

BRUNSWICK

# BRITAIN'S RESILIENCE GAP: ARE WE PREPARED FOR THE NEXT SHOCK?

As households are urged to keep three days' supplies and cyber incidents continue to tick upwards, new Brunswick research suggests a public doubtful about the UK's capacity to cope with security threats and their employers' ability to protect their companies and employees from a future of increasing security threats.



# EXECUTIVE SUMMARY

**On the day the UK government urged households to keep three days' food and water at home in case of a future crisis, 32 of its own services were unavailable. The disruption followed the discovery of security flaws in PHP, software used to run websites. It brought into sharp focus the importance of the launch of the *Be Ready* campaign on 22 October.**

The Resilience Pulse is a Brunswick Group study conducted online by YouGov among 8,576 adults across four European markets: the UK (n=2,260), France (n=2,017), Italy (n=2,075) and Germany (n=2,224). Data were weighted to be representative of the adult population (aged 18+) in each country. Fieldwork took place between 24 and 27 April 2026 in Germany and between 10 and 24 September 2026 across the UK, France and Italy. Differences involving Germany may therefore reflect the timing of fieldwork as well as differences between countries. The findings reflect respondents' perceptions and attitudes rather than objective assessments of preparedness. Results are representative of the individual national adult populations surveyed, not Europe as a whole.

Brunswick's Resilience Pulse offers insight into how resilient the UK public feels in weathering the next shock. It finds that most households doubt they could cope with a significant loss of income, while many employees have little idea how well their employer is prepared for security threats including disruptions and cyberattacks. The main findings:

- **Nearly two-thirds of people (63%) lack confidence that their household could cope with a significant reduction in household income.** Even among those expecting their finances to remain stable, just over half (51%) doubt they could manage such a loss.
- **People are least confident in the government's protection against disinformation campaigns:** 68% think the UK is not well protected against them, compared with 62% for cyberattacks. More than half (57%) feel poorly informed about security threats.
- **Around a quarter (26%) of employees say they do not know whether their employer is prepared to protect the business and its people from security threats.**[1] Four in ten (40%) think it is prepared; about a third (34%) think it is not.
- **The British public is more willing to accept reallocating government spending on security and resilience (41%)** than respondents in France (28%), Italy (11%) or Germany (26%). When asked specifically about willingness to pay higher taxes to fund measures that strengthen the UK's security and resilience, some 28% of respondents support this, while 41% would accept diverting money from other areas of public funds when presented with a range of funding options.

1 Results are based on a sample of 1,260 respondents in full-time or part-time employment in the UK.

# CYBERATTACKS AND DISINFORMATION

Half of UK adults think the government is overall not protecting the country sufficiently well against security threats, compared with 40% who think it is. Only 3% say the UK is very well protected.

Almost half (48%) think the UK is well protected against terrorism, the only threat tested for which more people think the country is well protected than not. This falls to 26% for cyberattacks and just 15% for disinformation campaigns.

These findings come as the government's Be Ready campaign has brought emergency preparedness into sharper focus. At the same time, the head of the National Cyber Security Centre (NCSC), Richard Horne, has warned that advances in AI could allow attackers to exploit existing vulnerabilities faster and on a greater scale. The recent PHP security vulnerability illustrates how difficult some of the decisions behind those assessments can be. The National Cyber Security Centre advised organisations to update affected systems, apply temporary protections or consider taking them offline if they could not be secured. An organisation following that advice could find itself explaining why it had deliberately interrupted a service on which people relied.

## WHAT PEOPLE KNOW ABOUT THE RISKS

More than half the public (57%) feel poorly informed about the security threats the UK could face. Only 35% feel well informed. Doubts about preparedness extend beyond security: 77% think the UK is insufficiently prepared for a major economic crisis, 75% for extreme weather and 65% for a major public health crisis.

The Be Ready advice recognises that people have different means. Alongside keeping supplies at home, it recommends free steps such as joining the Priority Services Register, which helps utilities identify customers who may need extra support. The Cabinet Office acknowledges that not everyone will be able to follow every part of the advice.

Employers face much the same practical difficulty. Telling staff to work from home, use a different site or contact a manager by another route is only useful if they can do it. Preparations need to account for people whose circumstances make those changes difficult. Otherwise, instructions that look reasonable to the crisis team may not work for the people receiving them.



