

When the lights go out

Why every board is responsible for protecting critical infrastructure and bracing for unpredictable shocks: lessons from the energy sector and beyond.

On the afternoon of 28 April 2025, Spain lost around 15 gigawatts of power, approximately 60% of the usual electricity demand at the time, within moments. The outage also swept through Portugal and parts of southern France, grinding trains to a halt, disabling payment systems and leaving millions of people in the dark. Many observers' first instinct was to suspect a cyberattack, but that suspicion proved unfounded. An investigation by the European network operators found a combination of technical factors to be at fault: gaps in voltage control, oscillations in the grid and cascading shutdowns that spread in a split second.

For boards of directors, there's an important message in this episode: resilience is about more than managing individual risks. It is also about maintaining critical services and returning to normal operations quickly, even in the face of exceptional disruption. The specific trigger is not the decisive factor; critical dependencies across the entire value chain must be recognized and managed, and their resilience regularly tested. Resilience, then, is a strategic leadership responsibility and a core component of effective governance.

Shocks cannot be predicted

Over the past five years, we have witnessed one shock after another: the pandemic, the risk of electricity shortfalls in Switzerland, global semiconductor shortages, the Iberian blackout and the exceptionally hot, dry summer of 2026. Few of these events had been anticipated in the way they ultimately unfolded. And this is precisely the point. The board of directors cannot predict what shock will come next, but it can build the capacity to absorb it.





“The board of directors cannot predict what shock will come next. But it can build the capacity to absorb it.”

This is nicely illustrated by Switzerland’s preparations for a possible electricity shortage in 2021 and 2022. The federal government activated its emergency plans for the winter of 2022/23 in response to a looming shortfall amid the war in Ukraine, outages at French nuclear power plants and low reservoir levels. The plans provided for four stages of escalation, from public appeals to conserve electricity and restrictions on certain uses, to consumption quotas for major consumers. Companies using more than 100 megawatt-hours a year would have been required to reduce their consumption by a specified percentage. As a last resort, rolling blackouts were on the table. Companies had to register, model their electricity consumption and prepare their business continuity arrangements for a scenario that would have affected production, payment systems and day-to-day operations.

A mild winter ultimately spared Switzerland from the worst-case scenario. Yet the episode was a matter of national security. A wealthy, stable country with strong infrastructure had suddenly found itself exposed to a supply risk it was unable to manage alone, given its reliance on imports and a European market under pressure. Even though no harm was done, the vulnerability was very real.

Resilience: from the engine room to the boardroom

Three developments have propelled resilience up the board’s agenda. First, the scope of what is deemed “critical” is expanding. Swiss law deliberately defines critical infrastructure in functional terms, i.e. as organizations whose failure would have serious consequences for the economy or the population. In practice, this means that an organization’s critical perimeter is almost always broader than its board assumes. It extends beyond the organization’s own property, plant and equipment to include control systems, IT service providers, cloud platforms and entire supply chains. In other words, it also includes third parties whose failure would have an immediate impact. Second, risks amplify one another. And third, new regulation makes individuals personally accountable for oversight.

When risks converge

The key takeaway for boards of directors is that relevant risks no longer occur in isolation. They are interconnected.

Cyber. Power grids and other critical systems are highly attractive targets for both criminal and state-sponsored actors. The transition to greener, more digitally connected infrastructure is expanding the attack surface through connected assets, cloud integration and the increasing convergence of information technology (IT) and operational technology (OT). At the same time, decades-old legacy systems and demanding availability requirements make security measures more difficult to implement. OT security is therefore becoming a core component of operational resilience and continuity of supply.

Climate and physical events. Extreme weather no longer just affects energy infrastructure. It can disrupt entire value chains. In summer 2024, exceptionally heavy rainfall caused the Rhône to burst its banks, flooding the Novelis and Constellium aluminum plants in Sierre, Valais, and forcing both companies to suspend production for several months. Since Novelis supplies European car manufacturers with sheet aluminum, companies such as Jaguar Land Rover and Porsche had to brace for significant production losses. A single, localized climate event reverberated through the supply chain of an entire industry.

Technical and systemic instability. As the energy system shifts toward renewable and decentralized generation, the grid’s physical inertia decreases. As we saw on the Iberian Peninsula, minor initial disturbances can then escalate through cascading effects.

Cross-sector dependencies. Electricity, telecommunications, water, payment systems and healthcare are interconnected. During the Iberian blackout, Portuguese hospitals operated on emergency power for hours and digital patient records were inaccessible, creating a domino effect that crossed sector boundaries. Electricity shortages and measures such as holding hydropower output in reserve can affect numerous, and sometimes unexpected, sectors. For instance, the tourism industry could be impacted by limited snowmaking capacity at lower elevations.

Geopolitics and supply chains. The global semiconductor crisis of 2021 and 2022 revealed just how critical a single dependency can be. Entire production lines in the automotive and mechanical engineering industries, both central to Switzerland's export economy, ground to a halt because components worth only a few francs were unavailable. Production of the most advanced chips is concentrated among a small number of companies and locations, turning a technical dependency into a geopolitical risk. Export controls and acts of sabotage targeting cables and pipelines are further sources of exposure in this area.

These risks are not additive but multiplicative: imagine a cyber incident during a heatwave, for example, or supply chain disruption in the midst of a geopolitical crisis. Organizations that consider risks in separate silos, cyber within IT, climate within sustainability and supply chains within procurement, systematically underestimate their compound effect.

