CRISIS RESPONSE:
Assessing the readiness of UK organisations to manage the impacts of a consumer crisis

White Paper

Responding with confidence in a crisis

CONTENTS

FOREWORD

Understanding the value of crisis-response preparedness

The Covid-19 pandemic has transformed the way many organisations operate, rapidly accelerating emerging technology-enabled trends such as remote working and digital service delivery. The upheaval caused by the pandemic brought into sharp focus the vital importance of adaptability, resilience and crisis management for organisations of all types.

It also exposed organisations to new risks, such that managing and mitigating operational risk has now risen to the top of the agenda for many UK organisations. But how is this focus on risk management manifesting itself? How are businesses organising their resources, plans and capabilities to better respond to future crises, whether medical emergency, natural disaster, product recall or cyber-attack?

In this report, we highlight the findings of our two recent surveys into the crisis preparedness and experiences of UK organisations and consumers. In our survey of C-suite leaders, more than four in five (84%) said that Covid-19 had made their organisations better prepared and more resilient to crisis going into 2022. But does the reality match this perception? Although many organisations are confident in their ability to respond to a crisis, many do not have plans in place, resources available or processes mapped out to mount an effective consumer response and recovery. Until an organisation has experienced a sudden crisis, it's difficult to appreciate the extent of communication and resource management required to minimise the impacts. A swift and effective response is the key to minimising financial, reputational and emotional damage – but how many businesses are well prepared for such a response and what are consumers' expectations?

The findings set out in this report may help business leaders to identify weak spots and risks in their organisations. The time, cost and resources involved in crisis response preparation are nothing compared to the huge costs and long-term impacts of failing to respond appropriately. Taking the time to implement an effective plan today can provide the peace of mind and reassurance needed. No business is immune to crisis, and the benefits of responding effectively when the worst happens are far-reaching, and key to securing the long-term viability and success of any organisation.

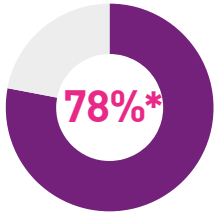
Jim Steven
Head of Crisis & Data Breach Response
Experian Consumer Services

ABOUT THIS REPORT

This report presents the findings of two independent research studies into crisis preparedness, response and recovery. The first study surveyed 500 senior C-suite leaders, business owners and directors from a wide range of industries, including retail, professional services, healthcare, education, hospitality and financial services. The second study surveyed more than 2,000 members of the public from across the UK. The research investigated the experiences of businesses and individuals during the 18 months up to December 2021, delving into their experiences of crises, the subsequent response and outcomes.

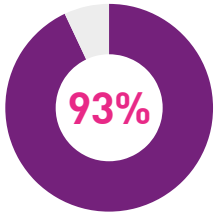
By comparing the views of businesses with the experiences and expectations of the public, this report aims to highlight the key issues facing organisations when preparing for any crisis, and the priorities they face in fulfilling public expectations of crisis management.

AT A GLANCE: TOP 10 FINDINGS

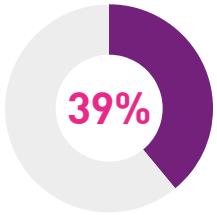


of respondents said their organisation had experienced a crisis in the previous 18 months.

felt they were at risk of a crisis within the next 18 months.

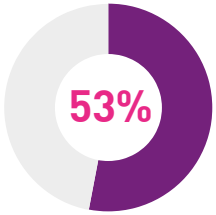


of C-suite respondents said they / their families had been personally impacted by a data breach.



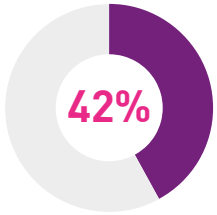
of leaders surveyed are worried about the financial impact of responding poorly to a crisis.

Failure to prepare and respond well to a crisis will cost UK organisations, on average, £61m over the next five years.

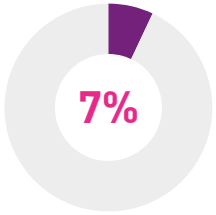


If an organisation handled a crisis poorly, 53% of consumers surveyed would file a complaint and 42% would move their custom elsewhere.

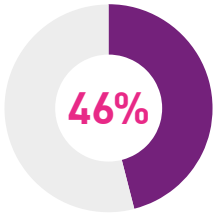
Only 50% of organisations surveyed have a crisis-response plan in place. 83% of consumers expect organisations to have such a plan.



of organisations surveyed have no consumer crisis notification process in place.



Only 7% of businesses that had experienced a data breach were able to inform customers within 24 hours. 55% of consumers expect to be informed within 24 hours.



of leaders thought responding positively to a crisis would increase customers and business.

RESEARCH FINDINGS

Crisis landscape

Organisations face a multitude of risks

In our C-suite leader survey, around three quarters (78%)* of respondents said their business or organisation had experienced a crisis in the previous 18 months that had caused some detriment to customer outcomes. More than a third (39%) said this had happened more than once.

The crises experienced by organisations included:

78%* Data breach of **customer** information | **39%** more than once.

76%* Product recall | **41%** more than once.

