Managing through crises: preparation is key

Headline risk seems to have risen in financial services. Ten years ago, as the financial crisis unfolded globally, the sector found itself on the front page every day – we all wondered which firms would be crippled or fail. We felt that again as the sovereign debt crisis played out several years later. News reports were peppered with the latest fine or settlement levied against a firm. Arguably, crisis management seemed relatively reactive in that context – no one firm stood out as managing crisis well or poorly in the industry.

Yet, in recent years, the nature of crises seems to have changed. They seem more frequent – major weather-related catastrophes seem common globally, as do industry – indeed cross-industry – crises, notably global ransomware attacks like WannaCry and Petya. Concerns about the spread of pandemics has started to feel more real – Zika joined common vernacular alongside Ebola and avian flu. Major system outages or problems with critical vendors seem almost commonplace, so much so that even relatively minor events can be mislabeled as crises.

In some ways, this reflects broader trends:

- Customer demands for 24/7 always-on access
- More dependence on third-parties, even for critical processes
- Much-heightened cyber threats
- Speed-of-light social media reaction to events, especially when corporate actions seem misaligned with its stated purpose and vision
- Long-term under-investment in core technologies
- Significant changes in business and operating models, as well intensified shareholder pressure for higher returns
- Challenges in building a strong corporate culture across large, often geographically dispersed, firms

This intense focus puts a premium on strong crisis management and, more broadly robust resiliency management. After all, crisis management – and its cousins, incident response and incident management – is only one process within the broader resiliency toolkit. A solid firmwide resiliency framework has to focus on managing and reducing resiliency risk and on building sustainable capabilities. The framework can help reduce the likelihood of an event happening and its impact, help firms react and recover quickly, and, once back up, hardwire in a continuous improvement cycle to learn from past events.

The enduring question remains, what can we learn from firms that have experienced a major crisis – the good, bad and the ugly?

The biggest learning can be summarized by the ubiquitous motto: Be prepared. It sounds trite, but it could not be more on point. During a crisis, it's too late to do what you should have done in advance. Every minute spent figuring out who should be responsible for a decision, how to phrase a press release, or which stakeholders should be contacted and in what order (e.g., board of directors, regulators and clients) takes away from a firm's ability to focus on the specifics of a response. That said, not everything can be preplanned – new issues arise in every situation; that's why developing corporate muscle memory through planned exercises (e.g., simulations) are so important, because they help build experience.

Preparation makes a difference in four main areas:

1. **Decision-making:** how decisions will be made in an informed manner, by whom and how quickly
2. **Communications:** how communications will be delivered to all stakeholders in a unified manner
3. **Operations:** how activities will be conducted and supported during crisis, as well as how operations resume
4. **Post-event activities:** how post-event activities should be conducted effectively

For each area, this article lists key actions that can help remove uncertainty during a crisis, enabling leaders to focus on things that can make the most difference in maintaining financial viability, helping customers, reassuring stakeholders, restoring service, and protecting the organization and its reputation.

EY
Building a better working world

Decision-making

Prepare the decision-making approach

Firms need to define the appropriate activities of the board and senior leadership during a crisis: who will be making decisions, how will those decisions be informed and made, and who will be brought in to assist?

Some key issues stand out:

1. **Clarify roles and responsibilities.**

   First, start with identifying the key decision-making in crisis. Who needs to be involved? In what capacity? Who determines when an event – and of what kind – necessitates moving from continuity plans to crisis? Does everyone appreciate how decision-making authorities shift in crisis? Ironing this out beforehand is essential, as is determining who owns the crisis management process so there is clear accountability for validating that it stays in line with evolving industry practice and regulatory expectations.