The board already has a duty to act

Amid an evolving risk landscape, the regulatory environment has also grown more demanding, as demonstrated by recent developments in cybersecurity. Since 2025, critical infrastructure operators in Switzerland have been required to report significant cyberattacks to the National Cyber Security Centre (NCSC), with non-compliance now subject to sanctions. In the EU, Network and Information Security 2 (NIS2) and the Critical Entities Resilience (CER) Directive significantly raise the requirements and explicitly hold management bodies accountable. Although Swiss companies are not legally bound by the EU regime, they remain closely intertwined with it through networks, customers and supply chains. Adopting the higher standard is therefore a strategic decision rather than a legal one.

Climate disclosure and due diligence obligations often receive less attention but are equally relevant to boards of directors. Switzerland's Ordinance on Climate Disclosures has been in force since 1 January 2024. Large publicly traded companies, banks and insurers must disclose their climate-related risks and opportunities in accordance with the TCFD categories (Governance, Strategy, Risk Management, Metrics and Targets) and include a transition plan and emissions across the entire value chain. Companies reported for the first time on the 2024 financial year. The key governance point is that the report on non-financial matters must be approved and signed by the company's highest governing body. The board therefore bears the risk associated with incomplete or inaccurate reporting.

This obligation does not stand alone. Swiss corporate law assigns the board a set of inalienable core duties; these are overall management, organization and oversight, including effective risk management. There are also due diligence obligations across the supply chain. The resulting requirements, including cyber incident reporting, climate disclosure and risk oversight, form an interconnected framework that ultimately underlines one key point: the board of directors is responsible for the resilience of its organization.





What this means for the board

Resilience is becoming a core oversight responsibility across industries. Whether the organization is an energy provider, bank, industrial company, hospital or retailer, the underlying mechanics are the same. Five questions can help board members honestly assess their maturity.

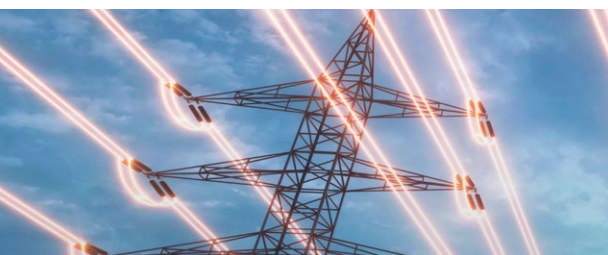
Five questions every board should ask

1. Do we understand our true critical perimeter, including our dependencies on third parties, cloud providers and suppliers?
2. Do we take a holistic view of resilience across technological, physical, climate-related, geopolitical, economic and supply chain risks?
3. Have we defined our “minimum viable company” and identified the resources, processes, technologies and third parties essential to maintaining it?
4. Are we meeting growing reporting, disclosure and due diligence obligations?
5. Is resilience oversight institutionalized through a regular reporting cadence, exercises, scenarios and clear board-level accountability?

All too often there is a gap between these questions and day-to-day practice. Closing it means translating growing obligations into robust resilience by regularly reviewing risk management and business continuity planning; ensuring reliable climate reporting; and actively managing cyber and supply chain risks. Scenario planning is the most effective tool to this end. Systematically working through specific crisis scenarios, such as the failure of a key supplier, a regional power outage or a cyber incident during a heatwave, reveals vulnerabilities and dependencies before they result in real-world disruption. Given the unpredictability of the next shock, this approach is vital, bringing together the separate functional silos into an overall picture that the board can assess and challenge.

Scenarios reveal where an organization is vulnerable, while emergency planning ensures that it remains capable of acting if a crisis occurs. The latter translates insights into concrete capabilities: business continuity plans for critical processes; clear roles and decision-making authority; established communication channels; and fallback solutions in the event of the loss of power, IT systems, sites or key suppliers. After the flood, for example, Novelis quickly transferred some of its production to sites in Germany, enabling it to continue supplying customers. Crucially, such plans must be rehearsed. An emergency plan that merely sits in a drawer will fail just when it is needed. Regular drills expose gaps before they have real-world consequences.

This all adds up to a mindset that transcends individual industries. Since the cause of the next shock is almost impossible to predict, it makes sense to plan around impacts rather than causes. Which functions and services are essential to the organization’s survival? What is our “minimum viable company”? Which processes,





technologies, data, sites and third parties must remain available even when operations are restricted? How long could the organization withstand a disruption? And how can it return to normal operations quickly? The answer depends less on the trigger than many assume. Whether it is a flood, cyberattack or supplier failure, the consequences are similar.

A board that thinks in these terms builds organizational resilience for an uncertain future, rather than merely defending the company against individual, supposedly known threats. The Iberian blackout only lasted a matter of hours, but its lesson has much wider implications. Critical infrastructure is broader, more interconnected and more heavily regulated than it was just a few years ago, and resilience has become a boardroom priority. Organizations whose boards recognize that resilience is a strategic, systemic leadership responsibility enjoy a genuine advantage: the ability to keep operating when others are left in the dark.

Authors:



Silvan Jurt
Partner, Head of Corporate
Sustainability Services,
Head of Markets
KPMG Switzerland

+41 58 249 50 25
sjurt@kpmg.com



Nicolas Tinguely
Partner, Cyber and
Digital Risk Consulting
KPMG Switzerland

+41 58 249 21 44
ntinguely@kpmg.com

This article is part of KPMG's Board Leadership News.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our **Privacy Policy**, which you can find on our homepage at www.kpmg.ch.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.