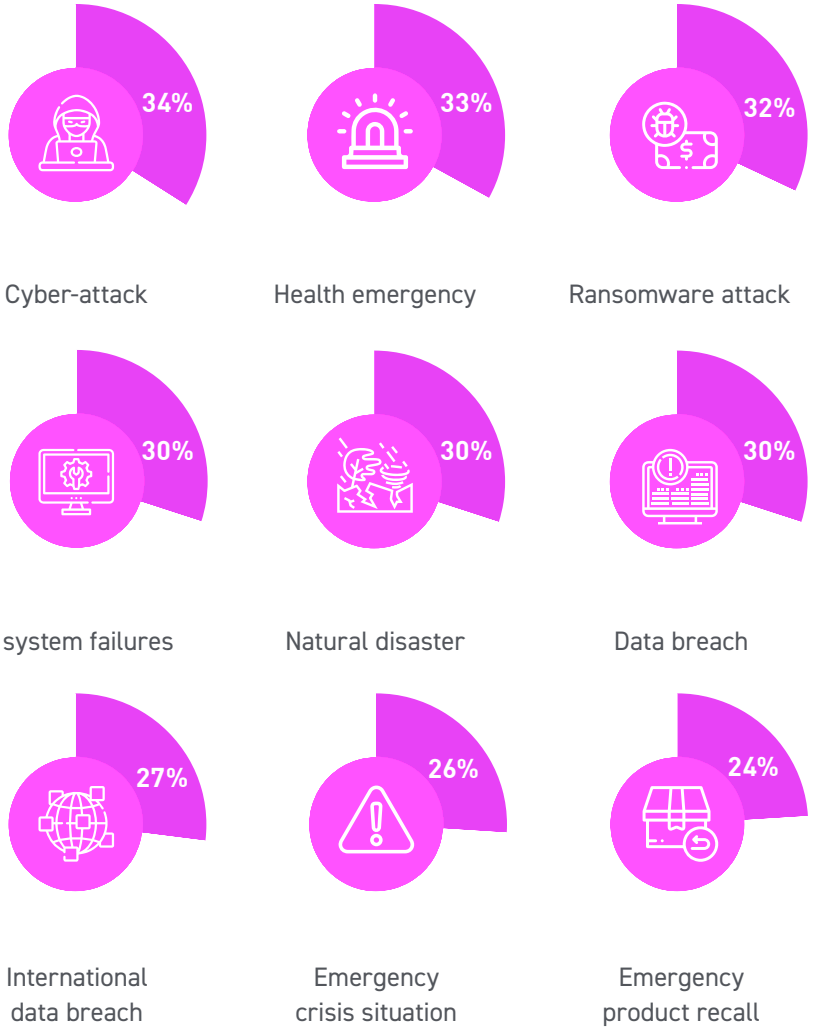
74%* Cyber-attack | **40%** more than once.

93% When asked about their personal experiences of data loss or theft, more than 9 in 10 (93%) C-suite respondents said they had or their families had been personally impacted by a data breach.

*See Methodology on page 25

100% **of businesses surveyed feel they are at risk of a crisis in the next 18 months**

When asked about the risks their organisations might face in the next 18 months, the surveyed leaders identified:



EXPERIAN INSIGHT

"No organisation is immune to risks. Since the pandemic, when every type of organisation was forced to adapt to survive, the need to build resilience by preparing to respond to a crisis has never been more apparent to business leaders. The ability of an organisation to respond effectively to a crisis – whether a cyber-attack, product recall, natural disaster or health epidemic – is key to its long-term survival. Preparing in advance is the key to mounting an effective response and achieving a faster recovery."

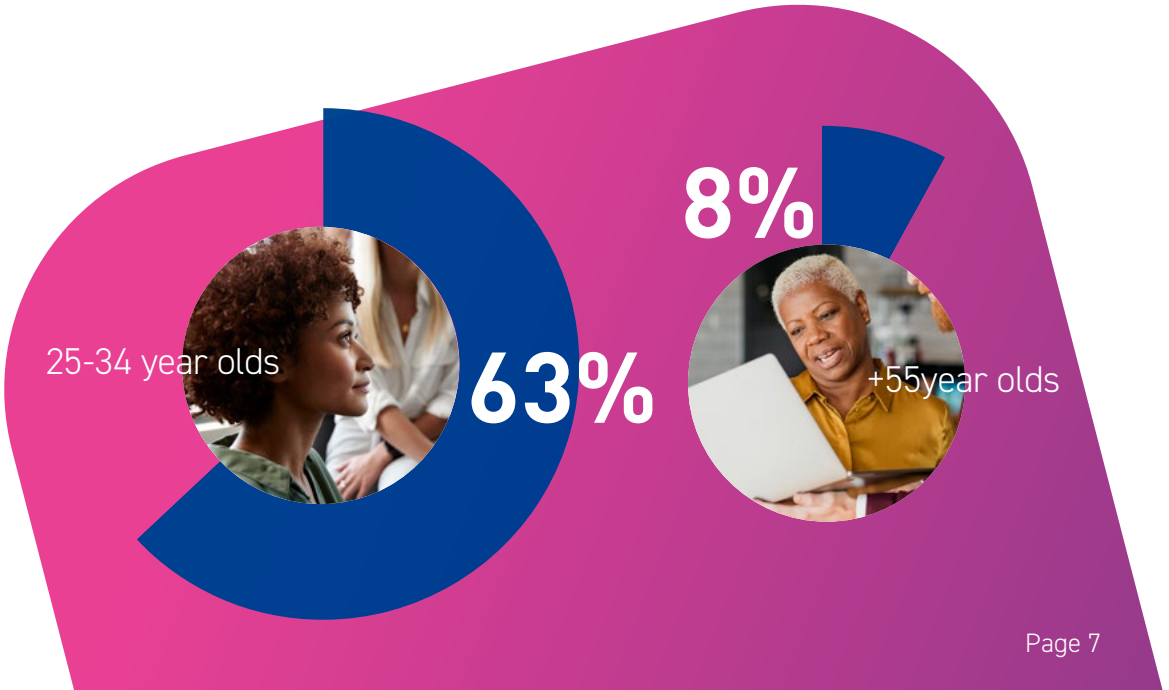
Sarah Williams
Senior Marketing & Communications Specialist

