CRISIS COMMUNICATIONS NETWORK

CRISIS COMMUNICATION FOR BOARDS

A Handbook for Good Governance

Published in association with IoD

TABLE OF CONTENTS

HOW TO USE THIS HANDBOOK

The handbook can be read from start to finish as a complete guide to crisis communication for boards. The handbook provides the main narrative but throughout the text, you will see coloured "Click Here" boxes marked with a hand icon. These interactive links will take you directly to a related case study, special feature or toolkit item that expands on the topic being discussed. Once you have reviewed the supplementary material, simply use the return link to navigate back to the relevant section of the handbook and continue reading.

The case studies illustrate key principles through real-world examples, the special features provide additional expert perspectives on important themes, and the toolkit offers practical resources, templates and checklists. Together, this supplementary material is designed to complement the handbook, allowing readers either to follow the main narrative uninterrupted or to explore topics in greater depth as they progress.

HANDBOOK 05

Preface by the Chartered Institute of Public Relations 06

Preface by the Institute of Directors 08

Introduction and Overview 10

Understanding Crisis 13

The Five Phases of Crisis 16

Predict 18

Protect 25

Prepare 32

Respond 38

Recover 44

Beyond Recovery: Building Enduring Resilience 47

Acknowledgements 50

Resources 57

CASE STUDIES 59

The Deepwater Horizon Oil Well Explosion and its Consequences for BP in the Gulf of Mexico by Dr Jon White 60

The Impact and Consequences of Misidentifying Risk by Katherine Sykes 62

Jaguar Land Rover: Crisis Communication Take-Aways from the UK's Most Economically Damaging Cyber-Attack to Date by Chris Tucker 64

Post Office Horizon: When Brand Protection Silences Critical Stakeholders by Stephen Waddington 66

A Study of Character vs Capability: The Kisscam Viral Video by Chris Tucker 68

Grenfell: An Industry Changed by Dan Gerrella 69

Crisis Preparedness at Heathrow by Sara Naylor 71

The 2024 Valencia Floods by Chris Tucker 72

Storm Kristin by Philippe Borremans 73

SPECIAL FEATURES 74

The Importance of Horizon Scanning as Part of Risk Mitigation and Management by Farzana Baduel 75

Cybersecurity Risk: Board Oversight and the Role of Strategic Communication by Chris Tucker 77

AI and Governance: Crisis Communication in the Age of Algorithmic Decision Making by Philippe Borremans 79

AI and Reputation by Ben Verinder 81

Mis/Disinformation by Shayoni Lynn 84

Strategic Communications: Protecting Reputation in a Crisis by Stephen Waddington 86

The Interplay Between Reputation and Relationships by Dr W. Timothy Coombs 90

The Importance of Organisational Culture in Preventing and Responding to Crises by Alison Arnot 92

Ignore DEI at Your Peril: How Inclusive Cultures are an Organisational Risk Mitigation Strategy by Avril Lee 94

What Publics Talk About When They Talk About Corporate Reputation: A Framework for Boards by Dr Craig E. Carroll 96

Issue or Crisis? How They Differ and Why it Matters by Dr Tony Jaques 98

After the Crisis: Boards, Recovery, and Public Inquiries by Amanda Coleman 100

True Crisis Preparedness and Resilience by Rick Cudworth and Swaraj Parameswaran 102

TOOLKIT ... 105
Reputation Risk: Board Checklist ... 106
AI Failure Modes ... 107
AI Governance: Board Checklist ... 108
What Boards Should Look for in the Ideal Strategic Communications Professional: Board Checklist ... 110
Strategic Communications: Board Checklist ... 112
Stakeholder Map and Risk Register for a Mining Company ... 113
Sample First Response/Holding Statements ... 116
Questions Boards Should Ask Management in a Crisis ... 120
Drafting a Crisis Communication Plan ... 122
Trusted Clarity Model: AI Governance Framework ... 123
Good Crisis Communication: Board Checklist ... 124
Recover: Board Checklist ... 125

HANDBOOK

Crisis Communication for Boards

PREFACE BY THE CHARTERED INSTITUTE OF PUBLIC RELATIONS

For every board, each passing month brings new threats and challenges to the risk landscape. As we map this new world in finer detail, we find there are undiscovered lands that we must label 'here be monsters'. A handbook like this is an essential navigational aid for every board that must steer past them, keeping its crew and cargo safe. Some of the risks we see are large and urgent, sudden supply chain shocks, for example; while others seem less immediately threatening, such as declining employee engagement or failure to innovate. What they have in common is that they can all cause serious damage to an organisation if its board is not managing them actively.

Communications professionals are uniquely well-placed to support boards in these challenging times, particularly with some of the more diffuse or interconnected risks. They are acutely alert to any gaps between what an organisation says in public and how it actually goes about its business. They know that this gap, perhaps above all, is the failing that publics and stakeholders find most difficult to forgive. They know that you cannot communicate your way out of a crisis that you behaved your way into. They understand how to ensure that your behaviour matches your words.

If you wait for a crisis to hit before you invoke your communications plans, you are already losing. Crisis communications is primarily a preparedness discipline that helps you anticipate and mitigate crises before helping you out of them as smoothly as possible. This handbook distils the experience of leading professionals who have supported many organisations through all kinds of crisis. I encourage you and your board colleagues to make good use of it while many of your risks are still distant prospects on your horizon.

Alastair McCapra
Chief Executive, Chartered Institute of Public Relations (CIPR)

The CIPR's Crisis Communications Network exists to drive best practice and promote excellence in crisis communications, boasting more than 1,100 members in over 40 countries, supported by more than 4,800 LinkedIn followers. Our events consistently rank as the top three most attended across all CIPR groups. We have already published two well-received best-practice guides, and this board-focused handbook is our most ambitious publication to date.

In the broader landscape of corporate governance, reputational risk and the management of resulting crises has taken on new urgency. What was once viewed as a consequence of operational or financial failure is now understood as a strategic risk, one that impacts valuation, access to capital, regulatory scrutiny and executive tenure. Increasingly, reputation appears explicitly on risk registers and board agendas.

To manage reputational risk and to respond to crises effectively, the boardroom and the communications function must be aligned. This handbook is intended to contribute to this alignment and to be useful to a wide range of board members from directors of FTSE companies and public organisations to trustees of charities.

Chris Tucker
Co-Chair, CIPR Crisis Communications Network

PREFACE BY THE INSTITUTE OF DIRECTORS

In an environment defined by volatility, uncertainty and heightened scrutiny, boards are increasingly required to lead through complex and fast-moving crises. The nature of risk has evolved: reputational threats can emerge quickly, escalate rapidly and have far-reaching consequences for organisational value, trust and long-term viability. In such conditions, effective crisis communication is not a peripheral concern – it is central to good governance.

This handbook therefore comes at a timely moment. As organisations operate within a landscape shaped by geopolitical instability, technological disruption and rising stakeholder expectations, the ability to respond clearly, credibly and with purpose has never been more important. Boards are expected not only to anticipate and mitigate risk, but to demonstrate leadership when events unfold, often under intense public and regulatory scrutiny.

Communication plays a critical role in this. It shapes how organisations are understood, how decisions are interpreted and ultimately whether trust is maintained or lost. When managed well, it can stabilise a situation and support recovery. When overlooked or delayed, it can amplify risk and compound harm.

At the Institute of Directors, we see first-hand the pressures directors face in navigating this demanding landscape. Good governance is not only about structures and compliance, but about judgement, accountability and the ability to act decisively under pressure.

We are pleased to support the CIPR's work in this area and commend it to directors across all sectors. Whether in listed companies, public bodies, family firms or charities, the principles set out here apply wherever trust, accountability and resilience matter.

In an era of overlapping crises and permanent visibility, the question is no longer whether an organisation will face a crisis, but how well prepared its board is to lead through it. This handbook provides an important foundation for that leadership.

Jonathan Geldart
Director General, Institute of Directors (IoD)

Reputation is one of the most valuable and fragile assets of any organisation. It can take decades to build and moments to lose. Yet when crisis strikes, too many boards find themselves without the right counsel and support at the table, or worse, resistant to the counsel that is there.

This handbook raises awareness of themes that at times we haven't paid enough attention to. The relationship between boards and communications professionals is too often defined by misunderstanding what PR and crisis communications specialists actually do, the strategic value they bring and what is genuinely at stake when that expertise isn't brought in.

The pages that follow highlight that crisis communication is not a reactive function to be called upon when things go wrong but a strategic discipline to be embedded in board thinking long before any crisis hits. The communicator brought in during a crisis to 'fix' the narrative is already working at a disadvantage. The one who has worked alongside the board, understands its priorities and culture, and has built the trust of its members – that is the adviser who can make a real difference.

What stands out for us in this handbook is its honesty about the responsibilities on both sides. Boards are challenged to examine their assumptions on the value communications professionals can add, the importance of outside perspectives and the risks of keeping issues too close.

Communications professionals are equally challenged to step forward with greater confidence, demonstrating business acumen, and earning their place as trusted strategic advisers rather than waiting to be invited in.

The landscape has changed dramatically. Geopolitical instability, cyber threats, social media and AI have raised the stakes of every crisis. What is needed now is genuine collaboration: a board that is open to expert counsel, and communicators who are ready to offer it with authority.

As a group that represents the industry, at IoD we are happy to give this report our endorsement. The question it poses is simple but urgent: when crisis comes, will you have the right people, with the right access, already at the table?

Trudy Lewis and Jeremy Duncan
Leaders of the IoD Marketing Communications Special Interest Group

INTRODUCTION AND OVERVIEW

INTRODUCTION AND OVERVIEW

We live in a world of global instability, insecurity and complex interdependency, facing escalating, interconnected threats. Poly and perma-crisis now define a complex, volatile and uncertain global disorder in which crises no longer arrive as isolated events, but as fast-moving, highly visible shocks that can escalate within hours. At any given time, a potential crisis is only just around the corner.

For boards, the question is no longer whether a crisis will occur, but how quickly it will escalate – and whether the organisation is prepared to respond.

Effective risk management has never been so important for boards and senior management teams. They are expected to identify problems that may be brewing within their organisations, anticipate external events that could cause damage and act on that knowledge quickly, decisively and with confidence. In this environment, the pace of risk has accelerated, while the margin for error has narrowed.

The buck stops with the board. This is not an abstract accountability – it is tested in the moments when events move faster than established processes and judgement must prevail. Boards are responsible for safeguarding their organisations' governance and viability: managing an increasing regulatory burden, overseeing risk and preparing for crises through a proactive governance framework that integrates compliance, strategic planning and crisis preparedness. Their role is one of oversight – setting the tone at the top and ensuring that management has the right strategies, structures and resources to respond effectively.

Boards are responsible for their organisation's strategy and articulation of purpose – and ultimately responsible for its reputation. ESG (Environmental, Social and Governance) has elevated the importance of reputation management, bringing it firmly to the heart of business strategy. Increasingly, organisations must view strategy through the lens of reputation, aligning decisions with the needs, expectations and demands of their stakeholders.

It is a complex and demanding brief, requiring careful judgement and sustained attention.

To identify, analyse, assess and challenge risks in today's environment, boards must actively and rigorously oversee organisational risk. Yet industry studies[1, 2, 3, 4, 5] consistently point to shortcomings in organisational resilience and crisis preparedness. Findings from the Business Continuity Institute, Deloitte, the World Economic Forum, International SOS and Aon indicate that many organisations continue to exhibit gaps in crisis management capability, uneven resilience maturity and limited preparedness for emerging and disruptive risks. Collectively, this research suggests that while awareness of strategic, operational and geopolitical threats has increased, many organisations remain underprepared to manage their potential impact effectively.

This gap between expectation and preparedness is increasingly exposed. It reinforces the need for stronger governance, deeper scenario planning and more robust crisis leadership across sectors.

[1] World Economic Forum (2025). *Global Risks Report* https://www.weforum.org/publications/global-risks-report-2025/
[2] Deloitte (2026). *Board Practices Quarterly: Crisis Management and the Board* https://www.deloitte.com/us/en/programs/center-for-board-effectiveness/articles/crisis-management-and-the-board.html
[3] International SOS (2025). *Risk Outlook* https://www.internationalsos.com/newsroom/press-announcements/risk-outlook-2026
[4] Business Continuity Institute (2025). *BCI Horizon Scan Report* https://www.thebci.org/news/complex-and-interconnected-risk-the-bci-horizon-scan-2025.html
[5] Aon (2025). *Global Risk Management Survey* https://www.aon.com/en/insights/reports/global-risk-management-survey

Crises can arise suddenly or emerge from layers of mistakes, failures and omissions. In a world that is increasingly disruptive, interconnected and dominated by 24-hour news cycles, unceasing social media and constant stakeholder scrutiny, risks can escalate into crises more quickly than ever before – often before organisations have fully understood what is happening.

A breaking crisis is often the most significant challenge of any director's or non-executive director's working life. It unfolds under intense scrutiny, with incomplete or conflicting information, and under severe time pressure. Decisions taken in the early stages can shape not only the organisation's immediate response, but also its long-term reputation and viability.

Consequently, crisis management must start long before a crisis hits. It should be owned by the board as an integral part of an organisation's wider resilience planning. Good governance requires boards to manage risk and act positively to avoid crisis, rather than react to it after the event. Boards must understand the role they will play well in advance; know how, why and when their organisations move into crisis mode, and be confident that the response will be effective.

A mismanaged crisis can have a profound impact on an organisation's value, its reputation and its ability to operate.[6] The inverse is also true. Adopting the right approach, attitude and mindset will not only reduce the likelihood and impact of crisis, but also establish the systems, processes and behaviours that underpin resilience.

Communication is the golden thread that runs through everything. It is the underlying bedrock of all crisis management – shaping how events are understood, how decisions are interpreted, and whether trust is maintained or lost. In practice, it is through communication that organisations demonstrate control, accountability and leadership in the eyes of those who matter most.

Yet too few boards include professional communicators at the table, and too often rely on external advice after a problem has already arisen. Communications professionals provide a vital external lens, enabling organisations to recognise when risks are emerging and to challenge assumptions about how actions will be perceived. They play a critical role in protecting organisational value – safeguarding reputation, strengthening stakeholder relationships, scanning for emerging risks and supporting prevention, response and recovery.

Consequently, boards are increasingly recognising the value of embedding executive and non-executive directors with communications experience. In a geo-critical and highly scrutinised environment, they are essential allies in effective crisis leadership.

This handbook is designed to be a practical resource for board members. It begins by defining what constitutes a crisis and examining its potential impact. It then moves through the phases of crisis – from prediction and protection to preparedness to response and recovery – outlining best practice communication at each stage. It is supported by a toolkit, alongside special features and case studies from leading academics and practitioners from around the world, providing deeper insight into the issues explored.

In a world of permanent visibility and accelerating risk, preparedness is no longer optional. It is a defining requirement of effective governance – and, increasingly, the standard by which boards themselves are judged.

Katherine Sykes
Founder and Co-Chair, CIPR Crisis Communications Network; Lead Author and Editor-in-Chief

[6] Marsh (2018) *To Survive or Thrive: How Crises Impact Company Value*

UNDERSTANDING CRISIS

UNDERSTANDING CRISIS

What is a crisis?

ISO 22361 is the International Standard for crisis management[7] which defines crisis as an "*abnormal and unstable situation that threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity*". It sets out seven principles which cover governance, strategy, risk management, decision-making, communication, ethics and learning. It recommends that organisations deeply embed these principles into their policies, frameworks, plans, procedures, training, behaviours and people.

A crisis involves high levels of uncertainty and complexity, disrupts core functions, threatens strategic objectives, severely affects reputation and may even affect an organisation's survival. It demands an immediate, strategic response from senior leadership to prevent severe long-term damage, making it distinct from everyday disruptions. It is not part of business as usual and may require a whole of organisation response.

No matter what the origin of a crisis, any organisational response requires strategic decision making by top management, including the board. Often these decisions need to be made in an extreme, high-pressure environment with incomplete or conflicting information. Sometimes decisions must be made that result in imperfect outcomes where the least bad option is as good as it gets.

Being 'crisis prepared' involves building crisis management capability, which involves building the right leadership and structures. It requires organisations to think about and respond to existential threats in a manner that aligns with their core values and strategic objectives.

Defining the crisis

Whether an organisation is facing a crisis or not is a question for each organisation to interpret and decide for itself. However, it is important to stand back and be objective. If the issue could have a disastrous effect on the business, pose a fundamental threat to its strategic objectives or its people, or damage its reputation or profits, then it is likely to be a crisis.

The impact and cost of crisis

Experienced risk and crisis communication practitioners find that boards and senior leadership teams may liken crisis preparedness to a costly insurance policy they may never need.

However, the business impact of an unpredictable and multi-faceted reputational crisis can be so significant that it makes a strong investment case, particularly when the empirical evidence is assessed.

For example, Echo Research's UK Reputation Valuation Report (2025)[8] says corporate reputation accounts for 29% of the FTSE 350's market value, amounting to £730 billion and with an £11 billion year-on-year increase. In the US, reputation accounts for $13.8 trillion of shareholder value across the S&P 500: equivalent to 26% of total market capitalisation.

[7] The International Organization for Standardization https://www.iso.org/standard/50267.html
[8] https://www.echoresearch.com/news-events/new-uk-reputation-valuation-report-2025/

The top UK value drivers are long-term value potential (£118 billion), product and service quality (£109 billion) and financial soundness and management credibility (both at £75 billion). And yet, according to the report, while 95% of UK-listed companies are gaining value from reputation, 5% are experiencing value erosion.

Australian consultancy SenateSHJ has created a searchable dataset 'Crisis Index 300'[9] which provides the world's first comprehensive analysis of the financial impacts of over 300 listed company crises from around the world over the past 44 years and reinforces the financial and organisational impact of crises specifically.

Capturing data from 27 stock exchanges, across 32 industry sectors and eight crisis categories, it allows users to explore the corporate and financial ramification of specific crises on share price, earnings per share (EPS), how long share price/EPS took to recover to pre-crisis levels (if it did) and whether the CEO left or stayed. Across the full multi-year dataset, the aggregate data which emerged found:

- An average share price drop of 35.2%.
- An average EPS fall of 68.3%.
- 425 days for the share price to return to pre-crisis levels, on average.
- 121 companies have never – or not yet – recovered.
- Telecoms and Energy saw the highest average impact on share price.
- Banking, Financial Services and Insurance show the slowest recovery time.
- Mismanagement and White-Collar Crime hit share prices hardest.
- Cybercrime had the lowest share price impact.

The evidence reveals a need to look beyond business continuity with its focus on easily quantified risks common to operational matters. Organisations must assess their cultural and behavioural vulnerabilities, which SenateSHJ research shows can be damaging in the long term.[10]

Systematic, collaborative risk readiness and crisis preparedness, properly embedded in organisational culture, are therefore a source of huge, tangible and material value.

To underline that point, seminal research from 1996[11] found that *"companies judged to have responded 'inadequately' to major emergencies lost an average of 15% of their net stock value in the following months". By contrast, "those which managed an 'effective' response gained an average 5% in net stock value over the same period of time"*. The difference between what the authors called 'recoverers' and 'non-recoverers' is stark and goes beyond the average share price hit being 8%.

If the proven value of corporate reputation and its erosion in a crisis are not persuasive enough, the clear and material benefits of structured crisis preparedness should be sufficient to prompt organisations to take it seriously.

FURTHER INFORMATION

CASE STUDY

The Deepwater Horizon Oil Well Explosion and its Consequences for BP in the Gulf of Mexico
by Dr Jon White

[9] https://senateshj.com.au/project/crisis-index-300/
[10] Rod Cartwright *'Reputation, Risk and Resilience'* report (2025).
[11] Rory F. Knight & Deborah J. Pretty Knight (1996), Oxford Metrica, *'The Impact of Catastrophes on Shareholder Value'* http://eternity.websurgeon.ca/papers/whitepapers/sedgwickreport.pdf

THE FIVE PHASES OF CRISIS

THE FIVE PHASES OF CRISIS

Crisis practitioners have identified common stages that crises typically follow, even though the specific nature of each crisis may vary.

This tool helps to plan a framework for preparing for and handling a crisis.

PREDICT

Effective risk mitigation and management

The UK Corporate Governance Code is clear that boards are responsible for managing and controlling a broad range of risk effectively, stating that they should *"establish and maintain an effective risk management and internal control framework"* and *"determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives"*.[12] In addition, they should *"carry out a robust assessment of the company's emerging and principal risks … which include, but are not necessarily limited to, those that could result in events or circumstances that might threaten the company's business model, future performance, solvency or liquidity"*.[13] Such risks will often include threats to reputation.

What is reputational risk?

Although boards widely acknowledge reputation as one of their organisation's most important assets, relatively few have robust frameworks in place to identify, manage and mitigate reputational risk.

Reputation is not something an individual or organisation owns. It is conferred by others and must be continuously earned. It is shaped by how well an organisation fulfils its promises in the broadest sense – by living its values, delivering for customers, making sound decisions, meeting performance standards, and consistently demonstrating integrity and positive behaviour across the organisation. Reputation is not built through rhetoric; it is built through action. It is not about telling but showing.

Reputational risk refers to the possibility that an organisation's standing, credibility or trustworthiness may be damaged or undermined by events, decisions, behaviours or external shocks.

It reflects the risk that negative perceptions – whether justified or not – drive stakeholder responses that materially harm the organisation, affecting revenue, value, regulatory relationships, market position, or confidence among investors, employees, customers and communities.

[12] Financial Reporting Council, *UK Corporate Governance Code* (2024), Principle O (Audit, Risk and Internal Control).
[13] Financial Reporting Council, *UK Corporate Governance Code* (2024), Provision 28.

Sources of reputational risk

Reputational threats are diverse and constantly evolving. Many originate in operational failures that later spill over into reputational harm, for example cyber incidents, data breaches, health and safety failures or environmental events, can quickly undermine public confidence and inflict lasting brand damage.

Governance failures present particularly acute risks: misjudgements, ethical lapses or misconduct at senior levels can erode trust in leadership, provoke regulatory scrutiny and destabilise investor confidence.

Reputational risk also arises from workplace culture and human behaviour, including discrimination, bullying, leadership conflict, lack of diversity, groupthink or development of a toxic culture.

Beyond the organisation itself, reputational harm may be triggered or amplified by political, regulatory or geopolitical developments, as well as by misinformation or deliberate disinformation. In today's environment, no organisation is insulated from external narratives shaping internal reality.

The modern reputation landscape

Each of these risks has the potential to inflict significant reputational damage. Importantly, the volatility and insecurity of today's world – combined with unprecedented interconnectivity – means that crises rarely remain contained. Single issue events are now the exception rather than the norm. Failures cascade across functions, sectors and stakeholders, amplifying impact and complexity.

Negative publicity spreads instantly. Minor incidents can escalate rapidly into headline news, often before organisations have fully assessed the facts. In this context, poor or delayed communication becomes a reputational risk in its own right – even when operational performance is otherwise sound.

Public scrutiny has never been higher. The boundary between personal and professional conduct has eroded; social and corporate behaviour increasingly overlap. Digital footprints are permanent and the risks of the increasing use of AI, in search engines and other applications, are still unfolding. In a world of non custodial data, forensic recovery and ubiquitous recording, there is no meaningful distinction between "on the record" and "off the record." Nothing that is written, said or captured truly disappears and can be made available to all.

Organisations that withstand scrutiny are those led by individuals who actively and deliberately safeguard reputation. At times, this requires difficult or costly commercial trade offs. But while managing reputation may be expensive, failing to do so can be ruinous.

The impact of reputational risk

Reputational risk directly affects long term organisational value, influencing revenue, public and employee confidence, regulatory relationships and investor behaviour. Safeguarding reputation is therefore a core board responsibility and an integral part of good governance, with regulators and stakeholders expecting clear oversight; failure can result in scrutiny, loss of funding or intervention.

Reputational damage escalates rapidly in modern crises as issues spread across media and stakeholder networks, and slow or poorly aligned responses can significantly amplify harm. Strong, pre established crisis communication structures are essential to limit exposure.

Recovery from reputational damage is slow and costly, often taking years to rebuild trust. By contrast, organisations that actively manage their reputations benefit from stronger relationships, greater influence, and increased long term value – advantages that become especially critical in times of crisis.

Differences in reputational risk identification across sectors

The identification and management of risk varies depending on whether an organisation is in the public or the private sector, and whether it operates in a highly regulated sector. Although many organisations adopt enterprise risk management frameworks influenced by standards such as ISO 31000,[14] their practical application reflects these differences.

In the public sector, reputational risk is closely tied to legitimacy and public trust. Government bodies and public agencies operate under intense political oversight, media scrutiny and statutory transparency requirements. A perceived failure – whether operational, ethical or financial – can quickly become a crisis of confidence with electoral or policy consequences. Risk appetite is therefore typically low. Reputational considerations are rarely separate from operational decisions; instead, they are embedded in questions of public acceptability and democratic accountability.

In the private sector, reputational risk is more explicitly linked to enterprise value. While financial and operational risks remain central, reputation increasingly acts as a multiplier of impact, affecting share price, investor confidence, customer loyalty and access to capital. Boards often define risk appetite in strategic terms, balancing growth ambitions with potential brand or ESG-related exposure. Reputational risk is therefore assessed not only in ethical terms but also in relation to materiality and long-term competitiveness.

Regulatory intensity further shapes risk practice. Highly regulated sectors – such as finance, healthcare and energy – operate within compliance structures that formalise risk identification and reporting. Here, reputational damage frequently follows regulatory breach. In less regulated sectors, however, reputation may function as a form of 'soft regulation' driven by stakeholder activism, media dynamics and social expectations.

The situation is more complex in the voluntary sector. Charities are increasingly professionalising their fundraising effort, so becoming subject to the type of risks seen by private enterprise. Charities need to market themselves effectively to maintain the levels of funding needed to provide for beneficiaries. Many charities also operate in highly regulated sectors with the accompanying reputational risks this brings. Many depend on public funding with its political pressures. Several recent scandals have led the public to question the charity sector more closely, which brings greater media scrutiny.

Similarly evolving public opinion and cultural practices also create emergent risks over time, such as the shift in attitudes about private relationships between colleagues, especially where there may be a power imbalance, which is now considered to be largely unacceptable.

Reputational risk is now a central organising principle of risk management, a consequence of the growing influence of transparency, ESG scrutiny and digital amplification.

