

STUDY

THE DUAL RESILIENCE GAP

Why businesses and the government need to take further security measures and communicate more transparently about them

1. GERMANY: THE NEED FOR SECURITY IN A HYPER-ANXIOUS NATION

Germany is experiencing a period of profound uncertainty. The geopolitical crisis, with wars and trade conflicts, is compounded by an economic crisis featuring job cuts in what were once Germany's flagship industries, high energy costs and the threat of cuts to the welfare state. Multiple crises have become the new normal: what was long considered an exception is now the background noise of the German economic and social model. Both public and politicians are increasingly reacting "hyper-anxiously" (Chancellor Friedrich Merz).

The current situation shows that Germany is vulnerable. Citizens in general, as well as many employees, are becoming increasingly aware of the lack of competitiveness, disrupted supply chains, hybrid attacks, cyberattacks, sabotage, and disinformation in their everyday lives. Although politicians and many companies have responded to this new vulnerability in recent years and introduced security measures, there is still a great need for more information, education, and reliable analysis.

The Brunswick Group has produced this study based on a representative YouGov survey[1]. It shows that, from the public's perspective, there is a twofold resilience gap in Germany. On the one hand, a clear majority of 66 per cent of respondents doubt that the government is protecting Germany effectively against security threats. At the same time, there is a communication gap. Both the general public and employees in companies feel that they are not being kept well informed by both the government and their employers about the threats and the measures taken to counter them.

Specifically, only 30 per cent of Germans feel well informed about the various security threats to which Germany might be exposed. 61 per cent do not feel well informed. This gap is central to political communication. After all, uncertainty and anxiety arise not only from the risks themselves, but also from a lack of context.

Resilience: A leadership and communication challenge for companies

But companies, too, face challenges in this situation. Resilience can no longer be understood solely as operational robustness: as a contingency plan, IT security architecture, backup system or insurance issue. Rather, resilience is becoming a leadership and communication task. The findings of the employer survey in this study show that almost one in two (44 per cent) of employees consider their company to be relatively well equipped to deal with security threats such as cyberattacks. 50 per cent of the workforce are even confident that their employer invests sufficiently in security measures. At the same time, however, 41 per cent of employees feel they are not sufficiently informed about these measures.

The key finding of this study is therefore: companies that want to be resilient in times of crisis must communicate better: preparedness must be visible, leadership must be credible, and the ability to act must be understandable. For in times of crisis, it is not only crucial whether a company is technologically prepared. It is also crucial whether employees, customers, investors, suppliers and the public understand what is happening, why certain measures are being taken, and what is expected of them in an emergency. Only in this way can trust be maintained, the necessary support secured and the company's reputation protected.

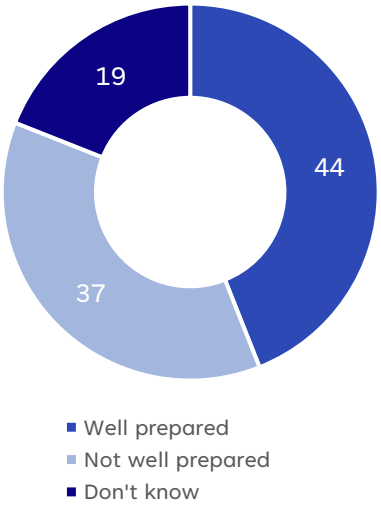
[1] The survey was conducted online by YouGov between 24 and 27 April 2026. A total of 2,224 adults in Germany aged 18 and over were surveyed. The results were weighted and are representative of the adult population in Germany.

2. R RESILIENCE IN COMPANIES: UNCERTAINTY AMONG EMPLOYEES

2.1. Employees are divided on the resilience of their employers

44 per cent of people in employment surveyed (part-time and full-time employees) say their employer is very or fairly well prepared to protect the company and its employees from security threats. By contrast, 37 per cent consider their employer to be ill-prepared. At the same time, 19 per cent say they do not know how well their employer is prepared.