Risks to consumer data

In our survey of members of the public, we asked specifically about experiences of personal data loss or theft – one of the major risks faced by consumers in the digital age. More than a third (35%), stated that in the past 18 months they were aware of instances in which their personal identifiable information had been compromised within the organisations they interact with. That equates to around 19 million adults in the UK[1]. The awareness of such incidents varied by age. Among 25-34 year olds surveyed, 63% were aware of data breach incidents compared to just 8% of 55+ year olds surveyed.

More than three quarters (78%)* of senior managers surveyed said they were informed in the past 18 months that their personal identifiable information had been compromised, whereas less than 2 in 5 (38%) unskilled manual workers surveyed said the same.

Awareness of data breach incidents



* [1] See Methodology on page 25

Crisis response concerns

What's on the minds of business leaders?

With so many potential crises facing every type of organisation – from data breaches and natural disasters to product recalls and medical emergencies – we wanted to find out what keeps most executives up at night.

If their organisations were forced to respond to a crisis, here's what surveyed leaders told us they were most worried about:

39% Financial impact and high costs to the business

36% Complaints / legal action due to poor response

29% Negative impact on customers if crisis not handled well

29% Lack of relevant insurance cover

28% Lack of resources to notify customers (e.g. access to call centre support)

26% Lack of knowledge about what to do

Financial impact:

We asked leaders for their estimate of the cost (as a percentage of turnover) of a failure to prepare for and respond well to a crisis in their organisation within the next five years.

On average, respondents in businesses with a turnover of £1m-£9.99m thought the failure to plan for and respond to a future crisis would cost 36% of turnover. That equates, on average, to a cost of £1.97m[2] for businesses with this level of turnover. For respondents in businesses with a turnover of £50m-£99.99m who think it would cost 43% of turnover/revenue, the average cost would be £32.24m[3] .

Insurance worries:

Less than half (45%) of respondents said their organisation had insurance in place to cover the cost of notifying customers in the event of a crisis. Just over two in five (42%) said they did not have such insurance – and 13% didn't know whether they did or not.

EXPERIAN INSIGHT

"C-suite leaders are right to be concerned about the risks posed by any crisis. Mitigating the impact is all about getting your response right. Businesses that respond swiftly and appropriately can minimise the impacts on their finances and reputation, as well as on their customers or service users. As our survey participants clearly recognised, failure to prepare and respond well to a crisis has real-world consequences. It can be financially and emotionally devastating both for the organisation, and for the individuals impacted."

Jim Steven
Head of Crisis & Breach Response Services

[2] [3] See Methodology on page 25

How do consumers react?

When it comes to crisis response, organisations only have one chance to get it right. Handling a crisis badly can cause more long-lasting damage than the consequences of the crisis itself. To find out how consumers felt about the way organisations dealt with crises, we asked what they would do if an organisation they dealt with handled a crisis poorly and failed to inform them.

53% File a complaint

42% Move their custom elsewhere

32% Tell others about the experience

21% File a lawsuit

19% Post about it on social media

63%
55+ year olds are the age group most likely to file a complaint

Prevention

How well-prepared are UK organisations?

Responding effectively to a crisis requires considerable upfront planning and preparation. We asked business leaders about the plans, resources and preparations they had in place within their organisations.

DATA BREACH PLAN:

51% YES
35% NO
15% DON'T KNOW

CRISIS RESPONSE PLAN:

50% YES
38% NO
13% DON'T KNOW

BUDGET ASSIGNED TO CRISIS RESPONSE:

49% YES
39% NO
11% DON'T KNOW

ACCESS TO THIRD-PARTY SPECIALISTS (LAWYERS, IT FORENSICS, ETC):

49% YES
39% NO
12% DON'T KNOW

IN-HOUSE TEAMS/ RESOURCES ASSIGNED TO CRISIS RESPONSE:

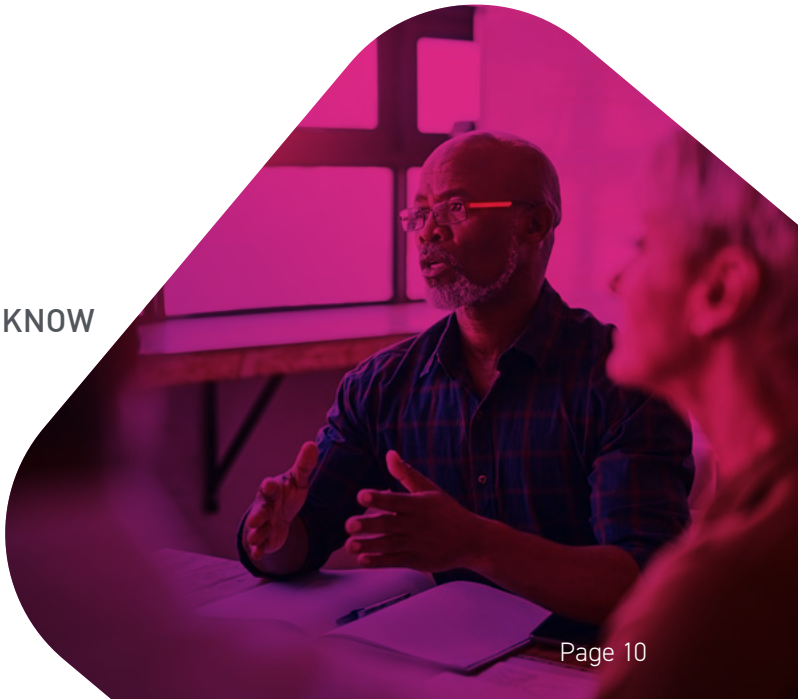
49% YES
39% NO
12% DON'T KNOW

CRISIS COMMUNICATIONS PLAN:

48% YES
40% NO
12% DON'T KNOW

REGULAR RISK AUDITS:

45% YES
42% NO
13% DON'T KNOW

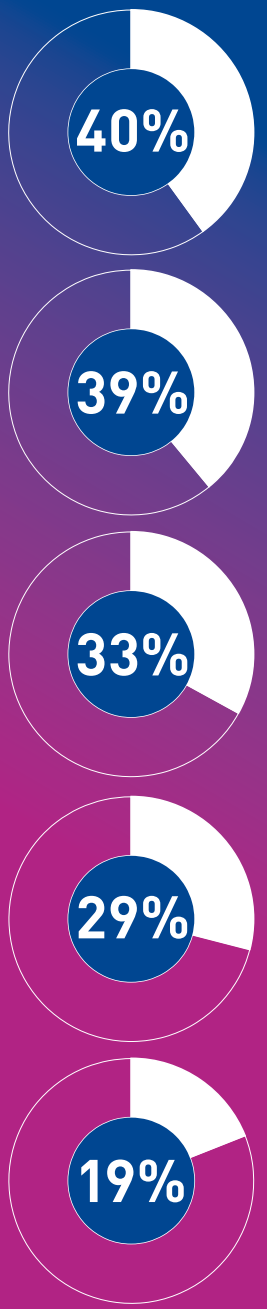


What do consumers expect?

To explore consumer expectations, we asked whether people expected the organisations they interacted with to have crisis-response plans in place.

More than 4 in 5 (83%) said that they did expect organisations to have a plan in place to prepare for and respond to a crisis. The highest expectations were among wealthier individuals. Of those surveyed earning more than £75,000 per year, 95% said they expected organisations to have crisis-response plans in place.

The survey also revealed that failing to plan for a crisis could have significant consequences for organisations, even if no crisis occurs. We asked people how they would feel if they discovered that an organisation they interacted with didn't have a crisis-response plan in place.



EXPERIAN INSIGHT

"Failing to plan for a crisis could not only have devastating consequences in the event of an emergency, but it can also damage consumer trust and the reputation of your organisation. Handling a crisis badly has impacts on health and well-being too, which should not be underestimated. It can cause emotional distress for employees dealing with the crisis, as well as for customers who may be facing financial losses, identity theft and wider impacts."

Ryan Bradshaw
Senior Crisis & Breach Response Manager

EXPERIAN INSIGHT

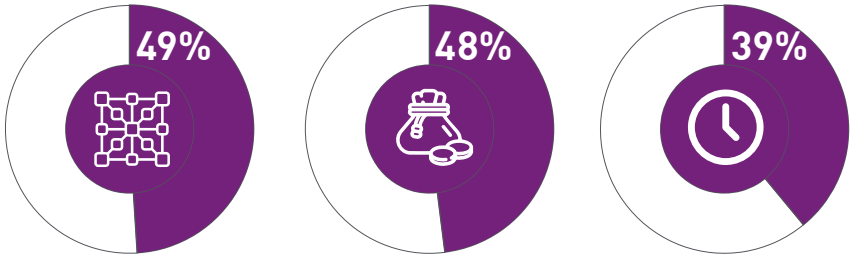
"It's completely understandable that crisis-response and recovery planning has not been seen as the number-one priority for most organisations. But the major disruption to business-as-usual during the pandemic has given businesses a new perspective on this. Key business areas, including IT, PR/ Comms, operations, customer services and legal can come together with a degree of experience to develop their crisis-response plans, and ensure they can orchestrate the next response with increased confidence."

Jim Steven
Head of Crisis & Breach Response Service

Obstacles to preparation

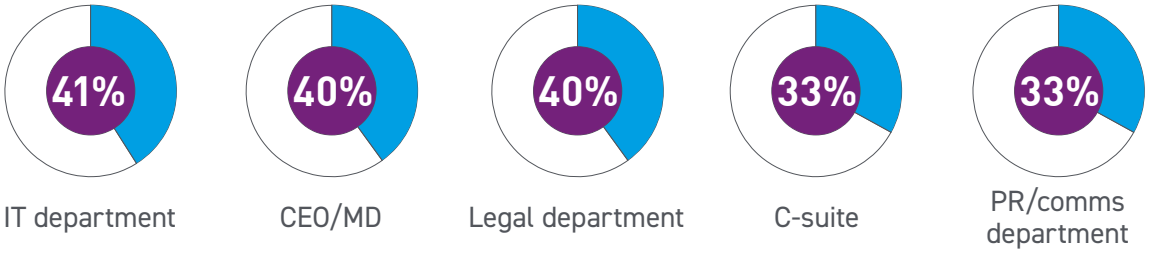
What's getting in the way of crisis planning?