Why reputational risk is a board level issue

Reputation and reputational risk must sit firmly at the centre of the board's agenda because:

- Reputational risk carries disproportionate weight. Its value may be difficult to quantify when strong but becomes unmistakably evident once lost.
- Once damaged, reputation is exceptionally difficult – and slow – to rebuild.
- Stakeholders judge organisations not only on what they do, but on how they explain, justify and respond to events.
- Reputational risk is inherently cross functional, cutting across leadership, operations, legal and compliance, ethics and behaviour, technology and cyber risk, and communications.
- Reputation cannot be compartmentalised. It is shaped by everyone in the organisation, led by the CEO and actively overseen by the board.

[14] ISO 31000 https://www.iso.org/standard/65694.html

- Understanding reputational risk is fundamental to effective board oversight. Gaining that understanding requires careful, sustained analysis of how the organisation is perceived by different audiences and stakeholder groups. Once these perceptions are clearly understood, reputation becomes far more manageable – and boards are better equipped to assess and respond to the impact of a crisis when it occurs.

For directors and senior leaders, personal and organisational integrity is foundational. It underpins fiduciary duty, institutional resilience and individual accountability. A board's fiduciary responsibilities should explicitly include oversight of reputational risk.

Embedding crisis preparedness, ethical leadership, and effective communication into governance structures is central to sustaining long term value, trust and resilience. Boards that fail to identify, monitor and mitigate reputational risks expose their organisations to avoidable and potentially severe harm.

Managing reputational risk

Reputational risk can and should be managed in the same way as other risks, through the use of internal controls, digital compliance checks and assurance mechanisms. Boards typically use a risk register to track key risks, their impact, controls and ownership, supported by Key Risk Indicators, with management reviewing it regularly and the board at least quarterly.

Mitigation of reputational risk includes internal controls such as clear and robust employee social media and media policies, an anti-fraud and corruption policy, and a cyber-hygiene communications programme.

Appropriate Key Risk Indicators set by a senior communications professional might include regular employee satisfaction surveys, media monitoring and brand tracking. Appropriate benchmarks for each serve as an early warning system.

Efficient floor to board information flows about risk are essential and must be supported by a clear escalation policy that triggers the formation of a Crisis Management Team (see page 34). Siloed information and blockages in the flow significantly increase risks so the communications director will support the flow of information to shape and deliver the crisis communication strategy.

Essential tools in crisis preparedness for boards are scenario planning and analysis which enable the safe testing and rehearsal for a wide range of possible events of varying severity. The senior communications professional will orchestrate these events but it is essential that boards understand they share the responsibility for corporate preparedness.

Another key risk mitigation factor is a positive organisational culture. Employees must feel safe to report incidents or concerns through trusted channels. The communications function has a key role in promoting organisational values and creating an open culture.

FURTHER INFORMATION

CASE STUDY

The Impact and Consequences of Misidentifying Risk by Katherine Sykes

TOOLKIT

Reputational Risk: Board Checklist

Horizon scanning

Horizon scanning underpins strategic intelligence, risk management and organisational resilience. It enables the early identification of emerging issues that may affect reputation, licence to operate, regulatory exposure and long term value, allowing leadership to respond while strategy, decisions, messaging and operations remain aligned. Emerging risks cut across functions so effective horizon scanning requires close coordination between regulatory, public affairs, legal, operations, HR and risk teams. The communications function acts as the integrator that identifies issues with material reputational and stakeholder impact.

Through systematic monitoring of policy, media, activist, regulatory, competitor and sector signals, horizon scanning maintains situational awareness of how external developments intersect with internal risks and stakeholder expectations. It assesses implications for trust, legitimacy and narrative control, and feeds this intelligence into enterprise risk management, scenario planning and crisis preparedness. This enables proactive measures such as early board and leadership briefings, development of holding positions, targeted stakeholder engagement and effective internal coordination.

Horizon scanning therefore provides early warning of emerging risks and external pressures before they crystallise into crises. It provides the intelligence boards need to assess whether appropriate controls, preparedness and decision making structures are in place to manage risk, respond effectively to disruption and sustain organisational resilience.

FURTHER INFORMATION

SPECIAL FEATURE

The Importance of Horizon Scanning as Part of Risk Mitigation and Management by Farzana Baduel

Artificial Intelligence: understanding the new governance risks

AI tools are now widely used across organisations – some with formal approval, many without. In the absence of clear governance, the data fed into these tools, the outputs acted upon and the decisions they influence can create significant risk. This is the source of most AI related crises. Robust AI governance is therefore not optional; it is a core element of the board's fiduciary responsibility.

The risks of AI

Six factors distinguish AI from every previous technology transition boards have navigated:

1 Speed

AI capability is advancing faster than governance frameworks. Organisations without clear policies are accumulating liability while regulation catches up.

2 Presence

AI is already embedded in organisations, often in active use before any formal procurement process – or even before the board has discussed it.

3 Visibility

AI failures rarely remain internal. Hallucinated outputs, biased decisions or undisclosed use quickly become news stories, regulatory triggers and reputational events.

4 Scope

AI has no natural owner because it has no natural boundary. It is already present across every function simultaneously, spanning the entire risk register and touching every category of risk the board already owns.

5 Accountability

Previous technology transitions primarily created operational risk; AI creates accountability risk. When an AI assisted decision causes harm, the critical questions are: who decided, who verified and what governance was in place?

6 Trust

AI reshapes both how an organisation operates and how it is perceived. Whether AI use is disclosed, well governed and aligned with stated values is now integral to organisational trust. Trust ultimately determines whether the other five factors are managed credibly under scrutiny.

Beyond the technological risks, the central concern for boards lies at the intersection of AI with trust, culture and public perception. How an organisation uses AI – and how it explains and defends that use – now directly influences reputation and legitimacy. Boards that govern AI well gain a credibility advantage; those that do not accumulate an often unrecognised liability that typically only surfaces once scrutiny begins.

AI governance

As AI capability expands, so too do the ethical, legal, operational and reputational risks. Effective AI governance provides the structure and accountability needed to ensure AI driven innovation is safe, responsible and sustainable. It must be established before a crisis occurs – to prevent governance gaps from escalating into reputational emergencies and to ensure the board can evidence responsible decision making when challenged by regulators, media, staff, customers or the public.

AI governance should be a standing board agenda item, not a periodic update. It must provide oversight across the full spectrum of organisational AI maturity – from organisations with no formal policy or visibility of use, to those where AI is embedded in core operations and the consequences of failure are far more significant. While many organisations point to existing governance structures following AI related incidents, the issue is rarely whether governance existed, but whether it was robust, enforced and credible under pressure. McKinsey's *State of AI* survey (2025)[15] found that nearly half of organisations surveyed had experienced measurable governance or ethical lapses linked to generative AI.

Effective AI governance is grounded in accountability. It ensures AI use is deliberate, responsible and explainable – not merely compliant. In practice, this requires clear decision making authority, defined lines of ownership and active management of reputational risk. Critically, boards must distinguish between AI used with meaningful human oversight and AI operating with de facto autonomy – and understand how AI driven outputs or decisions will be judged publicly once exposed to scrutiny.

Accordingly, boards should require:

- Clear, board approved principles for AI use.
- Defined thresholds for when AI may assist decision making versus when humans must decide.
- A single, documented point of accountability for AI governance.
- Regular review and adjustment as capabilities, risks and expectations evolve.

Understanding AI is the starting point; governing it is the obligation. The proof comes when that governance is tested from the outside. Legal may confirm compliance, and technology may confirm systems are functioning, but neither can confirm trust. Because AI failures are inevitably public, trust is the variable that determines whether a governance record holds or collapses.

Boards that manage AI risks credibly will not be those with the most sophisticated systems or the longest policy documents, but those that governed AI with trust as a guiding principle, communicated that governance clearly and honestly, and ensured accountability was visible from the outset – so that when scrutiny arrived, the record spoke for itself.

FURTHER INFORMATION

SPECIAL FEATURES

AI and Governance: Crisis Communication in the Age of Algorithmic Decision Making by Philippe Borremans

AI and Reputation by Ben Verinder

Mis/Disinformation by Shayoni Lynn

TOOLKIT

AI Failure Modes

AI Governance: Board Checklist

The Trusted Clarity Model

[15] McKinsey's State of AI survey (2025) https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai/2025/the-state-of-ai-how-organizations-are-rewiring-to-capture-value_final.pdf

PROTECT

Resilience is built on strong foundations

Organisations with strong foundations are far better placed to withstand and recover from crisis. Good governance requires boards to protect their organisations by safeguarding their health and resilience long before any crisis emerges. These foundations support genuine crisis readiness. Crisis management is not something that begins at the moment of disruption; it is a forward looking discipline that builds long term organisational resilience. Achieving this requires a structured approach, applied with purpose, consistency and rigour.

The critical role of strategic communications

Strategic communications is a critical capability that no board should be without. It is a value enabling function and a core governance responsibility, underpinning effective decision making, trust and organisational legitimacy. Effective communication is foundational to organisational health in day to day operations and indispensable in crisis, often determining whether disruption is contained or escalates into prolonged reputational and financial harm.

Strategic communications is fundamental to effective crisis management and integral to the board's fiduciary responsibility for risk oversight and organisational stewardship. It provides the discipline, pace and coherence required to protect reputation, mitigate financial and regulatory risk, maintain stakeholder confidence and support timely, well judged decisions under pressure. By embedding crisis communication into strategic and risk planning, boards ensure that roles, protocols, leadership messages and stakeholder relationship pathways are established well before a crisis emerges.

Over time, this capability strengthens organisational resilience, alignment and accountability, helping boards to avoid foreseeable harm, reduce avoidable costs and discharge their duties in the face of disruption. Consistent with ISO 22361, communication is a core governance and leadership capability, and a legal and regulatory requirement.[16,17,18,19]

---

16 The UK Corporate Governance Code 2024 emphasises the importance of robust internal controls and transparent outcomes reporting: Provision 29 asks boards to declare the effectiveness of material internal controls, which effectively elevates preparedness, decision making discipline and communications at boardroom level. Crisis communication is part of internal control effectiveness. Directors should be able to evidence that crisis roles, escalation paths, disclosure judgements and stakeholder communications have been designed and tested, and can operate at speed under stress. https://media.frc.org.uk/documents/UK_Corporate_Governance_Code_2024_a2hmQmY.pdf

17 Data protection breaches (UK GDPR) The ICO requires certain personal data breaches to be reported within 72 hours of awareness; high risk breaches also require prompt notification to affected individuals. Preparation demands internal detection/escalation, approved templates and a communications plan that can operate while facts evolve. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

18 Online harms, misinformation and deepfakes Under the Online Safety Act (regulated by Ofcom), platforms have new duties; Ofcom's work on deepfake attribution (watermarks, provenance metadata, AI labels, context annotations) underscores how misinformation environments can compound crises. Organisations should anticipate rapid false narratives and rehearse counter misinformation playbooks. https://www.gov.uk/government/collections/online-safety-act https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfake-defences-2--the-attribution-toolkit

19 The UK National Cyber Security Centre (NCSC) provides guidance to support organisations on their communications before, during and after a cyber incident. It makes three main recommendations: prepare in advance, communicate clearly to different audiences, tailoring messaging where necessary, and manage the aftermath over the medium/long term. Communications must be clear, authoritative, accessible and timely, while balancing transparency with operational security and legal obligations. https://www.ncsc.gov.uk/guidance/effective-communications-in-a-cyber-incident

Strategic communications creates long term sustainable value

Strategic communications professionals play a pivotal role in creating long term, sustainable value by articulating organisational purpose and values, strengthening cross functional integration, and cultivating trusted stakeholder relationships. They reinforce the 'G' in ESG by ensuring that governance, reputation, credibility, accountability and organisational behaviour remain aligned.

Communication professionals take a long term view of risk and reputation. Acting as organisational "sense makers in chief"[20] they distil complex and interdependent factors into clear, actionable insight, helping boards anticipate how decisions will be interpreted internally and externally. Their involvement supports more informed decision making, mitigates groupthink, constructively challenges assumptions and keeps boards attuned to external realities and stakeholder expectations that may otherwise be overlooked.

Ensuring that communications are fit for purpose

A dedicated communications professional provides boards with assurance that organisational communications are fit for purpose – clear, consistent and strategically aligned – both in stable conditions and during crisis. They advise on appropriate channels, formats and timing, ensuring communication choices are proportionate to risk, sensitive to context and supportive of long-term objectives.

Crisis conditions compress decision making timeframes and heighten uncertainty. In these circumstances, authoritative, balanced and timely communication must be planned in advance, rigorously tested and tightly aligned with governance responsibilities. Communications professionals safeguard narrative coherence across employees, regulators, investors, partners and the wider community, reducing the risk that inconsistent or ambiguous messaging undermines operational response, stakeholder confidence or board oversight. They also guide boards through digital, social and generative AI enabled communication environments, helping organisations manage scrutiny, misinformation and reputational threat with clarity and authority.

Communications expertise is a core governance capability

Modern boards increasingly recognise that communications expertise is a core governance capability. Operating at the intersection of legal, operational, reputational and regulatory requirements, strategic communications' place is not outside the governance structure, advising when called upon, but within it, with a seat at the board. A board that waits for a crisis before engaging its communications function has already ceded the ground on which trust is built. By the time the communications professional is in the room, the governance record that determines how the crisis resolves has already been written. Embedding strategic communications at board level – through executive and/or non executive representation – strengthens strategic alignment, public accountability and organisational resilience. Where communications responsibility rests with directors whose primary expertise lies elsewhere, boards lack assurance that communication risks and opportunities, stakeholder dynamics and reputational exposure are being effectively governed.

Strategic communications has long term consequences for organisational legitimacy. When communication expertise is fully embedded into strategy, risk management and board level decision making, it strengthens foresight, sharpens judgement and enables leaders to act with coherence under pressure. In an era defined by overlapping crises, accelerated scrutiny and fragmented information environments, boards that treat strategic communications as a core governance capability – not a peripheral function – are materially better positioned to protect value, uphold accountability and sustain confidence among stakeholders. Communication, when governed well, becomes a decisive source of resilience and a critical enabler of long-term organisational success.

[20] Professor Deborah Ancona, MIT Sloan Management Review, October 2020

What boards should expect from their strategic communications professional

Boards should expect their strategic communications professional to operate as a trusted governance partner, not a service function, providing clear, independent advice on reputation, trust, stakeholder impact, and risk in both stable conditions and crisis. This role should bring foresight and discipline to decision making by anticipating how board and executive actions will be interpreted internally and externally, ensuring communications are accurate, aligned with values, legally and ethically sound, and fit for heightened scrutiny.

Critically, the communications professional should support the board's fiduciary responsibilities by embedding communication into strategy, risk and crisis planning, maintaining narrative coherence under pressure, and enabling the organisation to demonstrate control, accountability and legitimacy when challenged.

FURTHER INFORMATION

SPECIAL FEATURE

Strategic Communications: Protecting Reputation in a Crisis by Stephen Waddington

TOOLKIT

What Boards Should Look For In The Ideal Strategic Communications Professional: Board Checklist

Strategic Communications: Board Checklist

The importance of building and developing relationships with stakeholders

Building and maintaining strong, resilient and trusted relationships with stakeholders is central to maintaining trust, protecting reputation and enabling sound governance. It is a core board responsibility and is fundamental to long-term business success. No organisation can expect to communicate effectively if it does not know who it should be communicating with and why. Identifying, understanding and prioritising stakeholders is crucial both for the smooth running of normal business operations and also for preventing crisis and reducing reputational risk.

Stakeholders' opinions matter, because the opinions and perceptions of stakeholders control both an organisation's 'licence to operate' and the ability it has to maximise opportunity and to minimise the damage that any crisis will cause. Consequently, organisations that take the time and trouble to identify their stakeholders in advance, and build relationships with them, fare much better in a crisis than those who do not.

A deliberate and strategic approach to stakeholder management is required. Success requires an organisation to first understand who its stakeholders are, their interests, significance, influence and the value they bring or risk they represent. Useful models for gathering this insight are a stakeholder map and risk register, which identify stakeholders and their associated risk levels.[21]

A stakeholder map plots all key stakeholders and clearly defines their levels of influence. It should be comprehensive, starting with those stakeholders without whom the organisation cannot function, for example, employees, customers or clients, suppliers and investors. Secondly, those who have significant influence, such as regulators, policymakers and government. Thirdly, stakeholders who have influence on the previous groups such as the media, social media influencers and NGOs.

Stakeholder lists and contact details must always be kept up to date and readily available electronically in a central location which can be accessed and used quickly. It makes sense to also have a secure back-up off site, on a dark site or on paper, in case of cyber-attack.

A targeted, tailored approach is required. The plan should identify the most appropriate method for reaching each stakeholder group: ranging from social media and email to direct outreach by named individuals. Messaging should be tailored appropriately to both the stakeholder and to the method of delivery (channel).

It is equally important to have a stakeholder risk register. This document plots stakeholders on a matrix to help determine how to engage them. This matrix reflects the risk levels and perceptions of each stakeholder group based on their stake, power and influence. This could be risk to operations, reputation and/or the organisation's bottom line. A stakeholder risk register highlights how a fallout with a particular stakeholder could impact the organisation and the severity of the consequences. This also guides the design of tailored engagement approach to help prevent or minimise potential conflict.

Communication professionals have the expertise, training and aptitude to build credible, constructive relationships across diverse stakeholder groups and to anticipate shifts in stakeholder expectations. In evaluating emerging pressures, identifying opportunities for deeper engagement and monitoring developments that could unsettle established relationships, they provide the board with early insight into risks that may otherwise go unnoticed. This foresight – supported by structured horizon scanning and continuous monitoring – helps the board manage issues proactively and improves overall crisis preparedness. In practice, this means communicators not only protect stakeholder trust in moments of

[21] Worked examples of a stakeholder map and a stakeholder risk register appear on page 113.

threat but also equip the board to understand how external dynamics are changing, where vulnerabilities are emerging, and how relationships must evolve to uphold organisational resilience.

Ultimately, a comprehensive stakeholder relations strategy, with a detailed, tailored and targeted engagement approach for each stakeholder group, is essential for all organisations. Organisations should aim to engage and build trusted relationships with stakeholders in peacetime so that when the worst happens there is already an open channel of communication and goodwill in the bank, creating a halo effect that can shape how actions and intentions are judged during a crisis. Boards must understand all aspects of this strategy and ensure it is reviewed and updated annually to reflect shifts in stakeholder dynamics and business needs.

FURTHER INFORMATION

SPECIAL FEATURE

The Interplay Between Reputation and Relationships by Dr W. Timothy Coombs

TOOLKIT

Stakeholder Map and Risk Register for a Mining Company

The character crisis

How stakeholders perceive events is critical to how a crisis develops and to the reputational consequences that follow. In this context it is useful to understand the difference between crises that are characterised by 'character' and those that are characterised by 'capability'.

Organisations have a capability reputation that is determined by their ability to do well at what they exist to do, but they also have a character reputation which is far more volatile, as this depends on individual human beings and the deep cultural issues within the organisation. Overall, character-led scandals cause far more frequent, deeper and longer-lasting damage to reputations and relationships than capability-led crises. They pose a greater challenge to the board as they are much more likely to imperil an organisation's recovery.

FURTHER INFORMATION

SPECIAL FEATURE

What Publics Talk About When They Talk About Corporate Reputation: A Framework for Boards by Dr Craig E. Carroll

CASE STUDY

A Study of Character vs Capability: The KissCam Viral Video by Chris Tucker

Building strong organisational culture

A strong and positive culture reduces the risk of crisis and is a powerful source of resilience and capability. Culture matters because it shapes how people behave when no one is watching, directly influencing performance and trust; when values are clear and genuinely lived, employees are more engaged, collaborate better and make decisions that align with the organisation's purpose rather than just short term targets, which reduces risk and improves consistency.

Culture also underpins reputation and governance, as poor behaviours and misaligned incentives are common root causes of crises and reputational damage, while a healthy culture supports ethical judgement, accountability and constructive challenge at all levels. Most complex reputational crises stem from questions of executive decision-making, cultural attitudes and values and behaviours within the organisation.[22] Ultimately, strategies, systems and structures are only as effective as the culture that sustains them. Organisational culture is a critical driver of sustainable success, not a 'soft' or secondary consideration. It shapes how an organisation performs both in business as usual conditions and when it is under serious duress.

The strategic management of organisational culture and the challenges of implementing it are well-known evergreen topics.[23] Work patterns have changed and people are now less likely to work together in one particular physical space. Increasingly, organisations feature greater diversity of age, experience and economic circumstances, meaning that business systems, processes and behaviours must evolve to accommodate them.

When financial and competitive performance takes precedence, it is easy for a culture of low accountability and intense internal competition to take hold. In increasingly turbulent trading conditions, organisations are often expected to do more with the same – or fewer – resources, placing sustained pressure on under resourced employees to meet equal or tougher performance metrics.

This can seed and entrench a toxic culture in which people are viewed as expendable rather than as critical ambassadors of the organisation, particularly where there is an oversupply of qualified job seekers.

Even if an organisation's poor culture escapes the headlines, it may not escape other harm: a poor culture may degrade an organisation's capabilities over time. An organisation known to have a poor culture often finds it more difficult to recruit and retain the calibre of employees capable of delivering the most value. Culture has the capacity to affect investor confidence and may result in sudden withdrawal of investment or a challenge to the board directly.

A strong communications function – which runs through the organisation from board to floor – will unlock the value of relationships with internal stakeholders, create the potential for an authentic narrative that reflects an organisation's values, ethics and behaviours, and contribute to a resilient culture. In addition, a robust HR function will hire, train and retain the staff committed to the organisation's values and ethics so minimising the risk of poor behaviours that too often lead to crises. An authentic, board level commitment to culture and communications working hand in glove is one of the most effective safeguards there is to minimise and mitigate the internally generated risks that can inflict serious reputational and commercial harm.

FURTHER INFORMATION

SPECIAL FEATURES

The Importance of Organisational Culture in Preventing and Responding to Crises by Alison Arnot

Ignore DEI at Your Peril: How Inclusive Cultures are an Organisational Risk Mitigation Strategy by Avril Lee

CASE STUDY

Post Office Horizon: When Brand Protection Silences Critical Stakeholders by Stephen Waddington

[22] Rod Cartwright *'Reputation, Risk and Resilience'* report (2025)
[23] See further Steve Gruenert and Todd Whitaker in *School Culture Rewired* (2015): *"The culture of any organization is shaped by the worst behavior the leader is willing to tolerate."*

Issues management

It is important to understand the difference between issues management and crisis management, as they are not the same. An issue is more akin to a problem which can be managed; it is not a crisis that is highly volatile and potentially existential in nature. Issues management could be described as sailing a ship in rough seas, whereas crisis management would involve trying to save the ship when it is approaching, or has struck, an iceberg. Issues do not demand instant resolution; they provide time for consideration and choice in ways to proceed. In contrast, there is no time in a crisis, and unless preparations have been made in advance, the choices, if any, may be extremely limited.

Effective management of issues builds capacity to anticipate, prepare for, mitigate and manage risk, prevent crisis, improve leadership and management practice and promote good governance.

Nonetheless, sometimes an issue, even if handled well, may turn into a crisis and there is no simple rule to determine when that tipping point might be. In these circumstances, questions the board should ask include:

- Have the risks at stake increased?
- Is control of the situation drifting away?
- How much focus does the issue need?
- Does organisational focus need to be ramped-up?
- Are external forces involved?
- Can the organisation still function in business as usual? If so, for how long?

Not everything is a crisis. Crises are extremely unusual and, potentially, existential events. Treating too many issues as a crisis devalues the term and weakens people and processes so that they are less effective when the real crisis arrives. Issues management usually takes place before crisis management, however there are circumstances in which it can take place or resume when the immediate crisis is over. For example, public inquiries and litigation may drag on for many years after the original crisis is over. In such cases, the risk of reputational damage will be just as great, if not greater, than it was during the crisis, and sensitive, careful management will be required throughout.

FURTHER INFORMATION

SPECIAL FEATURE

Issue or Crisis? How They Differ and Why it Matters
by Dr Tony Jaques

PREPARE

Preparedness determines outcomes

Modern disruptions are frequent, fast moving and capable of severely damaging an organisation's operations, reputation and long term value. Crises now cut across operational, digital, ESG, regulatory, geopolitical and information ecosystem risks, with escalation often occurring within minutes. In this environment, crisis preparedness is not optional; it is a core fiduciary and governance responsibility that protects reputation, safeguards strategic continuity and underpins long term organisational viability.

This imperative is reinforced by both business and societal evidence. A 2023 PwC survey[24] of 1,812 executives found that 96% of organisations had experienced multiple disruptions, with 76% reporting medium to high operational impact, yet many still lack the integrated resilience capabilities needed to respond at pace and scale. At the same time, the United Nations' 2025 *World Social Report* identifies a global erosion of interpersonal and institutional trust, driven by polarisation, misinformation and perceived exclusion, which weakens social cohesion and makes cooperation and consensus building harder. The report concludes that trust cannot be rebuilt reactively during crises, but depends on credible, transparent engagement sustained well in advance – reinforcing the need for early preparation and disciplined practice of both human and operational systems.[25]

24 https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html
25 UN World Social Report (2025) *Trust in a Changing World* https://social.desa.un.org/sites/default/files/inline-files/World%20Social%20Report_Dec2024.pdf

Human preparedness

The critical role that people play in crisis preparedness can never be overestimated. ISO 22361[26] cautions that *"crises can be so extraordinarily demanding that no assumptions should be made about the ability of personnel (of any seniority, grade or experience) to manage them and steer the organization out of a crisis"*. This focus on the human imperative should sit at the heart of any organisation's approach to issues, crisis and risk, whether operational, reputational or relational.

The National Preparedness Commission defines preparedness as a state in which an organisation has *"the right mindset, capabilities, information and governance structures to deal with adverse events – whether foreseen or unexpected"*.[27] The emphasis on mindset is particularly significant. It is the essential complement to technological infrastructure, and too often the missing ingredient.

Resilience is frequently misunderstood as a system, a process or a specialist function. In reality, it is a human and cultural outcome, shaped by leadership behaviours, organisational objectives and values, and decision-making under pressure. Guidance[28] from the UK Government's Resilience Academy distinguishes between 'operational resilience', which focuses on how the organisation currently operates and 'strategic resilience', which focuses on building greater levels of resilience into the future.

This dynamic has been repeatedly reinforced by the Business Continuity Institute's annual Horizon Scan Report.[29] In 2024, it identified an underlying wave of sickness absence, stress, anxiety and depression, stemming from the Covid-19 pandemic, as the leading cause of business disruption and productivity loss the previous year.