2. **Identify substitutes.**

   Once you have determined who can make decisions in crisis, make sure qualified, experienced backups are known. For example, if the treasurer is on vacation during a crisis, who should senior management call upon for questions regarding liquidity and capital? If they can't reach the CIO, who are the next three people in line, and are they prepared to step up? All of the identified decision-makers should be fully knowledgeable of the firm's contingencies processes and should have delegated authority to act in times of crises. This becomes especially critical when outages are prolonged – today, it's not difficult to imagine a firm's major site – or even a city or country in which it operates – experiencing major problems that last a week or more.

3. **Define escalation processes and triggers.**

   Make certain that crisis decision-makers receive information they need, when they need it, without being flooded with extraneous detail. Ahead of an actual crisis, decide which key issues must be elevated to business unit leaders, senior management, and the board and other governance bodies, including risk committees. Where possible, adopt explicit escalation triggers, so as to limit the degree to which upward communications are inadvertently delayed – it's all too easy for employees to wait another 5 or 10 minutes to problem solve, yet those minutes can be critical. Such triggers can be automatic – e.g., for so-called priority-1 events, which tend to have enterprise-wide impact – and others will require more judgment, such as potential impact of a division not meeting immediate customer needs.

Decision-making

Prepare the decision-making approach

4 Anticipate when established thresholds may need to be exceeded

During a crisis, a firm may need to accept greater financial and operational risks than typically expected. Confirm that decision-makers including the likes of second-line risk management, legal and compliance are engaged in those decisions. Review regulations, corporate policies (e.g., risk appetite thresholds) and insurance provisions to identify any "red lines" that should not be crossed. Document controls that may be overridden in crisis, by whom and when, and establish protocols for documenting such decisions.

5 Practice making decisions in a simulated crisis.

While some types of crises are predictable in the generic sense, each one has its own distinct characteristics. Moreover, inevitably, the crisis that hits the hardest is the one a firm doesn't expect. Building top executives' experience in making decisions in crisis – crisis muscle memory, if you will – is vital. Firms often conduct tactical simulations or tabletop exercises lower down the organization – say on liquidity or cyber – but it is important that these simulations are also undertaken at the most senior levels of the firm, so leaders know how they should operate in crisis. Such simulations often help firms determine how they would react for specific crises, e.g., how they would respond to a data breach or prolonged outage involving a key vendor.

6 Line up specialist resources.

Inevitably, firms need some specialist resources, during and after the crisis – whether it be outside counsel, forensics, cyber or other areas. Advice from privacy, compliance and public-relations executives may also be required. Identifying and contracting with credible sources of such advice ahead of time, cross-referencing those with approved-vendor lists in insurance policies, and making certain that they can be onboarded and situated at speed allows the firm to move quickly into accessing and using this experience and resources. The same is true for other contingent resources that may be required.

7 Designate someone to consider "what-if" questions.

In the early stages of a crisis, groups tend to focus on the detail of immediate actions and sometimes arrive at premature conclusions as to the scope and causes of the problem. To avoid groupthink, establish a protocol to give someone the responsibility of stepping away from the immediate demands of the event to evaluate alternate explanations and possible responses.

8 Design how to get back to business as normal.

As much as it is important to know when to escalate decisions and drive a sense of urgency, it is as important to determine the de-escalation approach, so the firm can transition back to business as usual, in an orderly, controlled and well-documented fashion. (See Prepare for post-event activities, below.)

Communications

Prepare the communications strategy

Firms should craft a crisis communications strategy that delivers consistent, unified messaging to all internal and external stakeholders:

1 Develop current reference materials for communications.

Some crises can be predicted – maybe not the specific detail, but the general situation – a major system (say, ATM network system) inaccessible, a vendor down, a major weather event. Firms can prepare for the 15-20 most common disruptions they may face, with messages suitable for different constituents, circumstances and media channels. They can draft press release templates and scripts that can be delivered through print and television news at the local and national level, and through key social media channels. They can develop a library of customer communications that covers likely experiences and alternatives, and craft specific messages for high-value customers for each major product or service. Draft crisis communications should also cover counterparties and vendors.