# COULD HOUSEHOLDS COPE?

Most people are not expecting their own circumstances to deteriorate. More than half (55%) are confident their household finances will remain stable over the next year, and 59% expect stability in their household's income or employment situation. That is a rather different picture from their assessment of the country's readiness for a crisis.

But there is little confidence about coping if something does go wrong. Just 29% think their household could manage a significant reduction in income, while 63% lack confidence that it could. Just over half (51%) doubt they could cope with a significant increase in essential living costs; 46% say the same of a large unexpected expense.

Among respondents confident their finances will remain stable, 51% nevertheless doubt they could cope with a significant loss of income. Even an apparently reassuring answer about the year ahead can conceal considerable anxiety about what would happen if things went wrong.

For employers, that complicates the task of identifying who might need help. Asking whether staff expect financial difficulties would miss some of those who doubt they could cope with an interruption to their income.

## WHEN WAGES AND PAYMENTS STOP

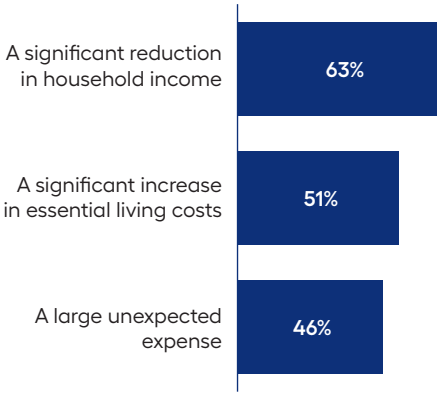
At a national level, four in five people lack confidence that the economy could withstand a major global shock without significant disruption to living standards. Three-quarters say the same about jobs and employment. Doubts are somewhat less widespread about business activity and investment (67%) and the delivery of critical services (61%), though still held by clear majorities.

An outage that cancels shifts could leave an employee short of money with bills falling due before work resumes. A supplier whose invoice goes unpaid may have to postpone its own payments. These are the kinds of consequences a crisis exercise should follow through, even when they occur outside the company.

Finance and human resources teams should therefore be involved before an incident, with agreed arrangements for wages, urgent supplier payments and support for customers in difficulty. Where help cannot be offered, leaders need to understand that constraint too. They may have to explain a decision that is defensible for the business but leaves someone else materially worse off.

**Household finances: coping with a shock**

Showing % not very or not at all confident that their household could cope financially




Base: 2,260 adults in the UK



# WHAT EMPLOYEES KNOW ABOUT THEIR EMPLOYER'S PREPAREDNESS MEASURES

Employees give their employers a mixed assessment. Four in ten (40%) think their organisation is well prepared to protect itself and its people from security threats, compared with 34% who think it is not. Only 7% think it is very well prepared. Another 26% do not know.

The size of that last group distinguishes the UK from the other countries surveyed. In France, Italy and Germany, 19% of employees say they do not know how prepared their employer is. British employees are less likely than their French counterparts to say their employer is unprepared, but are more likely to be uncertain.

Fewer than four in ten employees (39%) feel well informed about their employer's security measures. Some 37% feel poorly informed and a quarter answer 'don't know'. Asked whether their employer is investing enough in security, 29% do not know, again the highest proportion among the four countries.

Some of these employers may have made substantial preparations without staff knowing much about them. That would be worth finding out. A business spending money on resilience ought to know whether employees understand the changes being made and their own part in putting them into practice.

## INFORMATION AND CONFIDENCE

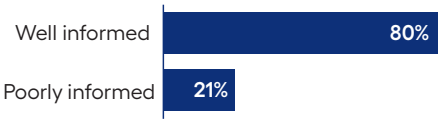
Among employees who feel well informed about security measures, 80% consider their employer well prepared. Among those who feel poorly informed, only 21% do. There is a similar difference in confidence about security investment: 77% of the well-informed group think their employer is investing enough, against 18% of the poorly informed group.

It would be rash to assume that better communication alone would close that gap. Employers that prepare thoroughly may also explain themselves better. But the difference warrants a closer look at what staff are actually hearing and whether they understand it.

This need not involve sharing sensitive technical information. Staff should know where they would find reliable updates if normal channels failed, what they could decide for themselves and whom to contact about a problem. Managers also need enough knowledge to answer questions about pay or working arrangements. Those conversations are easier to rehearse before an incident than to improvise when a worried employee asks for an answer.