Safety incidents affecting staff wellbeing were the most frequent and impactful events reported, highlighting that *"human factors continue to be underweighted in forward-looking risk assessments*. As the report notes *"people remain at the centre of every resilient system … it is the wellbeing, confidence and capability of individuals that define how organisations truly perform under pressure"*.

This challenge is intensifying. Mental health and wellbeing indicators are deteriorating, employee disengagement is rising, and polarised grievance driven by inequality and perceived injustice has become increasingly common. Against this backdrop, risks associated with character, culture, values and behaviours may represent the most significant and least well managed threats facing organisations today.[30]

In an environment characterised by intersecting risks, systemic shocks and permacrisis, crisis preparedness can no longer be confined to specialist teams or technical plans. It must involve all key business functions and actively embed preparedness into organisational culture. Building resilience therefore requires as much focus on developing human muscle memory through training, rehearsal and simulation as on technical systems and crisis materials.[31]

Unless organisations adopt a genuinely holistic approach to reputation risk management and crisis preparedness – one that prioritises whole team, cross functional and human centred capability building – human preparedness will remain fragile and unevenly distributed. In today's febrile operating environment, investment in critical human infrastructure should be viewed not as optional but as a core leadership responsibility and a standing item for board level oversight.

[26] https://www.iso.org/obp/ui/en/#iso:std:iso:22361:ed-1:v1:en
[27] https://nationalpreparednesscommission.uk/about/preparedness/
[28] https://assets.publishing.service.gov.uk/media/66a9fa3efc8e12ac3edb07ba/2024-05-14_UKG_Organisational_Resilience_Guidance_FINAL.docx__1_.pdf
[29] https://www.thebci.org/resource/bci-horizon-scan-report-2025.html
[30] Rod Cartwright '*Reputation, Risk and Resilience*' report (2025). This is an annual report which started in 2023, which synthesises and analyses major global reports by influential organisations, such as the World Economic Forum, AXA, Ipsos and Page Society, on the state of trust in the world and the nature of our risk environment.
[31] Rod Cartwright (2025) *'Reputation, Risk and Resilience'* report

Crisis management team

Every crisis should be managed by a Crisis Management Team (CMT), which should be established well in advance of any crisis arising. Normally, the CEO or COO will be responsible for establishing the CMT and determining which functions should be represented. The size and composition of the CMT will vary depending on the organisation and the nature of the crisis but should typically operate at the 'Gold' (strategic) level, bringing together senior decision-makers and representatives from key business areas. Communications should be a standing requirement alongside functions such as Legal, Finance, HR, Operations and IT. Any CMT roles should have documented deputies. Beneath this, 'Silver' (tactical) and 'Bronze' (operational) teams may be established within functions to manage delivery and execution, allowing the CMT to remain focused on strategic judgement, direction and oversight.

The CMT should be chaired by a leader who is accountable for the strategic management of the crisis. The individuals selected for this role must be senior and respected executives with the confidence of the CEO and the board. They must have vested in them the ability and authority to act decisively and swiftly outside of the usual norms of operation. The CMT leader should not usually be the CEO as the organisation needs to continue to function on its core business as usual deliverables as much as is possible.

The communications director should be responsible for developing the organisation's crisis communication strategy and coordinating the media and social media response, ensuring that all external communications are informed by appropriate legal advice.

The communications team oversees the drafting, approval and dissemination of all final messaging to relevant internal and external stakeholders and play a critical role in safeguarding the organisation's brand and reputation.

Board members should recognise that decision making in a crisis is fundamentally different from business as usual. Time pressures are intense, information is incomplete and decisions must often be taken without the depth of data a board would normally expect. This requires creativity and, at times, a willingness to think – and act – beyond established norms. One of the greatest risks in these conditions is groupthink. Boards must actively invite and test differing perspectives, reflecting and anticipating the views of all key stakeholders, and ensure that those most directly affected by the crisis – particularly any victims – remain at the centre of the organisation's decisions and communications.

Establish a clear, tested crisis communication framework

In a crisis, saying or doing nothing brings its own consequences and is not recommended. Consequently, every organisation needs a concise, operational crisis communication plan that clearly defines roles, responsibilities, actions and escalation protocols. This is a core requirement of effective crisis management and a key component of ISO 22361.[32] The plan should be board endorsed and regularly rehearsed, so that board members understand both its content and their own role if it is activated. Ultimately, the board is responsible for ensuring that, during a crisis, stakeholders receive timely, accurate and credible information on a consistent basis.

The drafting of the crisis communications plan is the responsibility of the communications professional/team.[33] The plan should be a concise, practical playbook that sets out how an organisation will communicate before, during and after a crisis, ensuring clarity, speed and consistency.

It typically includes:

- Clear roles, responsibilities and accountabilities.
- Rapid response protocols.
- Pre agreed escalation criteria and activation steps.
- Guidance on establishing verified facts and defining what is known, unknown and being investigated.
- A framework for creating truthful, timely, proportionate messaging with one coherent narrative across all channels.
- A list of media and communication channels to be utilised.
- Tools and systems to help manage social media monitoring and engagement.
- Real time monitoring procedures to track media, misinformation and sentiment; any specific considerations for social media.[34]
- Stakeholder mapping with tailored internal and external communication approaches.
- Templates for holding statements.
- Guidance for call-takers.
- Fact sheets and press kits.
- Locations for press conferences.
- Contact information for resources, including spokespeople.

It should also establish procedures and tested arrangements for activation, and identify resourcing options capable of supporting heightened operational demand.[35] Effective plans are short and usable under pressure – unlike the unwieldy 100 page documents that fail when speed is essential – and are regularly tested and aligned with organisational values and governance expectations.

A crisis communication plan should be supported by a dedicated crisis stakeholder map. While this will typically build on the organisation's business as usual stakeholder analysis, it must be adapted for crisis conditions, clearly prioritising stakeholders by influence, impact and urgency. Organisations should also anticipate that the media may seek comment from competitors or third parties, and consider in advance whether credible external voices, such as industry peers or relevant trade bodies, should be briefed.

[32] ISO 22361 states *"Crisis communication positions the organisation as the central source of information, demonstrates its control of the organisation and reassures interested parties."*

[33] Further information can be found in the CIPR Crisis Communications Network's '*Drafting a Crisis Communication Guide*' (October 2023) https://ciprcrisiscommsnetwork.com/publications/

[34] Further information can be found in the CIPR Crisis Communications Network's Guide '*Crisis Communication and Social Media*' (October 2024) https://ciprcrisiscommsnetwork.com/publications/

[35] ISO 22361

The plan should also specify the most appropriate communication channels for each stakeholder group. For regulators, this may require direct engagement from a board member, while engagement with policymakers or similar audiences should be led by those with the strongest existing relationships, which may again involve board level participation.

Employee communications should reflect the size and structure of the organisation. Frontline employees may be best reached through line managers, while internal digital platforms can provide timely organisation wide updates. Senior managers may reasonably expect direct communication from a senior executive or board member. Crises can have significant psychological impacts on employees, particularly those with long tenures whose sense of loyalty may feel tested. As highly credible voices during a crisis, employees can either reinforce or undermine confidence in the organisation, often shaped by how informed, supported and respected they feel.

During a crisis, mainstream and social media must be actively monitored and managed to the maximum extent possible. The CMT should receive regular, typically twice daily (or more frequently in some situations) briefings from the communications director on media coverage, emerging narratives and new issues as they develop. Strong media relationships built in peacetime provide a clear advantage in crisis, as does a well established social media presence. Crucially, organisations should establish a baseline for media and social media activity in advance, enabling them to distinguish normal fluctuations from genuine escalation in negative sentiment.

Lastly, the crisis communication plan should contain basic messaging for at least the most likely three to five crises the organisation may face. This means that once the CMT is brought together initial messaging is already in draft so that it is a case of adapting rather than starting from scratch. Good crisis messaging should help stakeholders understand what is happening and what, if anything, they need to do. Boards must ensure that draft holding statements are available and ready to be deployed shortly after the crisis hits.

There is no spare time in crisis. One way to relieve the pressure is to create a ‘dark site’ in advance, a web or micro-site that is not publicly available but which contains the full gamut of crisis materials, including, but not limited to, statements, messaging, Q&A, stakeholder information, photos and images. This can be kept regularly up to date and used when needed. In addition, it could be created as a separate site outside the organisation’s normal IT infrastructure so that in case of a cyber-attack the communications materials are still available and easily deployable.

Scenario planning, simulations and training

A crisis communication plan should never be allowed to become stale. Regular scenario based training and crisis simulations are essential to ensure it remains effective in practice. These exercises should test the full communications dimension of a crisis, not just operational response, and should recreate the speed, pressure and uncertainty of real time events.

Scenario planning helps organisations to anticipate how they would respond to a range of potential crises, from cyber-attacks and natural disasters to security incidents or personal and political scandals. It should be approached by both boards and management as a creative and disciplined process: considering what crises might plausibly arise, what their consequences could be, and whether the organisation is genuinely prepared for the worst case scenario.

Rehearsal builds the human muscle memory that underpins effective crisis management. Because crises are abnormal situations that unfold at speed, regular practice is the only reliable way to prevent paralysis, poor judgement or delay when pressure is highest. Crisis simulations are particularly valuable, as they place participants into realistic scenarios that expose the challenges of making decisions and communicating clearly under intense scrutiny.

Members of the CMT should expect to take part in a crisis simulation at least annually. Those identified as potential media spokespeople in the crisis communication plan should be media trained and undertake regular refresher training to ensure readiness.

As the ultimate stewards of organisational reputation and viability, boards should also participate in crisis simulation exercises and regular crisis training. Organisations are only as resilient as their weakest links, so involving senior leaders, the CMT and relevant staff is critical to overall preparedness.

FURTHER INFORMATION

CASE STUDIES

Grenfell: An Industry Changed by Dan Gerrella

Crisis Preparedness at Heathrow by Sara Naylor

RESPOND

Powerful communications during a crisis: critical success factors

The volatility of today's world, and the range of threats it creates, requires every board member to take personal responsibility for understanding crisis management. Effective oversight depends on a practical grasp of what management must do hour by hour and day by day. Modern crises move at 'machine speed', and organisations can fail when decision-making structures are too slow or cumbersome. The widening gap between early warning systems and human approval chains is now a critical vulnerability.

Managing the crisis: saying the right thing, at the right time, in the right way

Knowing how to say the right thing, at the right time, in the right way is the central tenet of crisis communication and because it doesn't come easily or naturally for many people, the only way to mitigate the risk of reputational damage caused by saying or doing the wrong thing is to prepare and practise thoroughly. There are several important factors to bear in mind:

The first response

Commonly referred to as the 'Golden Hour', the first hour after the crisis has hit, or been declared, is crucial. During that time organisations must work at speed to establish what facts they can and roll out their initial statement.[36] This statement sets the tone of the organisation's response. It must *acknowledge* that something has happened or may have happened, *regret* the consequences for those involved, *resolve* to work with emergency services/authorities and/or to conduct an internal investigation into what went wrong in order to ensure it doesn't happen again, and *commit* to provide regular updates as more information becomes available over coming hours/days/weeks. In certain circumstances, including incidents involving potential criminality, organisations may need to defer any further detailed statement to emergency services.

Misinformation loves a vacuum and it is commonly said that in the age of social media, organisations should issue their first response more quickly. Obviously, the circumstances of any particular crisis may support that approach. However, the unassailable benefits of using the full hour are that: the initial fact-gathering into what went wrong can begin, the initial statement – which should already have been pre-prepared and available in draft – can be tweaked for the particular circumstances at hand, key stakeholders (including the board and employees) can be informed of the situation before the first public response is made, and communications can be aligned so that the statement can be posted online and on social media channels at the same time. In other words,

[36] See example on page 116.

that valuable hour gives organisations time to get their arrangements in place before providing their considered response.

Do not delay issuing the first statement after the first hour. Delays invite misinformation and may unwittingly create a negative perception of obfuscation, or lack of transparency, or poor governance from which it may be hard to recover.

Spokespeople

The public – and the media – expects a response. Moreover, it is often the case that the media drives and exacerbates a crisis. Well in advance of the crisis, the board must decide or agree who the most appropriate person to represent their organisation publicly will be. Normally, this should be the CEO, although in cases where the CEO is the crisis (for example if there is an issue of personal misconduct) the Chair of the board will be the better choice. In addition, substitute spokespeople, including subject matter experts, should also be identified so that the organisation can still be represented if for whatever reason (i.e. death, extreme illness) the main spokespeople are not available. Sometimes crises run on high intensity for many days and even weeks and in such cases it is unreasonable to expect the same spokesperson to be available all the time; every human has basic sleep requirements and it is entirely foreseeable that a spokesperson who has been under media pressure for several days, not resting or sleeping, could potentially make a catastrophic mistake.

The spokesperson's performance is all-important. All spokespeople must be fully, rigorously and regularly media trained well in advance: so high are the stakes that both the spokesperson's and the organisation's futures are on the line. Think carefully about when the spokesperson should make their first appearance. In some circumstances the first hour may be appropriate. In other cases a delay would be acceptable (so long as other communications are made, including the initial statement). However, do not leave it for more than 24 hours.

Media relations

Effective engagement with the media is essential during the crisis response phase. Handled well, it will support the organisation in post-crisis recovery. In order to establish credibility, and to maintain narrative coherence, it is absolutely essential to respond early, even if there are still gaps in the information available. Stakeholders expect to hear that actions are being taken, even if those actions have not yet been completed.

How to say what needs to be said

The spokesperson must project an air of calm, confidence and control. They must keep their composure. While admitting that something has gone wrong, they want to reassure the public that everything will be done to put the problem right. At the same time, they must never forget that those affected by the crisis should be at the heart of all communication. Clear acknowledgment of the human and community impact of the crisis, and an ability to show empathy and concern for those affected, is absolutely crucial.

With some exceptions, people tend to remember how other people said things, and how they made them feel, more than what was actually said. This is typical in crisis when events move quickly and emotions run very high. It is important that the organisation and its spokespeople are seen to behave with emotional honesty and integrity, and that all written communications contain emotional content too.

Never be afraid to say sorry. Saying sorry in a genuine and empathetic manner shows empathy for the victims, or those affected by the crisis. It is not the same as admitting liability, which may have legal consequences. A simple form of wording, prepared in advance, agreed by both the legal and the communication teams, can reduce risk and save crucial time in a crisis.

The importance of language

Although boards will not normally be involved in drafting crisis communications, they should understand something of the communications professional's craft.

Perception is everything. In order to recover well from the crisis, an organisation must be judged to be responding in an emotionally appropriate, sincere and authentic manner. In addition, controlling the pace and timing of communications is essential as delays invite speculation and misinformation. Keeping control of the narrative, to avoid others doing so, is essential too. All these things require judgement and experience and cannot be left to chance.

During the height of the crisis, there should be frequent messaging designed to provide clear, factual updates clarifying what is known, unknown and being investigated. It is wise to avoid evasive language such as 'no comment', or phrases which may be perceived as insincere such as 'lessons will be learned' and to acknowledge responsibility and accountability when appropriate. In order to avoid confusion, which can deepen a crisis, all messaging should be simple, clear, consistent and aligned across all channels (internal, external, press, digital).

Consider the impact of the crisis on those affected. What do they need to know? What do they need to do? How can they get help that is specific to, and actionable by, them? How would you communicate to customers affected by a cyber-attack on the one hand and to people whose lives were at risk from a flood or forest fire on the other?

Words matter. The language used in crises where the ultimate outcome is financial or reputational is likely different from that in which human lives are at stake.

Situational awareness and stakeholder engagement

It is essential to understand how a crisis is evolving in real time. The communications team must keep on top of how the unfolding crisis is perceived by tracking stakeholder sentiment and monitoring public narratives. They must identify and rebut incorrect media reports and mis and dis information, identify shifts of interest and peaks of engagement and adjust communications on the basis of developments.

An organisation's relationships with its stakeholders are key to its success and long-term sustainability. During crisis, engagement builds trust, reduces uncertainty and offers two-way dialogue where possible. It directly addresses concerns in a way that is mutually beneficial. The strength and health of an organisation's relationships with its stakeholders will define whether, or how well, it recovers from crisis.

Setting the tone from the top

External stakeholder reaction, including activists and/or the media, can be at its worst during a crisis: persistent, intrusive, aggressive, provocative, rude. For senior leaders in the eye of the storm, the pressure is immense, and it cannot be escaped. When a crisis is playing out over the front pages of mainstream and social media, board members can expect their family, friends, colleagues, and anyone else they might encounter outside the office, to be approached. Being doorstepped by the media at home is an ever-present risk during a crisis and should be prepared for. Given the intensity of these circumstances, it is understandable that the CEO and board members may feel like victims of the crisis. But adopting this mindset is deeply damaging; it undermines clear judgement, slows decision making and pulls focus away from those who are, or are perceived by society to be, the victims.

The organisation must put those individuals and communities at the heart of its response and communications.

At the same time, leadership should recognise the immense demands that employees may be under. Moral support and pastoral care will be very valuable in these situations and is something that board members, especially in small organisations where relationships are much closer, can actively provide. Sadly, it is far from unusual for the personal contact details of employees to be shared online when emotions are running high. Board members have a positive duty to support the leadership team, especially the spokespeople, during crisis, both at a practical and an emotional level.

At the height of crisis, the board's responsibilities are directly tied to communication

At the height of a crisis, the board's responsibilities are inseparable from communication. Crisis communication is crisis governance – not an add on. ISO 22361 makes clear that leadership, planning, oversight and stakeholder engagement all depend on communication competence. Boards must therefore oversee and approve crisis communication plans, ensure adequate resources, monitor execution and champion transparency throughout the organisation.

In practice, this means ensuring the crisis communication plan is current, usable and rigorously stress tested; confirming that communication leaders sit at the decision making table; checking that communication is fully integrated with risk, legal and operational functions; and requiring scenario planning that anticipates likely developments and next steps.

When communication works, it creates stability, confidence and coherence. Boards should ensure:

- There is one clear, authoritative narrative.
- Structures support truthful, timely, human centred communication.
- Communication is empathetic, proportionate and mindful of legal risk.
- Clear distinctions between what is known, unknown and under investigation and no speculation.
- Verified information is shared quickly.
- There are regular, predictable updates.
- Organisational culture supports transparency over defensiveness.
- Decision making pathways support speed and clarity.
- Visible leadership – with the CEO front and centre and the chair providing strategic oversight.
- Communication supports operational continuity.

A full list of questions board members should ask management is provided on page 120.

Fundamentally, boards must treat communication not purely as messaging or reputation management but as a strategic governance capability essential to crisis readiness, response and recovery.

Why can crisis communication fail?

Crises are not caused by PR or social media. Instead, organisations often fall short through lax governance, insufficient preparedness, inadequate incident response and/or a failure to recognise when societal outrage has direct relevance to their operations.

These oversights amplify risk and can quickly escalate into reputational harm. Common failures include:

- Communications not involved early in risk assessment, leading to blind spots.
- Slow reaction times due to approval processes and bottlenecks.
- Delaying the approval of messages despite the urgency of the situation.
- Lack of scenario planning and next step anticipation.
- Failure to focus on affected people in messaging and actions taken.
- Structural or cultural barriers to transparency.
- Communicating in ways that are vague or fail to deliver key messages.
- Not selecting the most effective platforms or channels to reach the intended audience.
- Using wording that is unsuitable for the audience, including overly technical or complex language that may cause confusion.
- Overlooking public input and not adjusting communications based on feedback received.
- Misjudging what should be prioritised in communication efforts.
- Not recognising the emotional context of a situation, resulting in communication that lacks empathy, fails to resolve tension or does not connect with people.
- Poor coordination with relevant stakeholders, leading to inconsistent messaging.
- Allowing internal and external communications to become out of sync.

FURTHER INFORMATION

CASE STUDY

The 2024 Valencia Floods by Chris Tucker

TOOLKIT

Sample First Response/Holding Statements

Questions Boards Should Ask Management in a Crisis

Drafting a Crisis Communication Plan

Good Crisis Communication: Board Checklist

Navigating crises in an AI world

AI has fundamentally reshaped the conditions under which crises now unfold – compressing response windows, accelerating the spread of false information and placing sophisticated capabilities in the hands of bad actors that were once limited to well resourced organisations. Boards that govern AI effectively recognise it as both an internal risk to manage and a powerful external force that can shape how a crisis emerges, escalates and is resolved.

AI as an accelerant of crisis

While the technology might not always create the crisis, it can determine how far and how fast it travels:

- Deepfakes and synthetic media impersonating an organisation or its leadership.
- AI-generated disinformation spreading faster than any truthful, human-created content can.
- AI-enabled phishing and social engineering that exploits the moment.
- Volume amplification of negative narrative at a speed and scale that no communications team can match manually.

AI as a crisis management tool

The same capability that accelerates a crisis can contain it. Used securely, AI can significantly improve the speed and quality of crisis management:

- AI-powered monitoring for early detection of emerging narratives before they reach critical mass.
- Rapid synthesis of large volumes of incoming information across media coverage, stakeholder response and regulatory signals.
- Drafting speed for holding statements and internal communications when time is a constraint.
- Scenario modelling for how a story might develop across different audiences and channels.

FURTHER INFORMATION

SPECIAL FEATURE

Cybersecurity Risk: Board Oversight and the Role of Strategic Communications by Chris Tucker

CASE STUDY

Jaguar Land Rover: Crisis Communication Take-Aways from the UK's Most Economically Damaging Cyber-Attack To Date by Chris Tucker

RECOVER

Learning from experience and moving forward

The recovery phase begins once the immediate threat is contained, the urgent response has stood down, and the public mood allows for forward momentum. Its purpose is to stabilise operations, rebuild confidence, capture learning and restore trust with internal and external stakeholders. In some cases, a return to the previous 'normal' may not be possible if this is what led to the crisis in the first place; the board may need to define a 'new normal' and steer the organisation towards it.

Recovery is a critical board responsibility, as directors remain ultimately accountable for reputation, governance, strategic risk oversight and organisational stability. An effective board during this phase is:

- Visible but non operational – providing scrutiny and strategic direction without stepping into management roles.
- Transparent – insisting on honest evaluation and open communication.
- Decisive – converting lessons into governance, policy and cultural reforms.
- Future focused – using the crisis as a catalyst to strengthen resilience and preparedness.

Recovery is a process, not a single moment. The CMT must judge when to shift from response to recovery, based on the specific nature of the crisis.

Understanding what recovery involves is essential for knowing when it should begin. At its core, recovery is about rebuilding and re-establishing the organisation and its brand.

Steps the board should take in the recovery stage

1 Provide oversight of stabilisation and risk closure

The board must ensure that all residual risks – reputational, operational and cultural – are fully identified and mitigated, and that any temporary fixes deployed during the crisis are replaced with secure, permanent solutions. Oversight at this stage is essential to closing risk, restoring controlled operations and preventing vulnerabilities from re-emerging.

2 Direct a formal review of the crisis

The board should commission a structured, evidence based after-action review that reconstructs the timeline, analyses decision-making, evaluates communication effectiveness and spokesperson performance, and assesses crisis team dynamics, plans, processes, governance gaps, stakeholder feedback and any compliance considerations. The review must be independent, transparent and focused on reflection rather than blame, ensuring everyone involved has a voice. Findings should be documented, accompanied by an agreed process and timeline for action, and shared widely across the organisation.

3 Rebuild trusted relationships through strategic communications

Boards should evaluate how the crisis has impacted stakeholders and how effectively the organisation communicated with them during and after the crisis. They must ensure that a clear recovery communication plan is in place to explain what has been learned from the crisis, what corrective actions will be taken and what commitments will be made to improve governance, systems and culture. Because crises often reveal deeper stakeholder sentiment, rebuilding relationships is as important as repairing reputation, and requires deliberate, ongoing communication grounded in accountability.

4 Strengthen people, culture and leadership

Recovery requires careful attention to how the crisis has affected morale, culture and trust between the board, the CEO and the executive team. Boards must reaffirm expectations of transparency and cohesion, ensure leadership models recovery-aligned behaviours and confirm that appropriate wellbeing support is available to staff as the organisation stabilises.

5 Mandate long term structural improvements

Boards must oversee updates to risk registers, crisis and communication plans, escalation protocols and governance structures, ensuring these are adequately resourced and embedded. Management should be required to run new scenario exercises, to test whether lessons have been internalised, and check that improvements are functioning as intended.

6 Reassure regulators, members, funders and external stakeholders

The board should ensure all regulatory, compliance and reporting obligations are fully met and documented, and demonstrate visible leadership in showcasing strengthened governance. Any commitments made during the crisis must be honoured to rebuild credibility and trust.

7 Looking ahead

Boards should anticipate future milestones arising from the crisis – such as anniversaries, inquiries or public reviews – and plan responses in advance to prevent issues from resurfacing and to reinforce the organisation’s commitment to accountability and learning.

Communications during the recovery phase

Boards should understand how communications are recalibrated during the recovery phase. As the organisation shifts from stabilising immediate risk to repairing reputation, messaging shifts away from rapid crisis alerts and becomes calmer, less frequent and more predictable, signalling that control has been re-established. Updates focus on progress, restoration timelines and next steps, while greater transparency explains what is now known, what has been resolved and what remains outstanding.

This openness, combined with an honest explanation of what went wrong, is essential to rebuilding long-term stakeholder confidence and fulfilling board responsibilities.

At the same time, recovery communications must be action-oriented, human and visible, showing how the organisation is preventing recurrence and supporting those affected. Boards should be looking for:

- Clear explanations of corrective actions, governance improvements and resilience measures.
- Empathetic, human centred reassurance and practical, localised guidance for different stakeholder groups.
- Visible leadership through CEO and board communications, site visits and direct engagement.
- Consistent, multi-channel communication tailored to different audiences.
- Recognition of recovery milestones and a clear close-out message summarising lessons learned, permanent changes and ongoing commitments.

Together, these elements reinforce accountability, restore trust and signal responsible governance as the organisation moves forward.

FURTHER INFORMATION

SPECIAL FEATURE

After the Crisis: Boards, Recovery and Public Inquiries by Amanda Coleman

CASE STUDY

Storm Kristin by Philippe Borremans

TOOLKIT

Recover: Board Checklist

BEYOND RECOVERY:

Building Enduring Resilience

BEYOND RECOVERY:
Building Enduring Resilience

In a world of uncertainty, disruption and flux, resilience and preparedness have become a major focus for organisations of all kinds. No sector is immune. In 2025, 66% of respondents to the Office of National Statistics Public Survey of Risk Perception, Resilience and Preparedness[37] thought that the number of emergencies/disasters in the UK would increase in the next 10 years. Extreme weather events, power cuts and cyber-attacks topped the public's 'likelihood' list, while war, pandemics and terrorist attacks led the way on impact.

