Systems are locked. A ransomware attack brings business operations to a standstill. Then the crisis takes an unexpected turn: Armed police arrive at the CEO's door.

Elsewhere, an executive receives an urgent call from the CFO with an unusual request. The voice is familiar. The request sounds plausible. But is it really the CFO speaking?

None of these threats are just hypothetical. They reflect the kinds of cyber crisis situations businesses are increasingly preparing for.

Training for Uncertainty

A cyber crisis can unfold in countless ways. Your team can plan to navigate the unexpected together. By **SUNTKA VON HALEN** and **KATARINA REBELLO**

While no organization can know exactly what its next crisis will look like, teams can practice how they will respond when events take an unexpected turn: how they make decisions, share information, draw on different expertise and work through the unknown together.

That is what Brunswick's global Cybersecurity practice has been testing through cyber crisis simulations with senior business and legal leaders around the world. These exercises test not only incident-response plans and processes, but how corporate executives make decisions under pressure and uncertainty.

In Copenhagen this year at the Association of Corporate Counsel's Chief Legal Officer Global Summit, Brunswick put dozens of general counsels in the middle of a live ransomware scenario that escalated from compromised systems into a physical security threat.

Meanwhile, Brunswick's Code Red simulation series with global law firm Linklaters has been exploring how AI is changing the nature of cyber deception and providing participants from global companies with integrated crisis response perspective from Legal, Communications and IT in one workshop. Across sessions in Paris, Frankfurt, Munich and Düsseldorf, participants have faced scenarios in which cybercriminals use deepfakes to impersonate senior executives. In each case, the scenario is only part of what is being tested.

Simulations help corporate leaders answer a harder question: When the unexpected happens, is your organization ready to navigate it together?

BUILDING CRISIS MUSCLE MEMORY

A good simulation allows leaders to practice working under pressure: making decisions with incomplete information, coordinating across business functions and adapting as the nature of a crisis changes.

One of the most important assumptions to challenge during a simulation is that a cyber crisis will remain an IT problem. It rarely does. A cyber incident can quickly transform into an operational, legal or regulatory concern. An online threat can turn into a physical security risk. In the midst of it, employees, customers, regulators, investors and journalists may suddenly all be asking very different questions all at the same time.

That is why the most effective crisis exercises bring different parts of the organization together, deliberately cutting across silos. Senior leaders from the business, legal, communications and IT teams need to confront the same evolving crisis, each with different responsibilities, perspectives and priorities. For multinational organizations, that may also mean testing how teams coordinate across countries and jurisdictions.

The most revealing moments often occur at those intersections. Does the communications team have enough information to explain what is happening? Do local and global teams agree on who will speak with customers? Does the crisis response team really understand what happens to the business if a critical system remains unavailable for an extended period?

> **"The most useful part of a simulation can be what surprises you as a team and how you manage it. It may be a dependency you had not considered, a decision that takes longer than expected, or a question nobody is immediately able to answer. Those moments show you where there is more work to do."**
> **Daniel Foelting,** Carglass

