

**CU
NY** THE CITY
UNIVERSITY
OF
NEW YORK

Risk and Crisis Management:

**Are you as prepared as you *think* you are?
Are you as prepared as you *need* to be?**

Introduction

Level setting on terminology

Resilience is a state of preparedness and capability that is achieved, in part, through strong orchestration of disaster recovery, business continuity and emergency management disciplines, as well as the larger and more integrated incident and crisis management programs.



Emergency Response:

Processes, procedures, and capabilities related to the immediate response following an incident, emergency, or disaster in a coordinated, timely, and effective manner. Typically focused on physical, environmental, life safety concerns.



Incident Response:

The process, procedures, and capabilities for an organization to respond to a disruption from initial detection through resolution. This is often separate from Emergency Response because of the level of severity and spread of impact.



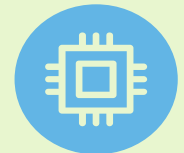
Crisis Management:

Executive-level command and control focused on high-impact decision making during an abnormal and unstable situation that threatens the organization's strategic objectives, reputation, or viability.



Business Continuity:

Capability of the organization to restore business operations, or supply chain, to an acceptable level of performance within a defined timeframe following a disruption.

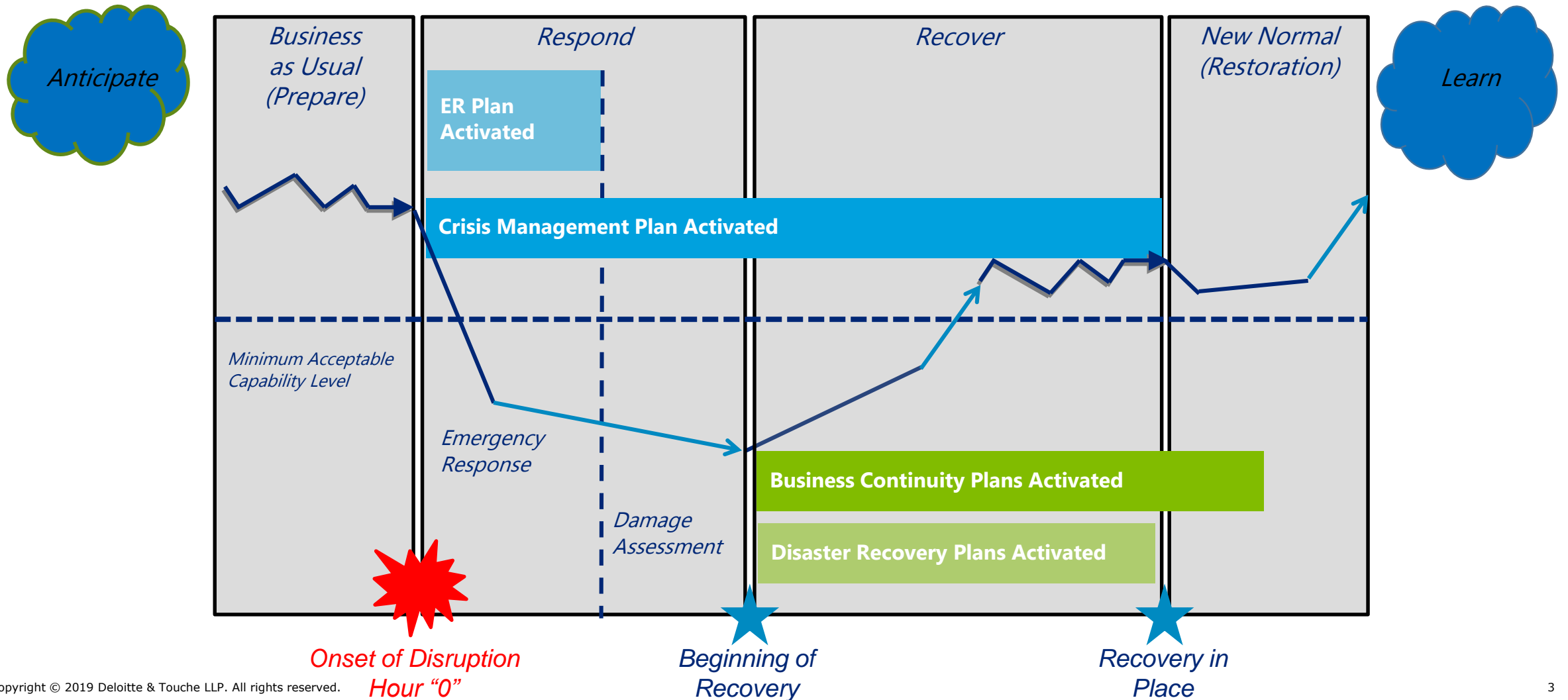


Disaster Recovery:

Infrastructure and procedures required to restore critical infrastructure, applications, and data in line with business expectations for recovery.

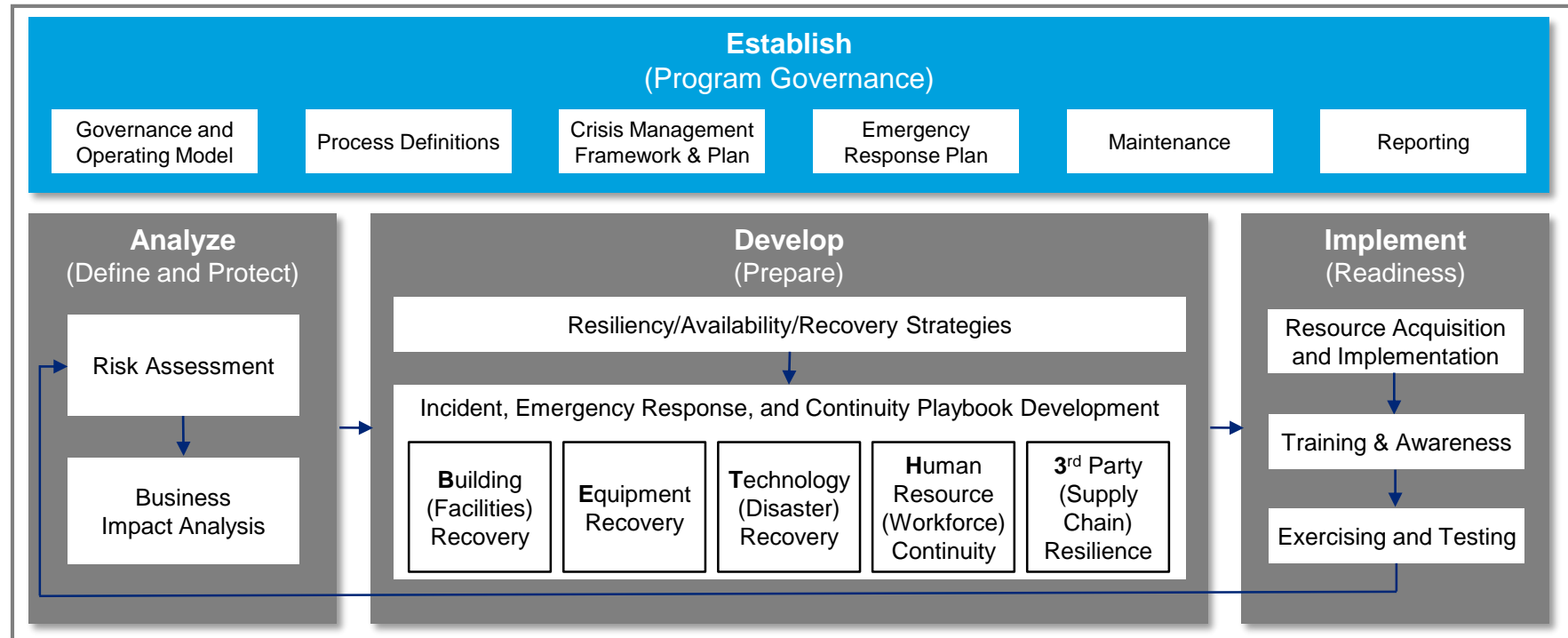
The role of each resilience discipline in response, recovery, and restoration

While developing response and recovery capabilities, it is important to consider a holistic and integrated approach that considers the dependencies between various, different but related disciplines. As shown in the sample event timeline below, an effective response and recovery depends on multiple teams working in a coordinated manner to create an effective response.