In 2025, the UK government published assorted analyses, strategies and plans, spanning national risks, resilience and security, including:

- **National Risk Register**[38] (January) *"the government's assessment of the most serious risks facing the UK"*.
- **UK National Security Strategy**[39] (June) designed to *"identify the main challenges we face as a nation in an era of radical uncertainty; and set out a new Strategic Framework in response, covering all aspects of national security and international policy."*
- **Chronic Risks Analysis**[40] (July) providing *"the first bespoke risk assessment for medium to long term risks"* covering 26 chronic risks across seven themes, namely Security, Technology and Cybersecurity, Geopolitical, Environmental, Societal, Biosecurity and Economic issues.
- **Resilience Action Plan**[41] (July) which aims to *"continuously assess how resilient the UK is, to target interventions and resources effectively, enable the whole of society to take action to increase their resilience and strengthen the core public sector resilience system."*

The many private sector and academic contributions to this area include:

- **Model for Organisational Resilience**[42] by Resilience First and Cranfield University;
- **National Preparedness: the New Strategic Issues**[43] (2026) in which the National Preparedness Commission argues that the UK's level of preparedness has *"barely kept pace with the scale and escalating nature of the challenges the nation faces"* and calls for a *"whole-of-government, whole-of-society approach"*.

Organisations can enhance their resilience and preparedness in the following ways:

[37] https://www.gov.uk/government/statistics/uk-public-survey-of-risk-perception-resilience-and-preparedness-2025/uk-public-survey-of-risk-perception-resilience-and-preparedness-2025-headline-findings
[38] https://www.gov.uk/government/publications/national-risk-register-2025
[39] https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html
[40] https://www.gov.uk/government/publications/chronic-risks-analysis
[41] https://www.gov.uk/government/publications/uk-government-resilience-action-plan
[42] https://resiliencefirst.org/what-we-do/organisational-resilience/
[43] https://nationalpreparednesscommission.uk/publications/national-preparedness-the-new-strategic-issues/

1 Build resilience and preparedness

Resilience – defined by Oxford Languages as *"the capacity to withstand or to recover quickly from difficulties"* – is all-important for any organisation but it also risks being a reactive state. By contrast, the National Preparedness Commission focuses on preparedness, which it describes as *"a state in which [an organisation] has the right mindset, capabilities, information and governance structures to deal with adverse events – whether foreseen or unexpected."* Boards are advised to focus on that more fundamental approach to threat preparedness and risk readiness.

2 Prepare for stable risks with greater intensity

Although it might feel like a new threat emerges every week, research suggests that the risk landscape is actually relatively stable – but with risks and threats intensifying. In its 2025 Global Risks Report, the World Economic Forum noted that *"the overall view of global risks is much the same as last year, if more negatively weighted"*, while AXA's 2025 Future Risks Report pointed out that *"stability in the top 10 risks is a call to action"*. While boards naturally wish to focus on emerging threats, remaining focused on compounding 'evergreen' risks is just as important.

3 Consider business continuity vs. relationship continuity and business as usual vs. reputation as usual

While organisations must manage and measure their reputations – particularly in crisis situations – it is even more important to gauge, track and respond to how their key stakeholders behave and act towards them, i.e. their relationships. While the maintenance of business continuity and the speediest possible return to business as usual are crucial crisis management and communication objectives, it is equally important to maintain relationship continuity and work towards a *sustainable* return to reputation as usual – which can have a far longer 'tail' than the resumption of business as usual.

4 Resilience is a human, cultural outcome, not a role, department or job title

Reputational crises are fundamentally human in origin and impact, and their effective management depends on human judgement under pressure. No level of technical infrastructure, processes or documentation will compensate for the absence of embedded capability, training and exercised decision making. As Mike Tyson observed in 1987, *"everyone has a plan until they are punched in the mouth."* Resilience, therefore, should be understood not as a system or function, but as an organisational capability shaped by leadership, culture and strategic choices. Effective risk preparedness requires sustained investment in human capability and cultural readiness across the whole organisation, rather than reliance on process ownership by a single function.

FURTHER INFORMATION

SPECIAL FEATURE

True Crisis Preparedness and Resilience
by Rick Cudworth and Swaraj Parameswaran

ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

Crisis Communication for Boards was created by the CIPR Crisis Communications Network Committee led by Katherine Sykes, supported by Chris Tucker and Kerry Knight, with contributions from Rod Cartwright, Adelaide Arthur and Sara Naylor.

We would like to thank the Institute of Directors for their endorsement, especially Trudy Lewis for her enthusiastic and consistent support.

Particular thanks to the many senior practitioners and academics who have so kindly contributed their time and insights to this handbook: Alison Arnot, Farzana Baduel, Philippe Borremans, Dr Craig E. Carroll, Amanda Coleman, Dr W. Timothy Coombs, Rick Cudworth, Dan Gerrella, Dr Tony Jacques, Avril Lee, Shayoni Lynn, Swaraj Parameswaran, Stephen Waddington, Dr Jon White and Ben Verinder. We are truly indebted to you all: thank you. Additional thanks are due to Amanda Coleman for so kindly reviewing the text and for providing feedback at a critical stage and to Kerry Knight for graphic design.

Finally, with grateful thanks to the Chartered Institute of Public Relations, especially Sarah Ion, for facilitating and funding this work.

This handbook is fundamentally a human endeavour. It was conceived, researched, curated, written, and brought together by the members of the Crisis Communications Network and our expert contributors.

While some authors may have used AI tools to assist with research, drafting, or editing, these tools served only as a support mechanism within the broader creative and editorial process. Every section of the handbook was subject to human review, judgement, and revision. Before publication, the complete manuscript was manually edited by the Crisis Communications Network, who take full responsibility for its content.

Biographies

CIPR Crisis Communications Network Team

KATHERINE SYKES FOUNDER AND CO-CHAIR

Katherine Sykes is the lead author and editor-in-chief of this handbook. She is also the Founder and Co-Chair of the CIPR Crisis Communications Network, a CIPR Fellow and Chartered PR Practitioner. A former City solicitor, she is an experienced non-executive director and trustee with over 30 years' professional practice across law, policy, communications and governance. She is Founder and CEO of Marland Sykes, a strategic communications consultancy, advising boards and senior leadership on strategic communications, crisis, reputation, risk and organisational resilience in complex, high pressure environments.

CHRIS TUCKER CO-CHAIR

Chris Tucker brings over 30 years' public relations experience across voluntary, public and private sectors. Formerly PR Director for the Barclays Group, she now runs a consultancy spanning fintech, ESG, overseas development and crisis communications, providing practical support, training and coaching in media relations and crisis communication. She is Co-Chair of the CIPR Crisis Communications Network, a founder member of CIPR's ESG Panel and course leader for CIPR's PR and crisis communications diplomas.

ROD CARTWRIGHT SPECIAL ADVISOR

Rod Cartwright is a senior independent consultant, specialising in issues, crisis, reputation, risk and resilience. He leads Rod Cartwright Consulting, is Special Advisor to CIPR's Crisis Communications Network, a Visiting Fellow at Cardiff University and the author of the annual, award-winning report *Reputation, Risk and Resilience*.

ADELAIDE ARTHUR

Adelaide Arthur is a multimedia journalist and communications professional with 18 years of experience. She is passionate about impactful storytelling and communication that connects people. Currently, she focuses on internal communication, helping to deliver business objectives, strategic decisions and change management through authentic messaging that engages internal stakeholders.

KERRY KNIGHT

Kerry Knight is a Chartered PR Practitioner and qualified non-executive director who advises boards and senior leaders on issue and crisis preparedness, specialising in AI governance. A 2026 Independent Impact 50 award recipient, Kerry writes about current and emerging risks via her Signals & Soapboxes newsletter, helping organisations prepare and stay ahead of threats.

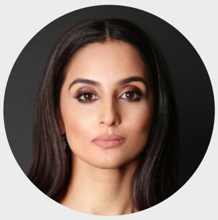
SARA NAYLOR

Sara Naylor is a strategic communications consultant and ex-national news journalist valued for delivering impact for public, private and third sector clients. She is a Chartered PR practitioner and one of the 2026 Independent Impact 50 award-winners.

Contributors

ALISON ARNOT

Alison Arnot CIIC, Chartered PR Practitioner and CIPR Fellow, is an award-winning consultant, trainer, author and speaker with 25+ years' experience specialising in internal and crisis communications. She is the author of *Internal Communication in Times of Crisis: How to secure employee trust, support, and advocacy in crisis situations* (Kogan Page).



FARZANA BADUEL

Farzana Baduel is a Chartered PR Practitioner, Honorary CIPR Fellow and CIPR President 2026. She is CEO of Curzon PR, advising governments and organisations on strategic communications. She is Resident PR Expert at Oxford University's Saïd Business School and a trustee of HALO Trust and Soho Theatre. She is a presenter of BBC Radio 4's *When It Hits The Fan*.

PHILIPPE BORREMANS

Philippe Borremans is a crisis, risk and emergency communication consultant with over 25 years of field experience across more than 50 countries. As Managing Director of RiskComms FZCO, he advises governments, international organisations and global corporations, and publishes the *Wag The Dog* practitioner newsletter.

DR CRAIG E. CARROLL

Dr Craig E. Carroll, PhD, is founder of the Observatory on Corporate Reputation (OCR), and Narrative Shield; editor of *The Handbook of Communication and Corporate Reputation* and the *SAGE Encyclopaedia of Corporate Reputation*; and co-host of the podcast *Communication Breakdown*.

AMANDA COLEMAN

Amanda Coleman is a crisis communication specialist and director with 25+ years' experience in crisis and emergency communication. Author of numerous books including *Crisis Communication Strategies* (Kogan Page), she is a Chartered PR practitioner and Fellow of both CIPR and PRCA, chairs the UK's Emergency Planning Society Communication Group and serves the Emergency Management External Affairs Association's international advisory committee.

DR W. TIMOTHY COOMBS

Dr W. Timothy Coombs (PhD Purdue University) is Editor-in-Chief for the *Journal of Contingencies and Crisis Management*. He is a Fellow in the International Communication Association, and his crisis communication research has won numerous academic and practitioner awards.

RICK CUDWORTH

Rick Cudworth is a board and Executive Director of Resilience First. Rick is a leading expert in organisational resilience. He advises the UK government, contributes to national and international standards, and holds academic roles at King's College London and Cranfield University. He co-edited *Resilience Reimagined: A Practical Guide for Organisations*.

DAN GERRELLA

Dan Gerrella is a CIPR Fellow, Chartered PR Practitioner and CIPR President Elect 2027. He is managing director of LMC, a PR consultancy specialising in construction and property. His expertise includes crisis preparedness, working with asset owners, property developers, law firms, local authorities and energy companies around building safety, product recalls and business failures.

DR TONY JAQUES

Dr Tony Jaques is a consultant and lecturer based in Melbourne, Australia. He is the former Asia-Pacific Issue and Crisis Manager for a multinational corporation and has written extensively in the field. His latest book is *Crisis Counsel: Navigating Legal and Communication Conflict*.

AVRIL LEE

Avril Lee is an Honorary CIPR Fellow and senior communications consultant with extensive experience advising global pharmaceutical companies and multinational organisations on corporate reputation, issues management and brand communications. She chairs the Taylor Bennett Foundation and the CIPR's Diversity and Inclusion Network, and advises on how inclusive leadership strengthens organisational culture, stakeholder trust and business resilience.

SHAYONI LYNN

Shayoni Lynn is a communications strategist and global keynote speaker specialising in behaviour change, misinformation resilience and public trust. A Fellow of the CIPR and PRCA, she is founder of Lynn, a behavioural science and counter misinformation advisory, advising ministers, NGOs and C suite leaders on strategic communications, trust and influence.

SWARAJ PARAMESWARAN

Swaraj Parameswaran is Memberships, Programmes and Partners Coordinator of Resilience First. Swaraj graduated from King's College London with a Master's in International Relations. He is also a freelance journalist and has written several articles for geopolitical publications.

BEN VERINDER

Ben Verinder is a strategic communications expert, one of 50 Founding Chartered public relations practitioners, a CIPR Fellow, a pioneering authority on AI in PR and leading commentator on the impact of AI on reputations and relationships. Ben is the co-editor of *AI for PR* (Kogan Page).

STEPHEN WADDINGTON

Stephen Waddington is a PhD researcher at Leeds Business School and professional advisor at Wadds Inc., supporting clients on management, corporate communications and public relations. He is a former President of CIPR, a CIPR Chartered PR Practitioner and Honorary Fellow, and a Fellow of the PRCA. He is the co-editor of *AI for PR* (Kogan Page).

DR JON WHITE

Dr Jon White is a chartered psychologist, Chartered PR Practitioner and Honorary Fellow of CIPR. An independent practitioner, he has consulted and provided training on crisis management. He is the author of numerous books and articles on public relations, including crisis management, which he studied at the London School of Economics and Political Science.

RESOURCES

Books and reports

- Crisis Communications Network *Drafting a Crisis Communication Plan* https://ciprcrisiscommsnetwork.com/skills-guide-drafting-a-crisis-comms-plan/
- Crisis Communications Network *Crisis Communication and Social Media* https://ciprcrisiscommsnetwork.com/skills-guide-crisis-communication-and-social-media/
- Arnot, Alison *Internal Communication in Times of Crisis: How to secure employee trust, support and advocacy in crisis situations*
- Cartwright, Rod *Reputation, Risk and Resilience: Where Are We Now and What Happens Next?* 2026 Edition https://www.rodcartwrightconsulting.com/what-we-think-2026
- Coleman, Amanda *Crisis Communication Strategies: How to Prepare in Advance, Respond Effectively and Recover in Full*
- Coleman, Amanda *Everyday Communication Strategies: Manage Common Issues to Prevent a Crisis and Protect Your Brand*
- Coleman, Amanda *Strategic Reputation Management: Identify Strengths, Manage Performance and Protect Your Brand*
- Conley, Edward L. *Promote the Dog Sitter*
- Coombs, W. Timothy *Ongoing Crisis Communication*
- Easthope, Lucy *When the Dust Settles*
- Griffin, Andrew *Crisis, Issues and Reputation Management*
- Hartley, Kate *How to Communicate in a Crisis*
- Haggerty, James F. *Chief Crisis Officer*
- Hemus, Jonathan *Crisis Proof*
- Lerbinger, O *The Crisis Manager: Facing Disasters, Conflicts, and Failures*
- Miles, A , Editor, *Reputation Management, Building and Protecting Your Company's Reputation in a Digital World*
- Omand, David *How to Survive a Crisis*
- Sellnow, Timothy L. and Seeger, Matthew W. *Theorizing Crisis Communication*
- Wheeler, Adrian *Crisis Communication Management*

Case studies

www.thecasecentre.org

Crisis Communications Network

Website: ciprcrisiscommsnetwork.com

LinkedIn: linkedin.com/company/cipr-crisis-communications-network

Blue Sky: CIPRCrisisComms (@ciprcrisiscomm.bsky.social) – Bluesky

You Tube: CIPR Crisis Comms – YouTube

Email: ciprccrisiscom@gmail.com

CIPR qualifications and training

Crisis Communication Diploma (Specialist PGDip)

https://cipr.co.uk/CIPR/Learn_Develop/Qualifications/Specialist_Diploma_Crisis_Communications.aspx

Crisis Communication courses

https://cipr.co.uk/CIPR/Learn_Develop/Training/Crisis_and_reputation_training.aspx

CASE STUDIES

THE DEEPWATER HORIZON OIL WELL EXPLOSION AND ITS CONSEQUENCES FOR BP IN THE GULF OF MEXICO

by Dr Jon White

On 20 April 2010, the Deepwater Horizon oil rig, operated for BP in the Gulf of Mexico, was rocked by an explosion that killed 11 workers and allowed oil to escape from the well head. This was located 40 miles off the coast of Louisiana and 5,000 feet below the surface of the sea. Oil flowed into the water for 87 days before the well was finally capped.

After the event, BP came to realise that it was subject to unprecedented media and political scrutiny, not least because of the ever-growing possibilities for social media commentary. For US President Barack Obama, the stakes were high. His predecessor, President George W. Bush, had run into heavy criticism for his perceived slow response to the consequences for Hurricane Katrina on Louisiana and other states bordering on the Gulf.

In addition to the deaths of the employees, the accident caused environmental and economic damage to affected states. For BP, the accident was a corporate crisis that threatened the existence of the company, wiping 50% off its market value and forcing it to set aside funds to meet potential claims against it.

The company's response to the accident and its aftermath was a reaction to a complex interplay of issues and there is much that can be learned from how the management set about dealing with the crisis. The issues included:

- The technical problems associated with attempts to cap an oil well in a deepwater location.
- The organisational requirements of managing several external partner and supplier organisations that provided services such as the operation of the rig to BP.
- The number of involved stakeholders, from the families of the employees killed in the accident to the US federal government, and to the local authorities and communities affected.
- BP's safety record had recently been questioned as a result of other accidents in the US and the company had already suffered reputational damage.

BP's CEO Tony Hayward became personally involved in the company's response to the accident, suggesting that he would not leave the site until the problems had been solved. He was, however, to be heavily criticised in his role and for a number of statements that he made to the media in the course of responding to the demands of the company's attempts to deal with the situation. He was also seen to take time off from his responsibilities for dealing with the situation. His credibility was irreparably damaged and he was replaced as CEO of the company as it later sought to retrieve its reputation after the oil well was capped.

Reflecting on his experience later, he recognised that he needed very specific preparation for the demands of representing the company and its approach to dealing with the crisis. He was criticised in the middle of the company's response to the situation for saying that he wished it to end so that he could get his life back, showing insensitivity to the fact that people had lost their lives in the explosion.

Media scrutiny of the company was intense. Attempts to deal with the oil leaking from the well and to explain the company's actions were under constant surveillance by the press and broadcast media and in discussions that took place through social media.

BP's experience in dealing with the accident in the Gulf and its aftermath takes its place alongside other oil industry case studies, such as Shell's experience with Brent Spar in the mid-1990s and Exxon's disastrous oil spill from the company's vessel, the Exxon Valdez, in 1989.

There are two lessons in particular for boards to learn from the Deepwater Horizon accident:

- First, the disaster highlights shortcomings in senior management's preparedness for the risks associated with advanced technology – specifically, the technologies enabling deepwater oil extraction. While such risks were known, the incident demonstrates that existing preparations were insufficient to enable a rapid and effective response to technological failure.
- Second, the accident exposes weaknesses in senior management's readiness to manage the complex relationships that arise in the aftermath of a major crisis. BP's CEO acknowledged after the event that he felt insufficiently prepared for the highly visible leadership role he was expected to play in managing the consequences of the disaster, including intense public, political and stakeholder scrutiny.

The Deepwater Horizon case study therefore reinforces the importance of preparing for worst case scenarios. Such preparation requires sustained attention at the highest levels of organisations, particularly at board and senior management levels. Effective preparation draws on multiple perspectives – technical, financial, economic, political and social. The social perspective, in particular, benefits from the expertise of communications professionals whose understanding of stakeholder groups, social issues and public expectations supports horizon scanning, foresight and risk assessment. These capabilities can now be further enhanced through the careful and responsible use of artificial intelligence.

Preparation – through structured planning and simulations that test decision making under extreme and uncertain conditions – helps build organisational resilience and senior leaders' confidence in their ability to manage crises effectively as they occur.

BACK TO PAGE 15

THE IMPACT AND CONSEQUENCES OF MISIDENTIFYING RISK

by Katherine Sykes

Misidentifying or minimising assessment of risk can lead to crisis. The Grenfell Tower fire is one such example. The Grenfell disaster, which occurred on 14 June 2017, was described as a 'black swan' event in that it was highly improbable and could not have been foreseen.

A 'black swan' event[1] is defined as *"a highly improbable event with three principal characteristics: it is unpredictable; it carries a severe impact and, after the fact, we concoct an explanation that makes it appear less random, and more predictable than it was."*

The term is frequently used in crisis communications and has been used to describe other major events including the September 11 attacks, the dissolution of the Soviet Union and the rise of the internet.

Pick your swan

Crisis theory describes events as black, grey and white swans based on 1) the probability of the event occurring and 2) the perception of the risk involved. Risk is complex and people's perceptions of risk even more so. Whereas 'black swan' events are outliers, which lie outside the realm of ordinary expectations, grey and white swan events comprise circumstances which are relatively more probable, relatively more likely and relatively more foreseeable, as set out below:

Black swan

Highly improbable

- Unpredictable
- Massive impact
- After the fact, explained to appear less random and more predictable

Grey swan

High probability

- Predictable
- Impact can easily cascade
- After the fact, shifts focus to errors in judgement or some other human form of causation

White swan

High certainty

- Certainty
- Impact easily estimated
- After the fact, explanation shifts the focus to errors in judgement or some other form of causation

Whether or not an event is a 'black swan' or a 'grey swan' or even a white one, depends on what is known and understood by the observer. It is a subjective test. What may be a black swan surprise for a turkey is not a black swan surprise to its butcher.[2]

[1] The term was originally coined by financier Nassim Taleb in his extremely successful book *'The Black Swan: The Impact of the Highly Improbable'*
[2] As Taleb observed.

What about Grenfell?

For those of us with no connection to Grenfell, its residents, or to Kensington and Chelsea council, or to any of the contractors and suppliers involved with servicing the tower block, the disaster that unfolded on 14 June 2017 came as a complete surprise. Time and time again, the question was asked – in central London in the 21st century, how could a tower block catch fire, appear to literally melt, and claim 72 lives in the process? It seemed unfathomable, catastrophic, wildly unpredictable and hard to imagine that anyone with any knowledge of any possible risk factors could have allowed them to go unmitigated.

A huge amount of information has emerged since the disaster, particularly during the public inquiry. This has shown a sequence of events, failings and oversights which indicate that the Grenfell fire was less random and more predictable than might have been previously thought. To that extent, it was truly a 'black swan' event.

And yet the evidence also reveals that some of Grenfell's former residents at least were aware of many of the risks. In November 2016, eight months before the fire, a blog written by Edward Daffarn, a 16th-floor resident, warned: "Only an incident that results in serious loss of life of residents will allow the external scrutiny to occur that will shine a light on the practices that characterise the malign governance of this non-functioning organisation."

The blog had been running for several years, raising concerns about the building's refurbishment and warning of a potentially disastrous fire. In 2013, Grenfell Tower's landlord (the Kensington and Chelsea Tenant Management Organisation) blocked residents access to the blog because they deemed it to be "scaremongering and potentially frightening to the residents".[3]

Consequently, from a residents' perspective, it is possible to conclude that disaster was a 'white swan' event, in other words likely to happen or with a high degree of certainty, with an impact that could be easily guessed.

A 'grey swan' event

Perhaps the real answer is somewhere in the middle. The Grenfell disaster was the outcome of cumulative failures by multiple parties over a long period of time, during which many opportunities were missed to remedy multiple issues, including a lack of evacuation protocols, ineffective communications, defective cladding, defective smoke systems, use of combustible materials and poor workmanship, during which there was plenty of time to address residents' concerns.[4]

To this extent, and to those involved, the Grenfell fire was a disaster which could easily have been predicted, was indeed highly probable, and which was brought on by multiple failures of judgement and other human causes. On that basis, the Grenfell disaster is arguably more akin to a 'grey swan' event and clearly demonstrates the impact and consequences of misidentifying or minimising risk.

BACK TO PAGE 21

[3] https://www.theguardian.com/uk-news/2021/apr/27/grenfell-tower-landlord-blocked-staff-access-to-residents-blog
[4] https://www.bbc.com/news/uk-55349395

JAGUAR LAND ROVER: CRISIS COMMUNICATION TAKE-AWAYS FROM THE UK'S MOST ECONOMICALLY DAMAGING CYBER-ATTACK[5] TO DATE

by Chris Tucker

In late August 2025, British luxury carmaker Jaguar Land Rover (JLR) experienced a severe cyber-attack forcing the shutdown of production lines across the UK, India, Slovakia, Brazil and China. The incident, widely attributed to a sophisticated hacker group, brought production to a standstill for weeks and caused extensive financial and reputational damage. It was not until early October 2025 that the company was able to restart production. The scale and impact of the JLR cyber-attack provides important lessons for boards considering their crisis communications.

Balancing transparency with operational security

Faced with a rapidly evolving situation, JLR had to walk a fine line between informing stakeholders and protecting ongoing forensic investigations. Initial communications acknowledged the cyber-attack and production halt but offered limited detail on the scope of data impacts or timelines for recovery.

This is a very common challenge, especially in a cyber-attack. The e-discovery phase, during which the organisation works out which systems have been impacted and what is the likely loss in terms of data and operations, is rarely short and can take up to a year. But stakeholders want assurance and concrete information immediately.

The JLR attack was first discovered on Sunday 31 August. JLR shut down its IT systems and workers at the company's Halewood plant in Merseyside were told by email early on Monday morning (1 September) not to come into work. JLR made their first public statement on 2 September, which is relatively rapid for such crises. The company went on to make a series of regular updates as the situation unfolded.

Reaching stakeholders quickly

The magnitude of the JLR attack and the structure of the organisation meant the number and type of stakeholders that needed to be reached with crisis communication was extensive.

- **Employees**, many of whom were told to stay home for extended periods and were obviously concerned for their future.
- **Suppliers and dealers**, whose cash flows and operations were disrupted and which for some brought their businesses to the brink of closure.
- **Customers and retailers** awaiting vehicles or parts, leading to reputational damage and trust issues.
- **Government and regulators** engaged in national economic and industrial continuity planning. This group was particularly tricky, especially local and national government waking up to the impact on the economic fortunes of a large area of the UK.
- **All of the above internationally** as operations were impacted in numerous sites outside the UK.

[5] The JLR cyber-attack with its resulting estimated loss of £1.9 billion has been recorded as the most economically damaging cyber event to ever hit the UK. https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/

Putting ‘victims’ at the heart of crisis management and communications

While the cyber-attack impacted JLR, the fall out spread to the company’s wider supply chain, many of whom were small, local businesses. To support these businesses, JLR implemented a new scheme to pay eligible suppliers much faster than standard terms, providing cash up front and easing financial pressure. The company also set up a dedicated helpdesk to communicate with suppliers about the recovery process and efforts were made to clear a backlog of unpaid invoices to keep suppliers afloat.

