2020 Strategic Road Map for Business Continuity Management

Published 21 February 2020 - ID G00466854 - 19 min read

By Analysts David Gregory, Roberta Witty

Security and risk management leaders targeting greater organizational resilience will need to ensure that their business continuity management programs are viewed as strategic imperatives by linking them to the development of corporate objectives and customer delivery commitments.

Overview

Key Findings

- The momentum of digital transformation projects will outpace the ability of organizations to accommodate the changes, introducing additional complex threats. Neither the pace of change, nor the evolving risk landscape will wait for business continuity management and organizational resilience strategies to evolve and catch up.
- The growing need to provide 24/7 technology services to support business needs and customer-facing services is changing organizations' internal and external interactions.
- The ongoing and increasing threat of cyberattacks is leading to the formalization of the relationship between BCM and digital information security functions.
- The future of BCM will be marked by the shift from an operational silo mindset to an organizational resilience mindset and the taking of a more strategic role in the business.

Recommendations

Security and risk management leaders tasked with the responsibility for technology, information and resilience risk should:

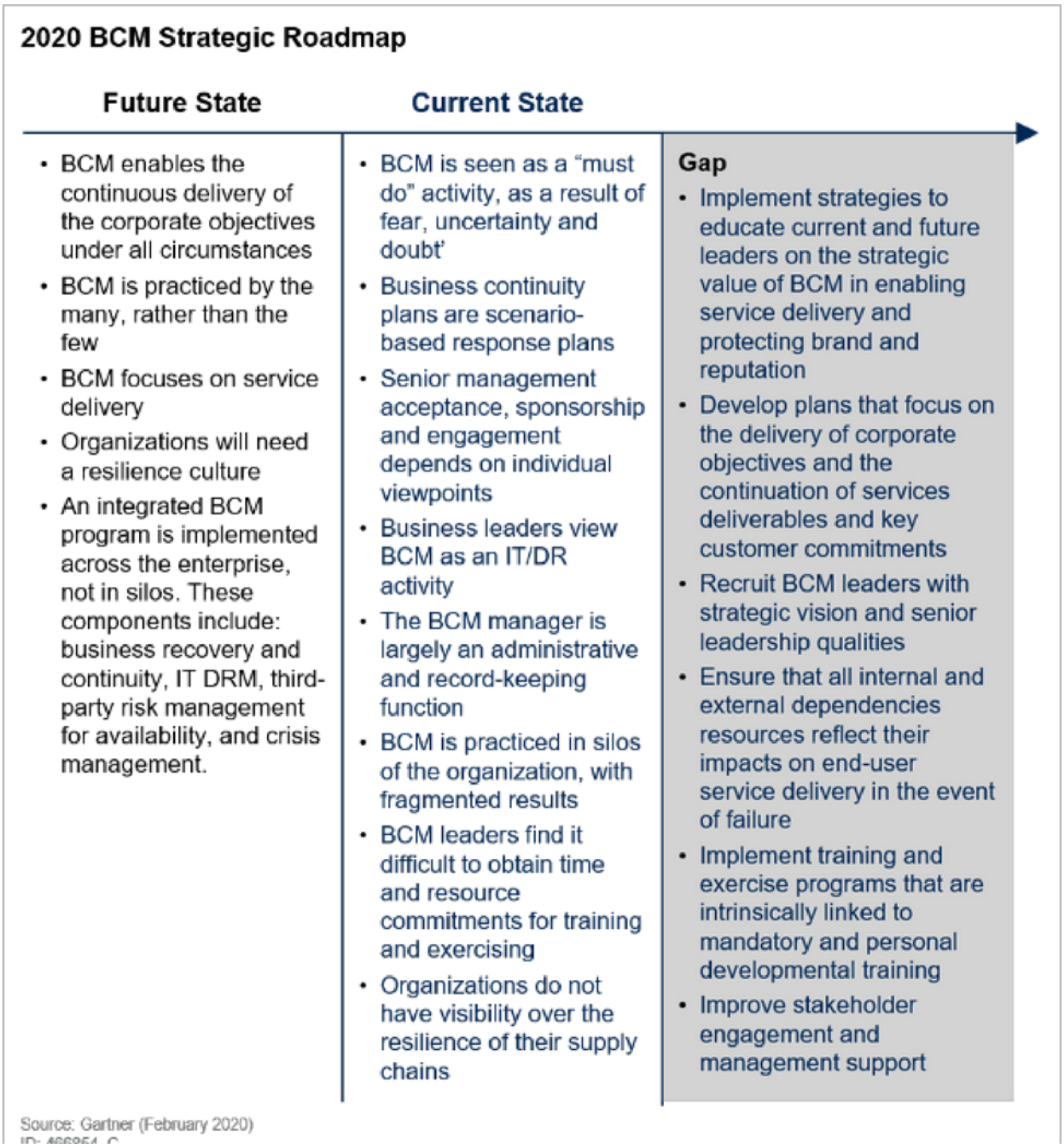
- Learn and adapt quickly to protect end-user service delivery, organizational brand and future sustainability proactively.
- Gain the skills necessary to engage with resilience planning as a business-as-usual function in an organizational resilience culture.