Deloitte's Resilience Methodology

Our resilience methodology is aligned with global and national standards and depicts a full, end-to-end implementation of a program. We have seen many programs aligned to standards that are not recoverable. Our methodology is based in standards, but not hamstrung by it.



A proven methodology: Deloitte named a global leader in Strategic Risk Management Consulting, based on capabilities, by ALM Intelligence, and advocates crisis preparedness and business continuity planning to prepare and be able to respond appropriately to crisis events¹.

¹ Source: ALM Intelligence; Strategic Risk Management Consulting 2018; ALM Intelligence estimates © 2018 ALM Media Properties, LLC. Reproduced under license

A crisis is...

- Misdeeds and financial crime
- Confrontations, technological and industrial disruptions
- Financial distress and bankruptcy
- Natural disasters or man-made destructive events
- Malevolence and cyber

“... a major catastrophic event, or a series of escalating events, that threatens an organization’s strategic objectives, reputation, or viability.”

- Market Share and Value
- Credit and Financial Resources
- Physical Infrastructure
- Intellectual property

- Credibility
- Brand
- Environment

- Profitability
- Solvency/Distress

Crises typically exceed existing mitigation techniques and risk management programs such as Business Continuity, Disaster Recovery, Health and Safety plans, or Emergency Response.

What makes crises different?



New leaders and procedures are introduced to the decision-making process



Normal decision-making cycles are compressed based on the urgency of the situation



Leaders have to make decisions without complete information



The stakes are higher - a tactical level decision can quickly have strategic level implications (e.g. threaten reputation and/or viability)

Crisis Management | An Overview

So What Could Go Wrong?

"A reputation crisis – where an organization may suddenly lose more than a fifth of its value – carries 80% likelihood in five year period."

2008

Corruption

An engineering firm pays a \$250M settlement to a foreign government and pleads guilty to U.S. corruption and conspiracy charges related to bribery to secure contracts.

2010

Data breach

Firm account information for 170K employees is stolen, activists attempt to harass employees via disclosed information

Industrial accident

An explosion and sinking of an oil rig results in the largest oil spill in U.S. history

2012

Reputation

An investigation reveals that a major oil company's own research warned of man-made climate change over 30 years ago, but the company chose to invest \$30M in climate denial activities

Natural disaster

Hurricane Sandy knocks out power to 2.2M customers and raises questions about utilities' preparation and response capabilities

Cyber attack

Hackers overtook control of a network of power systems, leaving 230,000 people temporarily without power and crippling the system for months

Environmental disaster

A mining tailings dam bursts, flooding communities with toxic sludge and killing 19 people

2016

2014

Labor strike

Multi-refinery employee strike disrupts operations for 200 production facilities and 65 refineries

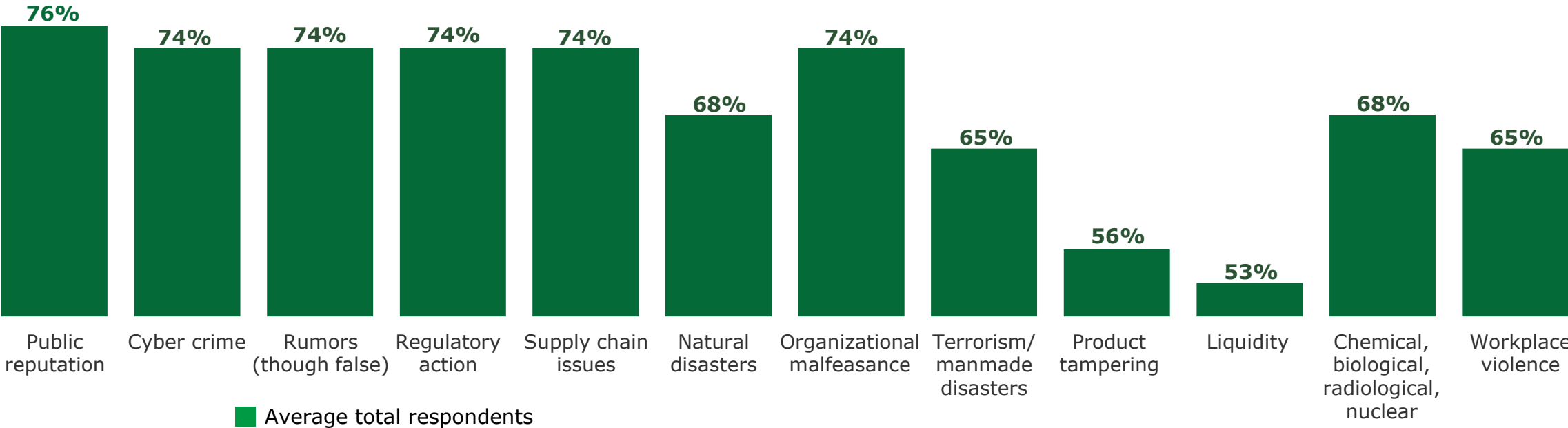
Liquidity crisis

A solar company declares bankruptcy following a liquidity crisis compounded by high debt, missed filings, a failed acquisition deal, and a federal investigation



Ranking the Threats

We asked organizations how vulnerable they might be to the following crises:



Excerpted from "A Crisis of Confidence." To assess the state of crisis readiness in large organizations, Forbes Insights, on behalf of Deloitte Touche Tohmatsu Limited, conducted a survey of more than 300 board members from companies representing every major industry and geographic region. The survey, conducted in the fourth quarter of 2018, targeted companies with annual revenues that ranged from US\$500 million to more than US\$20 billion (or the equivalent).

Importance of Crisis Management

Not all events are predictable, and events such as cyber attacks typically exceed existing mitigation techniques and risk management programs (including business continuity, disaster recovery, and emergency response).

Having an integrated and disciplined program that connects risk → issue → incident → crisis management in place can significantly reduce the financial, legal, and brand image impacts from a major disruption.

High Value Targets for Higher Education



Critical Infrastructure

- High visibility target with high downtime costs
- Complex control systems designed for high availability, not security
- Automation and interconnectivity have increased risk
- Vulnerability mitigation may be cost-prohibitive



Intellectual Property (IP)

- “Crown jewels,” may prime source research, publications, protected sources, etc
- Adoption of cloud computing, globalization, and third party services have increased risk
- IP theft can be difficult to detect and impact may not be felt immediately



Reputation and Brand

- One of the most important and valuable assets
- Highly vulnerable to negative events, including a cyber incident
- May take an extended time to restore reputation



Financial Data

- Highly regulated and exposure can adversely impact grants, endowments, and other funding
- Adoption of cloud computing, globalization, and 3rd party services have increased risk

