Crisis management in the age of disruption

Rethink risk.

Decisions that minimise impact
and maximise value.
Together, we can rethink risk.

pwc

Introduction

As described in PwC's ADAPT framework, the world is facing significant and increasingly urgent global challenges affecting individuals, organisations, governments and society. This age of disruption brings new complexities, opportunities, and risks for businesses. The potential for crises has intensified – driven by rapid technological change and amplified by societal expectations around social responsibility linked to environment, social and Environmental, Societal and Governance (ESG) criteria.

Over the course of the COVID-19 response we've seen how these trends have accelerated. And now, as businesses start to look beyond the pandemic and into recovery, our global findings show they have no intention of resting on their laurels. Our 2021 Global Crisis Survey has revealed that seven out of 10 organisations are planning to boost their investment in resilience and an overwhelming 95% of business leaders report that their crisis management capabilities need improvement.

Building on these insights we've outlined the ten considerations to prompt a crucial and timely discussion: why organisational leaders and crisis managers must adjust their approach for this new era.

> The World Economic Forum identified the growing interdependence of digital technologies and systems as a likely source of instability and disruption.
>
> **WEF Global Risks Report 2019**

The context: drivers of disruption

The age of disruption is upon us – we point to three main drivers which set the context for the 10 considerations below. They include systemic interdependency and concentration risk, velocity and declining trust.

1. Systemic interdependency and concentration risk

Many organisations are more entangled than they realise in far reaching, deeply embedded value chains – from interconnected in-house systems to data feeds between cloud mega-providers. Data and technology underpin operating models, drive decision making, and propel value creation – a trend that has only been accelerated by COVID-19 as many organisations switched to remote working.

On the surface, this is a smart strategy: leveraging the core competencies of well-matched counterparts in order to compete in an agile, accelerated fashion. But there is a downside: the inherent risk of systemic interdependencies. If your organisation relies on processes being performed by another organisation and something far beyond your control disrupts their business, such as a pandemic, then your resilience and continuity will be challenged.

This vulnerability is amplified when you consider the concentration risk: the scale and power of a relatively small number of tech giants upon whom such offerings depend.

This web of dependencies has created a situation where the origins and possible impacts of disruption are harder to predict – the entire system is becoming increasingly complex.

All of this means you may not know where the weakest points in your system are, and this knowledge gap translates into vulnerabilities that will be exposed when it matters most: in times of crisis.

2. Velocity

Whilst the outward face of the organisation may rightly be harnessing the pace of change and innovation, inwardly you must work harder to protect your organisation from the velocity of these emergent and unpredictable digital risks. The investment required to fully understand the consequences of a catastrophic failure of technologies and third parties remains significant.

3. Declining trust

It's hardly controversial to point out that society's expectations have changed dramatically. The erosion of trust is evident everywhere. According to the 2021 Edelman Trust Barometer there is an epidemic of misinformation and widespread mistrust of societal institutions and leaders around the world. COVID-19 has also accelerated this trend.