- Integrate BCM across the whole organization to ensure that business-led recovery time expectations are aligned with supplier capabilities and IT disaster recovery resources.

Analysis

This research presents a strategic roadmap for business continuity management (BCM). In the future, more organizations will need to ensure that IT and the business work collectively to develop joined up BCM procedures. Achieving this must be the primary target for all security and risk management (SRM) professionals and business continuity (BC) leaders when supporting the future well-being of the digital business. (Figure 1 provides an overview of this strategic roadmap.)

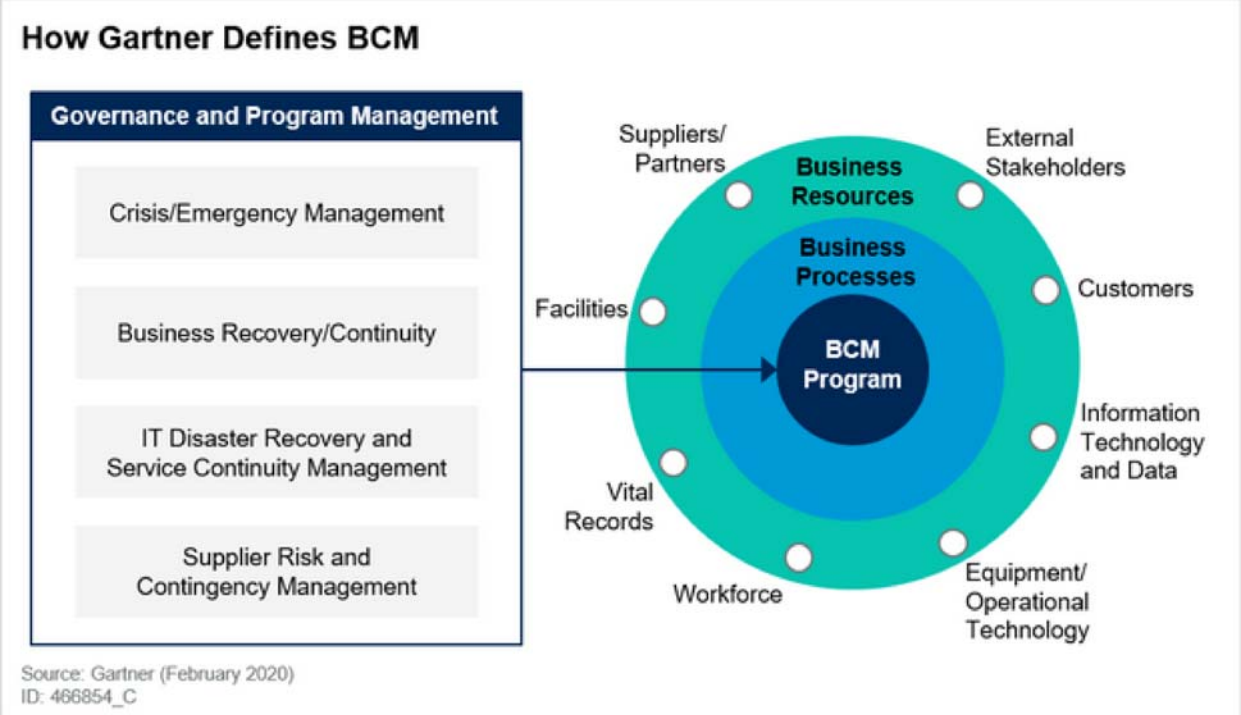
Figure 1. 2020 BCM Strategic Roadmap



Gartner defines resilient organizations as those that rebound and prosper after business disruptions (see Figure 2), because they're resistant to the impacts of disruption (through good risk management), as well as adaptive, elastic and sustainable in the face of disruption. Response, recovery and contingency are the basis of resilience. A resilient organization:

- Rebounds, resumes and sustains decision making quickly
- Coordinates, manages and mitigates organizational risks on a continuous basis
- Operates with dispersed, but interdependent, operations, electronically and physically
- Is communicative, collaborative, cooperative and creative
- Fosters a diverse and empowered workforce
- Invests in an adaptive, elastic and flexible infrastructure — physical, IT and suppliers
- Has committed leadership and program management
- Embeds resilience into the culture of the organization, and leverages its "resilience story" to be competitive and prosper

Figure 2. How Gartner Defines BCM



Future State

BCM Enables the Continuous Delivery of Corporate Objectives Under All Circumstances

A dynamic risk landscape and continuous digital business innovations will require BCM to be a