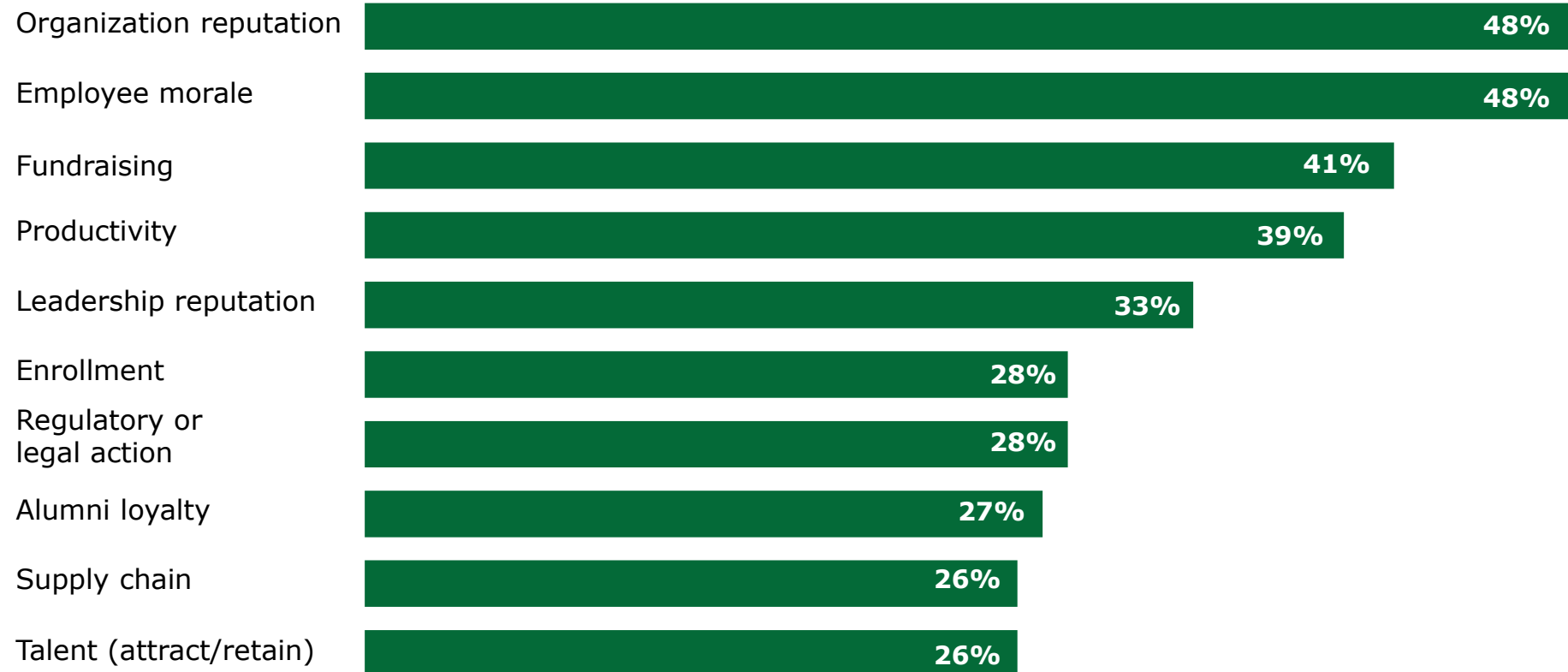
It Takes a Long Time to Recover. Here Are the Most Severe Impacts.

Board members with direct crisis experience shared the areas of the business where past crises have hit their organizations hardest. Respondents selected all answers that applied.

69% of organizations reported their public reputation took more than 1 year to recover

16% said it took 4 years or more

15% of organizations were able to recover their reputations in only 1 year



■ Average total respondents


Excerpted from "A Crisis of Confidence." To assess the state of crisis readiness in large organizations, Forbes Insights, on behalf of Deloitte Touche Tohmatsu Limited, conducted a survey of more than 300 board members from companies representing every major industry and geographic region. The survey, conducted in the fourth quarter of 2018, targeted companies with annual revenues that ranged from US\$500 million to more than US\$20 billion (or the equivalent).

Crisis Management | An Overview

Principles for Crisis Management



1
Lead decisively



2
Continually frame the crisis



3
Actively communicate



4
Be ready for the unexpected



5
Drive towards actionable intelligence

Additional Considerations

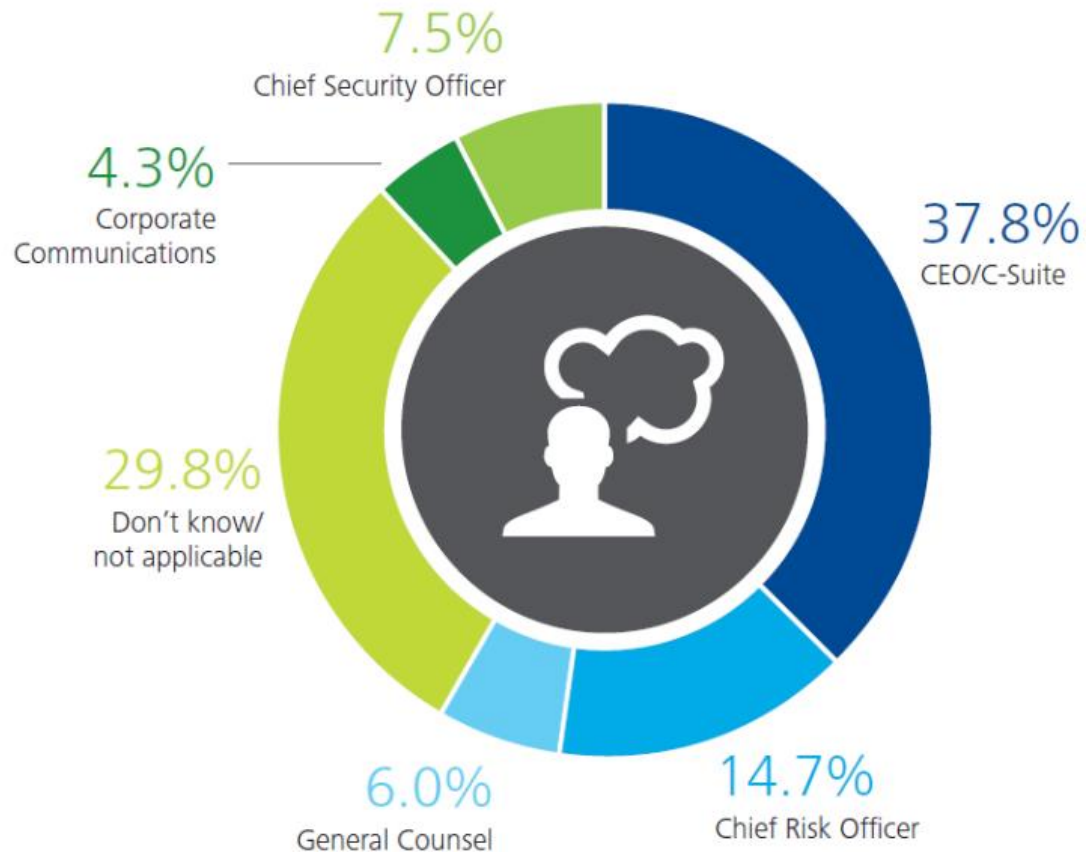
- **How** prepared are you for the next crisis?
- **Who** are your critical internal and external stakeholders, and what is the status of those relationships?
- **Do** you have a crisis management plan, and when is the last time you tested it?

Crisis Management | An Overview

Building Crisis Leadership

In a crisis, who in your organization would lead the crisis response?

Breakdown based on 2,060 responses received.



While any leader attempts to manage a crisis, they will need to avoid these common stumbling blocks, including...

- Excessive focus on fixing the incident, rather than leading the response and addressing the strategic impacts
- Failing to understand or underestimating the scale, breadth, and speed of the crisis and its unanticipated consequences
- Making inaccurate decisions and unintentionally causing harm, due to bad or incorrect information in the first few hours of a crises
- Not having enough time to make sense of the chaotic inflow of information and answering all of the direct inquiries

Quotes from C-Level and Senior Executives about Risk and Crisis Management

"The entire organization does not have a good sense of the true risks they face."

"There is a misunderstanding in the business about how prepared they are and what our priority risks are."

"We focus too much on recovery for the IT part of the organization."

"We've split this into 100 parts...and react when one thing comes up. No cohesiveness."

"It's easy to put a plan together, but it's hard if you want it to be executable."

"Integrated testing, which brings it all together, has yet to happen."

"If you're not carefully examining the true character...and how they're going to operate under pressure...you really put yourself at risk."

"We need somebody who can lead confidently during a crisis."

"A good leader, needs to be decisive, needs to get a quick grasp on the situation, needs to be able to make decisions and take action on less than perfect information."

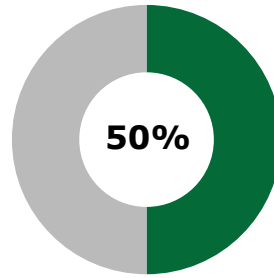
"As we became more powerful as a network, the key attribute was information sharing."