In addition, in late 2025, the UK government provided JLR with a £1.5 billion loan guarantee to stabilise its finances and support its struggling supply chain. The loan guarantee aimed to ensure that JLR could continue to support its supply chain, pay suppliers, stabilise finances and protect thousands of UK jobs in the automotive sector.

This was a unique intervention, being the first time government support was provided for a cyber-attack crisis of this scale.

BACK TO PAGE 43

POST OFFICE HORIZON: WHEN BRAND PROTECTION SILENCES CRITICAL STAKEHOLDERS

by Stephen Waddington

The Post Office Horizon scandal reveals what happens when a board fails to challenge how communications serves institutional self-protection rather than the people an organisation exists to serve.

It is the most significant corporate governance failure in recent British history. More than 900 subpostmasters were wrongfully convicted of theft, fraud and false accounting based on faulty Horizon data between 1999 and 2015. The court cases, criminal convictions, imprisonments, loss of livelihoods and homes, debts and bankruptcies led to stress, illness and family breakdowns, and were linked to at least 13 suicides.

Subpostmasters repeatedly reported problems with the Fujitsu-developed Horizon accounting software, yet their concerns were systematically dismissed. These were hard-working people struggling with a flawed computer system and an organisation that prioritised the reputation of that system over the welfare of its subpostmaster network.

Brand protection over truth

The Post Office's communications strategy centred on brand protection rather than truth. When forensic accountant Ian Henderson from Second Sight uncovered evidence of miscarriages of justice, the Post Office threatened legal action, explicitly citing the need to protect its brand.

When stakeholders, including subpostmasters, MPs and journalists, raised concerns, the organisation doubled down. Its public messaging was rooted in denial, its posture aggressive and defensive.

The crisis was deepened by a leadership culture that placed brand reputation above truth. Paula Vennells, Chief Executive of Post Office Limited from 2012 to 2019, presided over the period in which wrongful prosecutions continued and mounting evidence of Horizon's failings was met with institutional denial.

The public inquiry[6] into the scandal heard that in July 2013 Vennells agreed with her director of communications, Mark Davies, not to review past cases against subpostmasters because doing so would become "front-page news". She confirmed to the inquiry that her "most urgent" objective at that time was to "manage the media".

The inquiry also heard that Vennells and Davies regarded compensation claims from subpostmasters as "opportunistic and unreasonable", and that the Post Office used hardline tactics against them to protect the organisation's reputation.

In choosing to manage communication in this way rather than confront the truth, the organisation allowed the scandal to continue for years longer than it should have done.

Long-serving employees were reluctant to question the reliability of systems that had operated on their watch. Issues were not escalated or, when presented, were downplayed, avoiding independent scrutiny. Whistleblowers were ignored and legal action was pursued despite mounting evidence of system flaws.

[6] *Post Office Horizon IT Scandal* (2025) Report: Volume 1. Chaired by Sir Wyn Williams. Available at: https://www.postofficehorizoninquiry.org.uk

The board's responsibility

The Post Office had more than 80 directors between 2000 and 2023. Many were high-profile business leaders with a thorough grasp of governance principles. Yet not one of them appears to have challenged the institution's narrative on Horizon, even as evidence to the contrary accumulated.

Strategic communications is the foundation of good governance: how organisations listen to stakeholders, surface uncomfortable truths and make decisions that are genuinely accountable. Boards that understand this are better placed to ask the right questions, challenge executive assumptions and ensure that the people an organisation exists to serve are heard.

The Post Office scandal happened because the boards abdicated their responsibility to scrutinise how the organisation communicated and with whom. Had those 80 directors understood that communication is the foundation stone of good governance, events may not have developed as they did.

One of the greatest miscarriages of justice in British legal history was the consequence of unchallenged decisions made, year after year, in boardrooms where the right questions were never asked.[7]

BACK TO PAGE 30

[7] See also Brooks, R. (2025) Private Eye *Post Mortem: The Post Office Horizon IT Scandal*. London: Private Eye Productions.

A STUDY OF CHARACTER VS CAPABILITY: THE KISSCAM VIRAL VIDEO

by Chris Tucker

The Astronomer "kisscam" crisis of July 2025 serves as a modern, high-speed case study in crisis communication, showcasing how what could be seen as a private moment became viral and went on to trigger a boardroom crisis. The incident involved the CEO and Chief People Officer (CPO) of data tech company Astronomer being caught in an intimate moment at a Coldplay concert. There are lessons to be learnt from this crisis both in terms of preparation and creativity when the company made a surprising decision around how to handle the fall-out.

On Tuesday 15 July 2025, at a Coldplay concert in Foxborough, Massachusetts, a "kisscam" segment featured Astronomer CEO Andy Byron and CPO Kristin Cabot in a seemingly intimate embrace. Upon realising they were on the big screen and visible to the audience, both individuals appeared startled, with Cabot covering her face and turning away, while Coldplay frontman Chris Martin laughingly quipped: *"Either they're having an affair or they're just very shy."*

The video went viral on social media immediately and it did not take long for online users to identify the pair. Within days, both executives resigned following a "formal investigation" by the company.

An obvious lesson for senior leadership teams in this crisis is the necessity of clear, enforced disclosure policies for romantic relationships, particularly among senior leadership. There was power imbalance too between a CEO and a CPO that raises ethical concerns regarding workplace relationships and reporting structures.

Within days, the Astronomer board had placed both executives on leave and then accepted resignations to show accountability. Interim CEO Pete DeJoy used LinkedIn to address the situation directly, acknowledging the "surreal" attention while emphasising company values and continuity. Crisis communicators know that persuading organisations to prepare for crises involving senior executives' misdemeanours is often very difficult.

It is therefore to Astronomer's credit that the company was able to move relatively quickly.

In an audacious and creative move, Astronomer partnered with Maximum Effort (Ryan Reynolds' agency) to create a satirical video campaign, featuring Gwyneth Paltrow as a "temporary spokesperson". In the video, Paltrow turned questions about the incident into opportunities to sell the Astronomer product story. In this way, the company owned the humour of the event and turned the infamy into a brand-building moment. Crises are challenging strategic events when the senior management team are to an extent "flying blind". Being able to be creative in a situation where there is no real guide to actions can bring dividends.

The Astronomer case illustrates that reputational crises no longer require operational failure, financial misconduct or regulatory breach. Instead, they can emerge from perceived cultural missteps, visual content detached from context, leadership optics and rapid narrative construction online. Stakeholders increasingly judge organisations not only on compliance but on tone, judgement and symbolic behaviour. Organisations should scenario-plan for "optics events" – moments that are technically benign but reputationally sensitive. The reputation of the sector has been hugely damaged.

BACK TO PAGE 29

GRENFELL: AN INDUSTRY CHANGED

by Dan Gerrella

The Grenfell Tower fire on 14 June 2017 involved the tragic loss of 72 lives. It exposed deep failures throughout the construction sector, from planning and design to the maintenance and operation of buildings. It kickstarted a deep review of the sector. Nine years later, the story remains unfinished. Criminal investigations are still underway. The government is working through the public inquiry's recommendations. People are still living in high rise buildings with unsafe cladding. The reputation of the sector has been hugely damaged.

Why it has been such a defining crisis

Crises can be magnified and exacerbated by a combination of triggers when an organisation (or individuals within it):

- Does something wrong; or
- Is cross-contaminated by a problem elsewhere in the industry; or
- Is impacted by an issue affecting wider society.

Grenfell resonated because it combined all three trigger categories:

- It involved product failures, staff competency issues, misleading marketing information and poor ethical behaviour from organisations involved.
- The industry was questioned, with product manufacturers, consultants, contractors and building operators coming under scrutiny.
- The social background of people living in the tower was deemed to be a factor – complaints raised before the fire were ignored by the local authority.

When determining risk, boards often focus on the first trigger. However, the other triggers hugely influence perceptions, including how issues are reported by media. This contextual understanding must guide a crisis response if organisations are to emerge with their reputations intact.

Boards must regularly review their risk register with this in mind. Many potential threats can be identified in advance. Issues should be prioritised by likelihood and impact. Note that this is not a static exercise – the operating environment will change.

Leadership teams can then work to mitigate risks long before a potential crisis hits. Examples include refining organisational policies, implementing staff training, investing in business operations and building key stakeholder relationships.

Grenfell is an example of an all-encompassing crisis. It has proved to be exceptionally demanding for boards, requiring them to challenge the competency of their teams, the robustness of their processes and their interactions with stakeholders. They have had to contend with a public inquiry and new legislation. All this, against a wider context where survivors and the bereaved are seeking justice.

Communication failings

There are many lessons senior leadership teams can learn from Grenfell. Communication is one example.

A core principle of crisis communication is for organisations to take responsibility for their part in the crisis, readily acknowledge any failings and commit to ensuring that such failings will not happen again. Above all, organisations must express and demonstrate empathy and sympathy for victims and those affected by the crisis.

However, in Grenfell, product manufacturers were defensive from the start, denying problems or deflecting blame. For many involved in the tower's refurbishment, a holding approach was taken while facts were established. It meant no acknowledgement of the victims and created confusion about the potential causes and risks to others in similar buildings.

A criticism of many organisations involved was that their communications were often vague and misleading and hidden behind technical detail. This is no defence at any time, and especially not when so many lives were lost and otherwise affected.

While 2027 will mark the 10-year anniversary of the tragedy, many of the organisations involved, survivors and the bereaved remain in limbo. A Metropolitan Police investigation is still underway. Many implicated in the public inquiry's final report[8] have never formally apologised, or even publicly acknowledged it. This communications vacuum further damages the credibility of the organisations concerned.

Organisations that take accountability are in a better position to move forward strongly. Boards must help their organisations to communicate openly, acknowledge past failures and commit to measurable change.

BACK TO PAGE 37

[8] https://webarchive.nationalarchives.gov.uk/ukgwa/20250320032754/https:/www.grenfelltowerinquiry.org.uk/phase-2-report

CRISIS PREPAREDNESS AT HEATHROW

by Sara Naylor

Heathrow Airport was shut down for 18 hours in March 2025 when a fire at a nearby electrical substation knocked out its power supply and stranded around 200,000 passengers.

News spreads just as rapidly as fire in this age of instant communication. Passengers quickly took to social media and the mainstream media rapidly reflected their anxiety and concerns.

Subsequent formal inquiries into the cause determined that it was the energy infrastructure that failed and was not Heathrow's fault.

However, it did little to restore Heathrow's reputation with the travelling public, particularly as the airport's review noted that the CEO admitted sleeping through efforts to contact him as the crisis unfolded. His phone was on silent and he was unaware until 6am the following day.

The airport review recommended Heathrow consider options for notifying key individuals via a second means of contact. For crisis communications professionals, this recommendation strikes at the heart of questions about Heathrow's state of crisis preparedness and whether adequate steps were taken to ready its team from board to floor for a range of scenarios.

The crisis points to the need to have extensive and rigorous crisis preparedness rooted firmly in an appropriately scoped risk assessment that extends to critical third-party suppliers. And also, for the process to be repeated as often as is necessary for risks to be kept under review and reflected in planning.

Crisis preparedness done well includes live simulations, which means the guidance and planning in place is tested in as near real-world conditions as is possible, including out-of-hours.

Crisis communications specialists were virtually unanimous in their view that however unfair it might seem, leaders should accept that the perception damage which occurs in the initial phase lingers and may become an index for future exceptional events or crises.

An advantage of the rapidity of the news cycle these days is that a crisis might be overtaken quickly by fresh events driven by the pace of reporting in the digital age.

However, this is outweighed by the indelible nature of digital news which lasts indefinitely, which means it will remain in perpetuity for all to see and recall in exact detail. The ease of retrieving it also means that it is more likely to cross from news to other media formats, such as podcasts or documentaries, giving rise to fresh scrutiny and new audiences who can become aware of the crisis.

This is a step-change from analogue days when news could be relied upon to fade as quickly as the paper upon which it was printed.

BACK TO PAGE 37

THE 2024 VALENCIA FLOODS

by Chris Tucker

Spain has the fourth largest economy in the European Union and between the 12th and 14th largest in the world. So how do we explain the loss of 229 lives in the Valencia floods of October 2024? With changing weather patterns such disasters can no longer be thought to occur only in the developing world.

The floods in Valencia were the result of what the locals call a Gota Fria (or Depresión Aislada en Niveles Altos, Isolated Depression at High Altitudes or DANA), which is caused by the sea temperature remaining warm but the air on land falling rapidly as summer ends. Some years, the Gota Fria and accompanying heavy rainfall is worse than others and it was certainly bad in October 2024. In some Valencian areas, a year's worth of rain fell in just eight hours. Spain's National State Meteorological Agency (AEMET) says in the Chica area of Valencia an incredible 491 litres per square metre accumulated in eight hours.

This extreme weather front plunged the Spanish Valencian region into scenes you would expect to see in an end-of-days movie. People were left trapped in their homes, cars were swept away and bridges collapsed under the force of the water.

There are two important lessons to learn.

Sounding the alarm

A severe weather warning was not sounded until 8.00pm on the fateful day although the forecasts from official sources about the heavy rain were easily available much earlier: the flooding was well underway by 5.00pm.

Valencia's regional government admitted it only sent out text messages warning residents of the catastrophe eight hours after floods were first reported and 10 hours after AEMET issued a warning about "extreme danger" in the region.

Spain, in line with many nations, now operates a mobile phone messaging system in the event of emergencies such as this. Why there was such a delay in activating the warning will need to be looked at closely. There clearly needs to be a better interface between those with the scientific knowledge to understand the weather trends and those with the channels to warn those who will be impacted. There is clearly also a role for regular crisis simulations.

Building resilience

But it is not just the timing of the alarm. There is more to be done in advising people what to do in circumstances such as these. Speaking to the Valencian regional newspaper, a Professor of Hydraulic Engineering and the Environment warned of a phenomenon that only occurs in this type of catastrophe in the "First World": namely, 60% of deaths are related to vehicles.

People believe that taking to their cars and escaping the rising water is the best response. But in circumstances such as this, the water rises too high, too quickly, leaving drivers and passengers trapped in their vehicles.

Clearly what is needed is much more awareness among people as to the correct course of action to take in circumstances such as these. Drills and practices would help considerably not just to prepare people but help them appreciate that disasters such as this do sadly also affect Western Europe, not just the Third World.

BACK TO PAGE 42

STORM KRISTIN

by Philippe Borremans

Storm Kristin struck Portugal's central coast on 28 January 2026, with winds reaching up to 209 km/h. As the most damaging storm in the country's recorded history[9] it resulted in significant casualties, nearly one million power outages and total economic losses exceeding at €6 billion, representing more than 1.6% of Portugal's GDP in 2026. While the government responded with a substantial €2.5 billion recovery package, the event exposed a critical "last-mile" failure in crisis communication.

At the national level, the initial response was exemplary. The meteorological institute tracked the system early and named it "Kristin" on 27 January, providing a concrete threat for the public to reference. Civil Protection elevated readiness to maximum levels, 34,000 personnel were deployed and SMS alerts reached millions. Furthermore, official messaging strategically credited early warnings and responsible public behaviour for mitigating harm, a move designed to reinforce trust and future compliance.

However, significant weaknesses emerged in the transition from information to action. While alerts were delivered, they were primarily descriptive rather than prescriptive. Recipients were often directed to websites featuring technical maps and wind thresholds rather than receiving clear, behavioural instructions. In high-stress environments, citizens should not be required to interpret complex data; instead, warning systems must provide concise checklists – such as securing loose objects, charging devices and storing water – to facilitate immediate response.

The most profound failure occurred in the post-impact phase. As power and mobile networks collapsed, the digital-first communication architecture became irrelevant. During the critical days following the storm, when residents required updates on safety, water access and restoration timelines, official channels were effectively inaccessible.

In rural areas, this resulted in a total information vacuum. Many communities, including São Silvestre, saw no official presence for six days. In the absence of formal support, the "first responders" were neighbours who organised chainsaw crews, shared generators and checked on the vulnerable. Local nodes, such as petrol stations and cafés with backup power, became the default information hubs. A brief, daily visit from an official to these gathering points could have provided verified updates and collected vital intelligence, yet this opportunity was missed.

This gap is structurally predictable. Operational triage prioritises high-population corridors, and command structures often report progress in broad aggregates that offer no clarity to isolated villages. When digital networks fail, the lack of symbolic official presence creates a narrative of abandonment.

To bridge this gap, crisis communication must evolve. Warnings should be explicitly actionable, and authorities must plan for analogue delivery – such as parish-level contact trees and physical notice boards – when technology fails. Finally, emergency systems should measure "time without official contact" as a key performance metric. Kristin demonstrated that while early warnings can be technically excellent, they remain incomplete if they fail to reach the last mile.

BACK TO PAGE 46

[9] https://www.perplexity.ai/search/cb6a8026-995d-4028-9164-d6cf3f3deef6#0

SPECIAL FEATURES

THE IMPORTANCE OF HORIZON SCANNING AS PART OF RISK MITIGATION AND MANAGEMENT

by Farzana Baduel

Before there were boardrooms, there was the savannah. Our ancestors survived not because they were the strongest, but because they looked up. They scanned the horizon for predators, shifting weather and enemy tribes. Survival depended on pattern recognition, on spotting movement in the grass before it was too late.

Horizon scanning is not a modern management fad. It is instinct. Yet in today's corporate landscape, despite unprecedented volatility, many organisations have lost it. We are flooded with data yet lack foresight. We monitor dashboards obsessively during crisis, but too often they measure what has already happened. True risk mitigation begins earlier. It begins by looking ahead.

In the crisis lifecycle, mitigation and preparation are the stages that matter most. Once a crisis is live, options narrow. Reputation and confidence erode quickly. Horizon scanning is the discipline that widens your options before events force your hand.

It has never been more important. Communication channels are fragmented and instantaneous. A single post can ricochet globally within minutes. Global supply chains, once optimised for efficiency, are now exposed to geopolitical shock. We are moving from a largely unipolar world to a multipolar one, with intensifying competition between the United States and China reshaping trade, technology and alliances.

Regulatory and diplomatic norms are disintegrating at pace. Restrictions on materials, energy and components are becoming more frequent. What was once a niche geopolitical risk is now a board-level concern across sectors.

Organisations that fail to scan the horizon risk strategic whiplash: reacting late, pivoting under pressure, or watching competitors move first. Boards can become consumed by quarterly pressures while structural risks build slowly in the background: demographic shifts, regulatory change, geopolitical realignment.

Horizon scanning restores perspective. It requires disciplined curiosity: looking beyond your sector, beyond your geography, beyond your immediate competitors. What disrupts a fast-moving sector today will often reshape a slower one tomorrow. Competitor analysis must be paired with cross-sector awareness. What are technology firms seeing? What regulatory trends are emerging in adjacent markets? Where are consumer expectations shifting?

Importantly, horizon scanning is not solely about threat detection. Organisations that scan only for downsides miss half the picture. Regulatory change can create first-mover advantage. Geopolitical realignment can open new markets. Technological disruption can reduce cost or unlock innovation. Risk mitigation and opportunity capture are two sides of the same discipline.

The question, then, is not whether to horizon scan, but how to institutionalise it.

First, it must be integrated into governance structures. Risk registers should be segmented by time horizon: short term (zero to twelve months), medium term (one to three years), and long term (three to ten years). This prevents boards from conflating operational risks with structural shifts. Each horizon demands different indicators and strategic responses.

Second, horizon scanning should be embedded into annual board strategy days through structured workshops. Boards can construct plausible future scenarios: escalation in trade tensions, accelerated AI regulation, prolonged stagnation, demographic contraction in key markets. For each imagined future, identify the catalysts that would make it more likely. Then ask: what would we need in place today to reduce risk and capitalise on opportunity if this future materialises? This transforms foresight into preparation.

Third, horizon scanning must be continuous. Boards should consider dashboards tracking forward indicators: economic projections, demographic trends, geopolitical developments, supply chain vulnerabilities and regulatory shifts. Listening tools can monitor emerging narratives, misinformation and disinformation threats. In an era where reputational crises can be engineered or amplified, information risk is strategic risk.

Communications professionals have a critical role here. Trained in risk analysis and trend interpretation, they bring an external lens that complements financial and operational expertise. They understand narrative velocity, stakeholder sentiment and the catalysts that turn issue into crisis. Boards should harness this expertise explicitly.

Board composition also matters. Diverse professional backgrounds and lived experiences expand the field of vision. A homogenous board scans from a single vantage point; a diverse board sees in 360 degrees.

Finally, horizon scanning deserves a formal home. Risk committees should include it as a standing agenda item. Making space for it signals seriousness. It shifts culture from reactive to anticipatory

The savannah taught us a simple lesson: those who look up survive. In today's volatile landscape, organisations that fail to scan the horizon risk being surprised by forces that were visible, just not to them. Mitigation and preparation are not defensive acts. They are strategic advantages.

The horizon is always moving. The question is whether you are watching it.

BACK TO PAGE 22

CYBERSECURITY RISK: BOARD OVERSIGHT AND THE ROLE OF STRATEGIC COMMUNICATIONS

by Chris Tucker

Cybersecurity is now a standing board-level risk rather than a technical issue delegated solely to IT. With cyber incidents occurring at scale, and with increasing sophistication, organisations must assume that attacks are not a question of 'if' but 'when'. The board's role is therefore to ensure the organisation is prepared to prevent, withstand and recover from cyber incidents, including the reputational consequences that inevitably follow.

Digital systems underpin almost all organisational activity, from the protection of personal data and intellectual property to financial operations and supply chains. A cyber-attack can disrupt operations, trigger regulatory intervention, damage stakeholder trust and materially affect organisational value. For these reasons, cybersecurity must be treated as a strategic and reputational risk, requiring oversight that extends beyond technology to include legal, regulatory and communications capability.

Boards should satisfy themselves that the organisation has experienced, and learned from, previous cyber incidents, however minor. A clear understanding of historical attacks, near-misses and vulnerabilities provides insight into organisational resilience. The board should also ensure that there is a robust, tested cyber incident response plan in place, and that this plan integrates communication alongside IT, legal, risk and compliance functions. Cyber insurance may form part of the organisation's risk transfer strategy, and boards should understand whether such policies include access to specialist crisis communication support and under what conditions it may be deployed.

Third-party and supply chain risk requires particular board attention. A growing proportion of cyber incidents originate through suppliers with weaker controls. Boards should seek assurance that supplier due diligence, contractual obligations and ongoing monitoring reflect the organisation's own cybersecurity standards. Organisational resilience is only as strong as its weakest external dependency.

Cyber incidents as reputational events

From a board perspective, it is critical to recognise that cyber incidents rapidly become public-facing crises. Data breaches, ransomware attacks and system outages attract intense scrutiny from regulators, the media, customers and investors. In ransomware cases, threat actors may deliberately seek publicity to increase pressure on organisations to comply with demands. Boards should note that UK government guidance, via the National Cyber Security Centre, is clear that ransom payments should not be made.

Regulatory obligations add urgency to decision-making. UK organisations must notify the Information Commissioner's Office within 72 hours of becoming aware of a personal data breach where there is a risk to individuals' rights and freedoms. This requirement applies even where investigations are ongoing, placing pressure on organisations to communicate before all facts are known. Boards must therefore ensure that management is equipped to meet both regulatory and reputational expectations simultaneously.

Evidence from high-profile incidents consistently shows that reputational damage is driven as much by poor communication as by the breach itself. Delays, inconsistent messaging or perceived evasiveness can significantly amplify harm. Cybersecurity should therefore be overseen as a strategic risk, with communications capability embedded into cyber preparedness rather than activated reactively.

The board's interest in communications-led risk mitigation

Effective communication reduces cyber risk before an incident occurs. Boards should expect management to demonstrate how internal communications support cyber awareness, employee responsibility and escalation protocols. Human error remains a leading cause of cyber incidents, and behavioural risk cannot be mitigated through technology alone.

Boards should also be aware of the growing role of artificial intelligence in cybercrime. AI is being used to enhance social engineering attacks, including sophisticated executive impersonation through voice cloning. These types of deepfake attacks which have tricked employees into, for example, transferring large sums of money have already resulted in significant financial losses for organisations. This development reinforces the need for robust internal verification processes and clear communication protocols, particularly around financial authority and urgency.[1]

Communications teams should be involved in cyber scenario planning and simulations. Boards should seek assurance that cyber exercises test not only technical response but also decision-making, stakeholder communication and media handling. Prepared holding statements, Q&A materials and escalation frameworks reduce risk during the early stages of an incident.

Board expectations during a cyber incident

In the event of a cyber breach, the board should expect management to prioritise speed, clarity and credibility in communication. While forensic investigations may take weeks or months, stakeholder expectations are immediate. Early acknowledgement, consistent messaging and clear articulation of next steps are critical to maintaining trust.[2]

Boards should be alert to the tension between speed and accuracy. Over-reassurance or premature conclusions can damage credibility if later disclosures contradict initial statements. Communications professionals play a key role in managing this balance, ensuring communication is factual, empathetic and aligned with legal and regulatory obligations.

Media management is also a governance issue. Silence creates a vacuum that will be filled by external commentary. Boards should be confident that the organisation has the capability and authority to engage proactively with the media and other stakeholders during a cyber incident.

Recovery, assurance and learning

The board's role does not end when systems are restored. Post-incident communication is essential in rebuilding trust and demonstrating organisational learning. Boards should expect transparent communication with stakeholders about remediation, governance improvements and strengthened controls.

In the longer term, effective post-incident communication supports reputational recovery and reinforces confidence in board oversight. Organisations that communicate clearly about lessons learned are better positioned to retain trust than those that limit disclosure. A report published by the British Library,[3] a recent cybercrime victim, on its recovery and lessons learned process is a good example.

In summary, cybersecurity is a material board-level risk with significant reputational implications. Strong governance requires that communication capability is integrated into cyber risk management, tested in advance, and activated decisively when incidents occur.