A majority of employees believe their company is well-positioned to cope

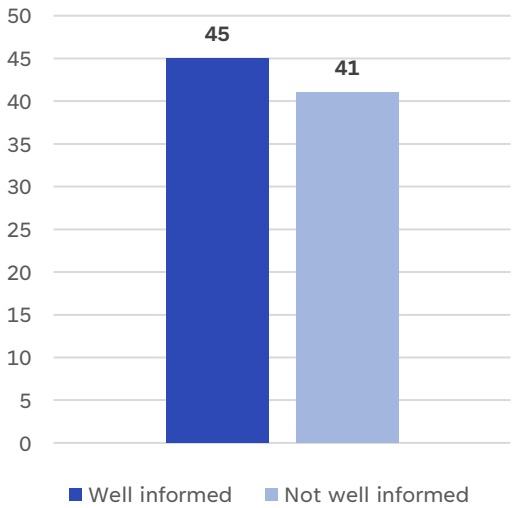


2.2. The security architecture remains unclear to many employees

45 per cent of employees feel very or fairly well informed about their employer's security measures. At the same time, however, 41 per cent feel they are not well informed.

The breakdown is particularly relevant: 13 per cent feel very well informed, 32 per cent fairly well. On the other hand, 28 per cent feel not very well informed and 13 per cent not at all informed.

Resilience in the workplace: a narrow majority of employees feel well informed



2.3. Investment: Trust in budgets is not enough without trust in priorities

When asked whether their employer invests enough in safety measures, the picture is somewhat more positive: 50 per cent of the working population are very or fairly confident that their employer invests sufficiently. 33 per cent are not confident. 17 per cent do not know.

Here too, the trend is encouraging, but remains limited in substance. Only 15 per cent are very confident, 36 per cent fairly confident. The majority of this confidence is therefore not firmly rooted, but rather pragmatic: employees assume that their employer is already doing something. Whether they understand exactly what is being done, why it is sufficient and how it fits the risk situation remains open.

3. GENERAL PUBLIC: GOVERNMENT IS FAILING TO PREPARE GERMANY ADEQUATELY FOR CRISES

3.1. Low confidence in the state's ability to protect – particularly against cyberattacks and sabotage

A majority of Germans doubt that the country is adequately protected against security threats by the federal government. Overall, only 25 per cent believe that Germany is well protected against security threats such as terrorism, sabotage or cyberattacks by the federal government. By contrast, 66 per cent say that Germany's government does not protect the country well enough. This low level of confidence in protection runs through all the risk areas surveyed.

The assessment is particularly critical when it comes to cyberattacks. Only 19 per cent of respondents rate the government's protective measures as good, whilst 71 per cent say the country is not well protected. Cyber risks are perceived as the greatest vulnerability among the risks surveyed.

The assessment is almost as critical when it comes to acts of sabotage, for example against infrastructure. Here too, only 19 per cent consider Germany to be well protected, whilst 70 per cent rate the protection as inadequate.

When it comes to military threats and armed conflicts, 25 per cent consider Germany to be well protected by the government, whilst 65 per cent do not consider the country to be well protected. Scepticism also prevails regarding disinformation campaigns: only 22 per cent consider Germany to be well protected, whilst 63 per cent do not. At the same time, the proportion of those answering 'don't know' is particularly high here, at 15 per cent.

The public views the state as being somewhat better equipped to deal with terrorism – albeit still at a low level. 31 per cent of Germans consider the country to be well protected in this regard, whilst 62 per cent do not. Terrorism is thus the only area surveyed in which the proportion of positive assessments exceeds 30 per cent.