Feeling Ready vs. Being Ready

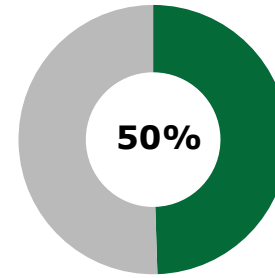
Most steps toward crisis preparedness go ignored

Half the total respondents or fewer reported having engaged in each of a list of specific crisis preparedness activities.

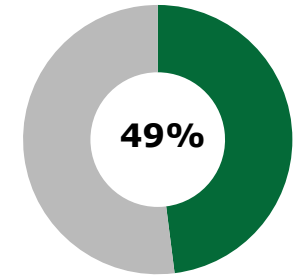
Evaluated
key crisis scenarios



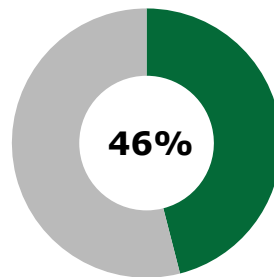
Evaluated
strengths/weaknesses/
opportunities/threats (SWOT)



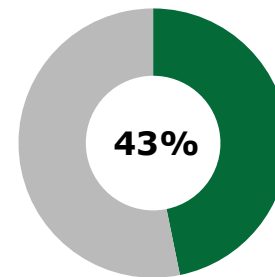
Identified
relevant stakeholders



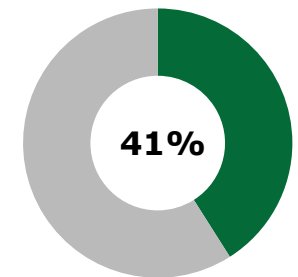
Evaluated risks with
multifunctional teams



Evaluated
worst-case scenarios



Engaged stakeholders in
analysis of specific scenarios



†Figures in black are total survey results. Graphical representations are based on these total results.

* Excerpted from "A Crisis of Confidence." To assess the state of crisis readiness in large organizations, Forbes Insights, on behalf of Deloitte Touche Tohmatsu Limited, conducted a survey of more than 300 board members from companies representing every major industry and geographic region. The survey, conducted in the fourth quarter of 2018, targeted companies with annual revenues that ranged from US\$500 million to more than US\$20 billion (or the equivalent).

Many organizations are prepared for 'routine' crises, but not 'novel' ones

A novel crisis is an emergency of unusual scale, unknown cause, or atypical combination of events where facts and implications cannot be ascertained in the moment of crisis.

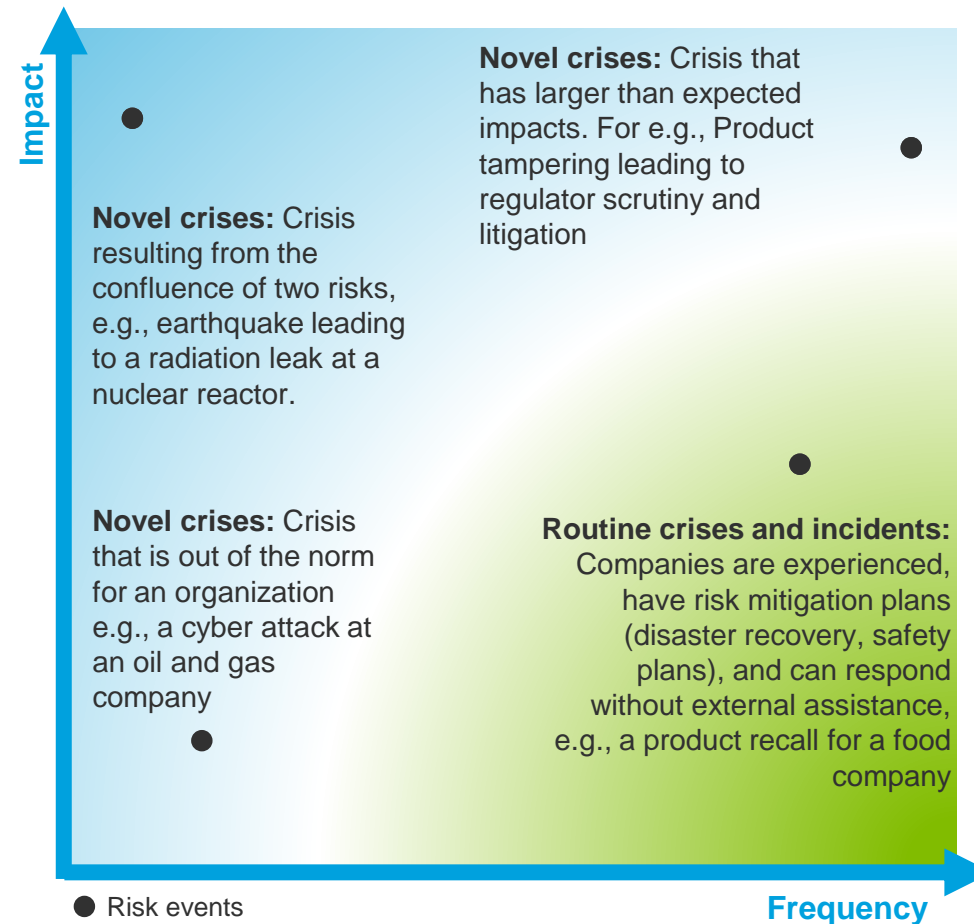
Identifiers include:

- *High level of uncertainty*
- *High stakes*
- *Unknown circumstances*
- *Intellectual challenges*

A routine (familiar) crisis is a particular kind of emergency that occurs frequently where resources have been established to organize and prepare for such an event.

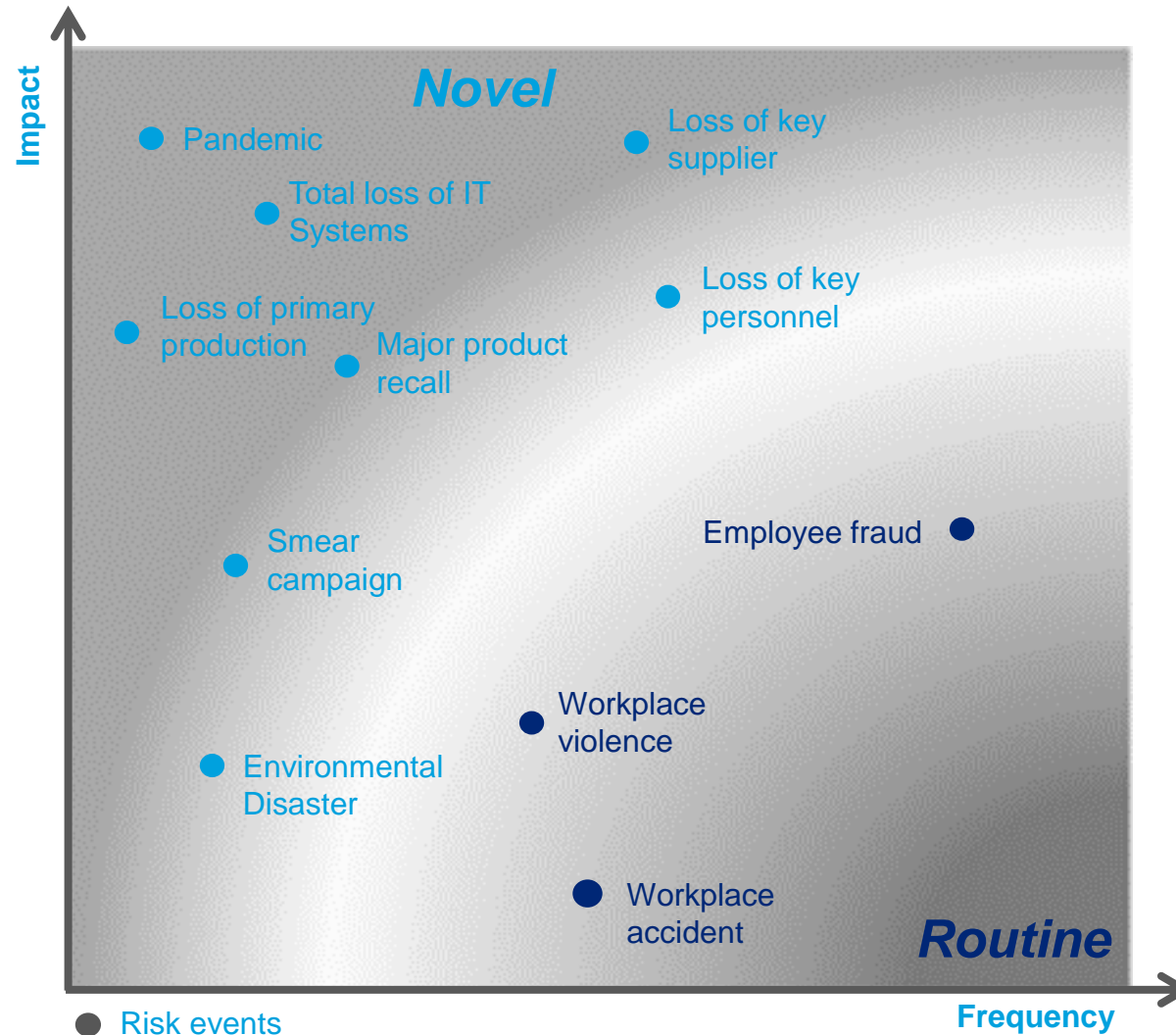
Identifiers include:

- *General pattern*
- *Organized preparation*
- *Practiced response*



* Based on interpretations from the work of H.B. Leonard and A.M. Howitt
Communicable Crises: Prevention, Response, and Recovery in the Global Arena, pp. 1-25

What potential crisis impacts do you want to assess?



Scale/ Magnitude: Would your CM response organization be able to handle a typical event if was 2x or 10x the normal size?

Complex/ Combined: Would your CM response organization be able to handle multiple typical events if they happened at the same time?

New/ Unknown: Would your CM response organization be able to handle known unknowns or unknown unknowns?

How could you be better?

CRISIS MANAGEMENT MATURITY MODEL

+ GOVERNANCE

Crisis management policy and framework
Executive support
Program ownership

+ ORGANIZATIONAL ALIGNMENT

Business continuity (BC)
Risk management (RM)
Stakeholder engagement strategy

+ RESPONSE ORGANIZATION

Response plans
Response structure
Support teams

+ CRISIS DECISION MAKING

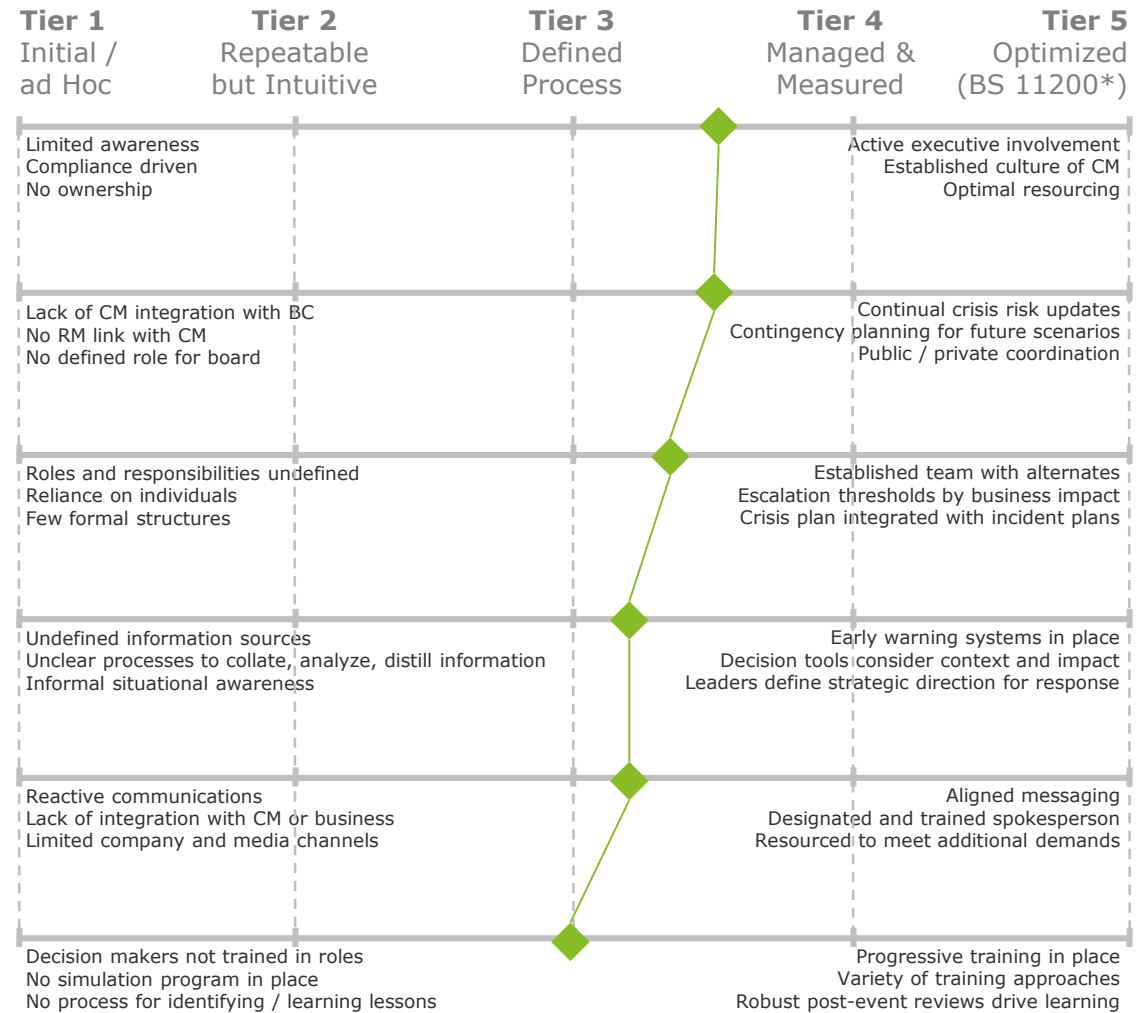
Monitoring
Information synthesis
Decision tools and templates

+ CRISIS COMMUNICATIONS

Communication plan
Real-time stakeholder engagement
Message authorization and synchronization

+ CAPABILITY DEVELOPMENT

Capability measurement
Capability development
Continual improvement



◆ Average

The average is calculated responses from 314 board members from companies representing every major industry and geographic region
*British Standards Institute (2014) BS 11200:2014 Crisis management - Guidance and good practice

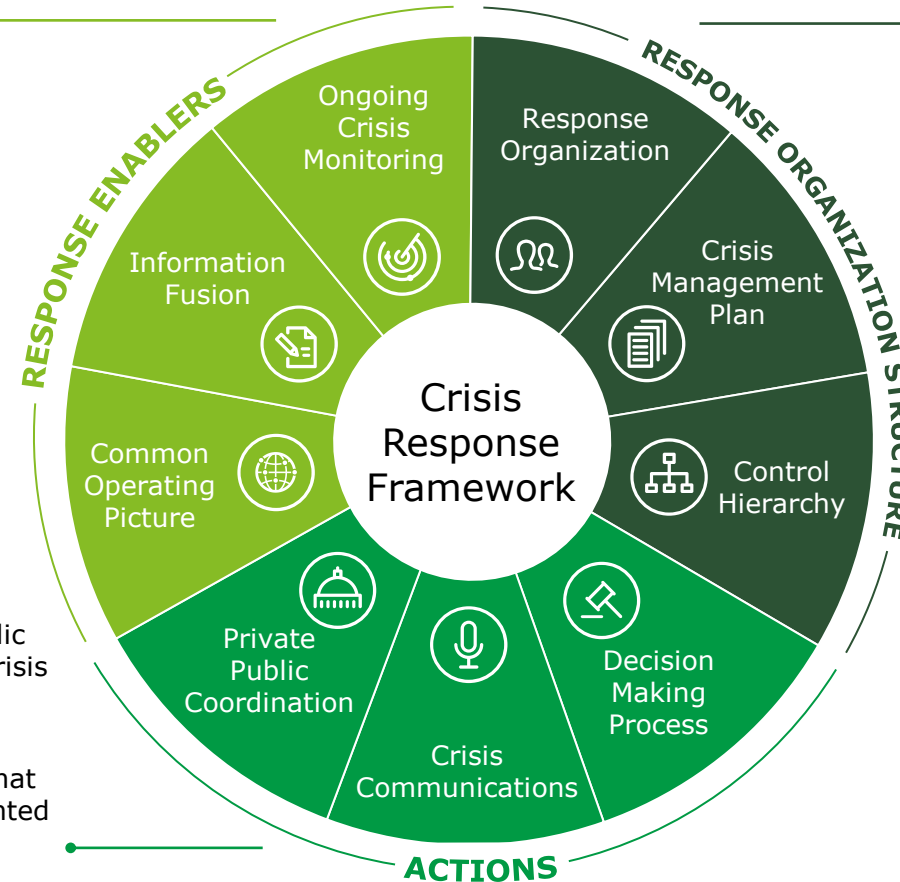
A good crisis management program has these elements...how prepared are you?