BACK TO PAGE 43

1 For more information on the impact of AI and deepfakes on cybercrime, note the 2026 report 'Data Breach Industry Forecast' from credit scoring agency, Experian. https://images.go.experian.com/Web/ExperianInformationSolutionsInc/%7B912d6768-8707-4986-9631-17ade0634ece%7D_FY26-Q3-2026-Data-Breach-Industry-Forecast_1e.pdf?cmpid=qrcode
2 An example of an initial statement can be found at page 116.
3 https://www.bl.uk/stories/blogs/posts/learning-lessons-from-the-cyber-attack

AI AND GOVERNANCE: CRISIS COMMUNICATION IN THE AGE OF ALGORITHMIC DECISION MAKING

by Philippe Borremans

AI as both weapon and weakness

Boards now face a dual challenge from artificial intelligence. Reputational threats emerge from two directions: when internal AI systems fail, and when external AI is weaponised against the organisation. Deepfakes of executives and AI-generated misinformation campaigns create crises that boards never initiated but must manage. Strategic crisis communication requires preparing for AI as both an internal vulnerability and an external threat.

The explainability gap

AI crises differ from traditional corporate failures because they often defy simple explanation. When stakeholders ask why an algorithm made a discriminatory decision or if a viral video of your CEO is authentic, straightforward answers may not exist. Admitting "we don't fully understand why our system did this" can destroy confidence exactly when you need to provide reassurance.

This paradox means boards must think about AI communication long before a crisis hits. Organisations that navigate these moments successfully build communication resilience as deliberately as they build technical firewalls. Crisis communication is not an afterthought to AI governance; it is a core part of it.

Stage 1: Mitigation through narrative control

Strategic mitigation starts with owning the story. Boards must ensure their organisations set clear public positions on AI use and threats before an incident forces a reactive explanation. A company with a visible track record of responsible AI use enters a crisis with far more credibility than one that stayed silent until it was forced to speak.

This foundation requires consistent work through annual reports, stakeholder briefings and transparency initiatives. When stakeholders already understand your AI principles and the safeguards you have in place, crisis communication builds on established trust rather than trying to create it under pressure.

Equally important is educating your stakeholders about AI threats. Public understanding of deepfakes and algorithmic bias is still low. Organisations that proactively explain these risks to their audiences are in a much stronger position when an incident occurs. The choice is simple: invest in this groundwork during peacetime or pay a much higher price during a crisis.

Stage 2: Preparing for dual threats

Crisis planning must address two distinct AI categories, each requiring a different approach.

Internal AI failures, such as algorithmic discrimination or safety failures, require communication centred on accountability and fixes. The board's role is to ensure the organisation can move quickly from the incident to a credible explanation and then to action. This requires "pre-positioned" tools:

- Holding statements drafted before a crisis occurs
- Notification protocols that balance legal duties with reputational needs
- Experts who can translate complex algorithmic failures into plain language for non-technical audiences

External AI attacks, like deepfakes or manipulated media, require strategies centred on verification and rapid response. A deepfake can reach millions of people in hours; a response process that takes days is useless. Boards must ensure the organisation has both the technical tools to verify content and the authorisation to speak at the speed of social media, not the speed of a traditional committee.

This is an uneven fight. Creating a convincing deepfake takes very little time or money. Debunking one requires technical analysis and legal review. If you wait for perfect information before responding, you lose control of the narrative. Boards must be comfortable with communication strategies that prioritise speed and directness over exhaustive certainty.

Strategic decisions that cannot be delegated

When an AI crisis occurs, the board must make several calls that cannot be left to management alone.

First is tone-setting. The board must decide if a crisis needs board-level visibility or can be handled by executives. Board involvement signals that the issue is existential; its absence can suggest either confidence or negligence.

Second is accountability framing. For internal failures, stakeholders expect the board to own the governance failure, not offer technical excuses. For external attacks, boards must show the organisation is defended without looking vulnerable. This framing determines whether you are seen as a victim, a perpetrator, or a responsible leader.

Finally, boards must manage the narrative timeline. AI crises rarely end quickly. One statement is never enough. Communication strategies must cover the full lifecycle: the immediate response, investigation updates and the long-term work of rebuilding trust.

Communication as governance

The gap between AI governance and crisis communication is closing. Effective governance requires being transparent about how you use AI. Effective crisis communication requires governance structures that allow you to respond quickly and credibly. Organisations that integrate these two functions, with active board oversight, build the resilience they need, whether the threat comes from an internal error or an external attack.

For boards, the question is not if you will face an AI-related communication crisis, but whether your preparation will limit the damage or make it worse. That decision is made in the months of preparation that happen now.

BACK TO PAGE 24

AI AND REPUTATION

by Ben Verinder

Artificial intelligence offers the communications function, and the organisations it serves, increased efficiency and new capabilities. AI can be fantastically useful in supporting crisis communication, improving the rigour of planning, the speed of response and the depth and breadth of analysis as to the impact of a public difficulty on an organisation's reputation and relationships.

But AI has broader implications for crisis and issues management. It is changing how organisations operate, structure themselves and interact with the outside world. These changes, if handled poorly, come with considerable reputational risk. It is the domain of the communications function to help mitigate that risk and handle issues if and when mitigation fails.

Here I am going to explore just three of the many areas in which AI deployment by an organisation can lead to public difficulty.

Hallucination

The term 'hallucination' refers to the generation of false or misleading information by an AI system that presents that information as factual. It is not a 'bug', but a consequence of the data and algorithms used to train and operate a model.

Failure to understand the nature of hallucinations and their prevalence, and to put systems in place to minimise them, can cause organisations (sometimes significant) reputational damage. It can lead to them making important decisions based on false information which in turn erodes stakeholder trust, disrupts operations and can even lead to regulatory or legal intervention.

In 2023, for instance, US law firm Levidow, Levidow & Oberman was fined $5,000 by a Manhattan judge after one of its employees, Steven Schwartz, cited hallucinated legal cases in a court filing after using ChatGPT. It was the first of hundreds of cases in which North American law firms have been caught out by AI hallucination.

In late 2025, and closer to home, West Midlands Police submitted an intelligence report to support banning Maccabi Tel Aviv fans from the Europa League match at Aston Villa.

But that report included events hallucinated by Microsoft Copilot. The incident led to an investigation by His Majesty's Inspector of Constabulary that the Home Secretary described as 'damning' and the resignation of the West Midlands Chief Constable.

While hallucination rates in large language models have been in decline over the past two years, we are likely to see a new spike in rates as users of large language models like ChatGPT, Copilot, Claude and Gemini make ever more sophisticated demands of the models. Agentic AI, which coordinates actions among systems and agents, can also boost the risk and cost of hallucinations if errors are propagated across workflows.

One of the most effective ways to minimise the risk of hallucination is training – to understand the risks, the data on which a model has been trained (and thus its limitations) and the best ways to 'prompt' or instruct a model, such as asking for citations as standard and avoiding leading questions.

The challenge for organisations – and for their communications function or agency – is that most people using AI in the workplace have not been trained on how to do so safely. Addressing this shortfall, I would argue, is a key role of modern governance.

Unacceptable use

As a new and emerging technology, our views of AI are in flux, and they are not necessarily consistent or rational. For instance, according to research undertaken by the Ada Lovelace and Alan Turing Institutes, the British public considers that the use of AI in personalised advertising is as unacceptable as its deployment in autonomous weaponry.

Organisations risk alienating the people who matter most to them if they use AI without taking account of these emerging attitudes.

In recent months, for instance, McDonald's withdrew a Christmas TV advert in the Netherlands after viewers criticised its quality and appropriateness. Bristol City Council became the latest in a string of local authorities under fire from designers, on the grounds that the technology is hurting the creative industries, for using AI in marketing materials.

Last summer, a Daily Mail investigation revealed how some estate agencies are using AI software to add furniture to empty rooms, brighten lighting and even fill properties with non-existent contents, and in doing so risk angering buyers and tenants.

There is a huge 'boundary spanning' role for communications professionals here in support of boards and the executive in researching the awareness, attitudes and behaviours of stakeholders and publics through secondary and primary research, and in working with leadership to ensure that this research helps shape the organisation's AI policies and procedures.

Illegal use and regulatory intervention

The estate agencies manipulating images with AI also risk legal intervention. Consumer protection regulations prohibit the use of images that contain false information or deceive average consumers, 'potentially causing them to make transactional decisions they would not otherwise take'.

This is one of many regulatory and legal ramifications of AI use, of which the communications functions, alongside the board and leadership, need to be aware if reputational risk is to be mitigated.

AI notetakers, for instance, proliferate in the UK public and private sector. A UK firm using such a system must have a lawful basis (typically consent or legitimate interests) for processing any voice data collected by it, inform participants before recording starts about what's being captured and why, and ensure recordings are stored securely with clear retention periods. Most companies aren't doing this.

Any AI-generated transcripts or notes created by a public body subject to the Freedom of Information (FOI) Act become 'recorded information' that can be requested by anyone and must be disclosed unless a specific exemption applies.

Accuracy issues with AI transcripts also mean public bodies could face reputational risk if inaccurate records are disclosed under FOI – so they need to review and correct transcripts before they become part of the official record. More broadly, the ways in which a public body uses AI and the decisions made as a result of that usage can also be subject to FOI requests.

Arguments about AI and copyright are being played out in courts around the world, and organisations need to keep abreast of the latest developments in statutory and case law in the jurisdictions in which they operate. In November last year, the English High Court ruled that the image generation model Stable Diffusion is not ‘infringing copy’ under UK copyright law because it does not contain or store reproductions of images, but this is unlikely to be the last word on the matter.

Independent of the law, using AI tools trained on copyrighted materials without consent may be seen as ethically problematic by stakeholders or a broader public. Actors’ union Equity, for instance, has threatened mass direct action over the use of artists’ images in AI content.

The advisory opportunity

AI risks extend far beyond those set out above. They include data and algorithmic bias, jailbreaking chatbots, breaches of confidence, slop, cognitive offloading and environmental double-standards.

This, in my view, represents a significant new governance and leadership responsibility. It also represents a huge opportunity for communications as the management function responsible for developing and maintaining goodwill and mutual understanding between an organisation and its publics.

If boards, leadership teams and communications professionals do this well, we can help support the responsible and ethical adoption of AI in our societies. In the absence of regulatory intervention, this is, in my view, a vital social good. The question is: will we step up?

BACK TO PAGE 24

MIS/DISINFORMATION

by Shayoni Lynn

Narratives, beliefs and crisis risk

Misinformation and disinformation have become defining risks for organisations operating in today's information environment. For boards, they should now be treated not simply as communications challenges, but as strategic governance risks with the potential to undermine trust, disrupt operations and escalate into full organisational crises.

At its simplest, misinformation refers to false or misleading information shared without intent to deceive, while disinformation is created deliberately to mislead. Malinformation describes genuine information presented selectively or out of context in ways that distort meaning.

In practice, however, these distinctions matter less than the impact on audiences and behaviour. False or misleading narratives can influence public perception, shape stakeholder decisions and trigger real-world consequences, regardless of intent.

For boards responsible for oversight of organisational risk, the central question is not simply whether misinformation exists, but how exposed the organisation is to information threats, and how prepared it is to respond.

The changing risk landscape

Several developments have accelerated the scale and sophistication of misinformation risks:

1. The way people consume information has fundamentally changed. Audiences are no longer simply consumers of information; they are also its creators, distributors and enforcers. Our information environment has transformed dramatically over the past 10-15 years. Social media platforms, encrypted messaging networks and online communities allow narratives to spread rapidly across multiple channels before organisations are even aware they exist.

2. Generative AI and synthetic media are lowering the barriers to creating convincing false content at scale. Deepfakes, manipulated imagery and AI-generated narratives can now be produced quickly and cheaply, increasing the likelihood of targeted information attacks against organisations. This production capability also means our information environment is becoming increasingly artificial, with automated accounts and coordinated networks amplifying narratives and making manipulation harder to detect. For organisations, this means that macro-level signals such as social listening alone are no longer sufficient. Effective monitoring must combine digital analysis with deeper insight into how audiences interpret and respond to information.

3. The velocity of information means that reputational crises now evolve far faster than traditional governance processes were designed to handle. Narratives can move from fringe forums to mainstream media within hours. The critical question is not simply what narratives are circulating, but what beliefs those narratives are creating.

Boards should therefore recognise misinformation as part of a broader information risk environment that intersects with reputation, regulatory scrutiny, operational resilience and stakeholder trust. They should consider how misinformation may shape public understanding, influence behaviour and create tangible risks for organisations and communities.

Beliefs, behaviour and organisational risk

People rarely act directly on information itself. Instead, they act on the beliefs they form about what is true and who is trustworthy. When misleading narratives take hold, they can shape public attitudes, alter stakeholder behaviour and create real-world consequences.

For organisations, this can manifest as declining trust, resistance to policies or services, reputational damage, or activism driven by false claims.

Boards should therefore encourage management teams not only to track narratives, but to understand how those narratives are affecting public beliefs and behaviours. Insight into belief prevalence – how widespread and deeply embedded certain ideas have become – can provide early warning of emerging risks.

Understanding the behavioural dimension of misinformation allows organisations to move beyond reactive crisis response and towards a more strategic approach to information resilience.

Governance responsibilities for boards

Effective governance of misinformation risk requires oversight across three areas:

- Visibility
- Readiness
- Resilience

Boards should ensure these capabilities sit clearly within organisational risk management structures and are supported by defined leadership responsibility.

1 Narrative visibility

Boards should ensure the organisation has the capability to detect emerging information threats. This includes monitoring the wider information environment and understanding how narratives about the organisation or its sector are evolving – and critically, how those narratives may be shaping public beliefs.

Early warning systems that combine digital monitoring with research into manipulation techniques and their impact on audience beliefs can help identify emerging risks before misleading narratives escalate into a crisis.

2 Organisational readiness

Boards should be confident that management teams have the skills, protocols and cross-functional coordination required to respond rapidly to misinformation events.

Management should also have clearly defined escalation procedures so emerging information risks are surfaced quickly to senior leadership and the board where appropriate.

This includes integrating communications, legal and operational leadership into crisis preparedness exercises. In misinformation incidents, the challenge is rarely confined to reputation; it can quickly create regulatory, safety or operational consequences.

3 Information resilience

Boards should also encourage proactive strategies that strengthen organisational resilience to misleading narratives.

Research in behavioural science shows that audiences can develop resistance to misinformation through techniques such as prebunking – exposing people to weakened versions of misleading narratives so they can recognise common manipulation tactics and question them before they take hold. While communications teams often lead these interventions, they should form part of a wider organisational strategy for information integrity and trust.

Ultimately, misinformation becomes a crisis when false narratives are widely believed and begin to influence behaviour.

BACK TO PAGE 24

STRATEGIC COMMUNICATIONS: PROTECTING REPUTATION IN A CRISIS

by Stephen Waddington

The organisations that come through a crisis with their reputation intact have one thing in common: Strategic communications capability was embedded at leadership level before the crisis began. Strategic communications is a governance capability. Its value is determined by the foundations laid well before disruption arrives.

Reputation is a financial asset

In 1975, tangible assets accounted for 83% of the market value of the S&P 500. By the end of 2025, that figure had fallen to 8%.[4] Intangible assets – brand, trust, reputation and stakeholder confidence – now represent 92% of market capitalisation. The assets that dominate corporate value are precisely the assets strategic communications exists to build, protect and manage.

Two recent studies put numbers on the reputational component of that value. Burson's Global Reputation Economy report estimates that reputation can deliver up to 4.78% additional annual shareholder return, producing a global figure of $7.07 trillion in reputation-linked value.[5] Echo Research finds that 28% of FTSE 350 market value, £841 billion, is attributable to reputation.[6] Both studies identify governance, leadership and workplace culture as the primary drivers. All three are domains where strategic communications plays a direct role.

Reputation risk is financial risk. It belongs on the board agenda alongside legal, operational and regulatory exposure.

What strategic communications brings to a crisis

Three capabilities distinguish organisations with strong strategic communications from those without it. All three matter most when they have been built well before any crisis emerges.

The first is environmental intelligence. The most effective communications functions operate as intelligence systems. They gather signals from stakeholders and the external environment, interpret them through evidence and judgement, and feed that intelligence into leadership before positions harden and decisions are made.

This is what allows an organisation to identify an emerging issue – the story gathering momentum, the stakeholder relationship under strain, the regulatory pressure building – while there is still time to act on it. Boards that receive this intelligence regularly make better-informed decisions. Boards that receive it only once the crisis has broken are already managing consequences.

---

[4] Ocean Tomo, *Intangible Asset Market Value Study* (2025), Chicago: Ocean Tomo.
[5] Burson, *The Global Reputation Economy: A New Asset Class for a New Era* (2025), New York: Burson.
[6] Echo Research, *UK Reputation Valuation Report 2026* (2026), London: Echo Research.

The second is stakeholder relationship management. Trust is built through sustained, honest engagement with employees, customers, investors, regulators and communities, and its value becomes apparent when things go wrong. Stakeholders who know an organisation, who have experienced its transparency in normal times, are more likely to extend goodwill in difficult ones.

This is reputational infrastructure. It is as important to organisational resilience as financial reserves or operational contingency plans.

The third is narrative coherence. In a crisis, what an organisation says and what it does must be consistent, and both must reflect its stated values. Inconsistency between the board's public position and the organisation's behaviour, or between messages directed at different audiences, compounds reputational damage faster than almost anything else.

Communications practitioners embedded in leadership decision-making ensure the organisation speaks with a single credible voice from the outset. They also provide something harder to find: an honest account of the gap between what leadership believes is happening and how it will be perceived externally. That perspective is frequently absent when communication sits outside the room.

It also means knowing when to hold back. Strategic restraint is itself a communications capability.[7] It is often the right call in the early stages of a crisis, when the facts are still emerging and premature statements create more exposure than they resolve.

Speed, clarity and control

Organisations that manage crises well move faster and communicate more clearly. This is preparation.

When communications practitioners have been part of risk planning, when protocols have been established and rehearsed, when stakeholder contacts are current and key messages exist for foreseeable scenarios: the organisation responds with speed and authority. The first hours of a crisis are the most consequential for long-term reputational outcomes. Speed, accuracy and spokesperson credibility shape public and stakeholder perception in ways that are very difficult to reverse.

That preparation requires the communications leader to understand the organisation's risk landscape in depth, to be present in the conversations where risks are assessed, and to have the authority to act when the moment demands it. It depends on communications being treated as a management discipline with a standing place in strategic decision-making.

Influence follows proximity to power

Research into how communications advice actually shapes crisis decisions confirms what experienced practitioners already know.

A study of senior crisis consultants published in *The Journal of Contingencies and Crisis Management* in February 2026 finds a clear and consistent pattern.[8] Communications practitioners included in the crisis management team play a strategic role helping shape how the organisation responds. Those working only within the communications function implement decisions made by others.

The study also identifies what makes communications advice most likely to be acted on. Long-standing trust between communications leaders and senior colleagues matters. Evidence-based recommendations carry more weight than instinct. And, critically, advice framed in terms of business risk, legal exposure or financial consequence is far more persuasive than advice framed in communications terms alone.

Speaking the language of management is a substantive choice. It is what determines whether communications counsel shapes a decision or is noted and set aside.

[7] Hoffjann, O., *Corporate Communications: An International Journal* (2025), 'Strategic non-talking: forms and functions of deliberate silence in corporate communications'.
[8] Balliu, L. and Claeys, A-S., *Journal of Contingencies and Crisis Management* (2026), 'Do communication consultants have management's ear? An exploration of how external public relations practitioners increase their influence on crisis communication decisions', 34, e70136.

The role of the board

Boards set the conditions that determine how well their organisation manages reputational risk. The most consequential of those conditions is whether strategic communications expertise sits inside the leadership team or outside it.

The research evidence is unambiguous. The senior communications leader should report or have direct access to the chief executive, with consistent access to board-level discussion.[9, 10, 11] A communications leader present in a strategic decision can protect the organisation's reputation in ways that one informed of it afterwards cannot.

A fifth of FTSE 100 companies either outsource the senior communications function or distribute responsibilities across other roles.[12] In an environment where political and regulatory risk directly influences enterprise value, that is a governance gap with material consequences.

Four questions test board readiness. Do the most senior communications practitioners have a standing place at the leadership table? Do they contribute to risk and strategy discussions as a matter of routine? Has the crisis communications plan been tested, and has the board reviewed it? Are the stakeholder relationships that would matter most in a crisis being actively maintained?[13]

Where the answer to any of these is no, the organisation is carrying reputational risk that is within its power to reduce.

Making the case for investment

The evidence base for the financial value of reputation has never been stronger. It is measurable. The dimensions that drive it (governance, leadership, workplace culture, products, innovation, financial performance) are consistent across multiple independent valuation frameworks.[14, 15] The financial consequences of reputational damage are well documented: regulatory exposure, legal liability, customer attrition, reduced investor confidence and long-term erosion of brand value.

Organisations with communications expertise embedded at leadership level contain crises more quickly, sustain greater stakeholder confidence during disruption and recover more completely in the aftermath. The cost of crisis mismanagement consistently exceeds the cost of the capability that prevents it.

Strategic communications is a risk management investment whose return is most visible, and most valued, precisely when it is most needed.

---

[9] Grunig, L. A., Grunig, J. E. and Dozier, D. M., *Lawrence Erlbaum Associates* (2002), Excellent Public Relations and Effective Organizations, Mahwah, NJ.
[10] Bowen, S. A., *Journal of Applied Communication Research* (2009), 'What communication professionals tell us regarding dominant coalition access and gaining membership', 37(4), pp. 418-443.
[11] White, J. and Dozier, D. M., in Grunig, J. E. (ed.) *Excellence in Public Relations and Communication Management, Lawrence Erlbaum Associates* (1992), 'Public relations and management decision making', Hillsdale, NJ, pp. 91–108.
[12] Ithaca Partners, *Chief Communications / Corporate Affairs Officer Turnover Study 2026*, (2026), London: Ithaca Partners.
[13] Chartered Institute of Public Relations, *State of the Profession 2024*, (2024), London: CIPR.
[14] Tench, R., Verčič, D., Zerfass, A., Moreno, A. and Verhoeven, P., Palgrave Macmillan, (2017), *Communication Excellence*, Cham.
[15] Zerfass, A., Moreno, A., Tench, R., Verčič, D. and Verhoeven, P., EUPRERA/EACD, (2023), *European Communication Monitor 2023*, Brussels.

Capability	What it delivers in a crisis
Environmental intelligence	Early identification of emerging issues while there is still time to act on them.
Stakeholder relationships	Pre-existing trust that provides resilience and goodwill when the organisation needs it most.
Narrative coherence	A single, credible organisational voice including the discipline to know when restraint is the right call.
Crisis preparation	Protocols, messages and contacts established in advance, enabling speed and authority at the moment of impact.
Leadership integration	A communications perspective inside strategic decision-making, framed in the language of risk and consequence that boards act on.

Table: Strategic communications capabilities and their value in crisis management (author's synthesis drawing on Grunig et al. 2002 and Tench et al. 2017)

BACK TO PAGE 27

THE INTERPLAY BETWEEN REPUTATION AND RELATIONSHIPS

by Dr. W. Timothy Coombs

Crises are disruptions to organisational strategy, relationships with stakeholders and, in some situations, even operations. Strategy is disrupted as attention shifts to managing the crisis and often will disrupt operations such as when a product must be recalled because it is harmful or a facility is damaged by an accident. Crises disrupt relationships with critical stakeholders including customers, employees and investors. Each of these stakeholders feels the effects of the crisis in some way and that disrupts the organisation-stakeholder relationship. Customers may have concerns about securing a product or service or the safety of a product. Employees have concerns about their wellbeing because of their dependence on and their feeling of connection to the organisation. Investors worry about the effects of the crisis on their financial situations.

Reputation is an accepted indicator of the health of the organisation-stakeholder relationship. Reputation has been proven to be a valuable, intangible asset for organisations. A reputation is a social evaluation meaning it reflects how stakeholders perceive an organisation. A core element of reputation is the trust the stakeholders place in the organisation. The disruption to the organisation-stakeholder relationship is why a crisis inflicts reputational damage upon an organisation. The crisis causes stakeholders to re-evaluate their relationship with the organisation. They ask themselves questions such as "Can I still trust the organisation?" and "Should I stay connected to this organisation?"

The amount of reputational damage a crisis generates and the level of disruption to the organisation-stakeholder relationship varies by the nature of the crisis. We can group crises into two broad categories: competency and integrity. Competency-based crises involve a failure of someone in the organisation not doing their job or not doing their job properly.

An employee might connect a hose from a chemical delivery to the wrong storage tank causing an explosion from a chemical reaction or an employee improperly cleans the food processing equipment resulting in a foodborne illness pathogen contaminating the food products. Competency-based crises are less disruptive to the organisation-stakeholder relationship. This is due largely to it being relatively easy to address the cause of the problem – employees need to perform their tasks better. Competency-based crises are considered unintentional.

Integrity-based crises involve a moral or ethical violation by the organisation. Examples would be management knowingly shipping a defective or contaminated product or management engaging in irresponsible behaviour for financial or personal gain (aka management misconduct). Integrity violations are viewed as a betrayal of the organisation-stakeholder relationship by stakeholders. Management within the organisation has intentionally violated an accepted moral norm in the relationship. Stakeholders might feel lied to, taken advantage of, or exploited by the organisation. Stakeholders then question the relationship because the organisation has acted in a way inconsistent with the values the stakeholders assumed they shared with the organisation.

That betrayal will be reflected in a commensurate loss of reputational assets – reputational damage from the crisis.

A key difference between competency and integrity-based crises is the perception of intentionality. This intentionality has a significant effect on how the crisis damages the organisation-stakeholder relationship and how the relational damage becomes translated into reputational damage and loss of reputational assets. The perception of intention alters perceptions of the organisation, and those perceptions change how stakeholders engage or choose not to engage in the relationship with the organisation. For instance, consumers might decide to temporarily not buy a product or switch permanently to a competitor.

The crisis becomes an even greater disruption when it has a sociopolitical element to it that feeds into polarization. When the crisis centres on a polarizing concern, such as diversity equity and inclusion (DEI), the threat to the relationship and reputation is intensified. In public opinion polls and industry research, stakeholders (including employees) report they are very likely to end relationships with organisations who support the other side of a polarizing sociopolitical issue. When a crisis highlights an opposing view by the organisation on a sociopolitical issue, there will be greater potential for the relationship to end and for stakeholders to perceive the organisation much more negatively. When a polarizing political dimension is added to a crisis, the disruption to organisation-stakeholder relationship is intensified.

The vitality of an organisation depends greatly on its relationship with customers, employees and investors. Reputations provide an indicator of the quality of the organisation-stakeholder relationship. Moreover, the reputation is a valued asset. Crises threaten reputations because they disrupt the organisation-stakeholder relationship and drain reputational assets from an organisation.