2 Make it clear who speaks to media, when and how.

Too often firms determine who should speak to the media in crisis. Yet, public relations 101 dictates that firms should only put trained, practiced spokespeople forward for comment and confirm that they receive periodic media training on press and television (and their delegates receive the same). Spokespeople need to be accurate and up-to-date in conveying information about known developments, while acknowledging unknown details. Avoid jargon at all times; plain English matters. Firms should keep an up-to-date list of media resources and maintain strong relationships with key journalists at the local and national level – those relationships will be invaluable in helping message the external story.

3 Prepare materials to share with employees.

Employees are the face of the firm. Any predetermined communications strategy has to prioritize them, and brief them quickly, with a focus on what should be communicated to customers and what should remain confidential. Also, employees will likely need guidance on how to access alternative services when disruptions occur – typically, these alternatives can be identified ahead of time to inform in-crisis advice to customers. Firms should remind employees periodically that they should refer media and social-media inquiries to official spokespeople and should adhere to corporate policy on social media, especially during a crisis.

Communications

Prepare the communications strategy

4 **Maintain coordinated, open communications with regulators.**

Establish a playbook for how and when to communicate with regulators on matters involving risk, compliance, legal issues or subject-specific areas. Know how and when to reach law enforcement, and if necessary, national security resources.

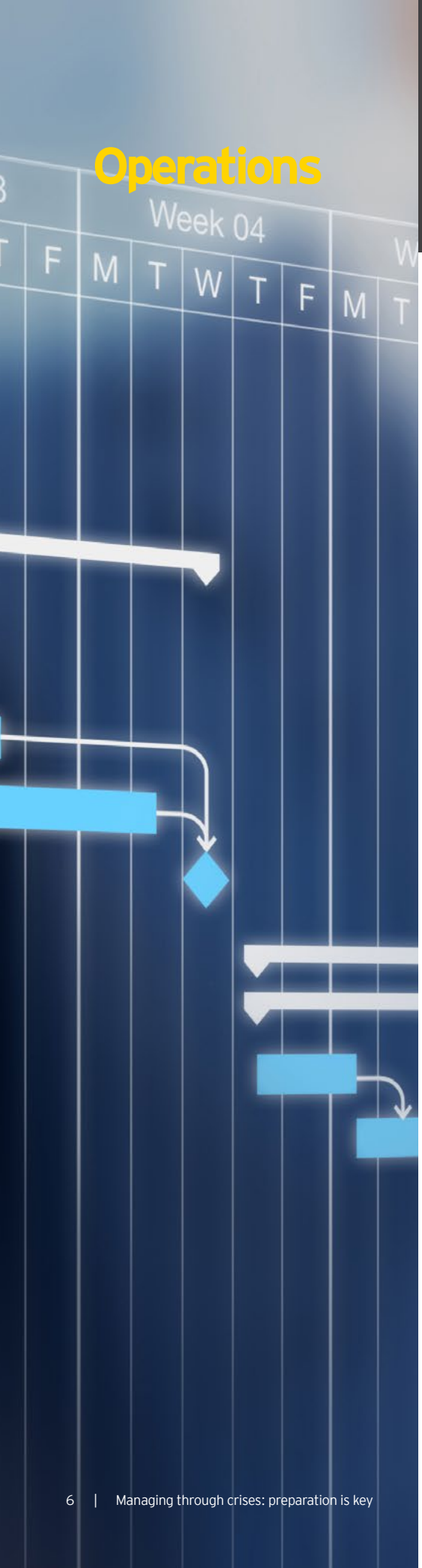
5 **Know the protocols to share information with peers.**

Several major industry-level initiatives have been established in recent years to enable information sharing across parts of the industry and to assist firms when they experience major outages or cyberattacks.[1] Firms need agreed, well-documented communication and escalation protocols in place ahead of time to be able to leverage these efforts in crisis and need agreed protocols with the groups leading those efforts on how external communications will be managed effectively.