Response Enablers

- What capabilities do you currently have to monitor your internal and external environment?
- During a crisis, how does your team track event details and response actions?
- To what extent does your team have the ability to collect, curate, and disseminate situational awareness in order to inform action?

Actions

- In what ways have your crisis leaders been prepared to lead coordination between the public and private sector, should a crisis arise involving critical infrastructure and resources?
- How does leadership ensure that communications are implemented with a tone "set from the top"
- What pre-established process/tools does your CM team use to analyze, assess, make decisions, and take action?



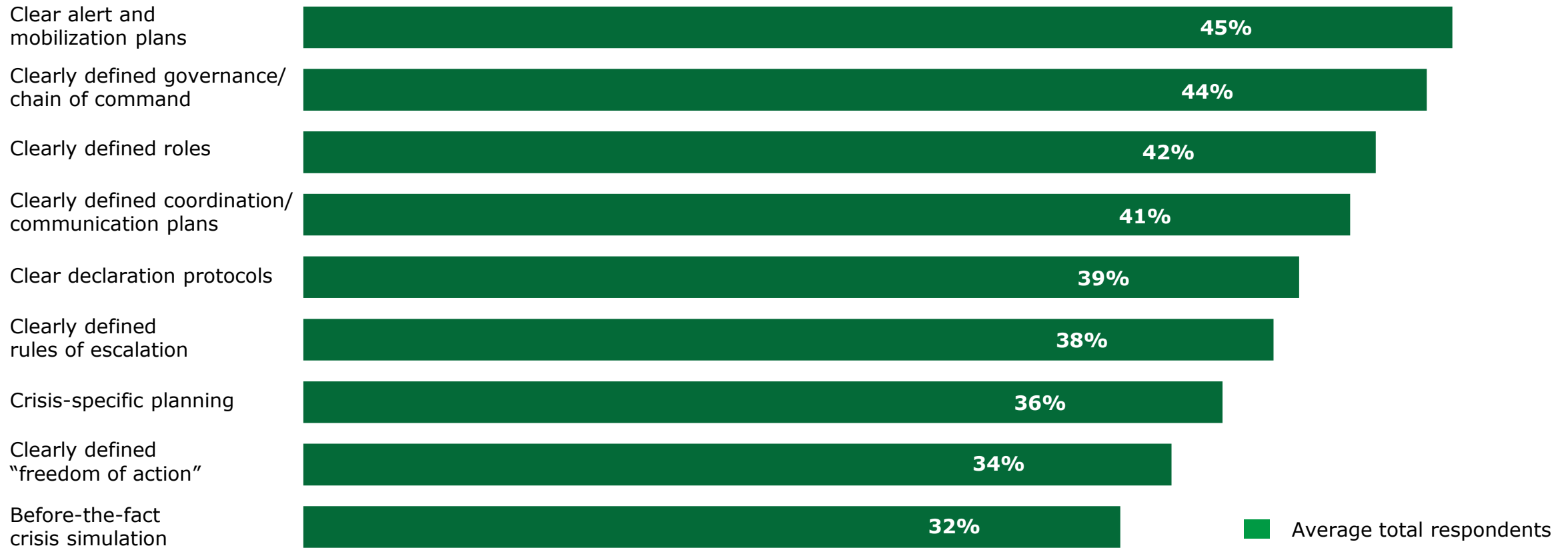
Response Organization Structure

- How many leaders are identified on your crisis leadership team, and how frequently are they trained on the plan?
- What guidelines exist in your plan to help the CM team identify actions and issues throughout a crisis?
- Where do you document and define thresholds and decision rights?

Does Your Plan Translate into Action?

A closer look at crisis plans and preparation reveals that key elements may be missing.

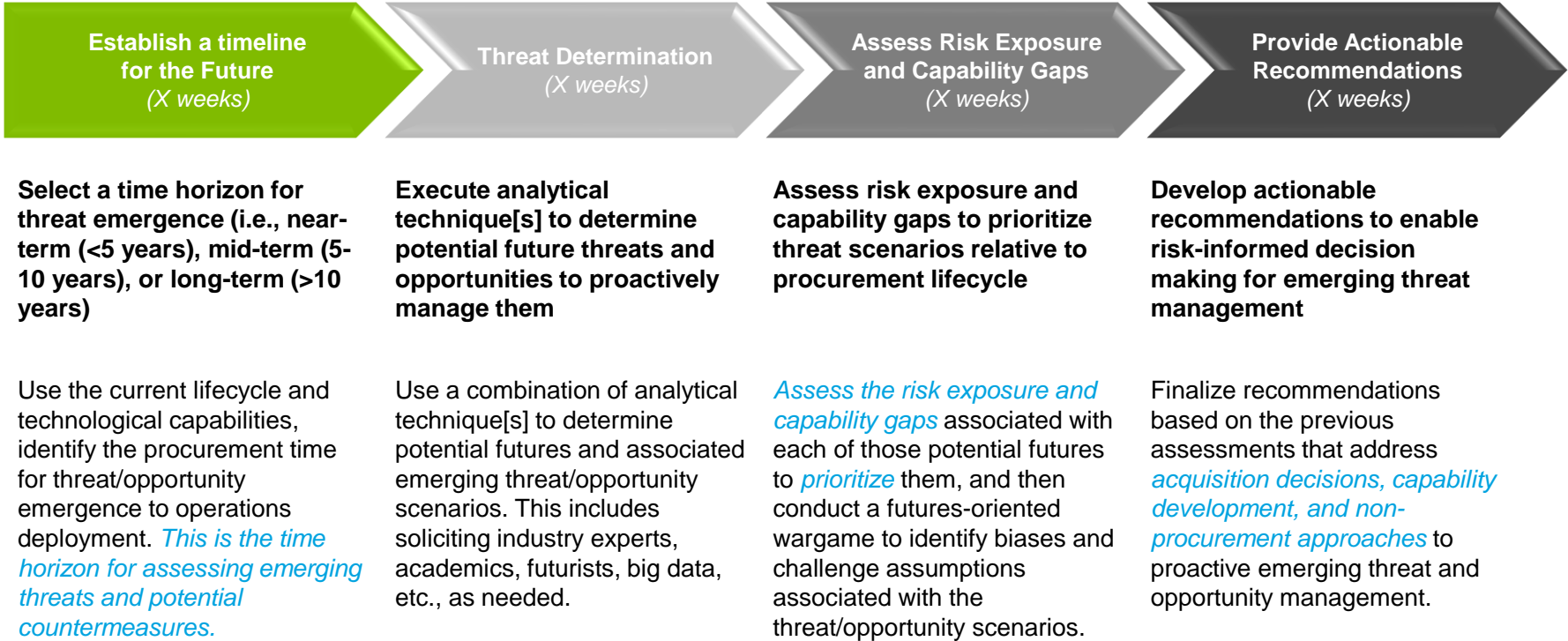
Fewer than half the total respondents reported that their planning included the elements below. Crisis simulations ranked last out of all planning elements overall.