All organisations face a plethora of competing priorities. With limited time, funds and resources, business leaders must focus on the tasks required to keep their organisations running efficiently and profitably. When it comes to risk and crisis management, leaders understandably focus on trying to prevent crises from happening – but far fewer spend time thinking about how the business should respond if an almost inevitable crisis did hit. In our survey, we asked business leaders what's stopping them from putting effective crisis-response plans in place.



More than a quarter (27%) said that crisis response was not a priority during Covid-19.

The research also uncovered uncertainty about who within an organisation was responsible for handling a crisis. Respondents felt the responsibility lay with:

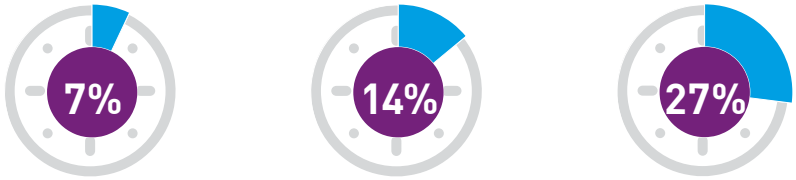


Crisis notification

Keeping customers in the loop

In the event of a crisis, keeping customers or service users well informed is often the key to a successful resolution. People understand that emergencies do happen, but they don't want to be kept in the dark. The sooner they are informed the better. The more open your lines of communication, the more likely you are to emerge from any crisis with your reputation and customer esteem intact.

We asked those businesses that had experienced a particular type of crisis – a data breach – how soon they had been able to inform customers who were impacted.



Within 24 hours | Within 48 hours | Within 72 hours

On average, respondents said they had informed affected customers within eight days.

Worryingly, when it comes to communication mechanisms for informing customers about a crisis or data breach, 42% of respondents said their organisation had no notification response process in place. Furthermore, 38% said they did not have processes to cleanse customer address data. In any emergency communication programme, it's vital to have up-to-date and accurate customer contact information to hand, including the preferred communication channels for each customer, as well as access to notification capabilities and outbound/inbound call centre support.

What do consumers expect?

To find out what customers expect from the organisations they deal with, we asked how quickly they would expect to be informed if there was a data breach that compromised their confidential information. On average, people expected to be told within five days of such an incident. However, more than half (55%) expected to be informed within 24 hours.

[4] See Methodology on page 25

EXPERIAN INSIGHT

"There seems to be a mismatch between the expectations of customers when it comes to notifying them of a data breach, and the reality achieved by businesses. In truth, a data breach and other security breaches can go unnoticed for a long time – if an organisation hasn't got a handle on its risk. According to research by the Ponemon Institute, it takes an average of 280 days to detect and contain a data breach[4]. Organisations need to have sufficient resources available to identify crisis incidents quickly and inform customers at the right time and with the right information, using their preferred communication channels."

Sarah Williams
Senior Marketing & Communications Specialist

EXPERIAN INSIGHT

"Responding well to a crisis and providing the support services customers expect will help to maintain the confidence of your stakeholders and retain the goodwill of customers – which is ultimately vital to the survival of your business.

So it is, businesses never think it's going to be as difficult as it really is to respond to a crisis. But when you begin to unpick the layers of complexity involved in simply notifying consumers, you begin to appreciate the value of preparing in advance. Crucially, if the people involved in responding to a crisis know what they're expected to do and have the tools in place to respond effectively, your response will be so much more successful and cause far less anxiety to employees and customers."

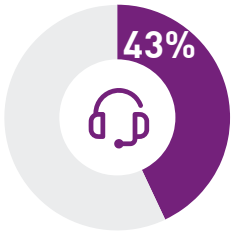
Jo Pritchard
Crisis Response Executive

Crisis support

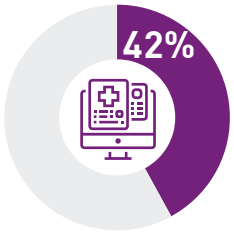
How can businesses support customers through a crisis?

The help and support organisations provide to their customers or service users following any crisis can make the difference between a successful resolution and a damaging outcome. Customers expect to be advised appropriately to help minimise the impacts of any incident on their finances, well-being or security.

In our survey, we asked business leaders what support they could provide to customers in the event of a crisis.

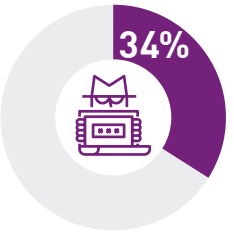


Call centre support



Identity theft protection/credit file monitoring and repair

Compensation



Fraud services/ support

What do consumers expect?

While customers may accept that any organisation can be hit by a crisis, they do expect the organisations they deal with to provide the support and services needed to mitigate any impacts. In our survey, we asked consumers to list the top five things they expected to be provided with if their personal identifiable data was lost or stolen due to a data breach:

1. Identity theft protection including alerts and support to help identify/protect against fraudulent activity **(49%)**
2. Victim of fraud service/support **(48%)**
3. Compensation **(44%)**. The expectation of compensation rises with age: **56%** of consumers aged 55+ expect compensation, compared to **27%** of 16-24 year olds.
4. Call centre support to answer questions **(42%)**
5. Credit file monitoring and repair to ensure their credit score isn't impacted **(40%)**

When asked what their biggest worries would be if they were the victim of a data breach that compromised their personal information, UK consumers said it was risk of fraud **(52%)**, financial cost **(52%)** and identity theft **(50%).**

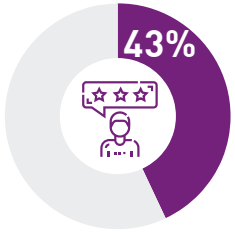
Future opportunity

Benefits of an efficient crisis response

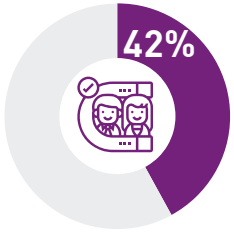
While failure to respond well to a crisis has all kinds of negative impacts – from financial losses to reputational damage – the consequences of an effective and efficient crisis response can be extremely positive. Organisations that deal professionally and openly with a difficult situation can enhance their reputation and build trust among their customers or service users.

