Control Risks

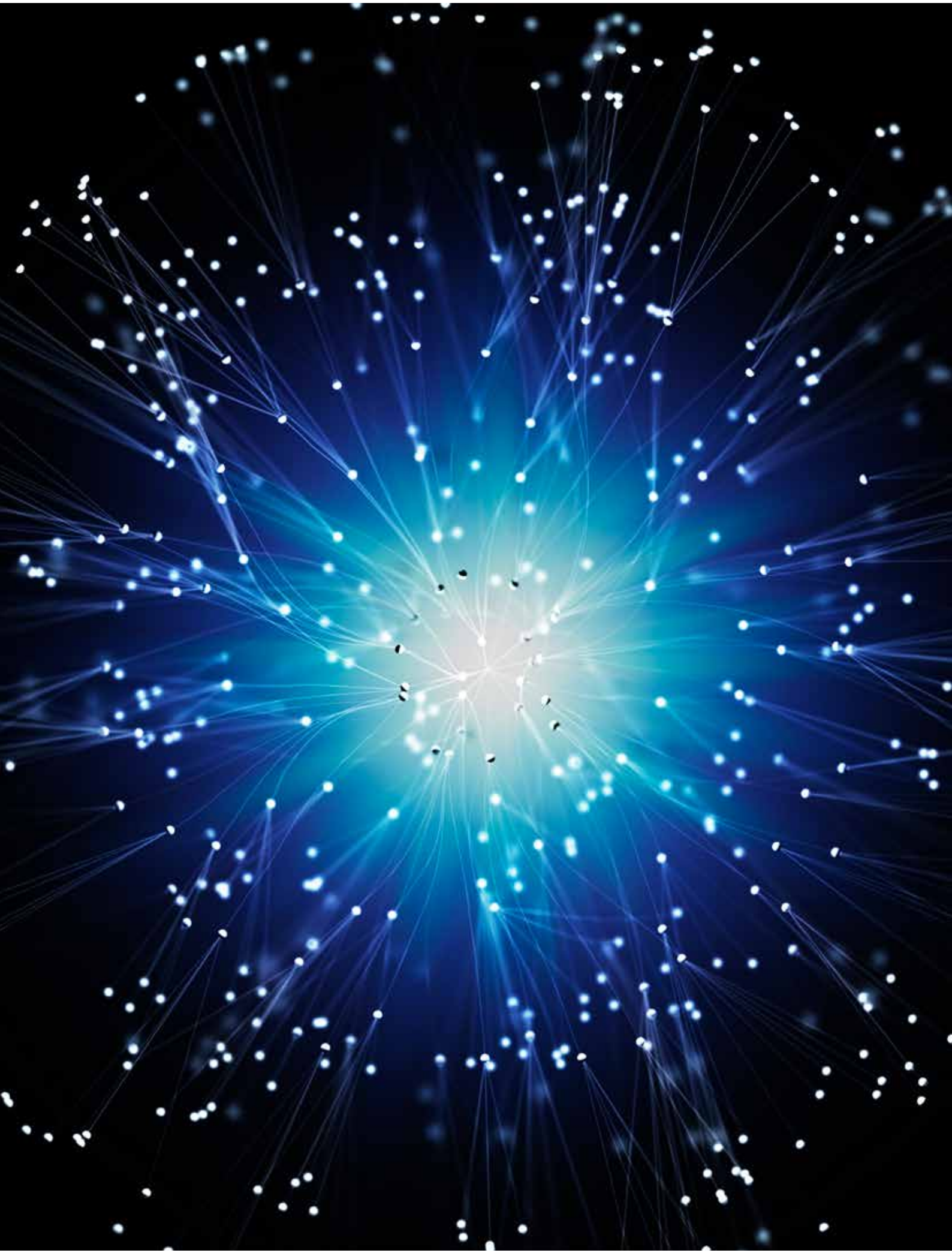
# Orthodoxy and innovation:

organizational crisis readiness, response and recovery

# Table of contents



Published by Control Risks Group Limited ("the Company"), Cottons Centre, Cottons Lane, London SE1 2QG. The Company endeavours to ensure the accuracy of all information supplied. Advice and opinions given represent the best judgement of the Company, but subject to Section 2 (1) Unfair Contract Terms Act 1977, the Company shall in no case be liable for any claims, or special, incidental or consequential damages, whether caused by the Company's negligence (or that of any member of its staff) or in any other way. © Control Risks Group Limited 2018. All rights reserved. Reproduction in whole or in part prohibited without the prior consent of the Company.



# Orthodoxy and innovation: organizational crisis readiness, response and recovery

Not a week goes by that the news isn't filled with stories of crises happening all over the world, affecting companies big and small, from start-ups to established veterans, in emerging markets and developed ones. Today's crises are triggered by events both inside and outside of a company's control: political interference, instability and unrest; terrorism; physical and cyber security breaches; workplace violence; insider malfeasance; IP theft; fraud; regulatory compliance failures; product recalls; natural disasters; and supply chain disruptions.

While the existence of crises is not a new phenomenon, a number of factors are combining to increase the frequency, complexity and types of crises companies face. These issues challenge organizations' ability to remain resilient in the face of uncertainty and while under scrutiny from stakeholders near and far. And with change to the very DNA of crises comes the need to change how organizations ensure they **stand ready**, **respond** effectively and **recover** stronger. The good news is that companies do not need to start with a blank slate or reinvent the wheel. Rather, success can be found through embracing an approach that melds traditional crisis management orthodoxy with modern-day techniques and technologies to focus on reducing the likelihood of crises occurring, maintaining organizational readiness, minimizing the impact when crises do occur and embracing continuous adaptation and improvement. The competitive advantage gained from such a process is immense.