Excerpted from "A Crisis of Confidence." To assess the state of crisis readiness in large organizations, Forbes Insights, on behalf of Deloitte Touche Tohmatsu Limited, conducted a survey of more than 300 board members from companies representing every major industry and geographic region. The survey, conducted in the fourth quarter of 2018, targeted companies with annual revenues that ranged from US\$500 million to more than US\$20 billion (or the equivalent).

Strategic Foresight is a critical element of preparedness and resilience

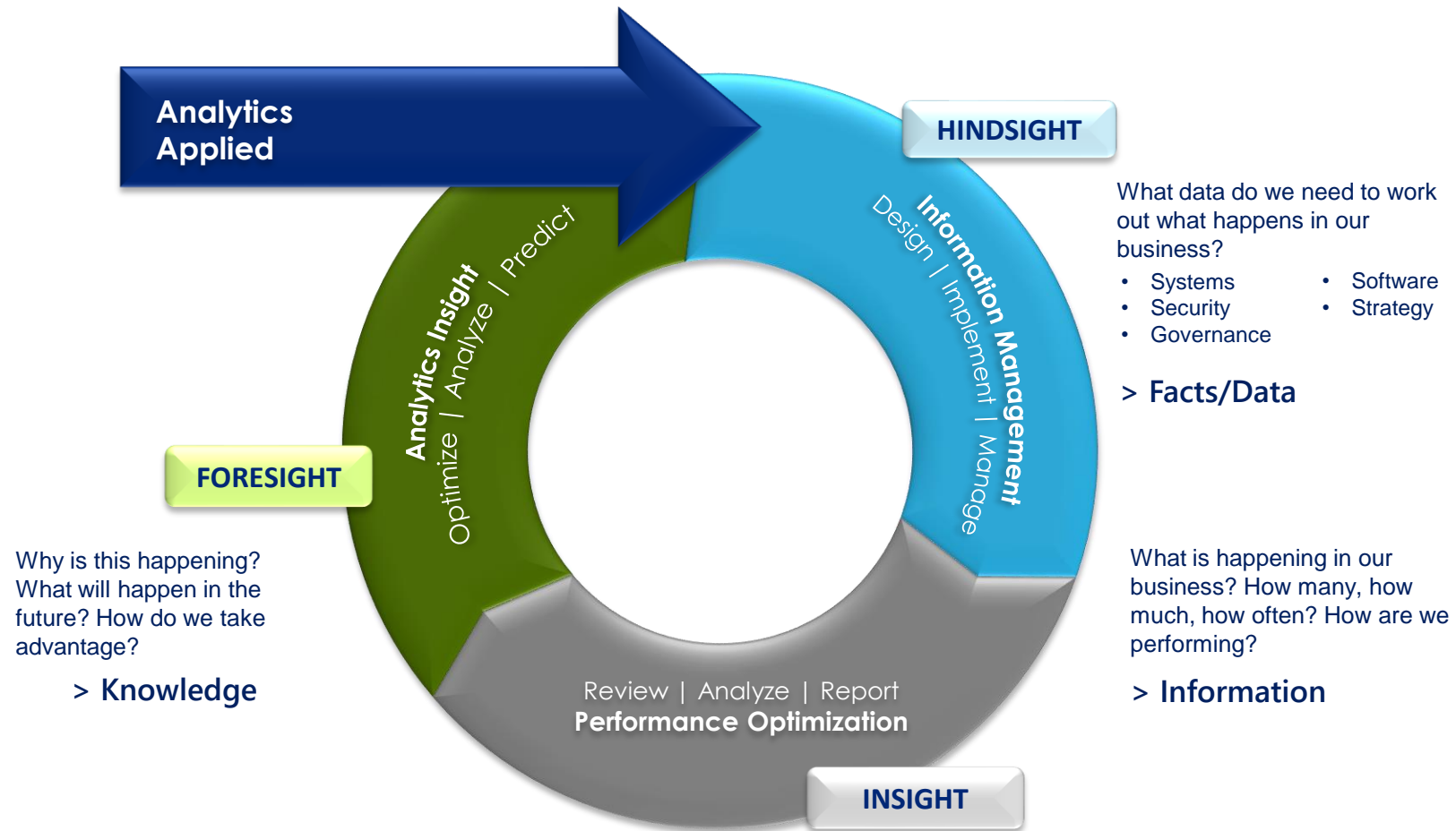
How can you proactively respond to potential emerging threats and identify emerging opportunities?



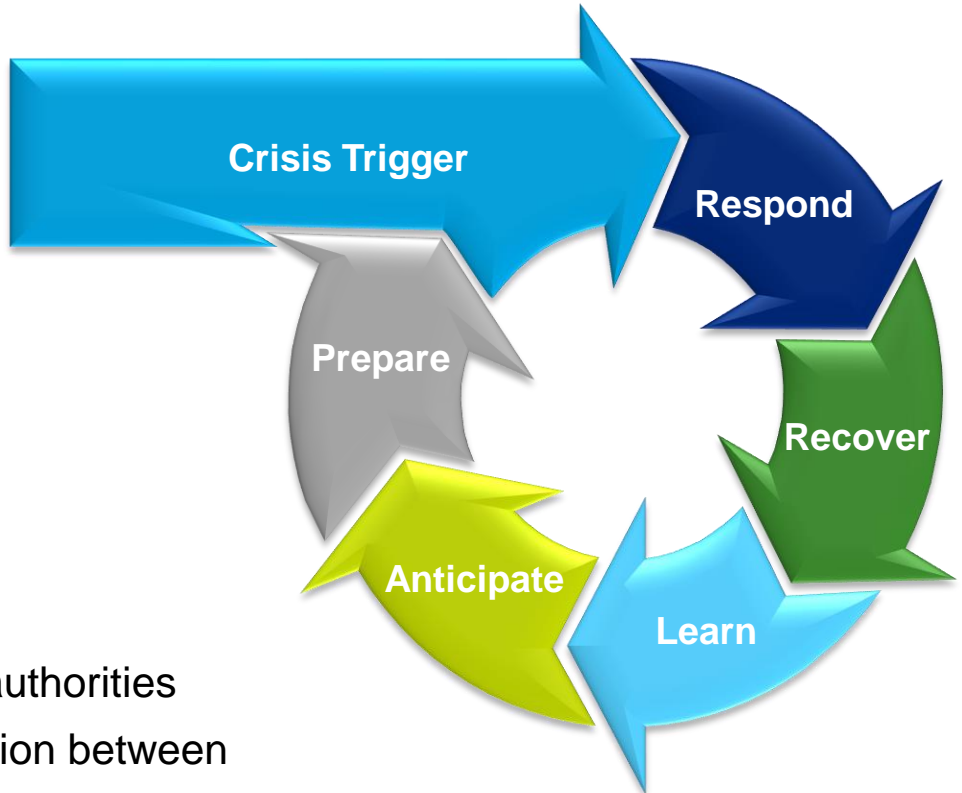
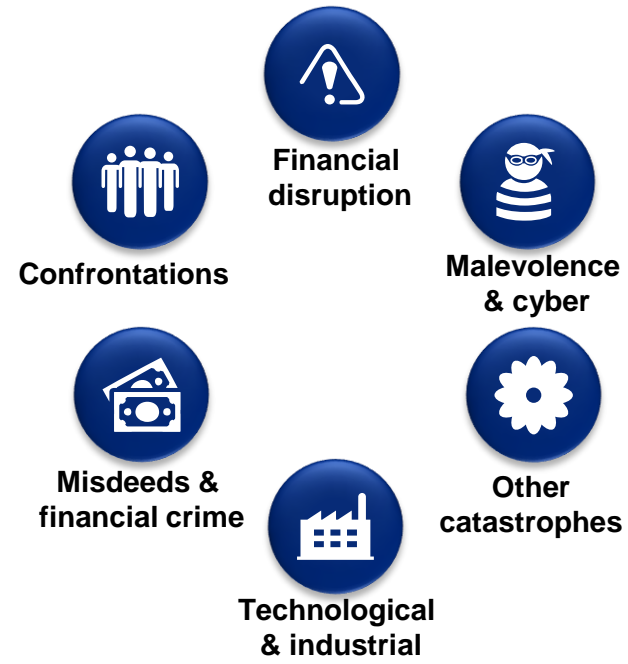
By identifying emerging threats and opportunities, and developing strategic foresight capabilities, organizations can proactively address future disruptions, *minimizing negative and taking positive risk.*

Risk Analytics—purpose

Risk analytics can be used to provide hindsight into what has occurred in the past, insight into present business dynamics, and foresight into potential futures.



