axiom
corestream grc

# There are no new risks, only new combinations: how pre-mortems and digital twins help GRC teams anticipate cascading risks

# Introduction: when risks combine resilience can suffer

When national governments began locking down in spring 2020, few risk registers anywhere carried a line for **"global shortage of automotive microchips."** Carmakers, forecasting a pandemic-driven collapse in demand, canceled their orders just as consumer electronics manufacturers absorbed the freed-up capacity to build laptops and games consoles for people stuck at home.

But when vehicle demand rebounded far faster than anyone had modeled, the chip capacity was gone. By September 2021, AlixPartners was forecasting the resulting shortage would cost the global auto industry **$210 billion in lost revenue and 7.7 million vehicles of lost production that year alone.**

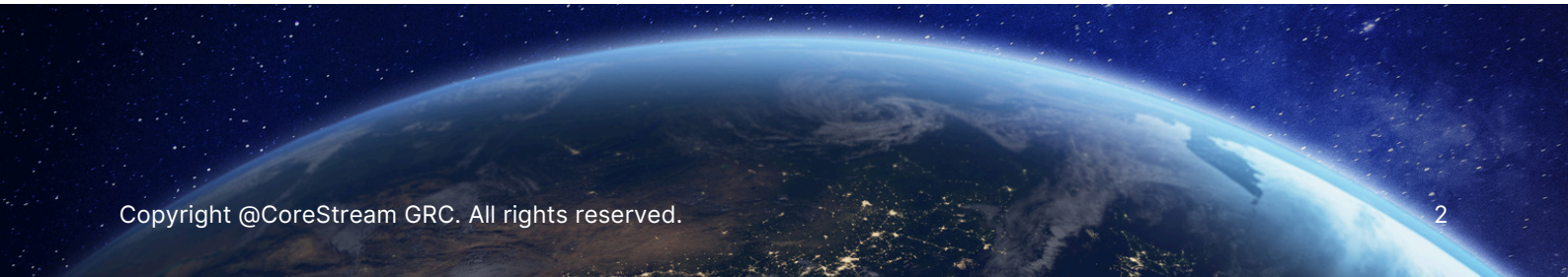
A public health emergency doesn't sit next to semiconductor allocation on any conventional risk register, yet one drove the other, and together they determined whether a car plant in Detroit or Stuttgart could build cars at all.

Three years later, a similar pattern played out in a completely different sector. On 19 July 2024, a routine software update from the cybersecurity firm CrowdStrike knocked out 8.5 million Windows devices worldwide. Airlines grounded flights, hospitals canceled procedures, banks froze services and some 911 emergency call centers went dark. More than 3,300 flights were canceled that day, and early estimates put the **global cost near $1 billion.**

It wasn't a cyberattack, and it wasn't a new kind of risk. It was just **one software update, at one vendor, cascading through sectors that had never considered themselves connected.**

Neither event makes it onto a typical risk register as a single line. As Emma Price, partner at the UK risk and governance consultancy Brave and formerly at Deloitte, explains on the Risk Is Our Business podcast, **"very rarely are there new risks."** What catches organizations out is known risks combining in a new and different way.

This article looks at why that combination is so hard to see coming and explores a **technique (the pre-mortem) and technology (digital twins) that can help spot those combinations before they occur.**



# There are no new risks, only new combinations

Ask most risk professionals what keeps them up at night and they will point to something specific: a **cyberattack, a key supplier failing, a regulatory change.** What Price's career has taught her is that the real damage rarely comes from any one of those risk factors alone. It comes from **several of them arriving together, in a sequence nobody modeled.**

Cascading risk gets missed, she argues, not through a lack of sophistication but a lack of effort: treating risks individually, she warns, can come back to bite organizations quite badly because properly mapping how one risk changes the odds of another is hard.

When asked what has scared her most in more than two decades in risk, Price called out the **failure to consider risk interconnectivity.**

The World Economic Forum's Global Risks Report 2026 and Allianz's Risk Barometer 2026 both identify risk interconnectivity as a defining feature of risk in 2026. The WEF reports on how “global risks continue to spiral in scale, interconnectivity and velocity” while Allianz identifies how, “As risk becomes more complex and interconnected, integrated resilience strategies can help to mitigate the impact.” Both point to the same remedy: not a longer risk register, but a **more integrated resilience strategy.**

The UK retail sector experienced this in 2025. A wave of social-engineering attacks against IT help desks compromised Marks & Spencer, Co-op and Harrods within weeks of each other, **cascading into empty shelves, halted online orders and an estimated $592 million in combined damages.**

That wasn’t an exotic risk. It was a **known vulnerability**, a help desk that could be talked into resetting a password, combining with a level of dependency on stock and distribution systems that none of the three retailers had mapped as a single, shared point of exposure. A resilient supply chain and a resilient IT estate turned out to be the same problem, viewed from two different departments.