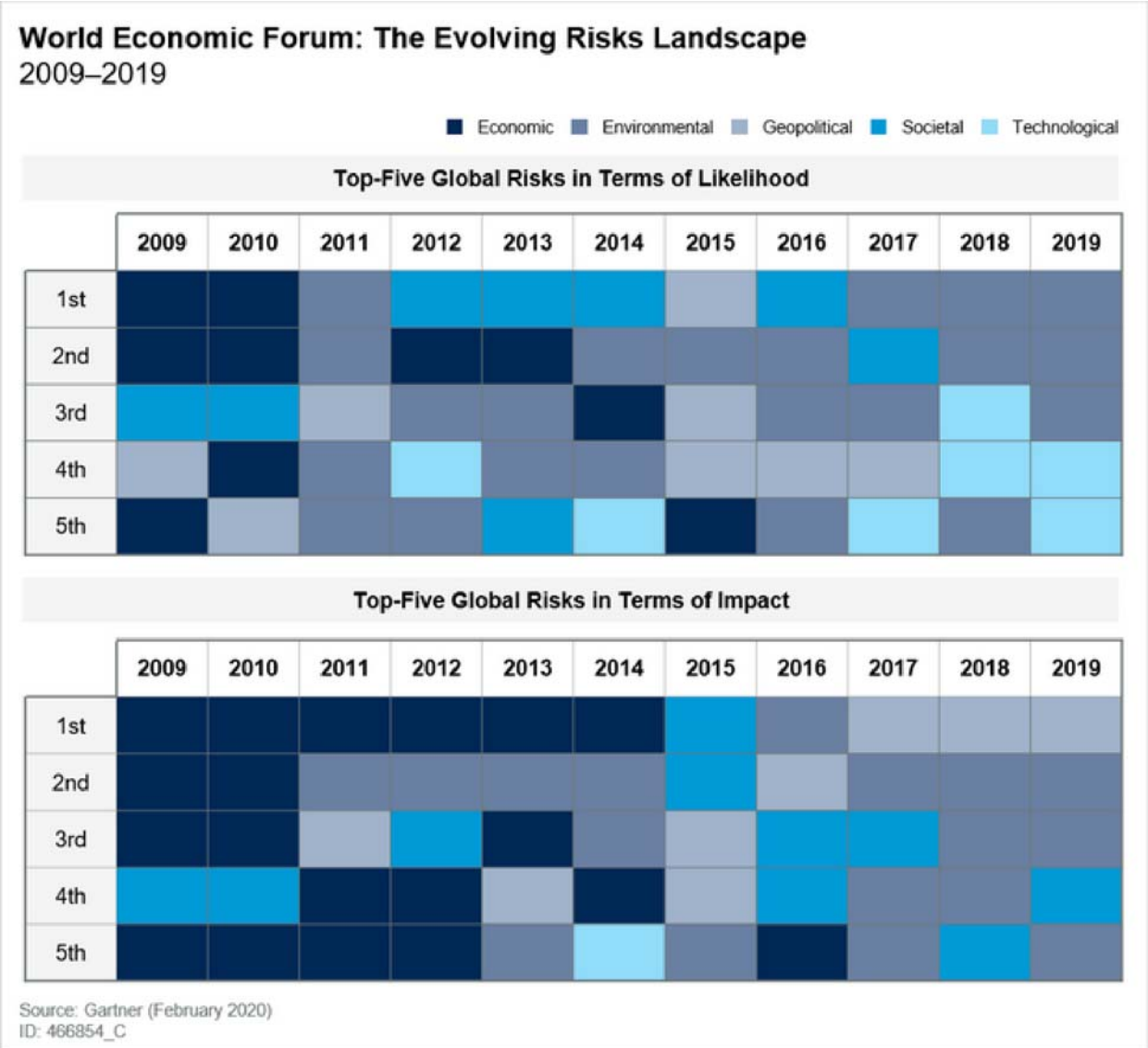
strategies must be integrated across the organization, built around organizational priorities and focused on the delivery of promises to the service users.

The future state of BCM will need to focus on BCM becoming a strategic partner in the digital business, where SRM leaders deliver organizational resilience through a business lens (see Figure 3).

Figure 3. BCM Through a Business Lens

Organizational resilience delivered through the business lens will be vital, because of the increasingly dynamic risk landscape and the rapid pace of organizational change. The World Economic Forum's risk register (see Figure 4) demonstrates how the risk landscape has changed during the past 10 years.

Figure 4. World Economic Forum: The Evolving Risks Landscape (2009 Through 2019)



This continuously changing and evolving risk landscape means that SRM leaders must focus on the following six key areas to achieve the 2022 vision for BCM:

- Continuity of delivery of corporate objectives
- Continuity of delivery of service to end users
- Resilience of service delivery dependencies
- Integrated resilience as a cultural norm
- Flexible and adaptable response, recovery and restoration procedures
- Integrated IT DR strategies

SRM leaders will need to ensure that any resilience strategy protects the organization's vision and

To achieve this BCM strategies will need to be adaptable and flexible to enable appropriate protection and a robust response to:

- Threats to intellectual property
- Regulatory changes
- The pace of digital change and the implementation of digital business projects
- Threats to brand and reputation
- Risks arising from climate change and emerging technologies