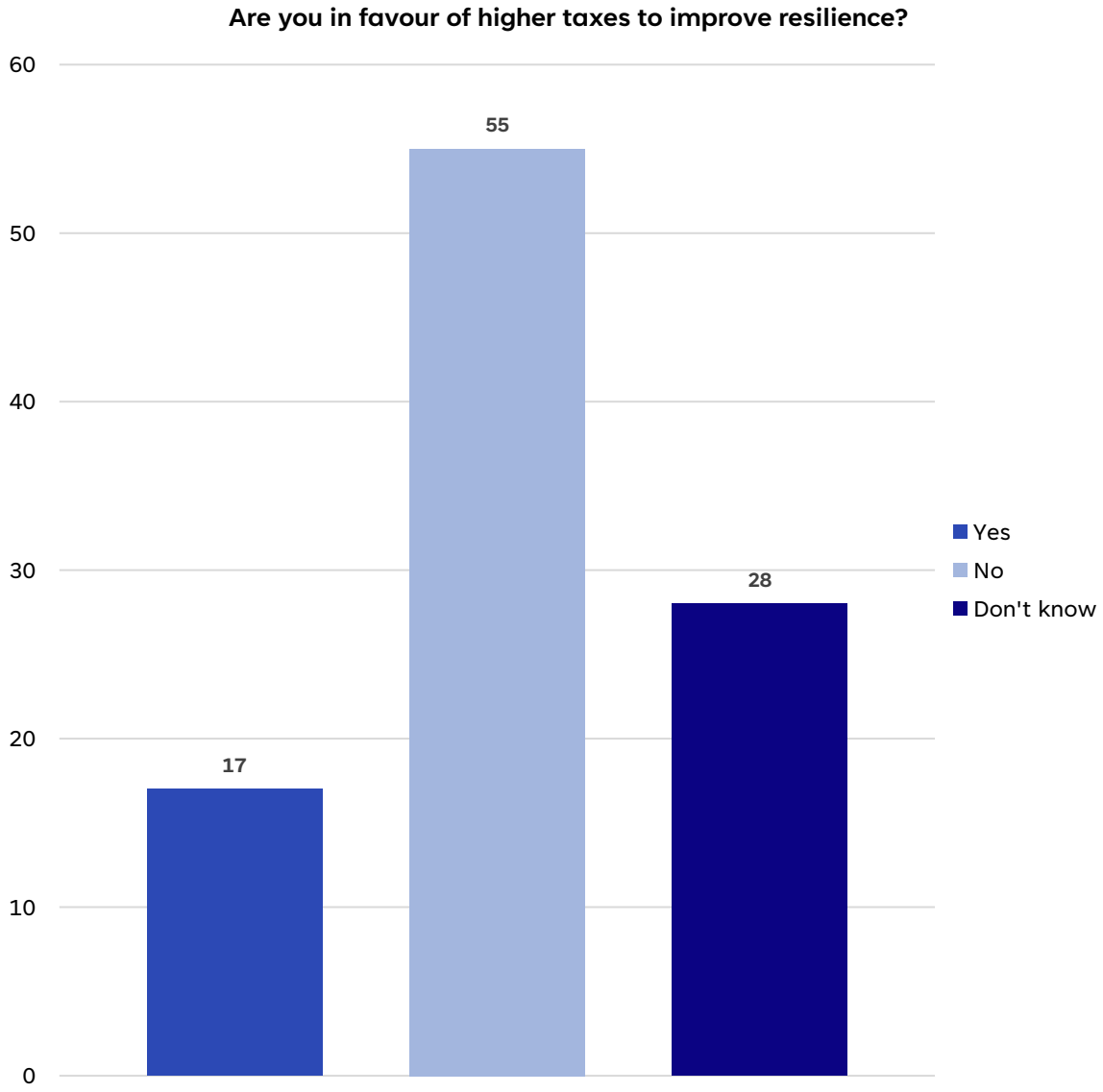
Threat	Protected	Not protected	Don't know
Terrorism	31%	62%	8%
Military threats	25%	65%	9%
Disinformation campaigns	22%	63%	15%
Cyberattacks	19%	71%	9%
Sabotage operations (e.g. against infrastructure)	19%	70%	11%

3.2. Information gap exacerbates uncertainty

Alongside low confidence in security measures, there is a marked information gap. Only 30 per cent of Germans feel well informed about potential security threats. By contrast, 61 per cent say they do not feel well informed. Here too, it is not complete ignorance that prevails, but rather a sense of insufficient guidance: 48 per cent feel ‘not very well informed’, 13 per cent ‘not at all informed’.

3.3. Limited willingness to pay more for resilience

Despite the perceived threat, there is little willingness among Germans to accept higher taxes for security and resilience measures. Only 17 per cent support higher taxes for measures such as infrastructure protection, cyber security or civil defence. 55 per cent reject this, 33 per cent of them strongly so. 28 per cent are undecided.



COMPANIES MUST STRENGTHEN RESILIENCE – BUT ALSO EXPLAIN IT

At a time of increasing geopolitical tensions, digital vulnerabilities, and complex supply chains, companies face the challenge of fundamentally rethinking their resilience. Resilience does not merely mean being able to react to disruptions, but designing structures, processes, and decision-making pathways in such a way that threats – ranging from sabotage to systemic crises – are identified and averted at an early stage. Putting many aspects under scrutiny is therefore no longer an option, but a strategic necessity. This can entail far-reaching decisions, for example regarding the selection of partners, the protection of critical infrastructure or internal governance. Companies that take this step consistently not only strengthen their ability to cope with crises but also lay the foundations for lasting trust among customers, investors and the public.

“Resilience is no longer merely a reaction to crises, but a strategic management task,” emphasises Joachim Peter, who has led the global defence industry sector at Brunswick for many years. This task must not be postponed. “Companies must now fundamentally question established structures in order to protect themselves effectively against sabotage and other systemic threats. Every day brings risks – which is why companies need to make far-reaching and uncomfortable decisions.”