1.0 There are no new risks, only new combinations

CoreStream GRC has described this interconnectivity before. The guide to modern enterprise risk management warns against the spreadsheet-driven risk register, which "makes it impossible to see how risks interact," and argues that **risks "no longer respect organizational boundaries."**

Paul Cadwallader, GRC Strategy Director at CoreStream GRC, makes the case from the value side:

> *"Effective, interconnected GRC achieves the desired outcome as efficiently as possible, meaning we **use our resources effectively and we minimize any unnecessary cost.**"*
>
> Paul Cadwallader, GRC Strategy Director, CoreStream GRC

Price's diagnosis and CoreStream GRC's are the same one: the individual risks are rarely the problem. The blind spot between them is, and seeing that **interconnection is the true value of an effective risk program.**

# Starting from failure: a pre-mortem approach to resilience and risk analysis

If interconnected risk is the problem, the starting point for a fix is surprisingly old-fashioned: **change the question you ask.**

Most scenario planning starts with a trigger. **What happens if a key supplier fails? What happens if we are hit by a cyberattack?** The trouble is that a predefined trigger anchors the conversation around risks the team can already imagine, which are rarely the ones that do the real damage.

The alternative is to conduct a pre-mortem: rather than predicting how something might fail, a pre-mortem assumes it already has, and **works backwards to find out why.** The technique was developed by the psychologist Gary Klein, described by him in an article for Harvard Business Review, and revisited by him recently in Psychology Today. He argues that imagining **a project has already failed, then explaining why, uncovers reasons for failure that conventional risk analysis overlooks.**

> *"The pre-mortem's appeal is that it is a risk assessment method that works."*
>
> Gary Klein Ph.D., writing in Psychology Today, The Pre-Mortem Method

Starting from a position of failure, Price says, **“gives people permission to think more freely,” because the team is no longer confined to a single predicted scenario. It “doesn't matter then what that cause of disruption is,”** since the exercise is concerned with the underlying assumptions and vulnerabilities, not the specific trigger.

That makes the technique reusable: the same weak assumptions tend to surface whether the eventual cause turns out to be a cyberattack, a flood, or the next pandemic. It is a broader discipline than what business continuity typically means inside most organizations: **not a fixed plan for one predicted disaster, but a habit of thought that works whatever the disaster turns out to be.**

The pre-mortem is a general decision-making discipline, developed in the United States and used everywhere from military planning to product launches. Any board or GRC team, anywhere, **making a decision it cannot afford to get wrong, can run one whenever required.**

# What is a digital twin and how can it support organizational resilience?

A digital twin, in a risk management context, is a **continuously updated virtual model of an organization's operations, risks and controls, built from real-time and historical data rather than a static snapshot.** It lets a risk team simulate how a disruption might actually spread through the organization before it happens, rather than relying on assumptions about how different parts of the business connect.

Price describes digital twins as a way of **locating an organization's real decision points rather than the ones an org chart suggests.** In supply chains, for example, a digital twin can help organizations **see past their first-tier suppliers into vulnerabilities sitting 2 or 3 tiers back.** That extended-enterprise visibility feeds supply chain agility: an organization cannot flex around a weak link it hasn't mapped.

AS GRC analyst Michael Rasmussen says,

> *"[Digital twin software] mirrors the enterprise: its structure, operations, risks, controls, policies, obligations, and external dependencies. But it's not a static mirror; it is context-aware and predictive. It continuously ingests real-time data, refines its assumptions, and runs simulations to project what might happen next."*
>
> Michael Rasmussen, GRC Analyst & Pundit, GRC 20/20 Research

A digital twin, he says, is an "engine of strategic foresight."

As Renee Murphy, principal analyst at Renee Murphy & Co, describes,

*"Every system in the enterprise suddenly becomes a data source ... Artificial intelligence gathers this noisy orchestra of information and begins to recognize patterns, relationships, and the occasional red flag that people might overlook while staring at a dashboard pretending it all makes sense. The twin then starts to simulate how these variables interact, allowing leaders to* ***see not just isolated risks but the chain reactions that turn small issues into full-scale crises three departments away."***

Renee Murphy,
writing on GRC Report,
Digital Twins in Risk Management:
Building the Intelligent Mirror of the Enterprise

"Digital twins," she says, "mark the moment when **risk management stops behaving like a historian and starts acting like a strategist."**

CoreStream GRC's own guide to value-based GRC describes the goal of a mature GRC program as building **"a 360-degree architecture – almost a digital twin – of the organization" to identify and mitigate risk before it bites.**

The catch is that, for many organizations, digital twin building is some way in the future. The foundation any digital twin needs, structured and interconnected data about how the organization actually works, is the one value-based GRC has always argued for, but the data quality and AI-driven processing power is often still work-in-progress.