BCM Is Practiced by the Many, Rather Than the Few

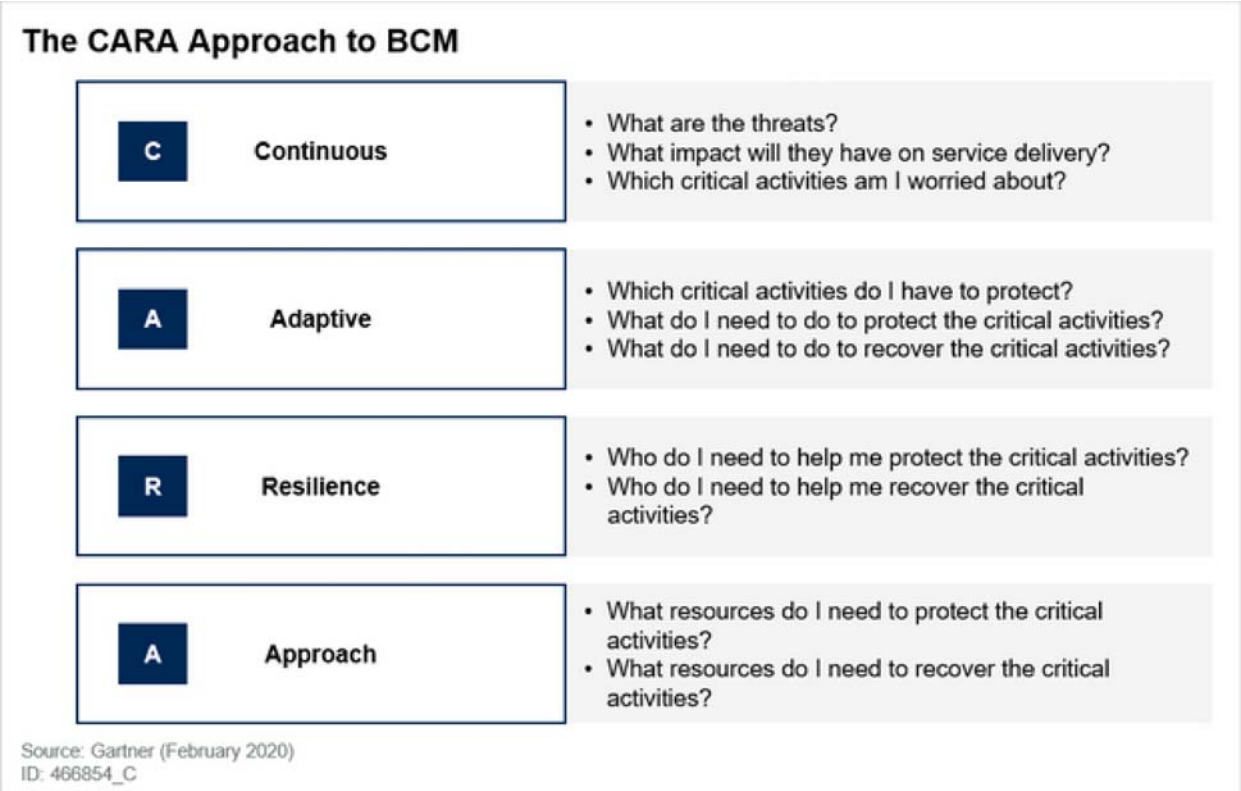
By 2022, successful SRM leaders will need to ensure that all managers are fully familiar with BCM methodologies to ensure that they're continuously implementing BCM strategies as part of good management practice.

SRM leaders will need to ensure that managers embrace BCM and are able to dynamically follow the BCM life cycle in an adaptive way with two key objectives in mind:

- Make the organization more resilient
- Ensure that response, recovery, and restoration plans support the organization through the crisis management journey.