BACK TO PAGE 29

THE IMPORTANCE OF ORGANISATIONAL CULTURE IN PREVENTING AND RESPONDING TO CRISES

by Alison Arnot

Whether they are harmed by a crisis or are working to resolve it, employees experience and respond to the situation differently and more directly than external stakeholders. They have unique crisis needs, expectations and responsibilities, and a vital role in prevention, management and recovery.

As they choose whether to fight for or against their organisation, they reflect on the norms and practices established in everyday work, on whom they believe caused the problem, and on whether the organisation's actions feel competent, caring and fair. They interpret multiple past and present experiences of leadership, teamwork and culture as they decide:

- How they think and feel about the crisis.
- How they think and feel about the organisation.
- How they think and feel about themselves.
- And what they say and do next.

It follows that successful crisis leaders don't rely on process alone; they also fully understand their organisation, and they equip their people to remain safe, effective and resilient in difficult or disruptive times.

Success depends on building a transparent, psychologically safe, accountable and adaptable culture that enables collaboration and supports crisis prevention, response and recovery. It also relies on facilitating trusting employee–organisation relationships and ensuring ongoing evaluation of which practices and systems build resilience, and which create greater risk.

Strengthen culture before crisis

Taking care of people and keeping them informed is the first step to crisis survival. But enabling teams to perform well and advocate under pressure requires cultivating an environment that allows them to do so.

A transparent, psychologically safe, accountable and adaptive culture sets the foundations for mutual trust and support. It embeds clear communication, constructive challenge and collaborative working as everyday norms, and it provides robust systems and processes that allow early risk detection and management in both normal and high-pressure conditions.

To enable such a culture, you must:

- Clearly define and reinforce organisational values and behaviour so everyday actions reflect expected standards.
- Promote transparency to break down silos, reduce blind spots and surface emerging risks.
- Normalise discussions of mistakes and near misses to encourage learning and early action.
- Enable two-way dialogue to share knowledge, highlight different perspectives and strengthen collective sense-making.
- Demonstrate visible, accountable leadership by role modelling non-defensive behaviour, encouraging diverse perspectives and facilitating constructive challenge.

- Encourage psychological safety so employees feel confident raising concerns, reporting errors and suggesting solutions.
- Embed effective and accessible systems, processes and training that support good practice, detect emerging risks and enable early action

Strengthening culture before a crisis shapes how quickly issues are surfaced and addressed and sets the tone for whether people step forward or back under pressure. The critical next task is to ensure positive foundations hold when they are most severely tested.

Sustain culture under pressure

The true test of culture comes under pressure, when the foundations built in ordinary times must guide behaviour, decisions and communication in extraordinary ones. When a crisis cannot be avoided, leaders must respond quickly to sustain the values and practices that maintain trust, clarity and collective action. In these conditions, the priorities are to:

- Protect all stakeholders and minimise crisis harm
- Help people make sense of what is happening
- Activate internal support, action and advocacy for overcoming the crisis

Yet this is easier said than done, as people at all levels may move into fight, flight or freeze modes – sharpening focus for some while triggering anxiety, withdrawal or inaction for others. Pressure can drive short-term thinking, systems can prevent people from acting in line with stated values and misjudged messages can erode trust, motivation and advocacy, potentially stalling recovery or creating new problems altogether.

Maintaining a transparent, psychologically safe, accountable and adaptive culture under pressure requires intentional strategic leadership. It is not easy to do, but the payoff is values-driven decision-making, effective information flow and respectful interpersonal behaviour when stakes are high. Employees draw on practised judgement, familiarity with systems and peers, and an environment that reinforces problem-solving, collaboration and early action.

To achieve it you must:

- Disclose what is happening and share verified information quickly, taking care not to breach legal obligations or duties of care.
- Reinforce values and behaviours so decisions reflect expected standards.
- Prioritise employee wellbeing and provide necessary practical, emotional and psychological support.
- Enable two-way dialogue to share knowledge, highlight diverse perspectives, quickly correct mis- or disinformation and strengthen sensemaking.
- Promote transparency to break down silos, reduce blind spots and surface new risks.
- Role-model accountable, non-defensive behaviour and align words with actions to reinforce leadership credibility, fairness and consistency.
- Show empathy for everyone affected and tailor information to the unique needs of individuals or groups.
- Involve colleagues in problem-solving and responding to emerging threats.
- Capture and integrate lessons into future practice, training and system design.

Preparing for and managing a crisis is not just about operational or reputational recovery. It is an opportunity to strengthen culture, renew trust and embed learning. When handled and communicated well, a crisis can reinforce trust in leaders and the organisation. Team members see themselves as part of the solution, and together they become more resilient.

BACK TO PAGE 30

IGNORE DEI AT YOUR PERIL: HOW INCLUSIVE CULTURES ARE AN ORGANISATIONAL RISK MITIGATION STRATEGY

by Avril Lee

Inclusive culture – a board-level risk and performance imperative

Too often diversity, equity and inclusion (DEI) initiatives and targets are viewed as soft HR objectives meant 'only' to put people-first into action or worse, as in the US, woke, unfair practices that provide some individuals with unfair advancement. In reality, DEI driven diversity of thought and practices are proven to improve business performance and innovation – critical corporate imperatives in these challenging and fast-changing economic times. But the business benefits of DEI supportive and inclusive cultures are broader – and critically include being a board-level risk imperative.

Too often, crises are still framed as operational failures: supply chain failures, cyber hacks or product failures. Yet experience and the current news agenda show us that the most damaging reputational crises are rarely capability related; they are character-led and often culturally empowered. Misconduct, toxic leadership, cultural or community insensitivity, ethical lapses and failures to listen to others cause far deeper and longer-lasting damage (internally and externally) than technical issues. Let's be honest, 'culture eats strategy and performance for breakfast' and in the eye of a reputational storm, culture overwhelms best intentions and hoped for outcomes, making crisis resilience and effective communications not purely an outcome of issues planning or process, but a product of good preparedness rooted in a DEI-led culture.

For boards charged with governance, risk management and long-term value creation, organisational culture informed by and embedded in DEI values must be understood as critical crisis infrastructure.

Cultural defence – crisis prevention, avoidance and early warning

True inclusion – across DEI characteristics such as ethnicity, sex, socio-economic experience, age, and other measures, e.g. professional discipline – increases organisational intelligence and boosts quality decision-making and healthy challenge, factors that make the difference in crisis situations.

A positive, inclusive culture can prevent and identify potential issues early. When diverse voices and different perspectives are heard, and when employees feel psychologically safe to raise concerns, the culture enables scrutiny, culturally specific insights and issues to be avoided or surfaced before they can escalate to become reputational threats. Leadership must therefore put in place credible internal systems and policies that allow them to hear from employees directly and recognise warning signs: for example, in-house platforms, Employee Resource Groups, engagement surveys, whistleblowing and exit interviews.

Critically, inclusion credibility and crisis resilience must start at the top; the board must itself be diverse and reflect an inclusive mindset as well as promoting it as business critical to the rest of the organisation. A homogeneous board creates inherent risk, while a diverse one strengthens challenge, reduces groupthink and improves oversight of management decisions during high-stakes moments. Beyond the board, DEI must not be viewed as a standalone initiative or a diverse workforce as a 'one and done' panacea. Boards must integrate and support authentic inclusive practices into formal risk frameworks, management reporting, accountability and rewards, and cultural norms.

Crisis-decision making: the power of cognitive diversity

When managing acute crisis, speed matters, but equally so does good judgement. Research has consistently shown that diverse teams outperform non-diverse ones when it comes to complex problem-solving. Diverse thinking challenges dominant narratives, tests assumptions and unconscious bias, and broadens the lens through which risk is evaluated. In the heat of crisis, the quality of decision-making and insight (e.g. disclosure, messaging and stakeholder liaison) directly impacts outcomes and reputational trajectory. When shaping issues preparedness strategies, boards should consider diversity and equity. Are crisis leads and teams representative of key stakeholder communities and the organisation? Do decision-makers reflect different lived experiences? Are unsupported assumptions being made about the affected communities?

Defenders from within

For successful crisis management, and more rapid post-crisis recovery, internal stakeholders can be influential both inside and outside the company. In a socially driven, hyper-connected communications world, they can be positive ambassadors or whistleblowers. An inclusive culture built on fairness and transparency generates and holds trust, creates a sense of collegiality and builds corporate resilience able to withstand mis-steps and mistakes, creating employee advocates who are vocal defenders. Alternatively, dissonance between stated values and lived reality is rapidly exposed during a major crisis and can fuel internal critics to action.

Another benefit of inclusive cultures and diverse thinking is improved innovation and adaptability; these skills, particularly adaptability, are key not only to business performance but often the critical capability in recovery from crisis. Diverse workforces support challenge, experimentation and learning from failure – and these behaviours enable organisations to not only survive crises but can ensure they emerge even stronger.

Competitive advantage, not HR 'wokery'

In an era defined by scrutiny, political instability and stakeholder activism, the reputational stakes have never been higher. Boards that dismiss DEI as a soft HR goal or too difficult in the current environment expose their organisations to avoidable risk, and reduce their ability to manage issues and crises.

Culture is not a soft intangible but a driver of resilience. And when pressure mounts, it shapes behaviours, adaptability and decisions. It determines whether leaders act with integrity or defensiveness, whether decisions are based by informed perspectives or outdated biases, and often is the deciding factor in whether stakeholders give the benefit of the doubt and 'allow' and accept mistakes from the organisation. Just as DEI should not be performative, crisis management does not begin when headlines break. It begins with the culture, and its commitment to DEI values, long before the crisis emerges.

BACK TO PAGE 30

WHAT PUBLICS TALK ABOUT WHEN THEY TALK ABOUT CORPORATE REPUTATION: A FRAMEWORK FOR BOARDS

by Dr Craig E. Carroll

Most boards encounter corporate reputation as a number. A score on an index. A rank in a league table. When that number drops, the instinct is to ask what happened to financial performance, customer loyalty or share price. But this response reveals a fundamental misalignment: it treats reputation as a leading indicator of business outcomes rather than as stakeholder feedback that demands a response on its own terms.

The result is that many organisations appear not to be listening. They collect reputation data and instrumentalise it for their own purposes – to forecast sales, justify investments or benchmark against competitors – rather than for the purposes of the source: the stakeholders who are telling them something important about what to stop, start or continue.

The ten reputation contrasts

Through extensive research into how publics actually discuss corporate reputation, I have identified ten contrasts that structure stakeholder evaluations. Each contrast represents a paired tension that stakeholders weigh when forming, revising or defending their judgements about an organisation:

Character and Consequence, Conation and Calculation, Culture and Compliance, Cadence and Calibration, Capacity and Capital, Capability and Culpability, Categories and Connections, Communication and Collaboration, Commitment and Controversy, and Conduct and Course Correction.

These are not dimensions that researchers impose on reputation from the outside. They are the terms in which publics themselves frame their assessments. Understanding them is the difference between measuring reputation and actually comprehending what your stakeholders are telling you.

Why the character–capability distinction matters for crisis

For boards navigating crises, two of these contrasts are particularly consequential. Character and Consequence asks whether the organisation's actions reflect who it fundamentally is or merely what resulted from a specific decision. Capability and Culpability asks whether the organisation lacked the competence to prevent a failure or chose not to prevent it.

Getting this distinction wrong leads to the wrong crisis response. When Boeing faced the 737 MAX disasters, the initial framing treated the crisis as a capability problem – a technical failure in a complex system. But as investigations revealed that engineers had raised concerns that were overridden by commercial pressures, the public narrative shifted to character and culpability. The company had not merely failed to catch a defect; it had made choices that reflected its values. The response playbook for a capability crisis – demonstrate technical fixes, bring in outside expertise, show the problem is contained – was wholly inadequate for a character crisis, which demands acknowledgement of deeper organisational failings and evidence of cultural transformation.

Contrast this with the CrowdStrike outage in July 2024, which grounded flights and disrupted hospitals worldwide. Despite the enormous operational consequences, the public narrative remained largely within the capability frame. Stakeholders attributed the failure to a flawed software update process rather than to organisational character. The crisis response – rapid technical explanation, transparent root cause analysis and process reforms – matched what stakeholders were actually evaluating. CEO George Kurtz's credibility survived the crisis largely because the response was calibrated to the right contrast.

Critically, these contrasts can shift during a crisis. What begins as a capability question can become a character question if the organisation's response reveals misplaced priorities. Boards must therefore monitor not just the crisis itself but the evolving terms in which stakeholders are judging the organisation's handling of it.

The broader lesson for boards

The character–capability distinction illustrates a principle that applies across all ten contrasts: stakeholders are making specific evaluative judgements and the organisation's crisis response must address the judgement that is actually being made, not the one that is most convenient to manage.

A crisis involving Culture and Compliance requires a different response from one involving Commitment and Controversy. A failure of Cadence and Calibration – where the organisation's timing and proportionality of response is at issue – demands a qualitatively different kind of accountability from a failure of Conduct and Course Correction, where stakeholders are watching whether the organisation can actually change.

For boards, the practical implication is this: before approving a crisis communications strategy, ask which contrast your stakeholders are activating. If the answer is not clear, you are not yet listening closely enough. Reputation is not a box to be unpacked for whatever data serves the organisation's immediate needs. It is a structured conversation in which publics are telling you what they expect, what they will tolerate, and what they will not forgive. The ten contrasts give boards a map not just for hearing what is actually being said, but for taking action on what matters most to their stakeholders.

BACK TO PAGE 29

ISSUE OR CRISIS? HOW THEY DIFFER AND WHY IT MATTERS

by Dr Tony Jaques

It is a major mistake to treat issue and crisis as interchangeable terms. Yet that is precisely what some organisations do. Too often, middle-level managers 'inflate' routine issues into crises. This may be through ignorance, but it can also be a deliberate attempt to command executive attention, justify headcount, accelerate approvals, or even unlock some extra budget. Boards need to be alert to this risk and make judgements based on a proper understanding of the distinction between the two.

Certainly, issues and crises are interconnected, but they need fundamentally different responses. Failure to understand that not only leads to misallocation of resources, it also desensitises management to the true potential impact of crises and creates a false sense of preparedness for when a real crisis strikes. When management ignores this distinction, it is more than a management failure. It creates a serious vulnerability and places the organisation at risk.

Issues management seeks early detection of potential problems and works towards planned, positive outcomes. By contrast a crisis typically endangers the entire organisation, and the immediate objective is damage control and recovery.

While the essential inter-dependence between issues and crisis management is critical, an executive level understanding of the specific dimensions where issues and crises diverge helps guide effective implementation across the organisation.

These dimensions are:

1 Choice

Issues management is designed to allow you to explore all strategy options, assess trade-offs and make informed decisions. In a crisis, the positive choices narrow rapidly as the situation deteriorates.

2 Certainty

Facing an issue, you can research every possible fact and analyse the views of key stakeholders and independent experts. In a crisis, you often must make decisions on incomplete information, when cause, responsibility, potential cost and likely solutions remain unclear.

3 Urgency

Directly linked to choice is the question of time. Issues usually allow time to fully assess and make the best decision. In a crisis, delay can be lethal. You are under pressure to make a decision right now.

4 Cost

In dealing with an issue, cost often informs strategy. By contrast, when a crisis strikes, the necessary money usually gets found. It is only after the crisis that lawyers and accountants start to argue about the dollars and cents.

5 Continuity

Issues management should be a normal part of executive activity during office hours while business continues uninterrupted. A crisis shatters any idea of 'business as usual.' It causes management to override all other priorities, and may severely disrupt continuity of the organisation's core activity.

6 Duration

Issues can extend over months, years or even decades. Crises generally have a more explicit time-frame and the triggering event usually has a defined beginning and an apparent end. However, the damaging aftermath of the crisis – particularly financial, legal or reputational – often persists long after the triggering event is over.

7 Impact

The impact of an issue is often measured in terms such as reputation, market share, brand, community concern, licence to operate and stock price. A crisis may have some of the same impacts in the longer term, but more immediately a crisis threatens life, property or the environment, and may compromise capability to operate or even threaten organisational survival.

BACK TO PAGE 31

AFTER THE CRISIS: BOARDS, RECOVERY AND PUBLIC INQUIRIES

by Amanda Coleman

When the frenetic activity has finished and the crisis has been brought under control, what happens next? Managing the aftermath of a situation is an essential part of recovering and rebuilding to ensure future resilience. Moving out of crisis and straight back into business as usual will leave an organisation vulnerable to a recurrence of the situation or a future crisis. The pressure to consider how to rebuild starts from the moment a debrief is considered, and for the most serious cases recovery can take months or even years.

An organisation that rushes ahead with a return to business as usual will miss opportunities to look at the potential impact the incident has had on the organisation's reputation and to strengthen systems and processes. Recovery communication should be considered after every significant crisis and a plan should be created to help take the organisation forward positively.

In the UK, there is the potential for any organisation to be involved in a public inquiry, either a statutory or non-statutory inquiry. This requires them to be prepared for all their decision-making and actions, and for communication to be scrutinised. The purpose of public inquiries is to find out where problems occurred, identify areas to improve and provide accountability for those who have been affected by the crisis. Consequently, it is important to be aware of the potential impact a public inquiry could have when moving out of crisis and into recovery.

Legislation is also being developed to legally require public bodies to be candid (the 'duty of candour') when providing information to public inquiries. The Public Office (Accountability) Bill was developed to address the experiences voiced by Hillsborough families who had to fight to get accurate information from public bodies. Boards and communicators need to work together to ensure that there is transparency as well as the provision of information to support the public inquiry considerations.

Transparency means committing to proactively sharing information, being open about decisions and failures, maintaining accessible records, engaging with stakeholders and opening to scrutiny when things go wrong.

Public inquiries can happen many years after the conclusion of a crisis. They have been criticised for taking too long to report back and longer still to ensure that their recommendations are taken forward. The UK government has established a dashboard to monitor progress on recommendations arising from statutory inquiries since 2024.[16] Its purpose is to enable recommendations to be tracked, scrutinised and publicly reported, addressing longstanding criticism of insufficient accountability and slow progress in implementing inquiry findings. However, progress has been limited. For example, nine years after the Grenfell Tower tragedy, only eight recommendations had been completed. Similarly, slow progress is evident across other inquiries, including those into the Manchester Arena terrorist attack and the Covid-19 pandemic.

[16] Public Inquiries: Recommendations and the Government Response – GOV.UK

Public inquiry reports and recommendations will be tracked and monitored by the media and social media influencers, as well as groups of affected people who come together in the aftermath of emergencies. An organisation that is slow to react and implement change following a public inquiry reporting recommendations will be subjected to public pressure, potential reputational damage and further scrutiny on how it operates.

Boards can also find themselves under pressure with inquiries and investigations after a crisis. Were they operating effectively and did they have sufficient scrutiny of the activities and decisions that the organisation was taking? In some situations, the board and the organisation can become diametrically opposed. While the board may need to consider its collective and individual members' reputations, the organisation may be considering safeguarding itself to continue to operate in the future. In these situations, the board may seek out communication consultancy support that is independent of the organisation and can provide strategic guidance. Where possible, this should be avoided as it can lead to further reputational damage to the organisation, which could limit its ability to operate effectively in the future.

Moving forward from a crisis requires consideration of four elements, review, rebuild, resources and re-establish:

- Review what happened during the crisis and what issues may remain, what areas of the organisation have been under pressure, what reputational impact may have occurred.
- Rebuild by considering what challenges and issues the organisation was managing before the crisis happened. Any of these areas may quickly come back into focus and could further damage the organisation's reputation.
- Resources are required to support the communication work in the aftermath of a crisis or emergency. To be able to focus on the communication effort, adequate communication staff with the appropriate skills should remain assigned to the work.
- Re-establish requires the development of a recovery communication plan that repairs and rebuilds the organisation's reputation and works to ensure changes are made to avoid a similar crisis occurring in the future.

Boards have a critical role to play in supporting a smooth transition from crisis into recovery and overseeing any changes required. The oversight and scrutiny at this stage is the final opportunity for a board to build a proactive position that can manage the impact of reviews, investigations and inquiries.

The key points for boards to operate effectively at the recovery stage of a crisis are:

- Ensure the organisation is providing an open review of the crisis with access to all documentation.
- Establish processes where board members are included in debriefs and organisational reviews.
- Be prepared to ask the hard questions and get the answers needed to develop operational and communication recovery plans before any public inquiry.
- Request organisational recovery plans and timelines for action then rigorously track progress and press for change when the organisation is slow to act.
- Help to build the culture of honesty, accountability and safety that encourages the organisation to act quickly and deliver visible change.

BACK TO PAGE 46

TRUE CRISIS PREPAREDNESS AND RESILIENCE

by Rick Cudworth and Swaraj Parameswaran

We are in a world undergoing unprecedented changes that threaten the unity of institutions, alliances and unspoken pacts. And, if geostrategic challenges are not enough, we must also deal with the effects of extreme weather events, technological acceleration and demographic shifts. One thing is clear, we are in a period not just of uncertainty, but of disruption.

Resilience is fundamental to the strength and health of any business – it's what success is built on

From a business perspective, this reality brings a unique set of challenges and opportunities, and in order to meet these, resilience cannot simply be defensive or reactive; it must be a strategic imperative that provides the cornerstone to creating and maintaining a strong and healthy business.

1 True crisis preparedness starts with organisational strategy and business model decision-making

These foundational choices determine how well an organisation can absorb and adapt to change and represent the primary opportunity to design resilience into the organisation.

So, what is organisational resilience? According to ISO/DIS 22316 2026, the revised draft international standard, it is *"the ability of an organization to anticipate, absorb and adapt to change, enabling it to survive and prosper"*.

2 Resilience is not just a set of capabilities to respond to and recover from events; it is the outcome of deliberate choices that shape how organisations operate, grow and evolve

These choices are, or should be, influenced by changes to the context in which the organisation operates. The standard makes the case that resilience must not be static, but it should adjust according to changes in this context. We see this in the real world, where organisations adapt supply chains to increase flexibility, reduce key dependencies and, in many cases, hold increased stock levels locally. Similarly, in times of economic uncertainty or disruption, organisations adapt to hold more cash or liquid assets. This is resilience in practice.

The draft standard, which is in public consultation until late March 2026, identifies five dimensions of resilience for any size organisation – finance, operations, workforce, environment and societal – and emphasises concepts such as 'resilience by design', promoting the attributes of modularity, diversity, redundancy and flexibility.

3 Business data can provide a clear indication of an organisation's resilience

The standard also sets out a data-led, measurement-based approach to resilience. For a business that could be represented by the number of weeks' cash in the bank (finance), absenteeism and sickness levels (workforce), supply diversity and stock holding (operations), natural resource usage rate (environment) and customer sentiment, churn or acquisition rate (societal).

This data-led, measurement-based approach is adopted from the Resilience First and Cranfield University co-developed Model for Organisational Resilience.[17] The Model helps organisations to prioritise what matters most in their specific context, and to define resilience indicators aligned with strategy. Crucially, the Model supports more informed strategic decision-making by linking resilience outcomes directly to business objectives. This approach can significantly advance existing understanding of the true resilience of an organisation, particularly when combined with rigorous stress testing.

4 True resilience also requires an organisational culture that enables trade-offs to be considered, and drives learning and improvement

It is important to build an organisational culture which supports resilience, enabling trade-offs between cost, risk and benefits of resilience investments to be considered and assessed transparently, and drive continuous learning and improvement.

Lessons should be actively drawn from experience, and setbacks treated as opportunities to strengthen the organisation rather than as failures to be hidden.

Such a culture is reinforced by an environment in which employees feel able to speak up without fear of blame or retribution. When combined with a shared sense of purpose, this strengthens internal cohesion and enables collective ownership of resilience outcomes and the desire to build a strong and healthy business, capable of anticipating change, and absorbing and adapting to it.

5 Resilience must be translated into genuine readiness. Building this capability across a large organisation requires serious effort

True readiness is developed through regular, realistic simulations, scenario planning and exercises that expose assumptions and decision-making bottlenecks. It requires the ability to rapidly re-organise how decisions are made across the organisation, and leaders who can deal with uncertainty and ambiguity, and can create novel solutions to complex problems.

6 More resilient organisations recognise they are dependent on the resilience of the wider system or sector, as well as the communities within which they operate

More resilient organisations design for failure as well as success. They apply the principles of flexibility, diversity, modularity and redundancy into all essential aspects of their business model. They adopt a 'systems-thinking' approach, recognising that their resilience is also dependent on the resilience of the system or sector, as well as the communities within which they operate.

[17] Resilience First – Organisational Resilience

7 True crisis preparedness cannot be reduced to a checklist or a plan

BACK TO PAGE 49

Organisations that weather crises most effectively are those that have invested in resilience based on strategic business objectives. They use business data effectively to know what resilience they have and where vulnerabilities exist. They understand the context in which they operate, balance trade-offs and adjust resilience accordingly. They create a culture that supports learning and improvement and takes crisis readiness activities seriously. They are organisations that influence and support the resilience of the wider system and the communities on whom they depend, remembering that their workforce is also part of those communities. They have built trust-based relationships with stakeholders which create shared commitment and mutual support, enabling the organisation to be able to navigate shocks.

True crisis preparedness must be embedded into strategy, business model, decision-making and organisational culture. In short, organisations must be resilient by design, purposefully structured to have the capacities and capabilities to absorb and adapt to a rapidly changing and disruptive world.

TOOLKIT

REPUTATIONAL RISK

Board checklist

Embed reputation into risk governance

- [ ] Embed reputation strategy into risk governance and core operations.
- [ ] Oversee robust, up-to-date crisis management and crisis communications plans.
- [ ] Ensure the risk register includes reputational risks and early warning indicators.
- [ ] Involve communications in risk management.

Hold management accountable for crisis preparedness

Ask management:

- [ ] What scenario-based exercises have been run?
- [ ] How are communications aligned with legal, operational and risk teams?
- [ ] Are roles, spokespeople and escalation routes clearly defined?

Ensure communications alignment and coherence across the organisation

- [ ] Ensure communications are clear and consistent.
- [ ] Put frameworks in place to activate communication at pace.
- [ ] Ensure internal and external messaging is aligned, as inconsistency undermines trust.
- [ ] Avoid slow decision making and/or mixed messaging as they undermine credibility.

Promote a healthy culture

- [ ] Model ethical leadership.
- [ ] Demand transparent reporting.
- [ ] Ensure psychological safety internally.

Strengthen relationships with stakeholders

Good reputation depends on trust and goodwill. Boards should oversee:

- [ ] Transparent communication.
- [ ] Timely updates during crises.
- [ ] Clear stakeholder mapping.