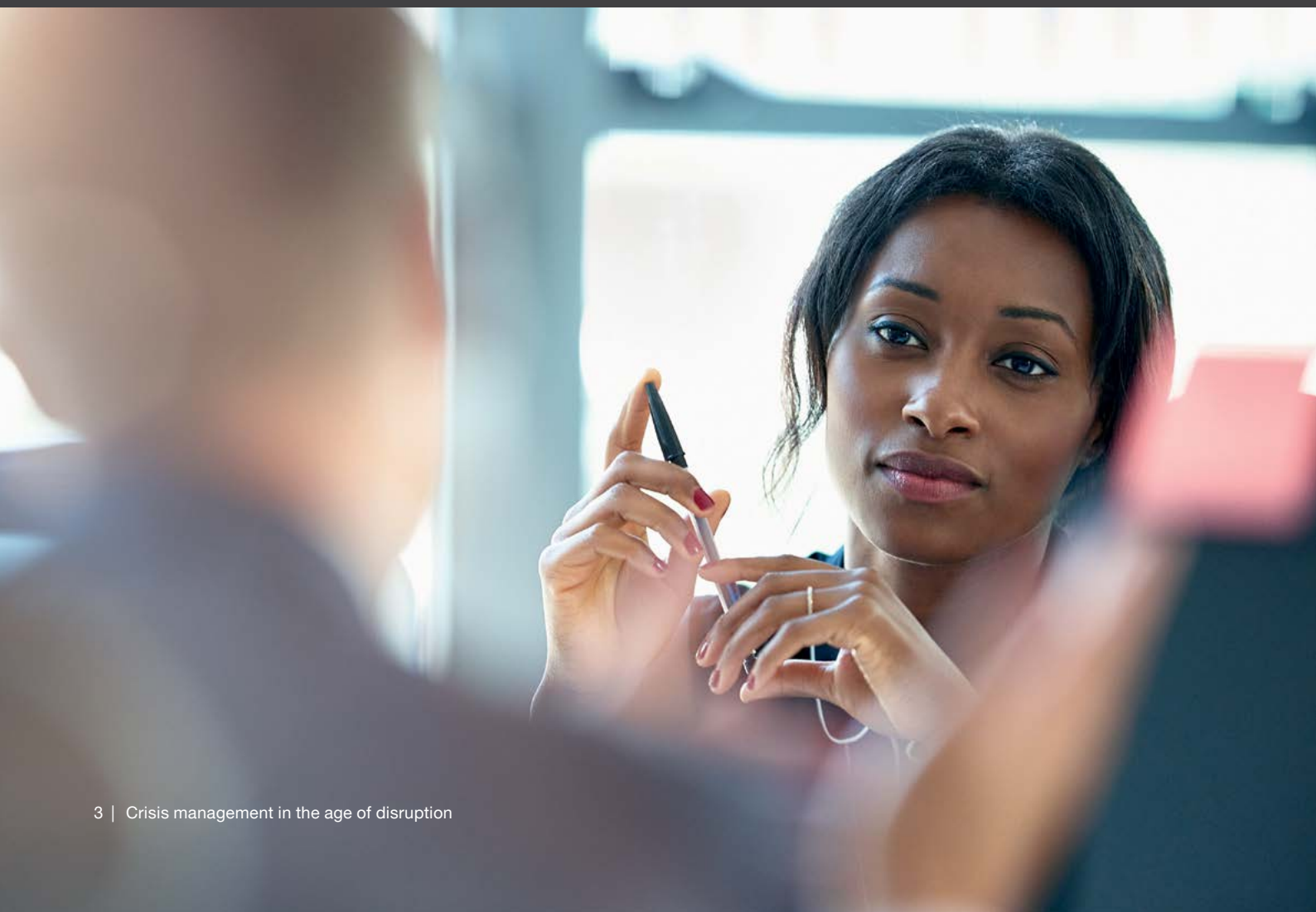
Shareholders, the media, employees and the wider community are increasingly emboldened to voice their views through their words (vastly amplified on social media), their money, and their feet.

Stakeholders expect that if you're introducing a new technology or service – e.g. building an algorithm for a driverless car, or a new medical device, or a surveillance technology – that you'll do so with baseline ethical and environmental considerations baked in. And you'll need to understand how those considerations vary from stakeholder to stakeholder, market to market, and country to country.

Additionally the growing scrutiny around ESG performance is set to accelerate in the face of activism and regulatory pressure; for example, around inequality and environmentalism. Value creation is increasingly about linking your business to societal impact, not just the financial bottom line. Organisations are working to understand ESG, what it means for their strategy and growth and how this will affect trust in their brand.

