The MEASURE of RESILIENCE

A major BRUNSWICK SURVEY in Germany lays out the challenge for surviving a crisis with public trust intact. By JOACHIM PETER

It was only by chance that Leipzig airport was spared a catastrophe. Reports came in thick and fast: During the night of August 5, a drone was detected near the runway. According to German investigators, the autonomous aircraft had been fitted with explosives and had struck the wing of a Ukrainian Antonov An-124 parked on the ground. The fact that the drone failed to detonate was apparently due to a faulty fuse.

The incident serves as a stark reminder that we live in a world of persistent and multifaceted crises, threats and risks. In recent months, Germany has seen attacks on its rail network, on Berlin's power grid and on a German company. Every year, thousands of cyberattacks are mounted against German governments, public authorities and businesses. The number continues to rise.

Calls for greater resilience are becoming increasingly urgent—and not only in Germany. "Europe must accelerate its resilience to keep the pace with this fast-evolving threat landscape," states an official Brussels document published in 2026. Public concern is high, as are demands for action and calls for greater transparency.

Brunswick recently published a representative survey of over 2,200 adults in Germany aged 18 and over. Conducted in April in partnership with YouGov, the results demonstrate just how much the issue is weighing on people's minds.

A clear majority of respondents, 66%, doubt that the government is doing a good job of protecting Germany against security threats. And only 30% said they felt well informed about the security threats Germany could face; 61% said they did not.

Resilience can no longer be understood only in terms of operational robustness—as a contingency plan, an IT security architecture, a back-up system or an insurance consideration. It is now a leadership and communications imperative.

Cybersecurity and geopolitical conflict are not the only sources of threats to society's resilience. The effects of climate change and other natural and environmental disasters, acts of sabotage, accidents, epidemics and other crises are also contributing. Over the summer months, large-scale wildfires swept across France, Spain, Greece, Belgium and Germany, causing significant environmental and economic damage and claiming lives. Extreme low-water levels also brought the transport of goods along rivers to a standstill in many places.

No government in the world can guarantee complete protection for production facilities, office buildings and supply chains—many of which operate across national borders. Resilience is therefore a corporate responsibility as well as governmental, and potential threat scenarios belong firmly on the agenda of executive and supervisory boards.

Our survey results show that 44% of employees believe their company is relatively well prepared for security threats such as cyberattacks. About half are confident that their employer is investing sufficiently in security measures. At the same time, however, 41% of employees do not feel adequately informed about those measures.

The central conclusion is clear: Companies seeking to remain resilient in times of crisis must do more than prepare effectively, they must also communicate that preparedness effectively. Preparedness must be visible and leadership must be credible. Employees, customers, investors, suppliers and the wider public must be able to understand what is happening, why certain measures are being taken and what will be expected of them should a crisis occur.

Uncertainty and anxiety are driven not only by the risks themselves, but also by a lack of information, context and guidance. Only through targeted, comprehensive preparation and clear communication can companies preserve trust and protect their reputation. ◆

DR. JOACHIM PETER is a Partner, Co-Lead of Brunswick's global defense industry sector and Head of the firm's Berlin Office.



ILLUSTRATION: EDMON DE HARO