Resilience is an investment. Inaction is a liability.

ABOUT THE AUTHOR

Loraine Phillips
is an independent advisor, guiding the board and senior leadership in the industrial sector through risk resilience and strategic transformation. She brings deep international experience in the Energy and Chemical industry, having spent over 30 years at ExxonMobil and more recently 2 years as global COO of a mid-size. Having held a range of roles across different parts of the value chain and corporate functions, she has dealt with real crises and spent time preparing organisations to be ready for what potentially might happen next.

›LORAINE PHILLIPS

Cyber resilience is not an IT challenge. It is a board challenge and accountability issue...and a strategic choice. The cyber risk landscape is moving fast, and not in a good direction. Boards and non-executive directors should ensure there is a validated cyber risk assessment, actively review and debate it, set clear risk appetite, and determine how far to invest in readiness. Done well, this can be a highly valued differentiator. Stakeholders will notice. If the board is only hearing about cyber risk through green dashboards and acronyms, resilience is being outsourced. That rarely ends well.

What's different now

Cyber incidents used to be unfortunate. Now they are inevitable. The only variable is scale – minor or major, how long the organisation is down, how confused leadership becomes, and how quickly regulators, customers and journalists notice. Boards no longer get credit for asking *"Are we secure?"* They are judged on *"How did you perform when it was compromised?"*

The comforting myth

Many boards assume cyber resilience is highly technical, wildly expensive and best left to people with impressive certifications and strong opinions about firewalls. In reality, what costs the most is indecision: executives waiting for clarity that never comes, legal and comms teams debating in parallel, and the board dialling in late to a crisis it doesn't fully understand. Cyber resilience is not about eliminating risk. It is about eliminating panic.

Why doing it differently actually works

Traditional cyber programmes optimise for prevention. Whilst that is part of the baseline, resilient organisations also optimise for readiness to be able to mitigate the impact - ideally better than their competition. They assume something will fail and plan accordingly, much like aircraft designers, emergency services and, frankly, anyone who has ever run a complex system in the real world. Boards that invest in resilience don't just reduce losses; they protect reputation, demonstrate control and avoid the uniquely uncomfortable experience of explaining to customers, employees and indeed investors why no one had practised this scenario before.

So what next?

1. **Decide what must not stop (in terms of processes or operations).** Not everything is critical. Be ruthless.

2. **Clarify who has authority.** If everyone owns the decision, no one will make it.

3. **Rehearse the awkward moments.** Run cyber scenarios that involve legal, comms and operations. Decide which of these elements should include the board.

4. **Measure what matters.** Time to recover beats number of risks logged every time.

5. **Treat resilience like capital discipline (i.e., how you prioritise financial returns).** You would not insure only half a factory. Why insure only half the business?

Bottom line

Resilience is an investment you notice only when you need it. Inaction, on the other hand, has a remarkable talent for making itself visible – usually at the worst possible moment, and potentially as *front page* news.

Boards have a choice: invest calmly in resilience or improvise publicly during a crisis—with a much larger audience!