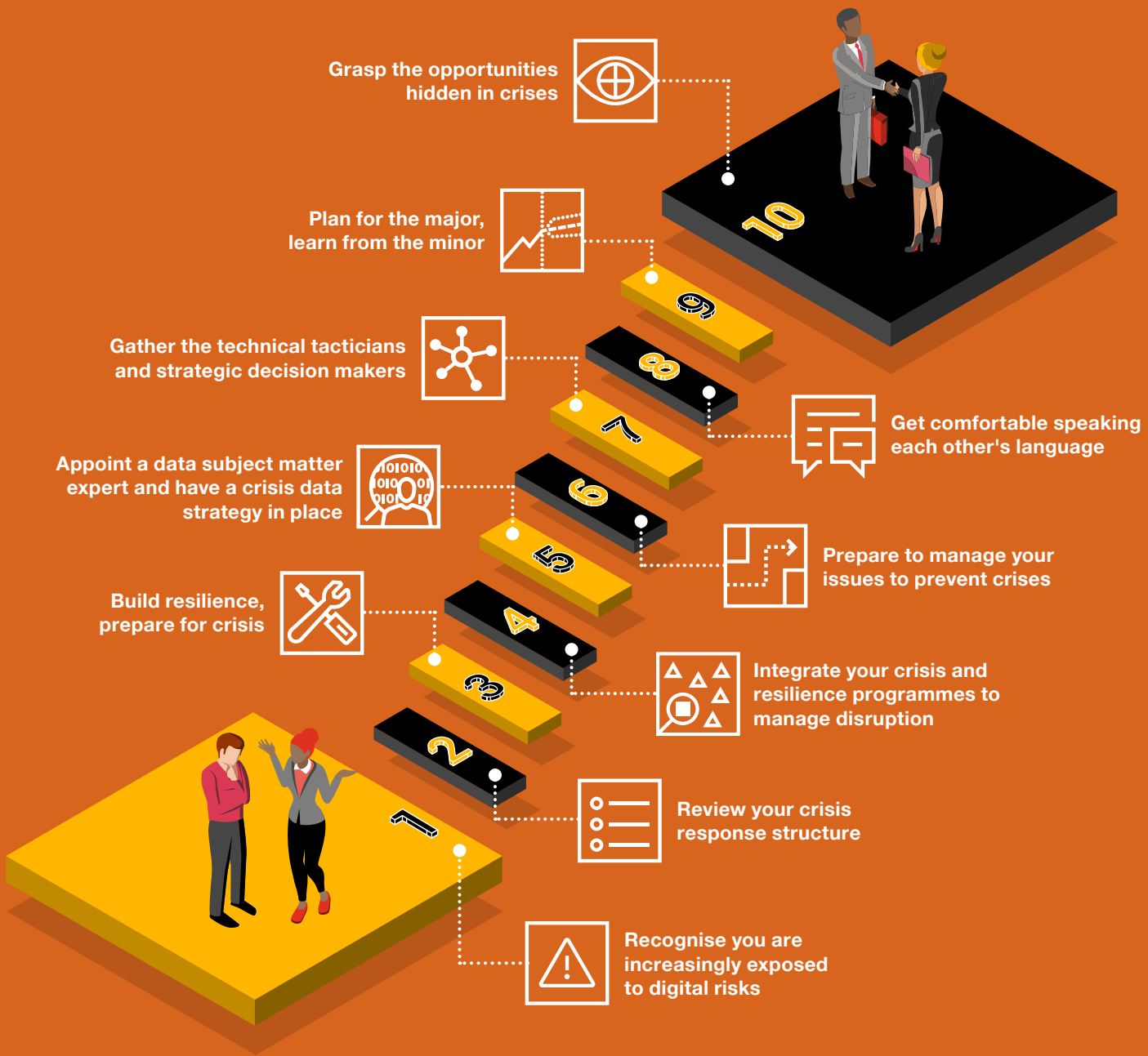
If you are responsible for your organisation's crisis readiness, the trust spotlight will shine on you at the most unsettling time. Your board, your people, your customers, your regulators – all will require the confidence that you are prepared for a crisis; and that you are factual, transparent and stay true to your values in your response.