6 **Get advice on communications.**

Even with the best preparation, firms should line up access to internal — and external advice, if needed — media and legal advice on the implications of a crisis. Even though firms may skip the full round of sign-offs for communications during a crisis, they need to clear any public statements with their legal team for advice on potential liabilities and with their investigative team regarding what can be said about ongoing breaches. In certain cases where legal advice is relevant, firms should keep lawyers involved to protect their ability to assert privilege of attorney-client communications, so having processes that necessitate strong legal involvement early on is important.

[1]Initiatives in the US include the Financial Services Information Sharing and Analysis Center, Financial Systemic Analysis and Resilience Center, and Sheltered Harbor.



Prepare the operations readiness

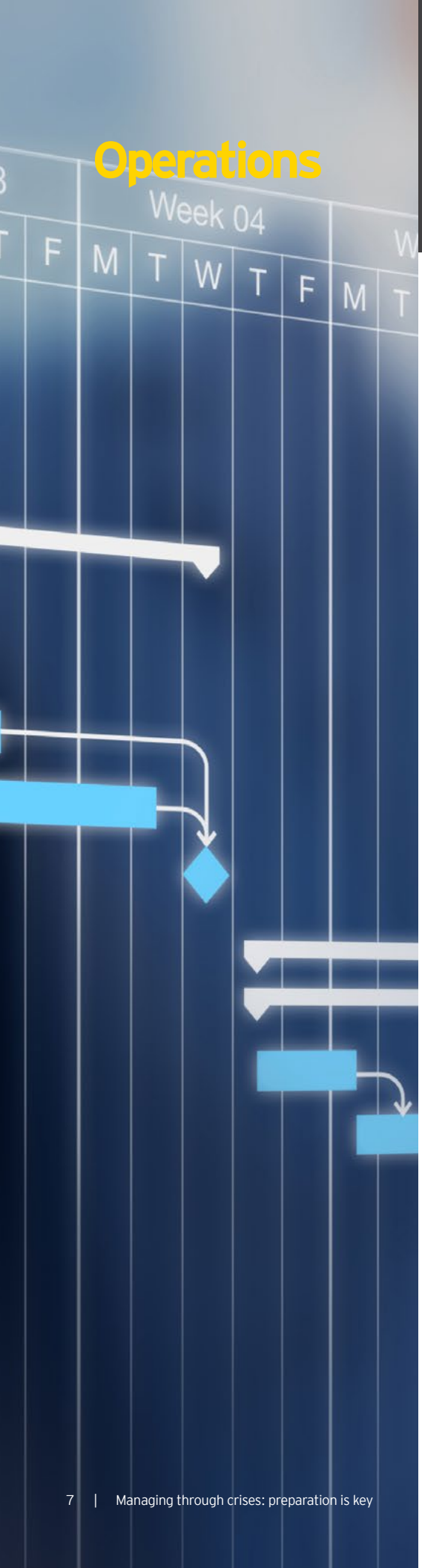
Numerous key decisions on how to operate during a crisis should be made beforehand with the active participation of the firm's senior leadership and, where necessary, the board. The trade-offs involved have a direct impact on customer and counterparty perceptions of the organization, firm liquidity and legal exposures, among others, so they should be considered ahead of time:

1. **Establish processes for identifying the likely most-affected customers.**
   For each scenario anticipated, firms can prospectively identify the most important customers who will likely be most affected — especially those who use the firm across business lines and products. Ahead of time, firms should plan for how to prioritize communications to the most affected customers and which types of transactions and customers should switch over manual or partially automated processes, and consider what concessions could be offered, such as advice, fee waivers or extensions.