## So why are crises changing?

Some will point to an increase in traditional crisis triggers, such as extreme weather events and natural disasters, which appear to be on the rise due to factors like climate change, or the persistence of greed and corporate malfeasance on both Main Street and Wall Street, or changing market conditions and increased expansion into unstable developing markets.

Others will focus on the realities of the world we live in today, including the politicization and weaponization of regulation and compliance regimes across the world, the undoing of established geopolitical orders with uncertain political transitions, or the wholesale migration to an interconnected digital economy and the resulting spread of globally connected and highly capable threat actors. Apart from all that, there is also the increase in organized criminality and the increasingly dangerous emergence of new types of terrorists and violent criminals (the self-radicalized individual, anonymous actors and motive-less active shooters all come to mind) both at home and abroad. This development is resulting in risks that were previously considered limited to emerging markets and are now increasingly appearing in the developed world, too.

Heightened mobility of goods, capital, people and information as well as concentration of economic activity and population density are key drivers. When coupled with the centralization of critical systems the breadth of impact of disruptive events and natural disasters is amplified. It is through these interconnected pathways that risk accumulates, propagates and culminates in a much greater scale of effects. What would have previously been an isolated risk can now have an impact across geographical areas and national borders.

Further complicating the realities of today's business environment are the speed of social media and its ability to turn any private problem into a very public crisis, as well as far-reaching regulatory bodies with the ability to enforce and penalize in ways we could not have imagined even 20 years ago. Think about it: Do you think the United Airlines passenger removal incident would have ever risen to the level of a crisis 20 years ago when cell phones and social media were in their infancy? Probably not – instead it likely would have been a story on page 4 or 5 of a local paper and would not have resulted in the financial and reputational damage United Airlines is still dealing with today.

So why are crises changing? Is it the increase in traditional crises triggers or the new reality of the modern world we live in? The answer probably lies somewhere in between, on top of, underneath, and all throughout all of the above. This speaks to the complex nature of crises and highlights a simple truth: Crises have always existed, and always will, but the shape, speed and sources of crises have become more complex than ever.

Ultimately, the impacts of these crises are far from inconsequential. They significantly challenge companies' ability to meet both their strategic goals and the rising expectation of shareholders, customers and stakeholders that they will live their core values: ensuring employee and customer well-being, sustaining and growing profitability and shareholder value, providing superior customer service, innovating products and services, and creating and maintaining a favorable brand and reputation. As any company that has been through a crisis can tell you, the fallout is real. It can include stock price drops, decreases in market share, intense and unwanted media coverage, attention from activists, brand value index hits, tarnished reputations, opportunistic competitors, and customer trust issues that could take years to repair, if they are even repairable at all.

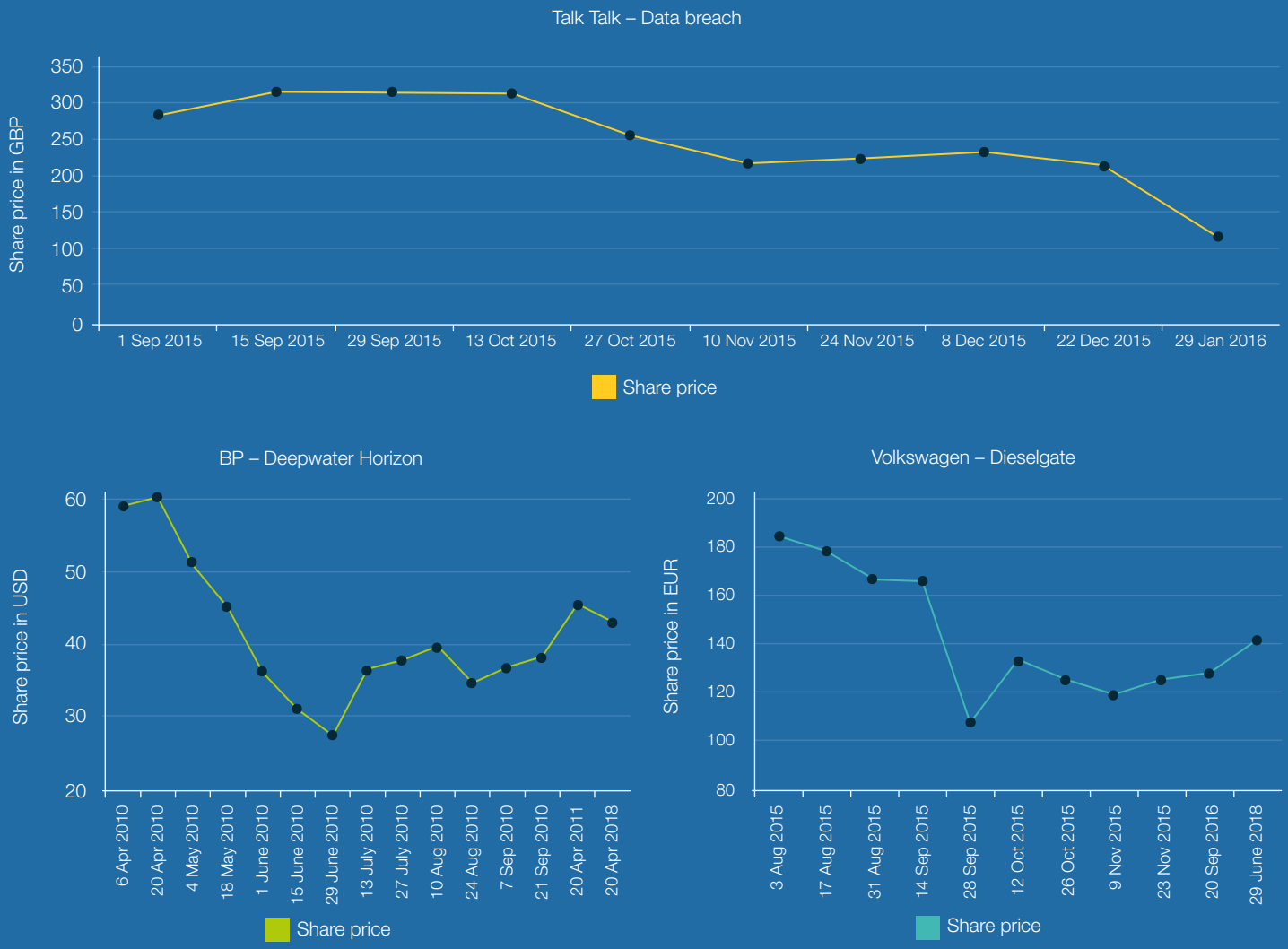
Thanks to today's incredibly complex risk ecosystem, companies and other organizations cannot afford to be caught flat-footed during crisis events. They must take proactive steps and be prepared to act with speed and efficiency. The real question then becomes: how does a company do that? Based on Control Risks' experience, companies must adhere to four core principles:

- **Reduce the likelihood** of reasonably foreseeable disruptions
- **Reduce the impact** of crises and critical business issues through appropriate response mechanisms
- **Respond with laser focus** on comprehensive business recovery
- **Embrace** continuous adaptation and improvement

Within each of these principles, companies must also recognize that effective readiness, response and recovery require a combination of long-standing crisis management orthodoxy – the best-practice guidance that Control Risks has been providing its clients with for 43 years – and innovations to keep pace with today's (and tomorrow's) threat environment, modes of operation and stakeholder expectation.

Source: Yahoo Finance © Control Risks 2018

**Fig.1, 2, 3** ▶ Crisis: immediate shareholder impact



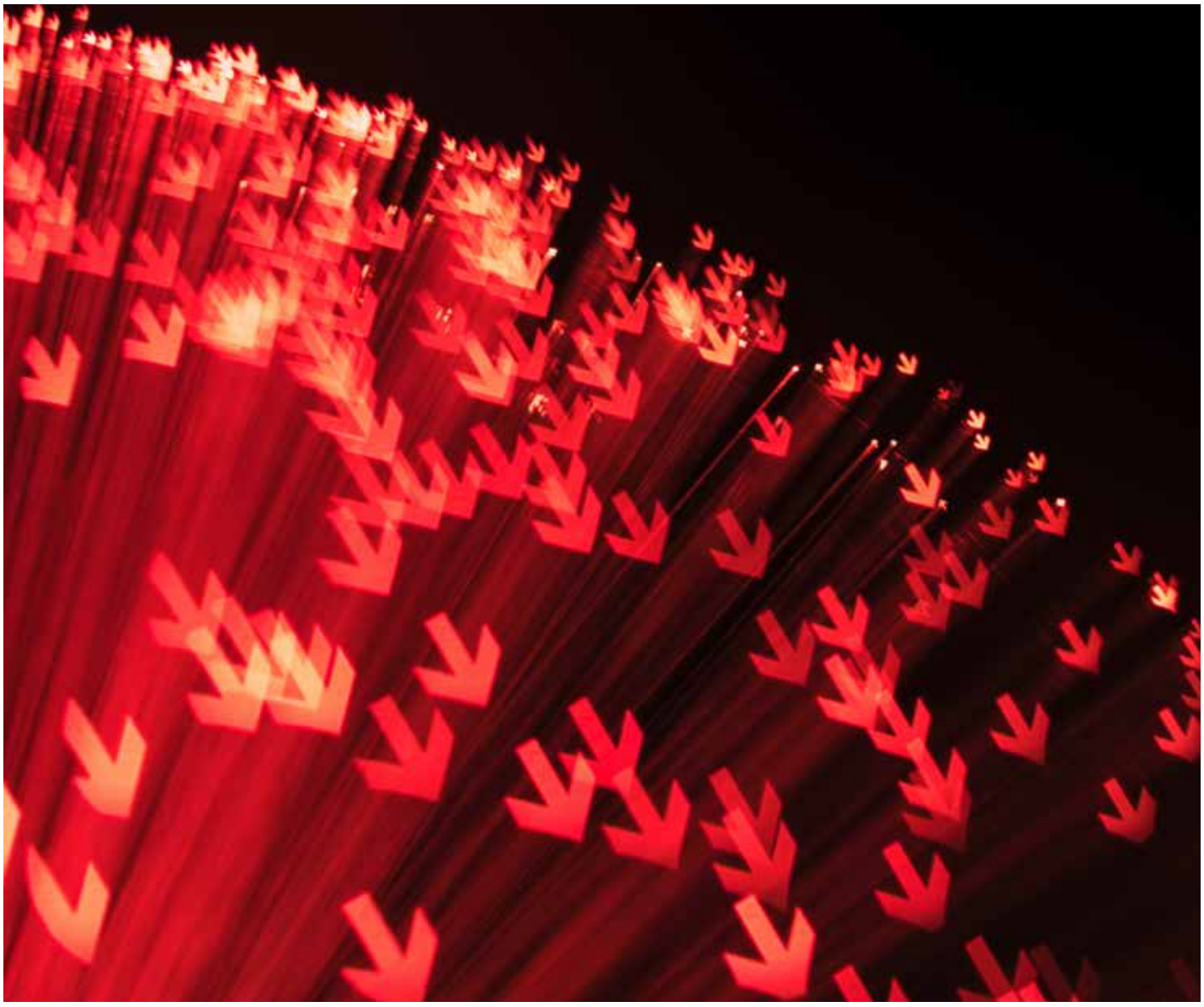

Source: "The Impact of Catastrophes on Shareholder Value", Knight and Pretty, University of Oxford © Control Risks 2018

**Fig.4** ▶ Crisis: the impact on shareholder value

One of the main videos of a passenger being forced off a United Airlines flight has been watched over 4m times on YouTube.