We asked leaders what they thought would be the biggest benefits to come from a positive response to a crisis.

Increased customers and business



Avoiding reputational damage

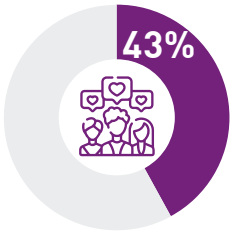


Retaining customers

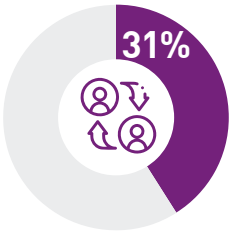
How do consumers feel?

Customers also express positive feelings towards businesses that deal effectively with crises. We asked people how they would react if an organisation they dealt with handled a crisis situation positively and kept them well informed.

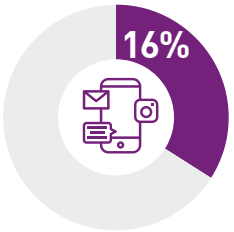
Continue to be a customer



Think favourably of the organisation



Recommend the organisation to others



Post about it on social media

EXPERIAN INSIGHT

"Doing your critical thinking and some of the decision-making in advance takes much of the pressure off when you're in the eye of the storm. You are simply triggering a pre-planned response procedure, rather than having to make decisions hurriedly in the heat of the crisis. That's good for the well-being of your decision-makers, as well as for the effectiveness of the response and recovery. By keeping customers well informed in a timely manner, you can deflect many incoming queries and generate positive feelings of trust towards your business – demonstrating your expertise and efficiency in dealing with the unexpected."

Ryan Bradshaw
Senior Crisis & Breach Response Manager

FINDINGS BY INDUSTRY SECTOR & BUSINESS SIZE

Industry sector spotlight

As part of our research, we surveyed C-suite leaders working in financial services, healthcare, insurance, retail, hospitality and education, among other sectors. We also asked UK consumers which industry sectors they had the most confidence in when it comes to notifying them of a crisis.

Across all sectors, **75%*** of respondents had experienced a crisis that led to a detriment to customer outcomes at least once over the past 18 months.

100% feel they are at risk of a crisis within the next 18 months.

Financial services

UK customers have the highest level of confidence (66%)** that organisations in this sector would be able to notify them of a crisis.

Healthcare

The biggest worry among healthcare leaders if they responded poorly to a crisis event was the financial impact and high costs incurred (40%). This sector is the least likely to have an in-house team assigned to crisis response – with 63% saying they don't have one or don't know if they do.

Insurance

Insurance leaders felt the failure to plan for and respond to a future crisis impacting their organisation would cost 44% of revenue. More than 2 in 5 (43%) are not confident in their organisation's ability to deal effectively with a data breach – the least confident of all the sectors surveyed.

Professional/business services

Firms in this sector are the least likely to have notification response processes in place to inform impacted parties/customers of a crisis quickly (53% did not have one). And 57% don't have a budget assigned to respond to a crisis.

Retail

53% of retail businesses don't have processes in place to handle international data breach incidents.

Hospitality

UK customers surveyed had the lowest level of confidence (46%)** in hospitality organisations being able to notify them of a crisis. Hospitality businesses are the least likely to have access to third-party experts such as insurance, lawyers and IT forensics – with 71% saying they don't have access or don't know if they do.

Education

Almost 9 in 10 (89%)* respondents in the education sector said they had experienced a cyber-attack in the past 18 months. Just over 2 in 5 (44%) said that if they were to respond well to a crisis event, the biggest positive would be avoiding or reducing reputational damage.

Ecommerce

More than a third (36%) of respondents working for an ecommerce organisation think that their business/organisation is at risk of cyber-attack over the next 18 months, whereas fewer than 3 in 10 (26%) non-ecommerce respondents share this fear.

* See Methodology on page 25

Business size spotlight

In the past 18 months, 100% of respondents in small (1-50 employees), medium (51-250 employees) and large-sized organisations (250+ employees) have experienced a crisis at least once, including:

Crisis	Small	Medium	Large
Data breach	70%*	79%*	82%*
Cyber-attack	71%*	72%*	79%*
Ransomware attack	66%*	71%*	82%*
Product recall	63%*	75%*	86%*
A crisis that has led to detriment to customer outcomes	63%*	79%*	80%*

Future risk

In the next 18 months, 45% of respondents surveyed in large organisations think they are most at risk of a cyber-attack, followed by a health emergency (39%), ransomware attack (38%), IT system failure (36%) or a data breach (36%).

Small organisations think they are most at risk of a natural disaster (33%), with medium-sized businesses saying IT system failures (32%) are their biggest risk. Small organisations are least confident in their ability to handle well an IT system failure crisis (41%) or a data breach (40%); medium-sized businesses responded ransomware attack (38%) or heath emergency (36%) and large organisations responded equally a cyber-attack (25%) or natural disaster (25%).