2. **Test playbooks and manual processes, and train employees to use them**.
   Firms should use simulations or tabletop exercises around continuity plans to identify and manage choke points and key supporting technologies, and to determine alternatives for each key process that supports customers. For example, if mobile networks and credit card networks are down, banks need a process to rapidly replenish ATMs. Firms should figure out how they would handle a surge in calls and branch visits, with processes for scheduling additional workers to support core functions. They should assess their onboarding requirements to validate they can bring on new resources quickly in times of needs. In addition, they need to have means to divert transactions to alternate electronic channels, manual processes or correspondent banks through emergency batch processes. New technologies — such as chatbots, programed effectively — can help. They should establish procedures to reduce queues, maintain confidence, and avoid inciting very negative customer or public reactions — at the most severe, a run on the bank. It is a balancing act between being transparent and not causing undue concerns.

   In crisis, firms may need to depend on manual workarounds. They should routinely test those processes to validate they work as planned, and make sure they have enough trained staff who can be readily deployed to perform backup processes, especially those linked to volume processing.

3. **Assess potential exposures with suppliers and counterparties.**
   Firms should determine how they would assess the potential impact of a crisis on third parties and should establish contingency arrangements with major business partners, especially critical vendors. Firms have to keep in mind that that their response to a crisis (e.g., reduced withdrawal limits) may undermine confidence in its solvency and liquidity, so they need to prioritize communications with key vendors and counterparties to calm their nerves.



Prepare the operations readiness

4 **Understand and protect your "high-value assets."**

The term "high-value assets" (HVA) refers not to financial assets, but rather the assets of the firm that have enterprise-wide impact on operations, compliance and legal functions, as well as on reputational risk, liquidity risk and disaster recovery. Firms need to document and deeply understand their HVA inventory so that, in crisis, they know where those assets are and how they may be affected. This knowledge can guide business-impact assessments during a crisis and decision-making through to resolution. The inventory should include points of connectivity between key systems and resources for protecting customer data, so that using this information firms have identified ways to protect HVA during different scenarios, e.g., choke points for repelling a ransomware attack or approaches for quarantining compromised systems or data.

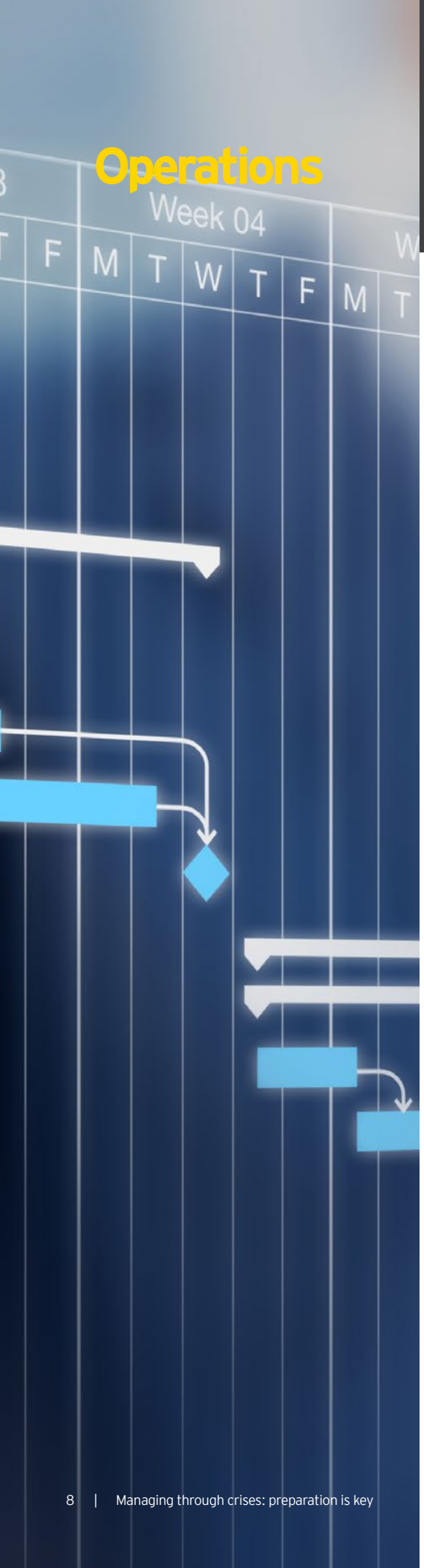
An important element here is knowing how to access "golden-source" data. Firms often emphasize the availability and confidentiality of data in crisis planning, but as important is data integrity given that bad actors' motives also include data destruction. Firms need to know how to quickly access backup data and be able to compare that data with a golden source to validate its integrity.