Today, role model organisations want and are expected to think, behave and operate in a way that is honest, respected and ethical as well as commercial, resilient and profitable – attributes that mean they are doing 'good business' both in commercial and an ethical sense.



Ten considerations

Against this context, we suggest 10 considerations to enhance crisis preparedness in this age of disruption.



1. Recognise you are increasingly exposed to digital risks

COVID-19 has accelerated the adoption of technology and digital transformation as a priority. Given most organisations are becoming tech or data-centric companies, you could face a crisis triggered by any number of new digital risks: introduction of new software, necessary IT upgrades or a cyber event such as a ransomware attack. As a data-centric organisation, your governance obligations increase with changes to regulation and evolving societal expectations. Consider your new digital risk environment, and inform your crisis planning through that lens.

2. Build resilience, prepare for crises

All organisations need to prepare for disruption. It might be incident-led (i.e. a short, sharp event) or issues-led (i.e. slow burning), but any disruption will have impacts on an organisation. The ability to navigate such disruption successfully depends on:

- **Resilience:** having robust plans and capabilities in place to ensure that organisations can withstand, absorb or recover from any disruption to ensure it does not cause intolerable impacts; and plans to support continuity and recovery when prevention is not possible or fails
- **Crisis preparedness:** where the resilience arrangements are inadequate, fail or are overwhelmed (typically due to the scale or nature of the disruption), being able to deliver the organisation's strategic aims and return to a viable operating state.

Critically, organisations need to start preparing for disruption now, so that the gaps can be identified and closed with care, preparation, and practice. Despite weathering a global crisis, there is now an opportunity to embed learnings and focus on preparing your organisation for the other high-impact events identified through your risk planning.

3. Integrate your crisis and resilience programmes to manage disruption

Review your systems, stakeholders, and current crisis framework – not an easy task, considering today's typically sprawling technology estates, business partners and third parties. Are there hidden dependencies or gaps that could cripple a cohesive response? What if your crisis was downstream of a larger service provider issue? If a high speed, high impact event were to hit you tomorrow, would your organisation be operationally resilient? How confident are you in your organisation's ability to weather sustained disruption – and emerge stronger?

Organisations that are prioritising enhancements to resilience, are focusing on integrating business continuity, crisis management and disaster recovery. Business leaders recognise that these areas should not be considered in isolation, but rather as interlinked disciplines that enable organisations to successfully navigate disruption.

As a data-centric organisation, your governance obligations increase with changes to regulation and evolving societal expectations.

> Organisations would benefit from recognising that issues should not be managed as business as usual; if left unmanaged they can be escalated into a crisis by a trigger (eg a whistleblower). Treat issues with the same degree of seriousness as an incident-driven crisis, such as a cyber attack.

4. Prepare to manage your issues to prevent crises

As well as preparing your organisation to respond to an incident driven crisis, such as a ransomware attack, recognise that your crises may come from issues, a non-acute threat to an organisation's strategic goals.

Organisations would benefit from recognising that issues should not be managed as business as usual; if left unmanaged they can be triggered by an external event (eg a whistleblower) and escalate into a crisis.

Treat issues with the same degree of seriousness as an incident-driven crisis, such as a weather event. Review your organisation's capability to identify and manage issues. An issues management capability does not need to be complex and should be simple to drive effective and swift decision-making to gain control – manage an issue with a clear structure, procedures and agreed pathways for escalation – before they can threaten the strategic objectives of your organisation.

5. Review your crisis response structure

Well established three-tiered crisis response structures, such as gold-silver-bronze or strategic-operational-tactical, have their place. However, it's important to recognise that today's risk landscape requires crisis managers to evolve their preparedness strategies.