* See Methodology on page 25

Crisis preparedness

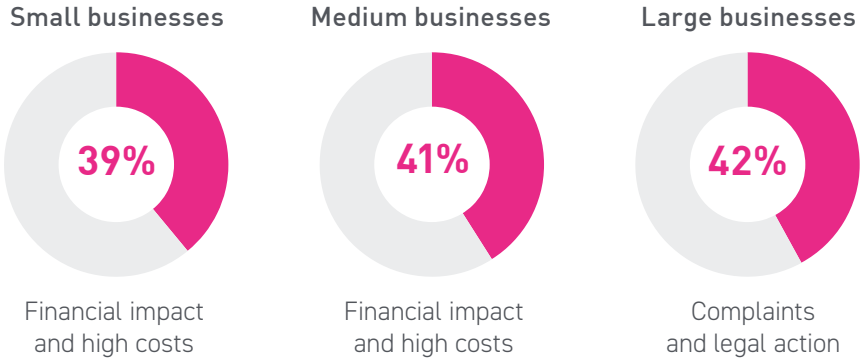
Respondents surveyed in large organisations are more likely to have crisis preparation and response plans in place, notification response processes to inform impacted parties quickly, and in-house resources assigned to crisis response. However, across all business sizes, 45% of organisations don't have or do not know if they have a crisis-response plan.

By business size, small, medium and large organisations, have the following in place:

CRISIS PLANS		NOTIFICATION PROCESSES		IN-HOUSE RESOURCES	
47%	SMALL	45%	SMALL	38%	SMALL
44%	MEDIUM	39%	MEDIUM	51%	MEDIUM
57%	LARGE	51%	LARGE	56%	LARGE

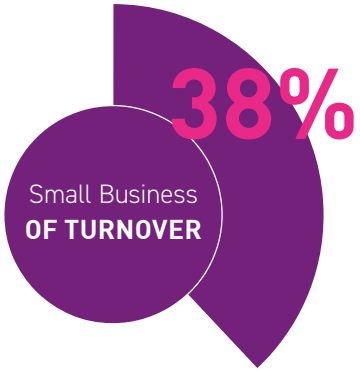
Impacts of poor crisis response

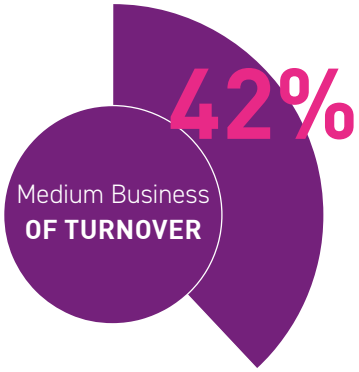
Organisations surveyed are well aware of the impact of responding poorly to a crisis. Their biggest concerns are:

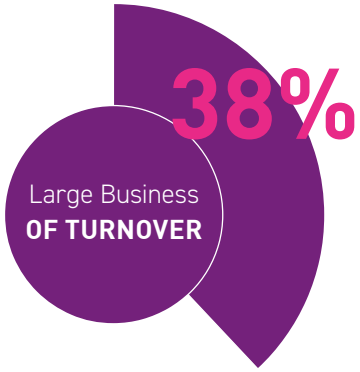


Financial cost of failure to plan

When asked how much they thought the failure to plan to respond to a crisis would cost their organisation, surveyed leaders said:

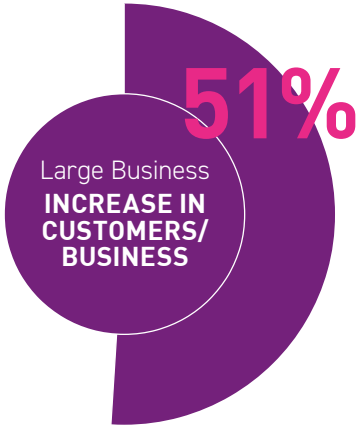






The positives of good crisis response

When asked to identify the number-one positive result of responding well to a crisis, the surveyed leaders said:



CONCLUSION

The reality of crisis readiness

In our survey, more than two thirds (72%)** of leaders said they were confident in their organisation's ability to effectively deal with an emergency crisis situation. The levels of confidence were similar for all types of crisis, including data breach (68%)**, emergency product recall (71%)**, natural disaster (68%)**, cyber-attack (67%)** and health emergency (67%)**.

But our survey findings on the readiness of organisations to respond effectively to a crisis show that this confidence may be misplaced. For example, 50% of leaders surveyed said their organisation doesn't have, or they don't know if they have, a crisis response plan in place. The concerns of leaders and the experiences and expectations of consumers revealed by our research cast further doubt on the true crisis readiness of UK organisations.

Any crisis is always a shock to an organisation, but the speed of decision-making required and the complexity of managing every aspect of a consumer response is often an even greater surprise. The solution to mitigating negative impacts is thorough crisis-response preparation.

There are huge benefits to preparing thoroughly and logically in advance, in a calm and measured environment before any crisis strikes. Relying on the ability of your organisation to respond effectively on the hoof, in the turmoil of a real crisis, is a situation no business leader or organisation wants to be in.

* See Methodology on page 25

How Experian can help: Respond with confidence in a crisis

The Experian Crisis & Data Breach Response team has more than a decade of experience in supporting businesses to resource and manage data-breach and crisis-response programmes on any scale.

Our specialists use proven methodology to guide you through the process of evaluating your resources, identifying skills gaps, developing response plans, building a response team, and preparing customer notification processes – so that your organisation is ready to handle any crisis when it occurs. Where required, we can provide inbound and outbound mass consumer notifications and call centre capabilities to support your response.