5 **Link crisis management and management of financial resources.**

During crisis, firms need access to solid financial resources inside the firm or from outside, and those resources have to last a prolonged crisis. Firms need robust, tested financial contingency plans in place, which are linked directly to firmwide crisis management processes, so that, when crises hit, the crisis and operational teams can work effectively with treasury resources to manage liquidity. The financial plans need to facilitate quick access to liquid assets such as securities, cash on hand and credit lines, and recognize that those plans may have to withstand industry-wide market failures, during which many banks and companies will be looking for liquidity and capital at the same time.

6 **Determine documentation protocols.**

As decisions are made during a crisis, it is important they be properly documented, especially when ones are made to go out of policy or take on more risks than is typically accepted. A robust, well-known process for documenting such decisions should be designed and implemented.

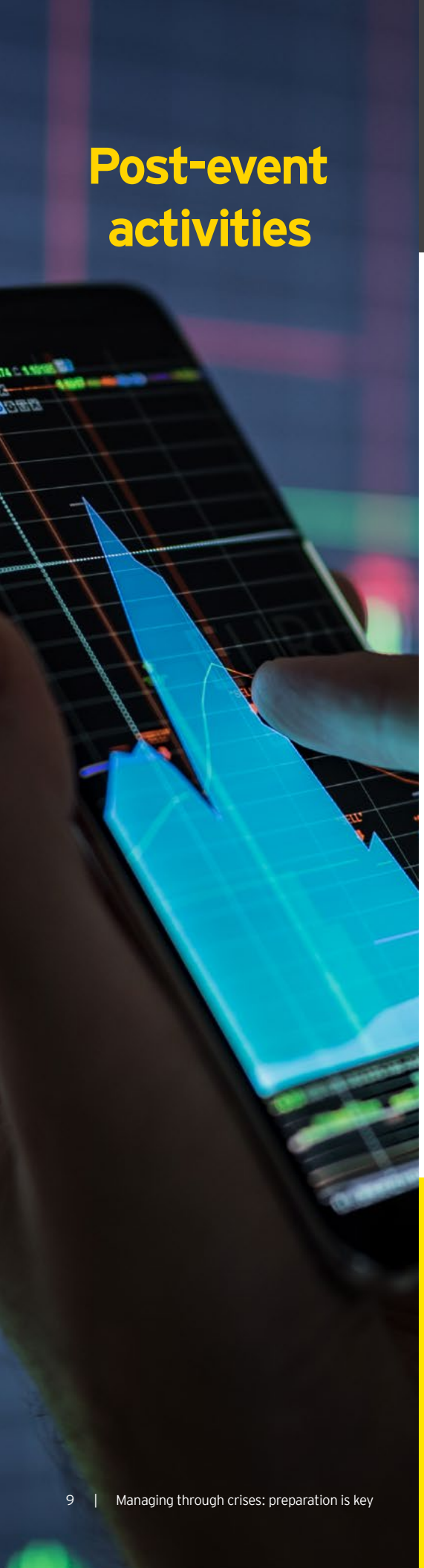


Prepare the operations readiness

7 **Consider how to maintain employee morale.**

Most firms survive through crises because of the sacrifices of their employees — long, extended hours in the office dealing with the crisis. During prolonged crises, employees can become exhausted, and morale can be low. Firms should develop plans for how to maintain morale during crises, such as through internal communications, combat pay and other such ways to reward commitment. Daily "thank yous" make the most difference, but a formal plan to offer reward and recognitions complements them.