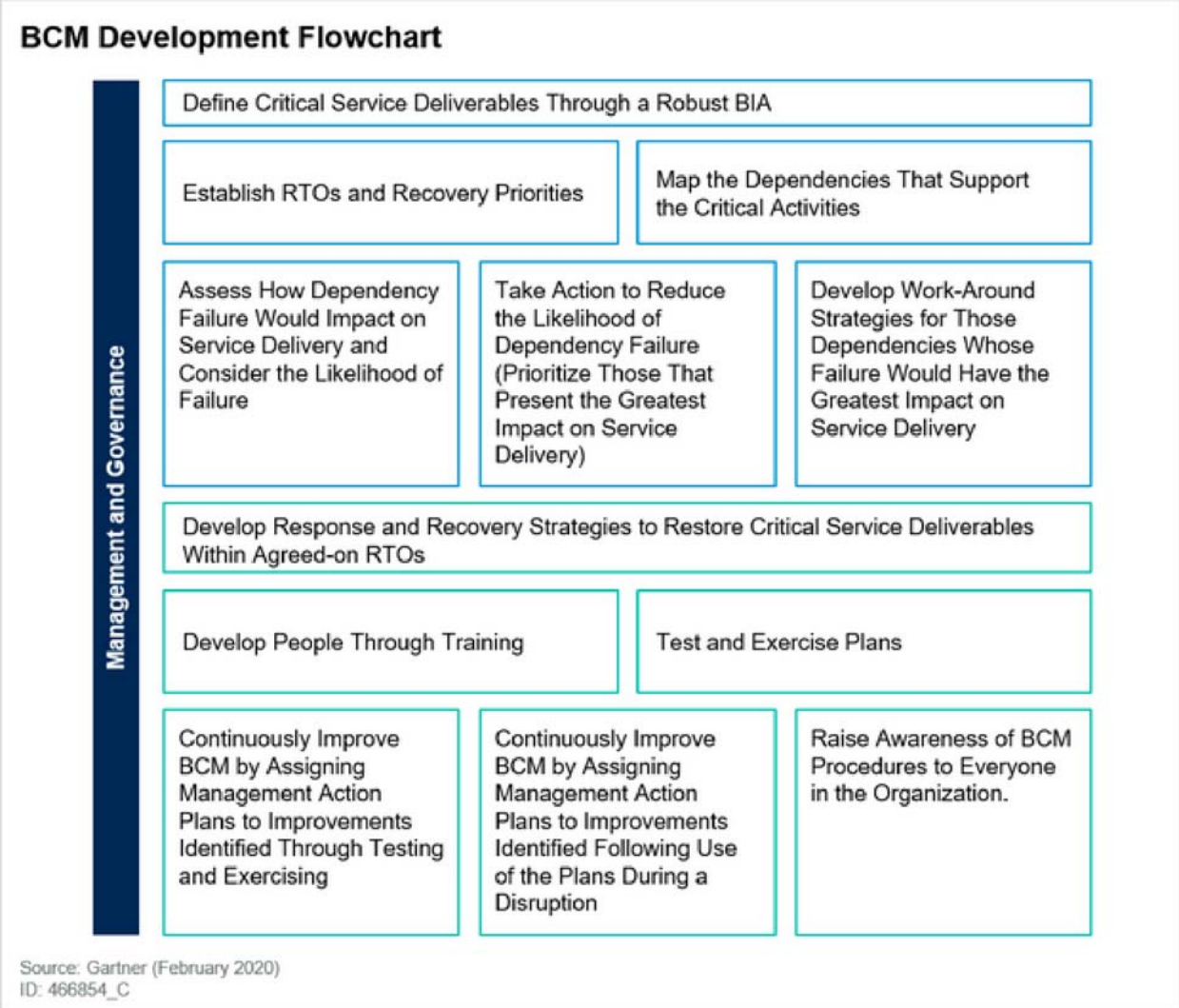
To achieve this, SRM leaders will need to coach management colleagues to take a continuous, adaptive, resilience approach (CARA) to ensure that they take an active role in organizational resilience strategies and assessments of new digital projects (see Figure 5).

Figure 5. The CARA Approach to BCM



SRM leaders must ensure that, when developing the organizational resilience strategy, unnecessary documentation or “text heavy” response plans are avoided. Instead, a clear process should be followed, related to the continued delivery of services to end users (see Figure 6).