Ensure communication expertise is represented at board level

- [ ] Professional communications is a vital part of effective risk governance.

BACK TO PAGE 21

AI FAILURE MODES

Ten critical failure modes

Even well-governed AI systems fail; understanding how is the foundation of effective board oversight. Failure modes define governance requirements and their consequences are specific, foreseeable and, in many cases, already occurring. Whether specific to generative AI, agentic AI, or shared across all AI systems, the risk origins can be internal, external or both. Occurring at different stages with real-world consequences have single or multi-points of impact.

Failure modes	What it means
Hallucination and misinformation	AI fabricates facts, citations and statistics with the same confidence as correct answers. The only safeguard is human verification before any output reaches a decision, client or publication.
Bias (structural and systemic)	Outputs appear normal while disadvantaging groups. AI systems trained on unrepresentative, incomplete or historically biased data reproduce and scale those biases in their outputs.
Shadow AI	Staff using AI tools with organisational data outside approved policy, typically free-tier consumer tools, without disclosure.
Prompt injection and adversarial attacks	Attackers override AI instructions to extract data or trigger unauthorised actions.
Autonomous action without authorisation	Agentic systems act before anyone reviews what they have done.
Data poisoning	Corrupted training data produces systematically harmful outputs. Invisible to the deploying organisation and behaves normally until it doesn't.
Black-box decision-making	Some AI systems' decision logic is opaque, meaning their reasoning cannot be understood, challenged or defended.
Sensitive information disclosure and data leakage	AI models produce sensitive information from their training data or processing history when queried in certain ways.
Sycophancy	AI models prioritise agreement over accuracy, validating false premises and confirming poor reasoning rather than challenging them.
Cascade and systemic failure	Where multiple AI systems interact, an error or attack can propagate and amplify across interconnected systems before anyone sees it.

AI failure modes extend beyond the ten critical technical failures listed, including governance, legal, strategic and organisational ones. For a comprehensive overview of failure modes, what they mean, why it matters to the board, governance implications and points of impact, see AI Failure Modes.

BACK TO PAGE 24

AI GOVERNANCE

Board checklist

Understand how AI fails

- [ ] Do we know the difference between AI prediction and verified fact, and has that distinction been communicated to everyone using AI tools in this organisation?
- [ ] Can the board identify failure modes most likely to produce an AI-related crisis: e.g. hallucination, data cut-offs, shadow AI, and the absence of human verification?
- [ ] Do we know which AI tools are in active use, including tools adopted by staff without approval?

Establish governance before it is needed

- [ ] Pass a written acceptable use policy and assign a named owner accountable to the board.
- [ ] Conduct a data audit to confirm what data the organisation holds, where it sits and whether using it with AI tools is legally allowed.
- [ ] Map regulatory obligations by jurisdiction, including GDPR and EU AI Act exposure, before scaling any AI use case.
- [ ] Apply AI governance to the entire lifecycle of each system in use: from purpose and oversight before deployment, through data quality, principles and testing to ongoing monitoring and review after launch.
- [ ] Ensure the board receives structured AI oversight reporting as a standing agenda item, not ad hoc updates.

Govern across the full scope of AI risk

- [ ] Confirm a named owner and documented position across each area of AI governance: strategy, implementation, risk and compliance, culture and people, and ethics and reputation.
- [ ] Review each area and identify which represents the organisation's highest current exposure.
- [ ] Ensure supply chain and third-party AI use is covered by contractual provisions and disclosure requirements.

Prepare to defend the governance record

- [ ] Can the board demonstrate, with documentation, that governance was applied at every stage of each AI system's lifecycle: from initial design and deployment through to ongoing monitoring and review?
- [ ] Is there a named individual responsible for AI oversight with a direct reporting line to the board?
- [ ] Does an AI incident response protocol exist, including for AI-generated disinformation targeting the organisation?
- [ ] Is the organisation's public AI position consistent with how AI is actually being used internally?
- [ ] Is there a strategic communications professional embedded in the AI governance structure, with a direct reporting line to or seat at the board, responsible for the trust and reputational dimensions of AI oversight?

Test crisis readiness

- [ ] Run a scenario exercise: e.g. an AI-generated disinformation incident, a shadow AI data breach, or a hallucinated output acted upon publicly. Can the board respond within the first hour with a credible governance account?
- [ ] Identify which governance triggers would prompt immediate board-level review and confirm the escalation route for each.
- [ ] Verify that the internal staff narrative on AI is consistent, honest and current, because in a crisis, it will be tested publicly.

Recommended conditions that trigger immediate board-level review

- Staff using AI to produce content that is published or acted upon without human verification.
- A regulatory inquiry, enforcement action or subject access request involving AI use.
- A supplier or partner AI incident that affects the organisation or its clients.
- Public reporting, accurate or otherwise, about the organisation's AI practices.
- A significant AI tool update that changes its capability, data handling or terms of service.
- A change in applicable regulation in any jurisdiction in which the organisation operates.

BACK TO PAGE 24

WHAT BOARDS SHOULD LOOK FOR IN THE IDEAL STRATEGIC COMMUNICATIONS PROFESSIONAL

Board checklist

Governance and strategic capability

- [ ] Demonstrated experience advising boards and senior executives.
- [ ] Strong understanding of corporate governance, fiduciary duty and risk oversight.
- [ ] Ability to operate independently and speak with authority under pressure.
- [ ] Clear grasp of the intersection between reputation, trust, regulation and organisational behaviour.

Crisis and risk expertise

- [ ] Proven crisis communications experience, including preparedness, live incident management and post crisis review.
- [ ] Ability to work at pace in high uncertainty environments without amplifying risk.
- [ ] Experience aligning communications with legal, regulatory and operational responses.
- [ ] Capability to establish protocols, decision thresholds and escalation pathways in advance of crisis.

Judgement and foresight

- [ ] Strong "sense making" skills: distilling complexity into clear, actionable advice.
- [ ] Ability to anticipate second and third order reputational impacts of decisions.
- [ ] Willingness and confidence to challenge assumptions and surface inconvenient truths.
- [ ] Sound ethical judgement and a strong instinct for long term consequences, not short term optics.

Stakeholder and reputation management

- [ ] Deep understanding of stakeholder dynamics, expectations and trust drivers.
- [ ] Experience managing communications with regulators, investors, employees, customers and communities.
- [ ] Credibility with external audiences, including media and institutional stakeholders.
- [ ] Ability to safeguard organisational legitimacy during periods of scrutiny.

Professional and technical competence

- [ ] Mastery of communication strategy, narrative development and message discipline.
- [ ] Strong written and verbal communication skills at board level.
- [ ] Good understanding of digital, social and GenAI enabled communication environments.
- [ ] Ability to manage misinformation, leaks and rapid information spread.

Personal attributes

- [ ] Calm, authoritative presence in crisis.
High personal integrity and discretion.
Resilience and stamina under sustained pressure.
- [ ] Strong collaboration skills across legal, risk, operations and leadership teams.

Qualifications and standing

- [ ] Relevant senior level experience (rather than purely technical or junior communications backgrounds).
- [ ] Professional accreditation or demonstrated alignment with recognised standards (e.g. CIPR, crisis management and/or governance qualifications).
- [ ] Track record of accountability for outcomes, not just advice given.

BACK TO PAGE 27

STRATEGIC COMMUNICATIONS

Board checklist

Assurance

- [ ] Ensure a communications professional confirms that organisational communications are fit for purpose in both routine and crisis contexts.

Strategic alignment

- [ ] Approve a strategic communications framework aligned with ISO 22361.
- [ ] Verify that communication is integrated into strategic planning, risk management and crisis preparedness – not treated as a standalone function.

Crisis readiness

- [ ] Confirm crisis communication plans are clear, rehearsed and aligned with board decision-making. Communications during crises must remain authoritative, timely and balanced.

Consistency and credibility

- [ ] Maintain strict alignment between internal and external messaging to protect trust and avoid confusion. Require clear, evidence based messaging that supports informed board decisions.

Digital and reputation oversight

- [ ] Ensure policies cover social media, digital communication and GenAI tools.
- [ ] Receive updates on misinformation risks, reputational threats and narrative amplification across digital platforms.

Stakeholder confidence

- [ ] Expect communication professionals to guide responses to scrutiny, cyber related communication threats or operational disruption, ensuring leaders deliver consistent, authoritative messages.

Resilience

- [ ] Commission regular reviews of communication protocols and stakeholder mapping.
- [ ] Support investment in monitoring systems and rapid response communication capabilities.

BACK TO PAGE 27

STAKEHOLDER MAP AND RISK REGISTER FOR A MINING COMPANY

A worked example based on general information and recommended best practice.

In recent years, investors have increasingly focused on Environmental, Social and Governance (ESG) performance. This has compelled companies to not only commit to ESG priorities and targets but to publicly disclose the impact of their activities. As a result, mining companies must balance economic gain with responsible mining practices.

The complex and capital-intensive nature of the mining industry means stakeholders are diverse and often hold conflicting interests. As mining operations require access to land and capital-intensive, fixed assets, host communities and indigenous landowners – who often hold the company's social licence to operate – are among the most powerful stakeholder groups. This is because of their proximity to operations, rights as landowners and potential to influence business continuity.

Below is an illustration of a typical stakeholder map and risk register for a mining company.[1]

Stakeholder map

This map categorises key stakeholder groups by their location, stake, interest, influence and power.

Internal

Stakeholder	Stake / Interest	Influence / Power
Shareholders / Investors	Focused on return on investment (ROI) and ESG ratings and performance	Can stop a project or withdraw investment
Board of Directors / Management	Determine business strategy and priorities, ensure delivery of targets and regulatory compliance	Can disapprove capital release for projects
Employees / Contractors	Safety, fair wages, job security and workplace culture	Provide critical skills for operations

[1] This example has been developed based on general information, industry factors and recommended best practice. It does not consider all factors, issues and stakeholders (including their interest, power and risk), as these may differ depending on the geographic location, core business and mineral of interest for mining companies. As such, this example is only meant to be referred to as a guide.

External

Stakeholder	Stake / Interest	Influence / Power
Government / Regulators	Permits, royalties, environmental and labour regulations and compliance, ensures accountability	Can shut down operations over unethical and illegal practices
Host Communities / Indigenous Groups	Land rights, employment, environmental impact; consent is legally and ethically paramount	Hold social licence to operate and can revoke it
Business Partners / Suppliers	Provide essential goods, products and services for operations	Influence varies; some critical operational activities depend on the products, technology and services they provide
Labour Unions	Conditions of service	Can make legally binding collective decisions for members
CSOs / NGOs / Media / General Public	Monitor activities; raise concerns over environmental activities, labour issues and workplace culture	Can influence public sentiment and government policy

Stakeholder risk register

All stakeholders are plotted on the matrix below, indicating their level of interest, power, risk and the recommended strategy for managing relationships with each of them.

Stakeholder	Interest	Power	Risk	Influence / Power
Shareholders / Investors	High	High	High	Manage closely – they fund projects
Board of Directors / Management	High	High	High	Manage closely – strategic oversight
Employees / Contractors	High	Medium	Medium	Keep informed – frequent two way communication, deliver operations
Government / Regulators	High	High	High	Manage closely – compliance is mandatory
Host communities / Indigenous groups	High	Medium - High	High	Keep satisfied – build strong, trusted relationships, hold social license
Business Partners / Suppliers	Medium	Low	Medium - High	Monitor, keep informed – maintain cordial business ties
Labour Unions	Medium	Medium - High	Low - Medium	Monitor – engage when necessary
CSOs / NGOs	Medium	Low	Low	Monitor – regular horizon scanning to pick up negative, unfavourable rhetoric
Media / General Public	Low	Low	Low	Monitor – track sentiment shifts, minimal effort

BACK TO PAGE 29

SAMPLE FIRST RESPONSE/HOLDING STATEMENTS

Cyber incident and natural disaster

Cyber incident: sample first response statement

[**Organisation Name**] – Statement

[**Date / Time**]

We are currently responding to a **cybersecurity incident** that has affected parts of our systems. We know this news may be worrying, and we are deeply sorry for the disruption and uncertainty this may be causing for our customers, employees and partners. At this stage, we can confirm the following:

- **What is known:**
  We have identified unauthorised activity within our network and immediately activated our cyber incident response procedures. Our security and IT teams, supported by external specialists, are working to contain the issue and understand the extent of the impact.
- **What is unknown:**
  We are still assessing whether any personal or sensitive data has been accessed. This work is ongoing, and we will share verified information as soon as we have more clarity.
- **What we are doing:**
  We have isolated affected systems, engaged cybersecurity experts, and are coordinating closely with relevant authorities. Our goal is to restore normal operations as quickly and safely as possible while prioritising data integrity and the protection of all individuals involved.

We understand how stressful incidents like this can be, especially when the data or services you rely on may be affected. We are committed to keeping you updated with accurate, timely information and avoiding speculation, in line with our values as an organisation.

If you have immediate concerns, please contact:

[**Name / Position**]

[**Email / Phone**]

Thank you for your patience and understanding. We will share further updates as soon as we are able to confirm additional facts.

BACK TO PAGE 42

Cyber incident: public facing social media statement

We're currently responding to a **cyber incident** affecting parts of our systems. We know this is concerning, and we're truly sorry for the disruption this may cause.

At this stage, we can confirm that:

- We've detected unauthorised activity in our network and activated our incident response procedures.
- Our teams and external experts are working urgently to contain the issue and understand what's been impacted.
- We're still assessing whether any personal data has been accessed. If that changes, we will update you directly with verified information.

We understand how stressful cybersecurity events can be, and we appreciate your patience as we work to resolve this safely and responsibly. We'll share further updates as soon as we have more information.

If you need support, please contact us via [**channel/contact**].

BACK TO PAGE 42

Natural disaster: sample first response statement

[**Organisation Name**] – Initial Statement on Flood Impact

[**Date / Time**]

We are responding to the effects of severe flooding that has impacted [locations / facilities], and our thoughts are with everyone affected by this damaging and distressing situation. Our immediate priority is the safety and wellbeing of our employees, customers and the wider community.

At this stage, we can confirm the following:

- **What is known:**
  Severe flooding has caused significant disruption to [operations / infrastructure], and access to some areas remains restricted. Our teams are working closely with emergency services and local authorities to assess conditions and ensure safety.
- **What is unknown:**
  We are still establishing the full extent of the damage and its implications for our operations. Some assessments are ongoing, and further information will follow once we have verified details.
- **What we are doing:**
  We have activated our crisis response procedures and deployed response teams to affected sites.
  We are coordinating with local emergency responders and supporting staff and community members who have been impacted. Our immediate priority is to protect people and stabilise the situation.

We understand that events such as this cause significant concern and disruption. We are committed to providing timely, accurate updates as the situation becomes clearer, and we will continue to keep you updated as new information is confirmed.

For urgent enquiries, please contact:

[**Name / Position**]

[**Email / Phone**]

BACK TO PAGE 42

Natural disaster: public facing social media statement

We're currently dealing with the impact of **severe flooding** affecting parts of our operations and local communities. Our thoughts are with everyone experiencing disruption, damage or distress; we are truly sorry for what you may be going through.

At this stage, we can confirm that:

- Flooding has caused significant issues in [affected areas], and our teams are working alongside emergency services to keep people safe.
- We're assessing the situation so we can understand the full impact on our services, sites and communities.
- Some details are still emerging, and we'll share verified updates as soon as we have them.

We know events like this are frightening and deeply disruptive. Thank you for your patience and for supporting one another at this difficult time. We are committed to keeping you updated as the situation evolves.

If you need immediate support or have urgent concerns, please contact [**channel/contact**].

BACK TO PAGE 42

QUESTIONS BOARDS SHOULD ASK MANAGEMENT IN A CRISIS

These questions help board members understand whether management is truly in control during a crisis – without slipping into operational involvement. They also help boards probe the depth, rigour and practicality of crisis preparedness, response and learning.

Readiness and preparedness

Foundational oversight

- What are the organisation's key vulnerabilities and potential crisis triggers?
- Has management identified high impact risks and early warning indicators?
- How does management monitor emerging risks and early warning signs?
- What is the current crisis response plan, and how often is it updated or tested?
- Do we understand worst case scenarios?
- What scenario based crisis simulations have been conducted, including communications components?
- How does management ensure crisis plans are adaptable to cyber, operational, reputational or natural disaster scenarios?
- What resources are allocated for crisis simulations, training and continuous improvement?
- What training and resources are provided to the Crisis Management Team (CMT)?
- How are legal, regulatory and compliance considerations integrated into preparedness?
- How does crisis preparedness integrate into overall risk management and business continuity?
- Are we appropriately resourced for a sustained crisis?
- What is the plan for recovery, trust building and restoring operational confidence after the crisis has passed?

Leadership and structure

- Who sits on the CMT, and do they have clear authority to act quickly?
- Who are the designated leaders responsible for crisis management, communication and decision making?
- How does management ensure coordination and alignment across departments during a crisis?

Communications

- Is communications involved in risk management and the risk register?
- Does the risk register consider reputational risks?
- Do we have a short, usable crisis communications plan, and has it been recently stress tested?
- Who will be the key spokesperson, and what are the plans for secondary spokespeople?
- Have all spokespeople been media trained?
- Have key messages been prepared in advance, and where are they stored?
- How is organisational communication planned and managed throughout a crisis?
- Are legal, communications and operations aligned on messaging and risk mitigation?
- Have all critical stakeholders been mapped and prioritised?
- What communication channels and technologies support rapid information flow?
- How will communication plans adapt if normal information channels (e.g. website, documents, email) are unavailable during a cyberattack or natural disaster?

Crisis: The first 60 minutes

Detection and assessment

- How quickly was the crisis identified and escalated?
- Has management established verified facts and clarified what is known, unknown and under investigation?

Communications

- Is there a single, coherent narrative to prevent conflicting messages?
- Is messaging consistent across internal, customer, regulator and market channels?
- Have employees been briefed before external stakeholders?
- Has the initial statement been made?
- Is the spokesperson ready to go? Is there a clear escalation route?

Operational response

- What is management doing to stabilise operations and reduce immediate harm?
- Are decisions being recorded in a proper log for later scrutiny?
- What practical, actionable guidance have we given the people affected, in plain language?

Communications

- Are victims, affected people or impacted communities being prioritised in communications?
- Is the organisation monitoring misinformation, media dynamics and stakeholder sentiment in real time?
- What deepfakes or misinformation are circulating; what are our counter measures?
- Are regulators, funders, partners and political actors receiving appropriate, tailored updates?
- How is stakeholder sentiment monitored?
- How does management balance transparency with operational security and legal considerations?
- How does management maintain employee readiness and morale during prolonged crises?
- How is psychological and physical safety ensured for employees involved in response?

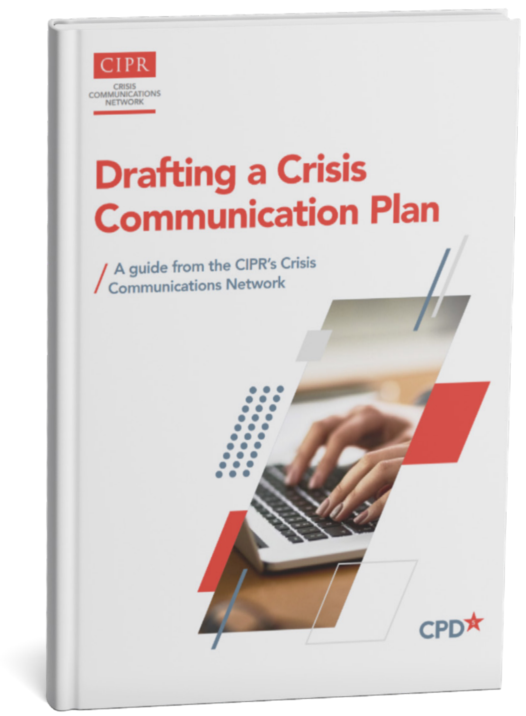
Recovery, accountability and learning

- What metrics or indicators are used to assess crisis preparedness and response effectiveness?
- What post crisis review processes are in place?
- Has management presented a lessons learned review, and have these lessons driven governance, capability or cultural reform?

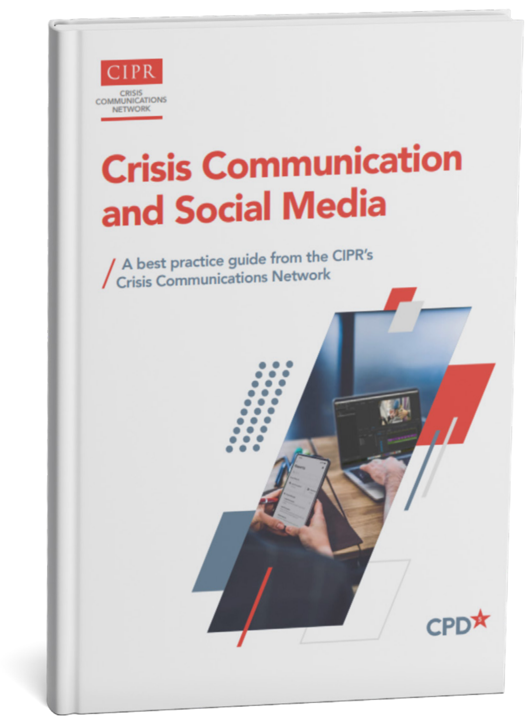
BACK TO PAGE 42

DRAFTING A CRISIS COMMUNICATION PLAN

The board must ensure that their organisation has a crisis communication plan in place. The Crisis Communications Network's first guide Drafting a Crisis Communication Plan is an indispensable introduction for those who are just starting to put one together or perhaps evaluating a current plan. In addition, the network's guide Crisis Communication and Social Media provides invaluable insight and advice on how to manage social media in a crisis.



Drafting a crisis communication plan



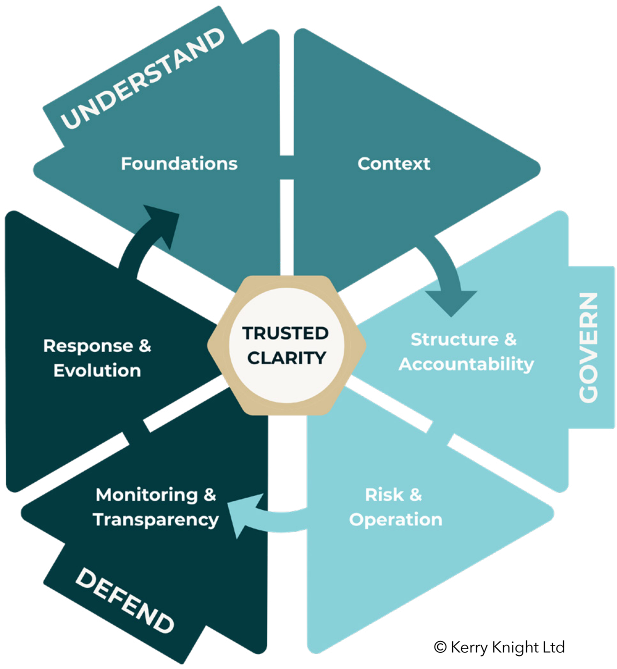
Crisis communication and social media

BACK TO PAGE 42

TRUSTED CLARITY MODEL

AI governance framework

"You cannot defend what you have not governed, and you cannot govern what you do not understand."



Understand

Foundations
- Scope and purpose
- Guiding principles

Context
- Regulatory and legal mapping
- Explainability requirements
- AI literacy and competency

Govern

Structure and accountability
- Roles and accountability
- Board reporting and escalation
- Employee rights and protections
- Workforce training and transition
- AI-specific whistleblowing
- Cross-discipline integration

Risk and operation
- Risk classification
- Testing and pre-deployment validation
- Ethical review
- Supplier procurement and accountability
- Environmental and resource risk
- Permitted and prohibited uses
- Data governance
- Accessibility and inclusion

Defend

Monitoring and transparency
- Monitoring, metrics and measurement
- Stakeholder engagement
- Transparency and external comms

Response and evolution
- Incident response
- Review and version control

Visit trustedclarity.uk for more information.

BACK TO PAGE 24

GOOD CRISIS COMMUNICATION

Board checklist

Establish a clear, authoritative narrative

- [ ] Ensure communications set a single, coherent narrative that all leaders reinforce.
- [ ] Verify alignment across executives, board members and frontline teams.
- [ ] Confirm employees are briefed before external audiences.

Insist on truthful, timely and proportionate communication

- [ ] Check that information is verified promptly before release.
- [ ] Ensure updates are regular and predictable.
- [ ] Guard against speculation or premature reassurance.

Maintain leadership visibility and accountability

- [ ] Confirm the CEO is the primary public voice, supported by the Chair providing strategic oversight.
- [ ] Ensure the board exercises proper oversight of all communication activities.
- [ ] Assess whether leaders project calm, competence and accountability.

Demand clarity over completeness

- [ ] Require communications to clearly distinguish what is known, unknown and under investigation.
- [ ] Ensure language is clear, direct and free of jargon or legalistic ambiguity.

Ensure effective two way communication

- [ ] Monitor media, stakeholder sentiment and misinformation continuously.
- [ ] Verify that inaccuracies are corrected rapidly and transparently.

Protect trust, reputation and continuity

- [ ] Confirm messaging is accurate, transparent and consistent across all channels.
- [ ] Ensure communication supports operational continuity and the organisation’s licence to operate.

BACK TO PAGE 42

RECOVER

Board checklist

Stabilise operations

- [ ] Confirm safe, predictable operations and close all residual risks.

Independent review

- [ ] Commission a no blame, evidence based crisis review with clear actions and owners.

Rebuild trust

- [ ] Communicate transparently, explain lessons learned and repair key stakeholder relationships.

Reset culture

- [ ] Address morale, trust and leadership alignment; ensure visible, unified leadership.

Embed improvements

- [ ] Update risk, crisis and communication plans; test reforms through scenarios.

Reassure externally

- [ ] Meet all regulatory obligations and honour every commitment made during the crisis.

Plan ahead

- [ ] Prepare for future crisis related milestones (anniversaries, inquiries, media cycles).

Steady recovery communication

- [ ] Provide predictable updates, show corrective action, maintain empathy and consistency.

Explain responsibly

- [ ] Clarify root causes and reforms within legal and regulatory boundaries.

Close the loop

- [ ] Issue a final summary of what happened, what changed and how accountability will continue.

BACK TO PAGE 46

CIPR

CRISIS
COMMUNICATIONS
NETWORK

ciprcrisiscommsnetwork.com

IoD Institute of Directors

iod.com