**Perceptions of employer preparedness amongst employees, by how informed they feel about their employers' security measures**

Showing % who say their employer is well prepared




Base: 1,260 full-time or part-time employed adults in the UK. Well informed (n=519) / poorly informed (n=455).

# WHO WILL PAY?

The public's willingness to pay for stronger protection is less straightforward than a story of people wanting more but refusing to fund it. British respondents are more willing to consider financial trade-offs involved in strengthening resilience than those in France, Germany and Italy.

Some 28% support paying higher taxes to fund measures that strengthen the UK's security and resilience, compared with 33% who oppose them. Another 29% neither support nor oppose the idea and 10% do not know. Support is higher than in Italy (21%), Germany (17%) or France (14%).

When asked about willingness to accept various funding options for increased government spending on security and resilience, 41% in the UK would accept reallocating existing government spending, the most popular choice. Almost a quarter (23%) would accept none of the options tested, although this is considerably lower than in France (39%), Germany (41%) and Italy (54%). The questionnaire cited social benefits, healthcare and education as examples of spending that could be reallocated. While this does not indicate support for cuts to any particular area, it suggests some willingness to consider difficult trade-offs between resilience and other public spending priorities.

## OLDER PEOPLE ARE MORE WILLING TO PAY

People aged 65 and over are markedly more doubtful about national protection: 63% think the UK is not well protected, compared with 40% of 18–24-year-olds. Yet four in ten of the older group support paying higher taxes to fund measures that strengthen the UK's security and resilience, compared with only 23% of the youngest group.

Financial confidence is relevant too. Support for paying higher taxes reaches 34% among those confident their household finances will remain stable, compared with 23% among those who are not. Concern about the country's security clearly does not settle the question of what people are willing to pay.

Businesses making the case for their own resilience spending will face questions about what it buys and who bears the cost. Being specific should help: which interruption would the investment prevent, how much disruption could it shorten, and what would happen without it? Employees and customers are entitled to ask how a proposal would protect them as well as the company.



# WHAT THE FINDINGS TELL US

Taken together, the findings suggest that the UK's resilience challenge extends beyond the strength of its defences and emergency plans. The gap between employees' awareness and confidence in their employers, alongside the financial vulnerabilities facing households, points to a wider challenge: organisations cannot assume that the people they depend on will have the understanding, resources or confidence to navigate disruption alongside them.

Building resilience therefore means investing not only in systems and processes, but in the relationships, trust and practical support that will sustain stakeholders when those systems are tested. The real measure of resilience is not simply how quickly an organisation recovers, but whether it has earned the trust and built the relationships needed to bring its stakeholders through the crisis with it.

## QUESTIONS FOR THE BOARD

The findings raise a more fundamental question for boards: what do the people who depend on our organisation trust us to deliver, and what happens to that trust when disruption strikes? Recovery plans may depend on employees working differently, suppliers waiting for payment or customers accepting delays. But these expectations need to be tested against the circumstances of those stakeholders, and the commitments an organisation has made to them.

### 1 Are we prepared for the difficult trade-offs that emerging threats can create?

Cyberattacks and disinformation are among the UK's greatest perceived security vulnerabilities, with advances in AI adding to the speed and complexity of these threats. But protecting an organisation from one risk can create another. Taking systems offline to contain a cyber threat, for example, may be necessary to protect customers and data, while simultaneously disrupting essential services, employee payments or supplier operations.

Boards should therefore consider not only whether their organisation can detect and respond to emerging threats, but how decisions taken to contain an incident could affect stakeholders, what new risks those decisions might create and how they would explain the trade-offs involved. In an environment where misinformation can spread rapidly, the ability to make sound decisions and communicate them credibly may be as important as the technical response itself.

### 2 Are we prepared to make the decisions that will protect stakeholder trust?

Trust is tested as much by what organisations do during a crisis as by what they say. Paying a supplier early, compensating a customer or keeping staff on full pay may require approval from stakeholders outside the incident team.

Boards should establish in advance who has the authority to make these decisions, what support the company could realistically provide and how competing stakeholder needs would be weighed. This is particularly important when decisions that are defensible from an operational or financial perspective may nevertheless leave employees, customers or suppliers facing significant hardship. Those consequences can quickly compound the original disruption – undermining workforce stability, placing further strain on supply chains and weakening the trust and relationships on which an organisation's recovery depends.