The three tiered structure may not be agile enough for an effective organisational response to technology-driven crises or indeed be appropriate for increasingly lean and agile organisational structures. The response to high impact events, driven by global technologies, cannot rely on escalation through multiple layers of teams that may have a limited understanding of their remits. Tactical actions in these scenarios generate strategic challenges, such as technical decisions taken during a cyber attack that limit strategic response options. Far too often decision making is postponed or delegated because of a lack of technical understanding at the strategic level.

To enable swift decision-making when responding to technology or digital-driven crises, consider establishing a structure aligned to impact categories, with clear accountable owners, rather than a three tiered response.

> For many organisations, one of the most significant challenges during COVID-19 was difficulty gathering data to inform and support their response – specifically their decision-making and communication to stakeholders.

6. Gather the technical tacticians and strategic decision makers

When it comes to crises, specifically those with technology impacts, less can be more. Isolate a small group of designated people who have the knowledge, the ability to triage the event, and the authority to make decisions quickly. Typically, this will require close cooperation between technologists – who have the information upon which the decisions can be made – and key senior members of the organisation, who have the power to make those decisions.

7. Appoint a data subject matter expert and have a crisis data strategy in place

For many organisations, one of the most significant challenges during COVID-19 was difficulty gathering data to inform and support their response – specifically their decision-making and communication to stakeholders. In a crisis, managers must make crucial decisions quickly – and those decisions will hinge on the availability, accuracy and comprehensiveness of information. Ensure you have a crisis-specific data strategy. It should enable you to quickly access large volumes of structured, validated data, at pace, and have a plan for how to visualise that data to inform swift decision-making in a crisis.

8. Get comfortable speaking each other's language

If there are blind spots, silos, or stress fractures between your operational groups and leadership, you can be certain that a crisis will expose them at the worst possible time. Avoid breakdowns in communication: get organisational leaders closer to the technology on which the organisation depends, whilst cultivating 'boardroom-savvy' technologists. This also holds for relationships with third parties and newly acquired organisations. Practising and stress testing brings teams together to learn each other's language and build muscle memory.

9. Plan for the major, learn from the minor

In 'peacetime', gather your impact owners and explore your top five risks as a team. Plan for high impact scenarios, extensive disruption, and long recovery timeframes. Develop playbooks and decision guides to prepare your senior management team. And be sure to treat minor incidents as warning signs that can help you identify patterns and deepen your understanding of the risks you face. Use tools such as exercising and wargaming to explore your strategy and decision-making against your top five risks.

10. Grasp the opportunities hidden in crises

Understand that in the age of disruption, 'business as usual' actually means falling behind. Even before the crisis has been resolved, the disruptive energy at its heart can be harnessed to strategic advantage. Visualise – and prioritise – emerging as a more agile, better tech-enabled organisation, but also foster the team bonds that will have formed.

> "Understand that in the age of disruption, 'business as usual' actually means falling behind.

Contact us

Bobbie Ramsden-Knowles
Director
Crisis and Resilience
M: +44 (0)7483 422701
E: roberta.ramsden-knowles@pwc.com

Johanna Peterson
Manager
Crisis and Resilience
M: +44 (0)7483 416849
E: johanna.peterson@pwc.com

Melanie Butler
Partner
Global Crisis Centre Lead
M: +44 (0)7801 216737
E: melanie.butler@pwc.com

The PwC Crisis Practice helps organisations prepare for, respond to and emerge stronger from disruption. We support organisations throughout their journey to crisis readiness and through any issues or crisis they may face, with a specialism in cyber crisis and ESG issues management.

The PwC ESG practice delivers value to clients by using our skills and experience to help them do 'good business' as a result of actively and proactively understanding, identifying and managing ESG-related risks. This, in turn, enables them to embrace ESG, doing the right thing more broadly and realising benefits in the form of value creation and enhanced trust.

pwc.co.uk

Mitie Design RITM4436940 (04/21).