Whilst a long-term effect on United Airlines is unlikely, between April 9 and 11, 2017 the 4% drop in share price wiped about USD 255m off its market capitalization.

**Source: CNNMoney**



**Too often my clients focus on their response capabilities. When challenged, they recognize that they may have been able to avoid the crisis but they never spent the necessary time and effort to do so.**

Matthew Hinton, Principal

# Taking steps to reduce likelihood

Reducing the likelihood of a foreseeable crisis seems like a logical first step on the path to crisis readiness. However, we have observed that risk management activities are too often siloed, based exclusively on regulation or financial loss, focused on one particular area of acute risk, or otherwise informal or incomplete. Enterprise risk management (ERM) programs are too often 'enterprise' in name only.

One consequence is the absence of linkages between activities that reduce the likelihood of disruption and those that reduce their impact. In fact, when asked about their programs, those responsible for crisis management almost always describe their organization's capabilities in terms of reduction of impact. They highlight crisis response teams, plans and exercises, but hardly ever mention any efforts taken to first reduce likelihood.

In contrast, in everyday life the reduction of impact and likelihood go hand in hand. Think about it: We install alarm systems in our homes to help mitigate the impact if someone were to break a window and try to enter, but we also reduce likelihood by installing signs to alert potential intruders to the existence of the alarm system. A family moving into a home with a swimming pool would get swimming lessons for all family members to mitigate the impact of someone accidentally falling in, but they would also put a fence around the pool to reduce the likelihood of such an accident happening in the first place. So why do companies fail to embrace a similar mentality when it comes to their profitability, reputation and brand?

Likelihood-reducing activities require commitment, resourcing and investment. There's no getting around that. But the question is: Would you invest USD 100,000 today in a compliance program if it helps prevent a future fraud that costs the company millions in financial and reputational damage? Or USD 300,000 in IT infrastructure and security measures if it prevents a debilitating and humiliating cyber attack in the next few years? You need not look far for real-life examples where inadequate understanding of the risk and subsequent underinvestment had detrimental and destructive impacts.

The Inland Regional Center, the site of the San Bernardino attacks in 2015, is still facing lawsuits from victims and families of patients alleging that adequate job applicant screening and broader security measures had not been in place at the time and could have prevented the incident. The Panama Papers scandal, fueled by a cyber attack and the leak of millions of private records, forced Mossack Fonseca, once a top-five global provider of offshore financial services, to cease doing business and shut down for good. In October 2015, TalkTalk, a large British telecommunication provider, was hacked leading to the theft of personal data (including bank account numbers, birth dates and addresses) of almost 157,000 customers. Elizabeth Denham, the information commissioner, said: "TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease." TalkTalk lost 101,000 customers and suffered costs estimated up to GBP 60m – in addition to the record fine of GBP 400,000.

So how can organizations evolve to combine activities that mitigate likelihood with those that mitigate impact?

### 1. Your gut feeling is not good enough anymore

Understanding and assessing your organization's key threats and risks at the outset and using those to inform your program have long been part of crisis management orthodoxy. More mature programs recognize that these threats and risks will change over time and can be influenced by both internal and external factors that could be out of the organization's control. Sounds obvious? You would be surprised at how many organizations we work with lack the basic risk management processes and protocols needed to make informed decisions. And for those companies that do see the value in understanding these risks, we find, unfortunately, that risk management processes are often based on static and uninspiring risk assessments that periodically raise awareness of risks and issues largely based on historical performance and 'gut feelings' rather than data and analysis. Threat and risk assessments need to be thorough, and they should be done periodically, with an external, objective pair of eyes – regularly our clients are surprised at what their most harmful, i.e. likely and impactful risks actually are.

### 2. Threat and risk assessments must not be a one-off

With the speed of change in today's threat environment and the resulting expansion of the variety of reasonably foreseeable risks, organizations must take a new approach. Crisis management professionals must ensure that the foundation of their programs remains dynamic. They should join forces with their colleagues


responsible for core risk management activities across the organization to ensure that risk assessments are consistently refreshed using reliable and comprehensive analysis. For companies with a focus on crisis avoidance, this information becomes a powerful tool to inform both likelihood and impact mitigation activities. It allows them to make investment and resourcing decisions both during the strategy setting process but also throughout the year as internal and external factors drive changes in their business.

### 3. Make use of technology

Leading organizations with a commitment to crisis avoidance are moving beyond basic risk assessment techniques and invest in real-time capabilities. The convergence of risk monitoring and incident response functions within global security operations centers (GSOCs) is part of that evolution. Control Risks is helping more mature organizations use intelligence analysis, forecasting tools, social media aggregation, internal alert data and other monitoring tools to not only predict and interdict potentially disruptive events before they happen but also to allow organizations to initiate their incident and crisis response plans quickly and efficiently. As GSOCs begin to go beyond tactical alerts and align more closely with critical business risks, they will become even more useful tools for all-hazards crisis managers.