And, as Price recently told CoreStream GRC's Spotlight on Women in GRC series: **"AI will give you insight, but it doesn't provide judgment. It'll give you data, but there's no context."**

Even when fully developed, an AI-enabled digital twin can **widen what a risk team is able to see but it still needs a person to decide what the pattern means.**

*"You don't need to buy a digital twin to start thinking like one. Map how your risks depend on each other today, in the tools you already have, and you'll be ready to plug in the technology as it reaches GRC."*

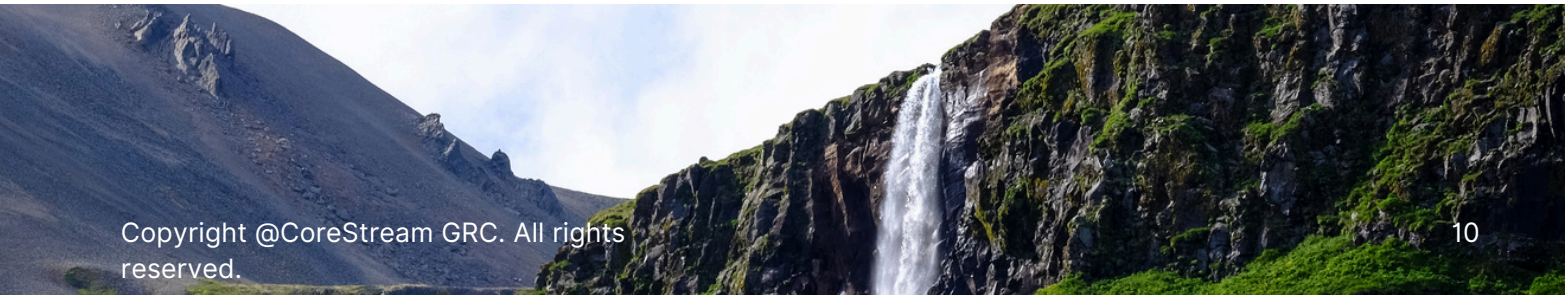
Paul Cadwallader, GRC Strategy Director, CoreStream GRC

# What pre-mortems and digital twins mean for your risk management framework today

Spotting cascading, interconnected risks before they become a major incident doesn't require new software. At root, it requires a change of habit.

The first step is procedural: **run a pre-mortem on the next decision your organization genuinely cannot afford to get wrong**, whether that is a major system migration, a new market entry or a critical supplier relationship. **Assume it has already failed 18 months from now**, and work backwards through the assumptions that let that happen. Klein's original guidance still holds: this works best as a **facilitated group exercise, not a solo thought experiment, precisely because different people surface different vulnerable assumptions.**

The second step is structural, and it is where value-based GRC, CoreStream GRC's own long-standing approach, becomes directly relevant. **Value-based GRC starts from the premise that risk management should be judged not by how many risks it lists, but by how confidently it helps an organization achieve its actual objectives.** Applied here, that means starting to tag the dependencies between existing risk register entries now, however manually, rather than waiting for a digital twin to do it automatically. A risk register that shows how a supplier failure could compound with a reputational story and a regulatory inquiry is already doing something most peers are not. **Good risk mitigation has always started with structure, not with a longer list, and that structure is itself a form of organizational resilience.**



axiom corestream grc

# Conclusion

The organizations caught out by the pandemic-era chip shortage and the 2024 CrowdStrike outage were not short of imagination. Between them they had almost certainly logged a demand-forecasting risk, a single-supplier risk and an IT-outage risk, each in its own line, each scored on its own likelihood and impact. What none of them had done was ask what happens when 2 or 3 of those lines move at once. That is the gap a pre-mortem is built to find, and the gap digital twins are starting to map inside GRC too. Getting ready for that does not mean waiting for the technology to arrive in a GRC platform. It means **starting the discipline now, and building the interconnected view of risk** that value-based GRC, and any genuine business resilience strategy, have argued for all along.

If you would like to explore what that could look like for your organization, CoreStream GRC offers a **one-hour, bespoke workshop with GRC Strategy Director Paul Cadwallader** and your enterprise risk and compliance team, covering **practical risk strategies for connecting your risk data and building towards a more resilient, value-based approach to GRC.**

Book a demo

Book a workshop

Follow us on LinkedIn