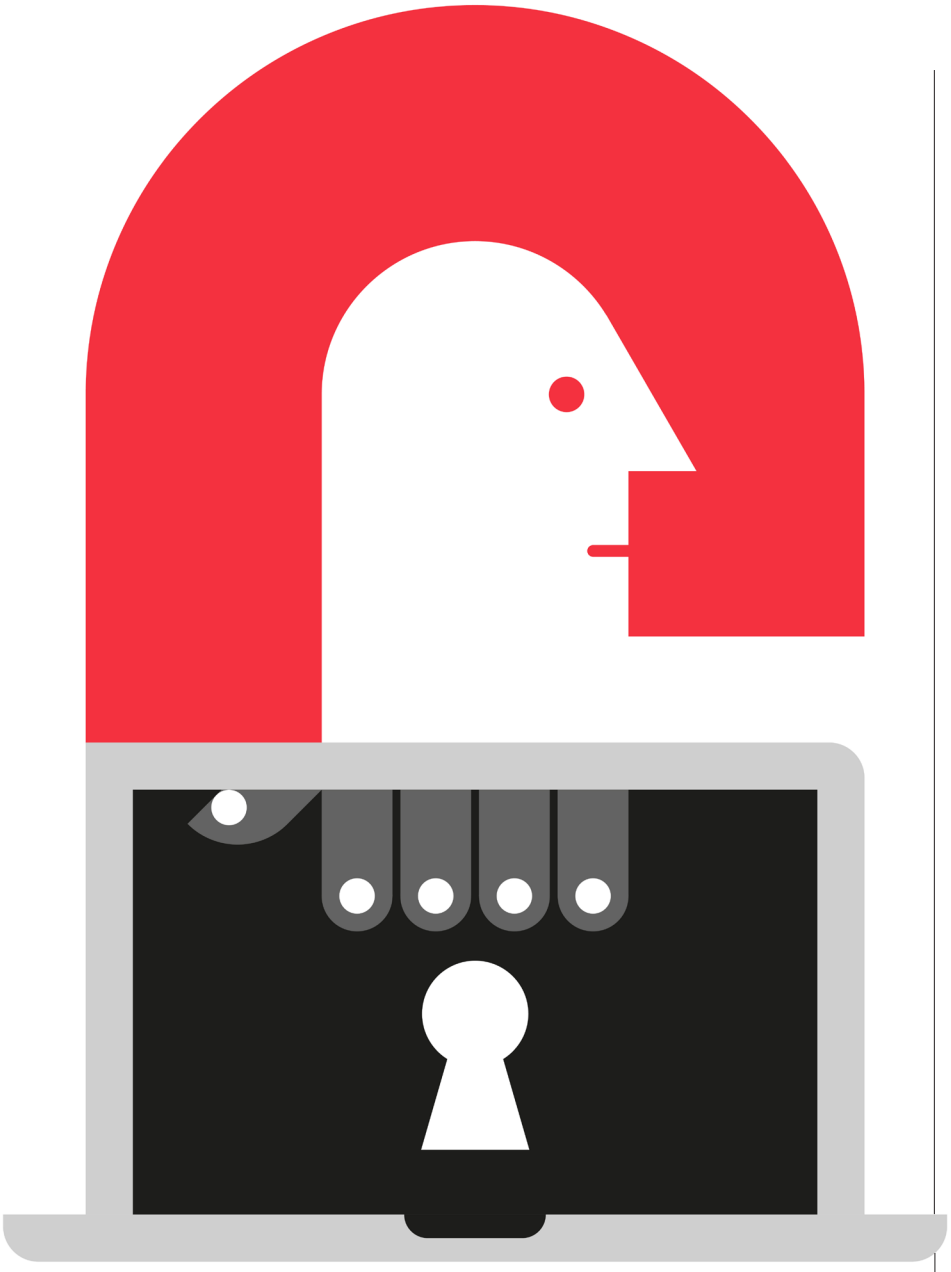


ILLUSTRATION: PETER GRUNDY

TESTING THE RISKS THAT MATTER

The strongest simulations also start with the organization itself, its operations, sector, technology, stakeholders and vulnerabilities. They consider not only which risks appear most likely, but how severe their consequences could become and how one risk might trigger another.

The purpose is not to construct the most spectacular disaster imaginable. It is to identify the assumptions an organization is relying on and then put them under pressure.

A ransomware attack, for example, is not only about restoring affected systems. What happens if critical operations stop for weeks and it affects the entire supply chain? Or if a sensitive data breach puts people's safety and wellbeing at risk?

SUNTKA VON HALEN is a Partner in Brunswick's Munich office and co-lead of Cybersecurity.
KATARINA REBELLO is a Director in Brunswick's Paris office, and a member of the firm's global Cybersecurity team.

"In a real cyber crisis, you are unlikely to have all the information you need. You have to understand what you know, what you don't know and what cannot wait. Simulations are valuable because they are an opportunity to make those decisions together under pressure."

Brunswick client, global professional services firm

PREPARING PEOPLE, NOT JUST PLANS

In these situations, another critical variable needs examination: the participants around the table. Exercises need people who understand the relevant processes. But they also need the people who will be expected to lead when events become ambiguous and fast-moving.

There can be value in asking participants to see the crisis through somebody else's eyes. What does an employee need to know? A regulator? A customer? An investor?

"A general counsel may look at a decision and immediately see the legal or regulatory risk. A communications advisor or a forensic expert may see a different risk. Bringing those perspectives together is important because the right response to a cyber crisis is rarely about managing one risk in isolation."

Sonia Cissé, Partner, Linklaters

No organization can write a playbook for every combination of cyber, operational, physical, reputational, legal and regulatory risk. Nor can a simulation predict exactly what its next crisis will look like. But prediction is not the measure of a successful exercise. The real test is what it reveals: unclear responsibilities, hidden dependencies, untested assumptions, gaps between teams or decisions for which ownership is not clear.

Finding those gaps is a critical part of the value. It gives organizations the opportunity to strengthen their plans and processes, and leaders the confidence to apply them.

You cannot foresee every crisis. But you can practice being ready. ◆