**The application of technology to crisis management brings significant gains in terms of preparedness, co-ordination, speed of response and efficiency. We have clearly seen a value in this during a crisis, but have also run highly efficient, technology-supported micro-exercises maintaining awareness and key skills amongst teams spread over multiple-locations.**

Bill Udell, Senior Partner

# Get ready to respond and reduce impact

Even if organizations take reasonable steps to minimize the chances of a crisis occurring, it is unrealistic to think that all crises can be avoided. With that in mind, it is important that companies take steps towards response readiness and reducing the impact of future disruptive events. The good news is that, as noted above, many companies already invest in some elements of crisis management orthodoxy and have baseline capabilities to aid in impact reduction. Unfortunately, however, while some investment might have been made, very often companies have either underinvested in these capabilities, let them go stale after years of little activity, or have insufficiently focused on the areas that provide the most return on investment when it comes to impact reduction. So how do companies get this right?

**"There is a law of diminishing marginal returns in relation to crisis management preparedness. There is no excuse for not putting the basics in place, it costs little, and has the most significant impact on your crisis response."**

Alex Martin, Director

### 1. Do your homework

It starts with the basics. You need executive support; empowered governance and defined roles and responsibilities; effective teams with thoughtfully-selected members; robust all-hazards-based planning; and informative training. Without these elements, your chances of successfully navigating a crisis with minimal impact is about as likely as a successful acquisition without proper due diligence. Simply put: The basics provide the platform for the success – the next step now is what you do with them.

Equifax, a consumer credit reporting agency based in the US, suffered a massive cyber security breach in September 2017 in which personal information of 148 million US citizens was compromised.

As the public felt that the company had no response plan whatsoever and stumbled along, the company's stock price dropped by 37% after the breach.