> “
> Nowadays, resilience is no longer simply a response to crises, but a strategic management task.
>
> Dr. Joachim Peter, Brunswick

The vast majority of companies, particularly large enterprises, have invested heavily in technological safeguards and organisational preparedness for cyberattacks in recent years. Nevertheless, the threat is growing exponentially. Suntka von Halen, a partner in the global cybersecurity practice at Brunswick, explains: “The number, scale, and complexity of cyberattacks on companies will continue to rise, fuelled in part by artificial intelligence. Resilience is the decisive factor in limiting the impact: solution-oriented strategies, close collaboration, good communication, flexible processes.” Nor is the Federal Office for Information Security (BSI) giving the all-clear. On the contrary: the Office is even calling on all societal stakeholders to “take even more effective measures to protect their attack surfaces” in future. (“The State of IT Security”, 2025).

Communication is a central component of corporate responsibilty

Communication plays a crucial role in building resilience. It is not enough to invest in technology alone. As the YouGov survey commissioned by the Brunswick Group shows, employees do not feel very well informed about threats and measures.

Resilience does not arise solely from structures, budgets and technical safeguards. It arises when people understand what their company is preparing for, which risks are relevant, what role they play as employees, and how they must act in an emergency.

This makes communication a central component of corporate responsibility. Companies must develop a clear narrative on resilience: Which threats are relevant to us? What are we doing to be prepared?

> “
> Resilience is the key factor in times of crisis: solution-focused strategies, close collaboration, flexible processes and effective communication.
>
> Suntka von Halen, Brunswick

What are our expectations of managers and employees? How do we respond to cyberattacks, sabotage, physical security incidents, business interruptions or disinformation campaigns? And how do we deal with a highly volatile political and geopolitical situation?

Employees are not merely the target audience of internal communication but are themselves part of the resilience. Their behaviour is particularly crucial when it comes to cyber risks, disinformation or operational disruptions. Companies must therefore prepare their employees carefully – the necessary attitude towards resilience, the 'resilience mindset', does not arise from abstract appeals or occasional warnings – but through everyday, concrete, and action-oriented communication, regular updates, scenario planning, and crisis training. Good crisis communication does not begin during the crisis, but long before it.

Managers must establish the link between the geopolitical situation, risks, internal measures and the concrete realities of everyday work

Managers play a key role in this process. In times of crisis, people do not trust official channels alone, but above all, individuals. Managers must therefore establish the link between the geopolitical situation, corporate risks, internal measures, and the concrete realities of everyday work. They must explain, contextualise, and empower people to act. To do this, they themselves need preparation: briefings, training, communication materials, and robust, flexible crisis processes.

A clear and lived understanding of resilience makes companies beacons in times of crisis for employees, customers, partners, investors, and society. This role brings with it responsibility. Companies and leaders must view resilience not merely as a matter of their own self-interest, but as a contribution to societal stability.

Security policy, defence, disaster management, and the protection of critical infrastructure remain core state responsibilities – yet companies are a crucial pillar of our society's overall resilience.

OUR EXPERTS



Dr. Joachim Peter

Partner, Head of the Berlin Office

+49 173 8780701

jpeter@brunswickgroup.com

Before joining Brunswick in 2013, he worked as a correspondent for the daily newspaper DIE WELT in Berlin and was part of the management team at the newswire dapd as head of political reporting. For a time, he also headed the Strategic Communications Unit within the then Executive Staff of the Federal Ministry of Defence. Dr. Joachim Peter advises clients in sectors such as energy, finance, technology, and defence.



Suntka von Halen

Partner, Co-lead Crisis & Cybersecurity

+49 151 1688 2769

svonhalen@brunswickgroup.com

Suntka von Halen specialises in crisis communications and cybersecurity, as well as transformation, change, and restructuring. As Co-Lead for Cybersecurity, she works with the Brunswick team to support companies worldwide with crisis preparedness and cross-border crisis communications and crisis management assignments. Before joining Brunswick in 2016, she spent many years working in corporate communications and as a media spokesperson.

Imprint:

Text: Alexander Gruber

Brunswick Group GmbH
Friedrichstraße 95
10117 Berlin
www.brunswickgroup.com

USt-IdNr.: DE 213 923 472
Handelsregister: HRB 51768, Registergericht: Frankfurt a. Main
Geschäftsführer: Andrew Fenwick, Alan Parker, Christian Weyand