### 3 Have we built the relationships and understanding needed to sustain trust under pressure?

Only 39% of employees feel informed about their employer's security measures. Those who feel informed are substantially more likely to believe their organisation is prepared (80% versus 21%), although the research does not establish that communication alone drives confidence.

The findings raise questions about whether organisations are doing enough to build understanding and credibility before a crisis occurs. Employees should know what is expected of them, where to find reliable information and whom to contact when normal arrangements fail. Leaders must also be ready to explain difficult decisions, acknowledge uncertainty and demonstrate through their actions that stakeholder concerns are being taken seriously.

In short, trust cannot be established through crisis communications alone. It is built through the relationships, preparedness and actions that precede a crisis – and tested by how an organisation responds when those commitments come under pressure.

# COMMUNICATING WITH EMPLOYEES ABOUT RESILIENCE

## REGULAR BRIEFINGS

Resilience should feature in regular staff communications, with updates tied to changes in the world and the company's operating environment. Explain why a development matters to the business, what preparations are under way and how employees can help. After a disruption elsewhere, for example, a briefing could explain which arrangements are being checked and whether staff need to do anything differently.

These messages should feel like a routine part of running the business. An ominous warning, delivered without context or anything useful to do, can cause more anxiety than silence. Use familiar channels and a measured tone, reserving urgent language for situations that genuinely require it.

## EMPLOYEES' ROLE IN RISK

Companies should examine how everyday behaviour could create or worsen a problem before an incident exposes it. The thinking behind phishing exercises also applies to physical security, the handling of sensitive information and the ways staff improvise when normal processes are unavailable. Where might a shortcut bypass an important safeguard? Could an unverified message be mistaken for an instruction?

Employees can help identify those weaknesses. Ask where procedures are unclear or difficult to follow and make reporting straightforward. Staff need to be able to admit mistakes without fearing that the exercise is about finding someone to blame.

## INSTRUCTIONS AND PRACTICE

Before writing the message, agree what each group of employees would need to do to prevent a problem or respond to one. A site team and a payroll team will need different instructions. Set out what to report, who can take decisions and where to find updates if the usual channels are down. Be clear about what people should not attempt themselves.

As with a fire drill, give people a chance to rehearse. A short exercise can test whether instructions are understood and can actually be followed. Managers need answers to likely questions, including those about pay and working arrangements, and a route for escalating anything they cannot resolve. Revise the guidance where an exercise reveals a problem.



> “A warning about resilience that arrives out of the blue can leave people more worried than before. Staff need to understand why the company is talking about a risk, what it is doing and what they should do themselves. Regular, matter-of-fact conversations and a chance to practise are much more useful than a one-off message that simply tells everyone to be vigilant.”
>
> Sarah West, Managing Partner, UK & Europe

> “For someone waiting for their wages, a cyberattack that stops payroll is also a financial emergency. A flood that closes their workplace can have the same effect. Government and business need to plan for those consequences together. When so many households doubt they could cope with a loss of income, assuming people can manage until normal service resumes is a serious weakness in a crisis plan.”
>
> Dan Roberts, Global Co-Lead, Crisis

## OUR EXPERTS



**Dan Roberts**
Global Co-Lead, Crisis

Dan Roberts is Global Co-Lead of Brunswick's Crisis, Litigation and Cybersecurity practice, specialising in helping companies manage their reputation through both proactive transformation programmes and reactive crisis management.

Over eight years at Brunswick, he has advised clients facing reputational crises in 14 countries, supporting more than a dozen FTSE 100 clients and other European and US multinationals through some of their highest-profile financial, political and social challenges.



**Sarah West**
Managing Partner
for UK & Europe

Sarah leads the firm's business across the region and its integrated offer to clients in increasingly complex geopolitical, regulatory, and reputational environments.

Sarah is a senior adviser to boards, CEOs, and leadership teams, helping organisations navigate the moments that matter most to their business, reputation, and future.




## EDITORIAL CREDITS

**Authors**

Sarah West, Partner

Dan Roberts, Partner

Laura Sullivan, Partner

Simon Finkelstein, Director

Beverly Liew, Associate

**Research**

YouGov, commissioned by Brunswick Group

Brunswick Group, London
16 Lincoln's Inn Fields
London WC2A 3ED
United Kingdom

+44 20 7404 5959

londonoffice@
brunswickgroup.com

www.brunswickgroup.com