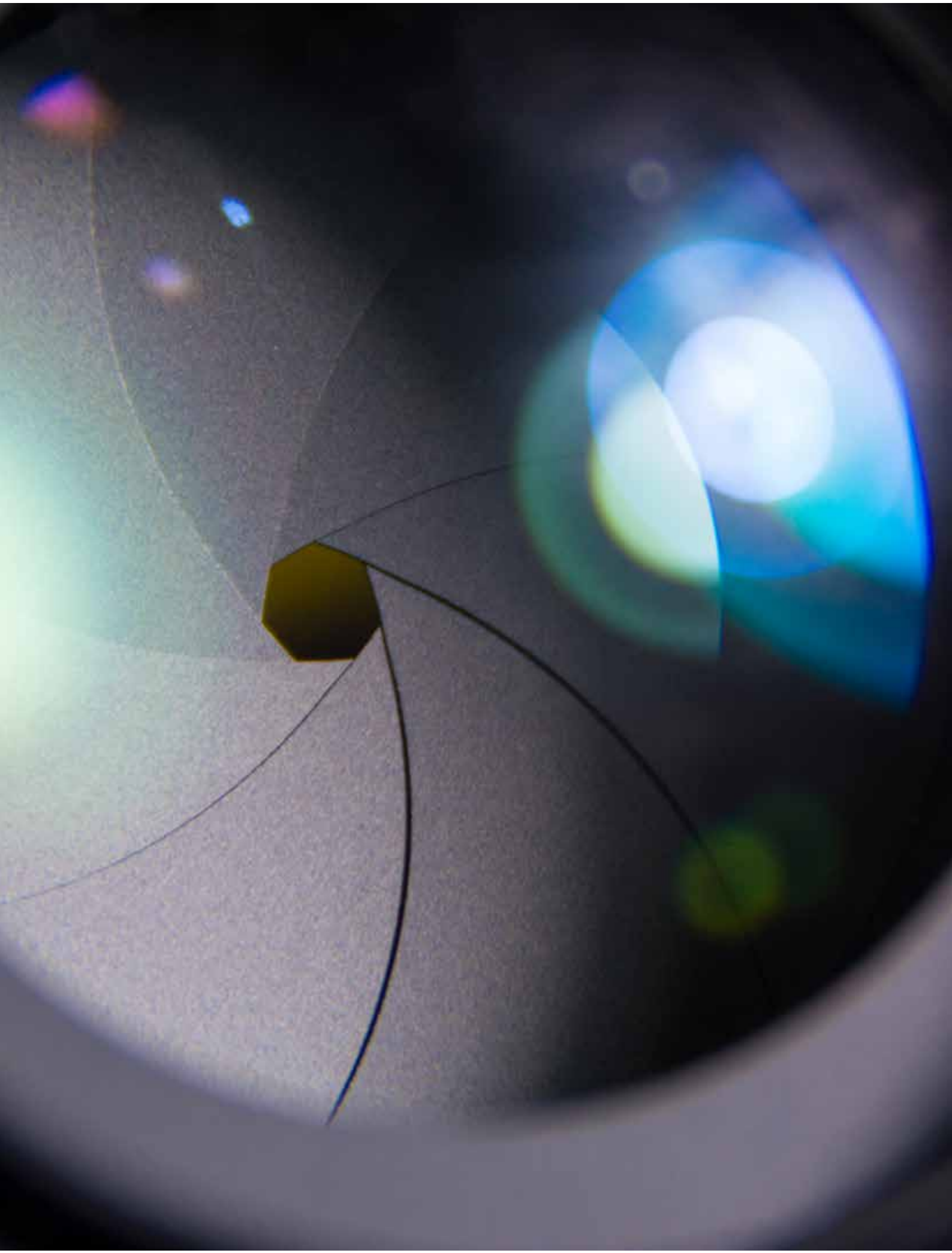
**Source: CNNMoney**

### 2. Practice makes perfect

You cannot overstate the value of crisis exercises and the importance of moving beyond a 'check-the-box' mentality aimed at merely meeting internal and external compliance obligations. Instead, leading-edge organizations understand that response capabilities – the very heart of impact reduction – rely on conducting exercises of increasing complexity using diverse scenarios. Organizations seeking to both enhance executive buy-in and ensure that their programs are forward-looking increasingly build their exercise scenarios around key emerging and complex risks that they are facing, or are likely to face in the near future. These exercises may pull in diverse teams from across the enterprise to join the corporate crisis team and test the organization's ability to respond both tactically and strategically. In addition, they are increasingly using technologies (e.g., tools for mass notification/accounting for staff) in exercises and asking key response providers such as their legal counsels and crisis responders to participate in order to intensify realism and identify gaps that illustrate a more realistic picture of how the organization will respond in an actual crisis.

### 3. Break down your silos: integration, flexibility and agility

A truly integrated and therefore effective response is only feasible if based on a better alignment of previously complementary yet disparate capabilities around crisis management, business continuity, disaster recovery and emergency response. If today's crises are increasingly complex, their impact is equally so, resulting in events that touch people, processes and technology across an organization. As a result, the ability to successfully manage crises in today's world relies on a connected, seamless response that more closely aligns to the actual unfolding of a crisis rather than artificial and unrealistic standalone focus areas. Companies must also ensure stress flexibility and agility so that they are able to tackle whatever they encounter, especially given the challenging and changing risk environment.



# Respond with an eye toward recovery

At our founding in 1975, Control Risks' sole mission was to help organizations respond to and recover from acute crises. Since then we have partnered with our clients to meet the challenges of a wide range of disruptive events – some contained and tactical and some uncontained and enterprise threatening – across more than 150 countries. We have seen some of the best organizational responses to issues such as corporate malfeasance, cross-border regulatory infractions, terrorist attacks, kidnaps, expropriation, political interference and cyber compromise. Unfortunately, we have also seen organizations make critical and impactful errors. Throughout our history, there remains some enduring orthodoxy. Organizations can emerge stronger regardless of the type of crisis, if they:

- Put people first
- Lead with their organizational values
- Focus on recovery from the start of and throughout the response
- Holistically attack impact while determining root cause, not after
- Enable their crisis leaders with authority and decision-making abilities
- Use lessons learned from previous crises

That said, organizations are being pushed ever harder to evolve the way they approach crisis and incident response itself. They are forced to rethink the response process and support model that organizations need to ensure stability and effectiveness in their response while focusing on core organizational performance.

Key points for the further evolution of crisis and incident response are:

### 1. Support from experts

Successful crisis management that focuses on impact reduction and rapid recovery in today's world also includes looking outside one's company walls and recognizing the need for external assistance. Many companies have external counsel and/or crisis PR firms on retainer but external needs often go beyond that. Social media and other platforms have connected disruptive events around the world directly to mass global audiences who are empowered to pass their own judgments and assign blame.

In this rapidly developing environment, organizations focused exclusively on conveying the right tone from the top struggle to 'own the narrative' during a crisis. While it remains important to execute well-prepared and well-timed PR and crisis communications messaging, holistic, tangible and immediate action – wherever the crisis has hit – has never been more important for a successful corporate crisis response. With that in mind, we are also seeing a rise in organizations partnering with crisis response providers that have localized on-the-ground expertise and can provide in-the-moment support during any crisis, including in far-flung geographic areas.

### 2. Alignment of on-the-ground action and strategic management at headquarters

The nature and speed of disruptive events requires that this on-the-ground support remain closely linked to and in alignment with the headquarters team managing the incident, which is focusing on core elements of strategic crisis management and a strong recovery. For these teams,

The response of multi-national companies to the 2017 hurricanes in the US and Caribbean illustrated the importance of a number of evolutions in corporate crisis management and response.

First, these events showed how increasingly difficult it is for companies to be ready to respond on the ground with in-house resources to the increasing complexity and diversity of disruptive events. A number of companies therefore relied on specialist third parties like Control Risks to fill the gaps, engaging them to rapidly deploy multi-disciplinary teams to provide immediate security and welfare services and also set business recovery in motion.

Second, the corporate responses to the hurricanes showed how vital it has become for the on-the-ground response to be joined both strategically and tactically and in real time with corporate crisis decision-making.

And third, in the face of devastating events like natural disasters, if companies focus on recovery, maintain a people-first approach and invest in their values during a response, the market and their employees will reward them.