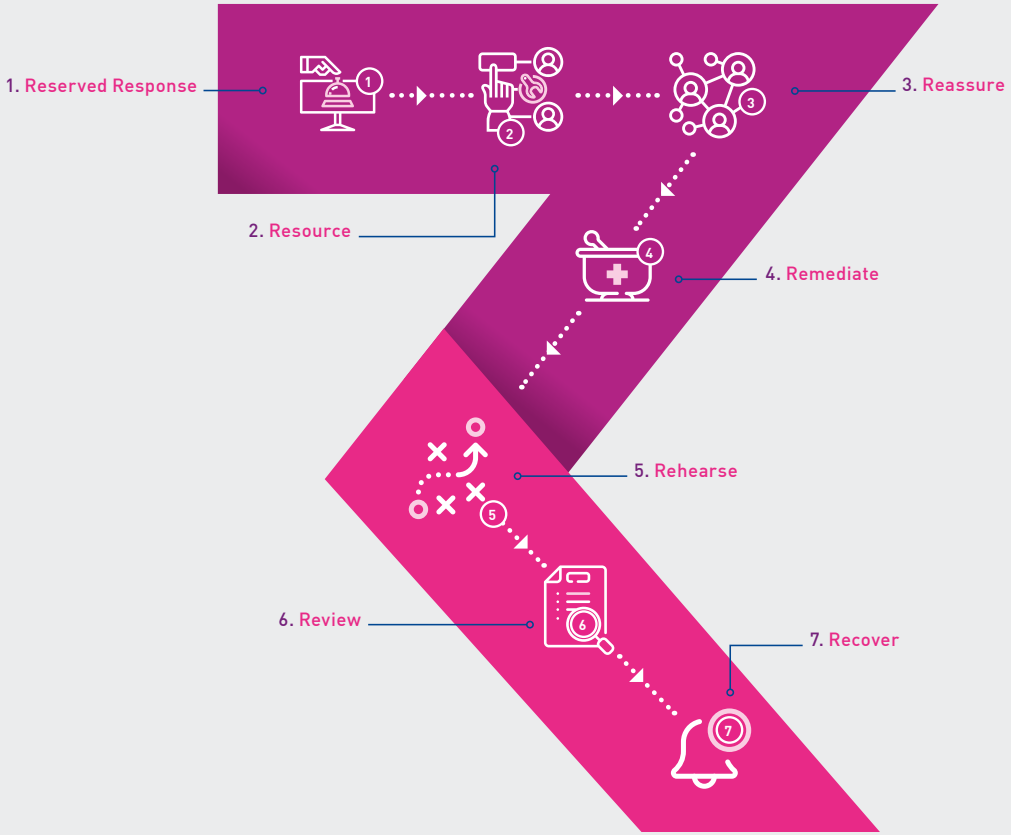
We can adapt our services and resource provision to suit businesses of all sizes. At the simplest level, we can help you to build a basic recovery plan using our free Experian readiness hub. Or we can offer more tailored advice, support and services, including delivering a fully supported, account managed and guaranteed reserved response service, in the UK and internationally.

EXPERIAN RESERVED RESPONSE

Working with you to build out your plan

Building out your consumer response plan is one of the single most important steps your business can make to ensure you have the right resources in place to deliver a comprehensive response to an incident in a timely and confident way.

Our proven experts have developed a service which includes insight into why certain readiness steps are important, ensuring your team are knowledgeable about the key components of a consumer recovery plan.



Experian consumer crisis response capabilities

Get in touch

To find out how we can help your business cope with any crisis, and mitigate financial, reputational and emotional damage, please contact **jim.steven@experian.com**

To book one of our free bespoke insight sessions and hear about recovery strategies, approaches and your potential blinds spots, please contact **breachresponse@experian.com**

www.experian.co.uk/databreach

Consumer notification and fulfilment management

- Postal letter outreach
- Email outreach
- SMS outreach

Consumer response inbound resourcing and management

- Call centre facility
- Call centre agents
- Live web chat
- Email response management

Consumer response messaging templates

- Frequently Asked Questions library
- Communication templates, (sample letters/emails)

Response planning, managing & reporting

- Response readiness planning
- Management of resources and fulfilment schedules
- Management information reporting

Address verification and cleansing services

- Contact data verification, quality checks and updates

METHODOLOGY

These surveys were conducted by Censuswide, an independent market research company. Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles. 500 C-suite respondents and 2,004 UK nationally representative adults (aged 16+) were surveyed in December 2021.

* 'Yes, once' and 'Yes, more than once' responses combined.

** 'Very confident' and 'somewhat confident' responses combined.

*** 'Not too confident' and 'not confident at all' responses combined.

**** mean days excluding 'unsure'

[1] 54,098,971 / 100 x 35% = 18,934,639.85

[2] £1.97m (midpoint of £1m-£9.99m is 5.49 / 100 x 36 = 1.97)

[3] £32.24m (midpoint of £50m-£99.99m is 74.99 / 100 x 43 = 32.24)

[4] 'Cost of Data Breach Report', July 2020.
Ponemon Institute and IBM Security.

About Experian Crisis and Breach Response, UK

Powered by the nation's largest credit reporting agency, is a leader in helping businesses plan for and mitigate consumer risk following a crisis. With more than seventeen years global experience, Experian has successfully serviced some of the largest and highest-profile breaches. The team offers swift and effective incident management, consumer notification, call-centre support, and reporting services while serving millions of affected consumers with proven credit and web (identity) services.

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