BM&T

Insights

FEB 26

Polycrisis demands a new kind of crisis leader. Most businesses don't have one[1]

"Polycrisis" is most often discussed at the level of nations and global systems: wars, energy shocks, pandemics, elections, supply chain breakdowns - shocks colliding across different spheres.[1] Mid-market companies rarely use the word. But they recognise the experience: distinct overlapping pressures that amplify each other.[1]

This insight contends that polycrisis is not confined to geopolitics. It applies directly to SMEs, and the interaction risk is higher still in cross-border businesses, where currency, regulatory, data, supply chain, and governance complexities create more potential points of failure.[1]

Here's what interaction risk looks like in the real mid-market: *a cyber incident interrupts invoicing, cash tightens within days, the lender tightens terms, suppliers flip you to pro-forma, delivery slips, customers wobble, and suddenly you're not managing "an incident", you're managing a cascade.*

BM&T Insights

And here is the provocation: the old model of crisis management is now a material risk

In the less prepared boardrooms, “crisis management” still means:

- keep cash tight
- keep stakeholders’ calm
- keep operations moving
- call advisers
- “hold the line”

That model assumes crises arrive as a single primary event with secondary consequences.

Polycrisis do behave like that. They entail interaction risk: multiple issues colliding across spheres, where the combined impact exceeds the sum of the parts; a compounding cluster, not a single fire.[1] So the job is no longer to manage the incident. It’s to prevent the cascade.

Why the SME version is at least as hard, if not harsher, than the nation-state version

SMEs suffer polycrisis differently because they have less “shock absorption”:

- less redundancy (people, suppliers, systems)
- less cash headroom
- more outsourcing (IT, payroll, platforms, data handling)
- more key-person dependency
- faster reputational exposure (clients, lenders, staff)

This means that a small trigger can quickly become existential. Within days, you’re not dealing with “a problem”. You’re dealing with interacting failures. And increasingly, those interacting failures are not just commercial in nature. They also pose governance and disclosure problems, as stakeholders now expect leadership to demonstrate oversight, decision-making discipline, and credible communication amid uncertainty.[2,3]

BM&T Insights

The modern threat surface: five domains that now define credibility

If you want a simple lens for what a modern crisis manager looks like, it's this:

A credible crisis manager in 2026 must be able to integrate *five domains* rapidly under scrutiny.

01. Cyber

Cyber is no longer an IT risk. It's an operational continuity and cash risk. The evidence base has caught up. National Institute of Standards and Technology CSF 2.0 makes GOVERN a core function, explicitly elevating cyber risk management into strategy, roles, oversight and supply-chain accountability.[4] In the UK, the National Cyber Security Centre's Cyber Assessment Framework similarly puts governance and risk management at the centre (Objective A, including Principle A1: Governance).[5,6] And the UK government's Cyber Governance Code of Practice is blunt about intent: it sets out "the most critical governance actions that directors are responsible for."[7]

A modern crisis manager must be able to:

- ask the right questions of technical teams and vendors
- understand containment trade-offs (and business impacts)
- make decisions without fantasy timelines

02. Data

Data is now a crisis accelerant because it converts operational disruption into:

- regulatory exposure
- contractual exposure
- customer trust collapse
- litigation and insurance friction

In the UK, the Information Commissioner's Office is clear: when a personal data breach is notifiable, you must notify "as soon as possible," and, where feasible, within 72 hours, and, in some cases, notify affected individuals without undue delay.[8] In the US, the baseline reality is fragmentation: across all states, they have data breach notification laws, and response expectations can vary by jurisdiction and sector.[9]

A crisis leader who cannot translate "data incident" into stakeholder consequences is flying blind.

03. Governance

Polycrisis punishes fuzzy authority. When decisions are slow, the organisation doesn't pause; it fragments. That is why cyber and resilience have moved from "management issue" to "director issue" in the UK's governance framework.[7] And it is why US governance expectations are rising in capital markets: the U.S. Securities and Exchange Commission now requires public companies to disclose material cyber incidents (Form 8-K Item 1.05) and to describe cybersecurity risk management strategy and governance in periodic filings.[10,11] In polycrisis conditions, governance isn't paperwork. Governance is operational control. *(UK lens: directors' duties to promote the success of the company sit in statute, and when insolvency is on the horizon, the risk calculus hardens, including potential exposure where directors fail to take steps to minimise creditor losses.)*[12,13]

04. Supply chain

Supply chains are no longer just about cost and logistics. They are continuity, reputation, working capital, and (increasingly) cyber exposure via third parties in multiple jurisdictions. NIST cybersecurity framework is explicit that cyber supply chain risk management should be integrated with broader organisational risk management[4] and in the UK, where businesses fall within the regime, incident notification duties reinforce that "continuity impact" is a regulatory matter, not merely operational inconvenience.[14]