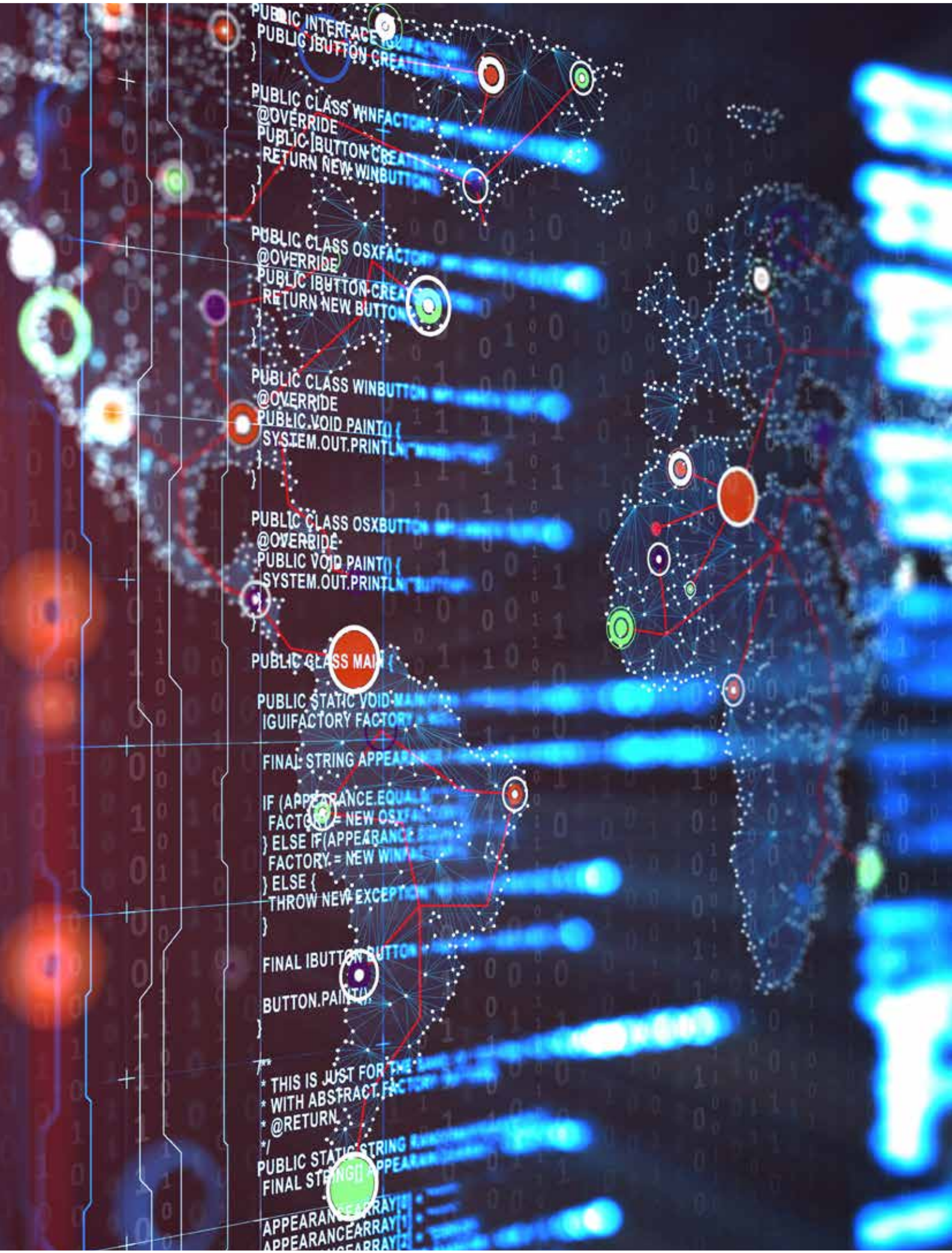
Control Risks has long used a proprietary First Response Protocol. This protocol is often placed within the crisis management plans of our clients and used throughout a response to help teams follow an orderly process that focuses and refocuses them on assumptions, facts, stakeholders, communication and objectives. As the complexity of crises increases, organizations will increasingly need to embrace intelligence-led scenario planning. This approach focuses on evaluating factors such as the organization's operating model, culture, geographic footprint and industry across best, worst and most likely case scenarios. These are informed by intelligence feeds supplied by in-depth knowledge of local realities and/or expertise on the specific type of incident and the relevant background on it, to help companies determine what might happen next in an evolving disruptive event and inform their actions to limit its impact.

### 3. Use of technology for real-time risk monitoring

To power scenario planning during an incident or crisis and provide critical information on the internal and external context, we are increasingly seeing organizations using either their GSOC functions or external providers for real-time risk monitoring. They receive this advice and support via a variety of engagement models, ranging from access to online tools to retainer-based approaches, all of which are informed by both local and global intelligence and data. By working with providers whose job is to monitor the global risk environment and provide intelligence and analysis to businesses, companies can utilize that information to minimize the impact of crises and also to reduce their likelihood.

### 4. Consider insurance cover to manage costs

Despite the increasing complexity of crises, crisis- and continuity-related budgets have been reduced in many sectors, and organizations taking a thoughtful and business-centric approach are naturally concerned about the cost of crisis response services, premium rates and expensive consulting contracts. They are seeking tools to provide cost certainty and ensure availability of multi-disciplinary expert capability. To meet this need, many are exploring specialized insurance policies, such as the Hiscox Security Incident Response (SIR) insurance policy, which ensures a 24/7 indemnified response to 38 different incident and crisis types. The policy taps into Control Risks' 43 years of crisis management expertise and ensures our engagement without additional in-the-moment costs. Premiums for these policies not only cover response services when crises emerge, but also allow for portions of the premiums to be applied to a wide variety of preparation and mitigation services aimed at reducing both likelihood and impact. This approach reinforces an organization's readiness to respond long before a disruptive event strikes. This often includes, but is not limited to, services such as crisis management governance, planning, exercising and training as well as threat information feeds, security awareness training and travel security membership.