Post-event activities



Prepare for post-event activities

It's not just about preparing for an event. It's important to plan for after the event — the recovery period — and learn from it to improve over next time:

1. **Compile a library of post-event processes.**
   During a crisis, firms should not focus on determining the root-cause analysis, however tempting. Nevertheless, one will be required eventually, as will other the performance of post-event processes, such as disaster recovery failback, data reconciliation (especially when the firm's data was corrupted) and operational-loss analyses. So firms should fully document those processes, along with when and how they should be initiated or restored after the event.

2. **Keep an audit trail.**
   A critical input into post-event processes is documenting what happened during the crisis, and what decisions were made and why. In addition to helping organizations learn, such an audit trail helps demonstrate the reasonableness of decisions made considering the circumstances and information available, which can be invaluable given the potential for post-event litigation or regulatory or insurance-related discussions.

3. **Learn from past disruptions.**
   Above all, firms have to learn from past events — theirs and others' — to continually enhance crisis management. Sound analysis looks at near misses and considers what-if scenarios as to what might have happened if decisions or actions had been different.

Conclusion: Prepare, prepare, prepare

Crises involve complex questions and decisions that are wholly unsuited to being resolved during the heat of a crisis. Accordingly, it is an incredibly valuable use of time for firms' senior leaders to examine their preparedness for crisis, taking the steps necessary to make sure they are well placed to actually manage effectively through a crisis so their businesses and reputations stay intact.

Firms may not be able to plan for every circumstance, but preparation can make a difference in how every situation is addressed in crisis.

Asking better questions afterward

As the dust settles, it is important that every firm learns from how well it managed through a crisis or material business disruption. This is more than a technical exercise. It is about installing a learning culture, where continuous feedback and action elevates firm preparedness.

Areas of note and questions to consider include:

Detection failure

Rarely is a crisis not foreseeable or at least somewhat visible before it becomes a full-blown crisis – what early warning indicators failed or were missing? What indicators were present, but not acted upon?

Control design failure

Rarely is an important control so poorly designed at the outset that it fails completely – has the process or environment evolved so much since the control was implemented that its effectiveness has waned to the point it is now ineffective or insufficient?

Systemic control failure

One control or set of controls rarely causes a crisis – why did the entire system of controls – from preventive through detective to corrective – fail?

Complexity failure

Crises usually are not caused by simple systems – does the way a system of controls interact create problems, such that sheer complexity was to blame?

Sheer luck

Sometimes, firms get through by the seat of their pants depending on the quality of live decision-making or on luck – what controls could be put in place or enhanced to lessen the dependence on judgment or luck?

Contacts

Americas - United States

Lisa Choi
lisa.choi@ey.com
+1 212 773 8947

John Doherty
john.doherty@ey.com
+1 212 773 2734

Cindy Doe
cynthia.doe@ey.com
+1 617 375 4558

Sundeep Nehra
sundeep.nehra@ey.com
+1 212 773 3888

Dan Stavola
dan.stavola@ey.com
+1 201 551 5073

Mark Watson
mark.watson@ey.com
+1 617 633 5570

Latin America

Bismark Rodriquez
Advisory, Risk
bismark.rodriguez@pa.ey.com
+1 239 7383643

Ariel Koch
Advisory, PI
ariel.koch@cl.ey.com
+56 2 676 1329

EMEIA

Ali Kazmi
akazmi@uk.ey.com
+44 20 7951 9052

Steve Holt
sholt2@uk.ey.com
+ 44 20 7951 7874

Asia-Pacific

Chris Lim
chris.lim@sg.ey.com
+65 6309 6320

Jeremy Pizzala
jeremy.pizzala@hk.ey.com
+852 2846 9085

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. 04243-181US
1808-2837500 BDFSO
ED None

ey.com