44 7972 298698
E: BreachResponse@experian.com
www.experian.co.uk/databreach