PUBLIC INTERFACE
PUBLIC IBUTTON CREA
PUBLIC CLASS WINFACTORY
@OVERRIDE
PUBLIC IBUTTON CREA
RETURN NEW WINBUTTON
PUBLIC CLASS OSXFACTORY
@OVERRIDE
PUBLIC IBUTTON CREA
RETURN NEW BUTTON
PUBLIC CLASS WINBUTTON
@OVERRIDE
PUBLIC VOID PAINT() {
SYSTEM.OUT.PRINTLN
PUBLIC CLASS OSXBUTTON
@OVERRIDE
PUBLIC VOID PAINT() {
SYSTEM.OUT.PRINTLN
PUBLIC CLASS MAIN {
PUBLIC STATIC VOID MAIN
IGUIFACTORY FACTORY
FINAL STRING APPEA
IF (APPEARANCE.EQUA
FACTORY = NEW OSX
} ELSE IF(APPEARANCE
FACTORY = NEW WIN
} ELSE {
THROW NEW EXCEPTION
}
FINAL IBUTTON BUTTON
BUTTON.PAINT();
}
/**
* THIS IS JUST FOR
* WITH ABSTRACT
* @RETURN
*/
PUBLIC STATIC STRING
FINAL STRING[] APPEA
APPEARANCEARRAY[
APPEARANCEARRAY[
APPEARANCEARRAY[

# Embracing continuous adaptation and improvement

Let's be honest – the term 'continuous improvement' gets tossed around a lot and is often met with eye-rolling and disinterest. Why? Because all too often the term is used in an ambiguous way, implying that an organization is theoretically interested in getting something right but not motivated enough to be specific about driving change. In other words, it is a 'business-as-usual' cliché, built out of convenience, with built-in excuses.

But when it comes to crises, business-as-usual goes out the door and so should a lukewarm reception to continuous improvement. In fact, a failure to embrace continuous adaptation and improvement will not only minimize a company's chances of reducing the likelihood and impact of crises, but also potentially doom its ability to survive, let alone thrive, during a crisis. There lies an opportunity in a crisis situation to not only recover, but to adapt and change for increased resilience in the post-crisis environment.

**So how do companies truly embrace continuous improvement and reap its benefits for greater resilience?**

The good news is that if you are already embracing the first two principles discussed above (aka focusing on likelihood and impact reduction), you are halfway there. For instance, exercises are a fantastic way to continually improve response skills and readiness for whatever a company may face. Regularly revisiting team membership and structure, and the plans and tools that support them, often improves response capabilities and minimizes in-the-moment inefficiencies. But organizations should not only improve capabilities before a crisis hits, but continuous improvement needs to extend beyond the crisis response and into the recovery phase as well. Unfortunately, we often see companies skipping this vital step. Relieved to have managed through a crisis and eager to resume business as usual, many companies do not take the time to pause, reflect on what they learned during the crisis (good and bad), and make changes to ensure they are better prepared next time.

With that in mind, we recommend companies formalize mechanisms that allow them to review their performance during a crisis and dig into not only how they responded but also how well prepared they were for it in the first place. These types of reviews are called a variety of things: lessons learned analysis, post-incident reviews, and post mortems. Most software solutions that support the readiness and response phases also have powerful reporting functions that assist in reviewing every step taken. Regardless of what they are called, they have proven to be an underutilized but incredibly powerful tool to aid helping prevent history from repeating itself during subsequent crises.

In order to fully embrace continuous improvement, these reviews must result in action. Leading practice organizations not only share these results with leadership for both awareness and support, but also formally assign responsibility for resolving identified gaps as well as monitoring progress. Where possible, it is helpful to share these risks and issues across the organization as many of these discoveries point to organization-wide issues and could be connected to other risks being addressed in the company by related risk management efforts (e.g., enterprise risk management).

Post-incident reviews have been around for quite some time, raising the question: What changes are required to meet the demands of today's changing environment? The answer is ongoing risk monitoring. If one of the goals in recovery is the avoidance of similar crises in the future, there are fewer more effective tools than proactive risk monitoring. Once again, this should be informed by global and local intelligence, should be designed to identify emerging trends early on, and should lead us back to our first principle focused on increasing a company's chances of avoiding a crisis.

**"Often it is not a member of the crisis management team that engages us to conduct post-incident analysis, but the board or another executive from the C-suite. They want to understand how an incident turned into a crisis, why and what they can do better next time. Objectively identifying and closing gaps in preparedness is critical for enhanced response and recovery the next time a crisis hits."**

Jacqueline Day, Senior Partner

# In closing…

Companies face an increasingly complex global environment, complete with complicated and interconnected risks that can inflict significant damage on reputation, brand and profitability. They can successfully navigate these challenges by taking a more holistic approach to crisis management that stresses proactive risk management, effective collaboration and continuous improvement, all while embracing 'old-world' crisis management orthodoxy with modern-day technologies and techniques. In doing so, companies will naturally experience a variety of benefits, both quantitative and qualitative, all focused on fewer crises occurring, less impact should they occur, and fewer questions and more confidence from boards of directors, shareholders, partners, employees and customers about the company's readiness.

Perhaps most importantly, these steps can result in competitive advantage for the company that embraces these four important principles. Odds are that many of that company's competitors are not taking similar approaches or are doing so in a fragmented, underinvested manner. This leaves them exposed to unnecessary and unrelenting levels of risk exposure should a crisis occur that impacts a large geographic area (e.g., natural disaster), industry (e.g., collapse of a foreign market), or general way of living and working (e.g., terrorism). The prepared company, on the other hand, is not only able to withstand the crisis but may also come out ahead of its competitors when the crisis subsides.

Control Risks helps companies every day, all around the world, improve their crisis management and broader risk management capabilities using proven methodologies, using lessons learned, and tapping into our broad and deep base of subject matter expertise. For more information on how we can help, contact **enquiries@controlrisks.com**

Authors:

**Bill Udell**
Senior Partner

**Matthew Hinton**
Principal