A crisis manager needs to map dependencies beyond Tier-1:

- third parties, and their supply chain
- hidden single points of failure
- operational workarounds that preserve revenue

05. Crisis leadership and crisis communication

Here's the uncomfortable truth: In polycrisis, communication is not "reputation management". It is coordination. It determines whether:

- staff stay aligned or start freelancing
- lenders stay steady or tighten
- customers wait or walk
- suppliers collaborate or clamp down

Silence creates a vacuum. Over-reassurance can erode credibility later. Over-sharing creates panic. A credible crisis leader is visible and empathetic, communicates during times of uncertainty without destroying confidence and keeps decision-making clean enough to withstand hindsight.

The real question is:

Who do you want flying the plane while multiple systems fail, and everyone is watching?

Because "smart" and "senior" are no longer sufficient filters. Polycrisis demands people who can do three things at once:

- Stabilise (cash, operations, authority)
- Integrate (cyber, data, governance, supply chain)
- Communicate (truthfully, calmly, with action)

That is a craft. And it's rare.

BM&T Insights

A BM&T perspective

At BM&T, we work with mid-market organisations where crises are rarely single-cause events. They are interacting failures across cash, operations, stakeholders and governance. The organisations that stabilise fastest are the ones that treat crisis leadership as an operating system: decision rights, information discipline, stakeholder choreography, and communication as coordination.

Author Anton de Leeuw is an award-winning Certified Turnaround Practitioner (CTP) and crisis manager. He works with boards as a trusted adviser, NED and interim executive in complex stabilisations and cross-border situations. He has guided organisations through business continuity programmes and practical cyber resilience uplift, including Cyber Essentials alignment and broader Cyber Assurance accreditation pathways, strengthening governance, control environments, and operational readiness under the scrutiny of lenders, insurers, regulators, and boards.

This insight was prepared with the collaboration of Magda Vakil, an independent senior legal and governance leader with a track record advising at the intersection of law, risk and business strategy. Her career includes senior in-house roles across offshore and energy ecosystems, with leadership responsibilities spanning governance, stakeholder complexity and risk oversight.

HAYNES BOONE

Both Anton and Magda serve on Haynes Boone LLP's Crisis Management Academy 2026 Board of Directors, contributing to cross-industry dialogue on emerging threats, preparedness, and response practices.

1. World Economic Forum, "We're on the brink of a 'polycrisis' – how worried should we be?" (13 January 2023).

2. UK Government (DSIT), Cyber Governance Code of Practice (publication page).

3. U.S. Securities and Exchange Commission, Press Release No. 2023-139, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" (26 July 2023).

4. National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29, 26 February 2024).

5. National Cyber Security Centre, Cyber Assessment Framework (CAF): Objective A – Managing Security Risk (guidance page).

6. National Cyber Security Centre, Cyber Assessment Framework (CAF): Principle A1 – Governance (guidance page).

7. UK Government (DSIT), Cyber Governance Code of Practice (text: "the most critical governance actions that directors are responsible for").

8. Information Commissioner's Office, "Personal data breaches" (UK GDPR breach reporting guidance; 72-hour reference where feasible).

9. National Conference of State Legislatures, "Security Breach Notification Laws" (summary of U.S. state breach-notification laws).

10. U.S. Securities and Exchange Commission, Press Release No. 2023-139 (material incident disclosure and governance/risk management disclosure requirements).

11. Federal Register, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (final rule notice, 4 August 2023).

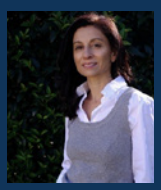
12. Companies Act 2006, s.172 (UK): Duty to promote the success of the company.

13. Insolvency Act 1986, s.214 (UK): Wrongful trading.

14. Network and Information Systems Regulations 2018 (UK), reg. 11: Duty to notify incidents (in-scope entities).

Authors

Anton de Leeuw
Chief Executive Officer



Magda Vakil
Independent senior legal and governance leader

Stabilise. Turnaround. Transform.

At BM&T, we bring this philosophy to life through hands-on company-side experience. Our team acts as CROs and Crisis Managers — operators who value human capital as much as financial capital. We combine financial expertise and operational excellence with empathy. Experience. Integrity. Tenacity.

BM&T European Restructuring Solutions Ltd, founded in 2008, is one of the most respected names in middle market corporate turnaround and restructuring.

Telephone: 020 3858 0289 From overseas: +44 20 3858 0289
Email: info@bmandt.com Website: bmandt.com