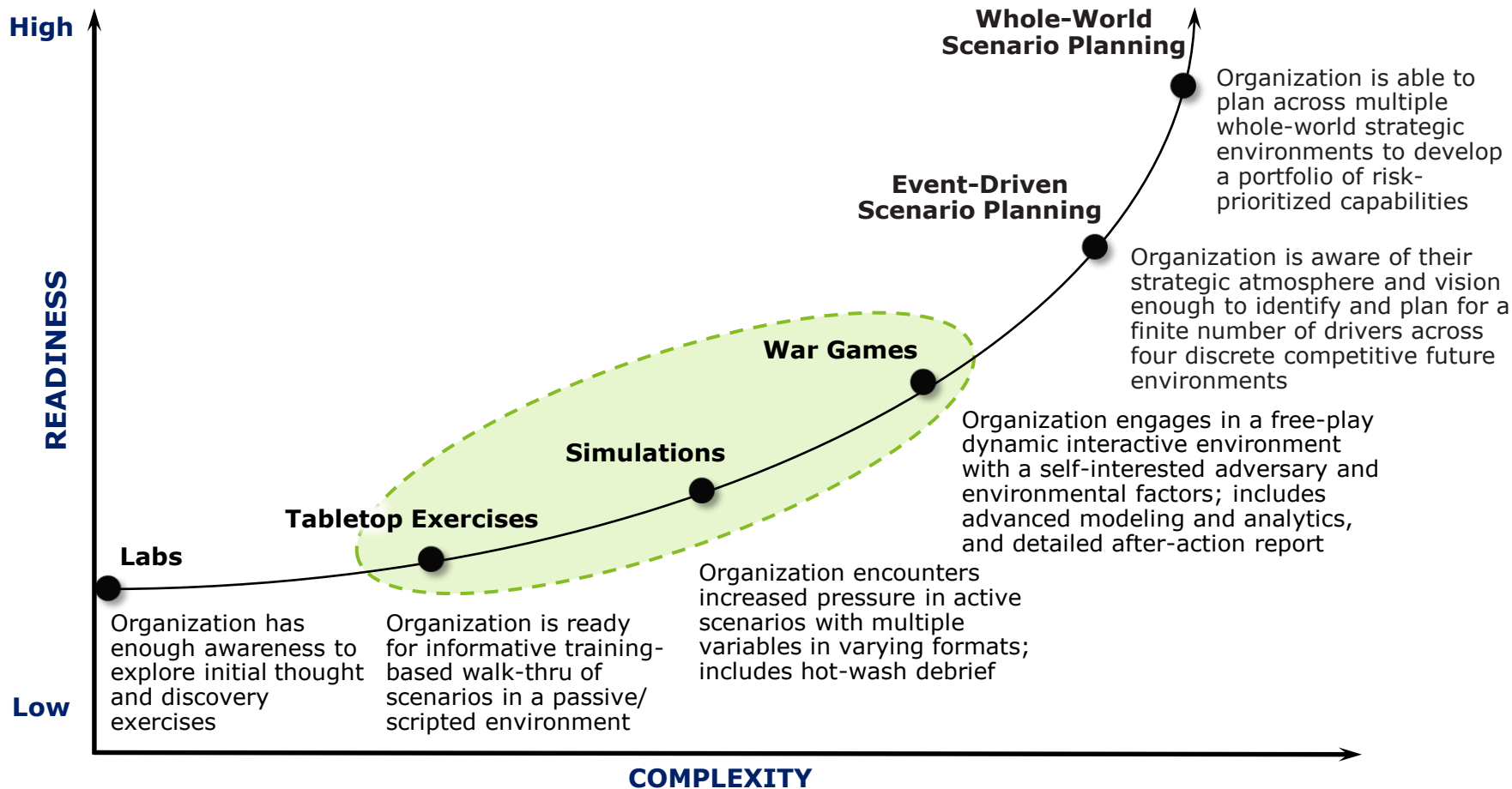
Rehearsing and practicing *before* a crisis leads to greater success in responding and recovering *afterward*



- ✓ Defined roles and authorities
- ✓ Practiced coordination between groups
- ✓ Prepared clear guidance
- ✓ Developed tools and templates
- ✓ Integrated lessons learned









Immersive Experiential Learning

Organizations will fall along different stages of the Readiness Complexity curve as they understand their environment and prepare for their future. Understanding where you are on the curve will help identify conversations and tools to help increase your awareness and foresight.


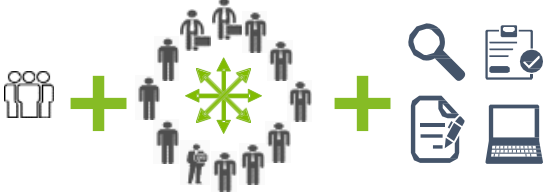

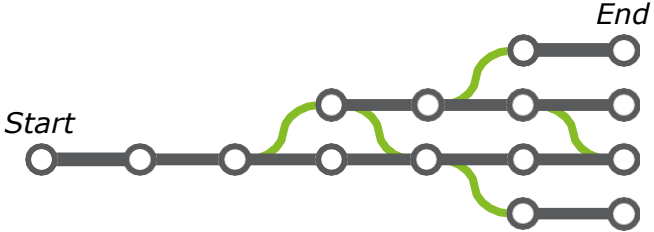


Methodology remains constant across all 3 types of events—complexity and maturity change

For Added Complexity:

-  Games Within the Game
-  Stop/Start/Pause/Rewind/Replay
-  Insertion & Extraction of Key Players
-  Automation and Modelling & Simulation
-  Blue Force Tracker
-  Extended Duration & Multiple Locations
-  Double-Blind Moves & Countermoves
-  Virtual Reality and Biometric Feedback

What if we already do exercises?

| | Traditional tabletops | War game |
|-----------------------------|--|--|
| Exercise structure |  <p>Players engage in a theoretical discussion of disruption response activities</p> |  <p>Players, with facilitator support, simulate response to an evolving business continuity event</p> |
| Exercise progression |  <p>Exercises are static in nature – scenario progression is planned in advance</p> |  <p>Exercises are dynamic – scenario progression is based upon player actions and decisions</p> |

War games are more realistic and more dynamic than traditional tabletops, resulting in increased participant engagement and learning

Considerations for building a practical and sustainable crisis management program

- ❑ Establish the vision and mission that aligns the leadership, operations, and stakeholders
- ❑ Build a governance program – get business leaders involved
- ❑ Develop the plan and include the right stakeholders (including the “*unusual suspects*”)
- ❑ Prioritize sensing, scanning, and anticipating in the areas biggest risk (threats *and* opportunities)—this may not always be the business functions with the most revenue and brand impact
- ❑ Understand the connectivity and progression from risk→ issue→ incident→ crisis
- ❑ Exercise, Exercise, Exercise...capture lessons, train to learn them
- ❑ Maintain the right focus—address the strategic impacts; avoid fixation on the tactical
- ❑ Be ready for the unexpected—the “enemy” gets a vote, as does the market...honestly answer:
 - ✓ What if...?
 - ✓ Are you as prepared as you think you are?
 - ✓ Are you as prepared as you need to be?





This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, which provides audit and enterprise risk services and is a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2019 Deloitte & Touche LLP. All rights reserved.