Figure 6. BCM Development Flowchart

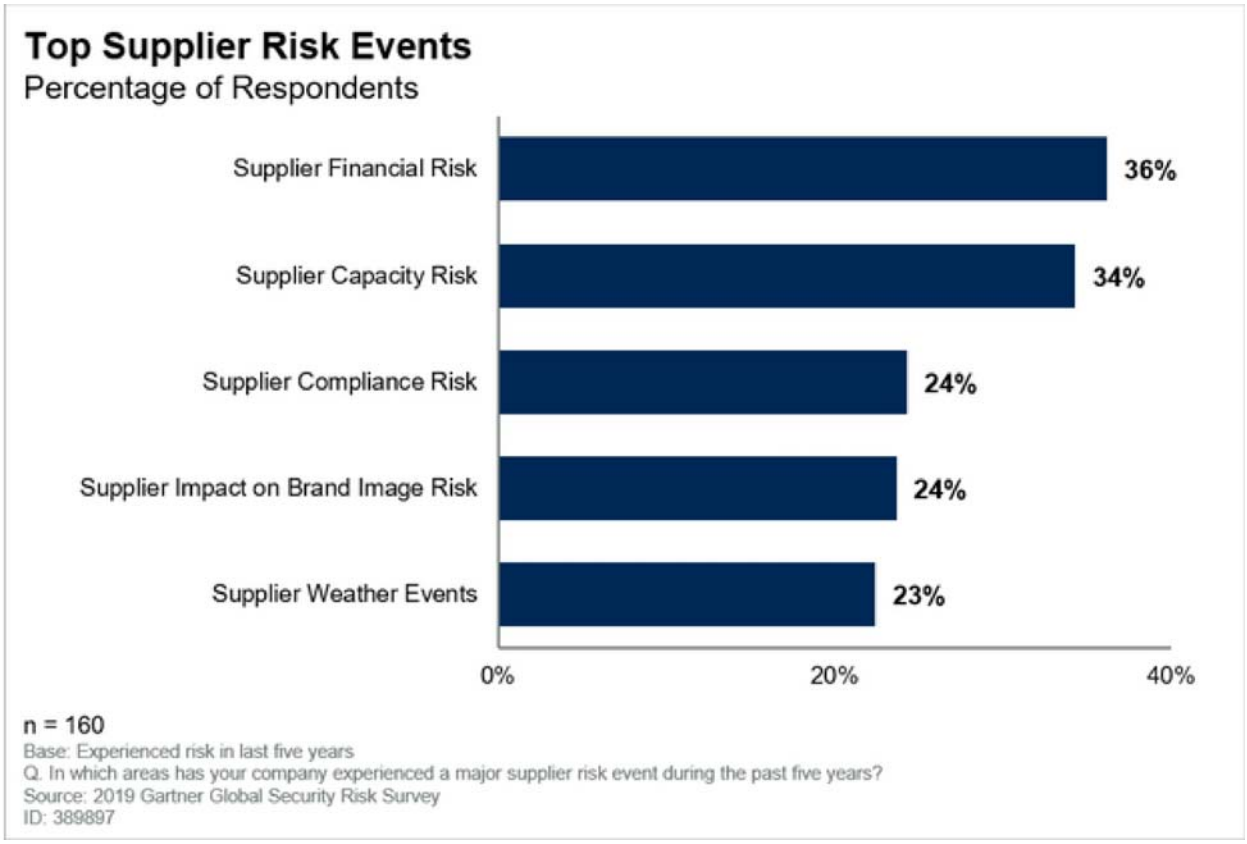


BCM Focuses on Service Delivery

As businesses continue to outsource their key business functions, it will become increasingly important to ensure that there is complete transparency of the end-to-end journey that leads to the delivery of services to end users.

As relationships with external partners (such as strategic suppliers and manufacturing service providers) broaden, third-party supplier networks are increasing in complexity, making third-party resilience ever more important. Gartner research confirms that today's third-party suppliers are exposed to growing risk threats (see Figure 7).

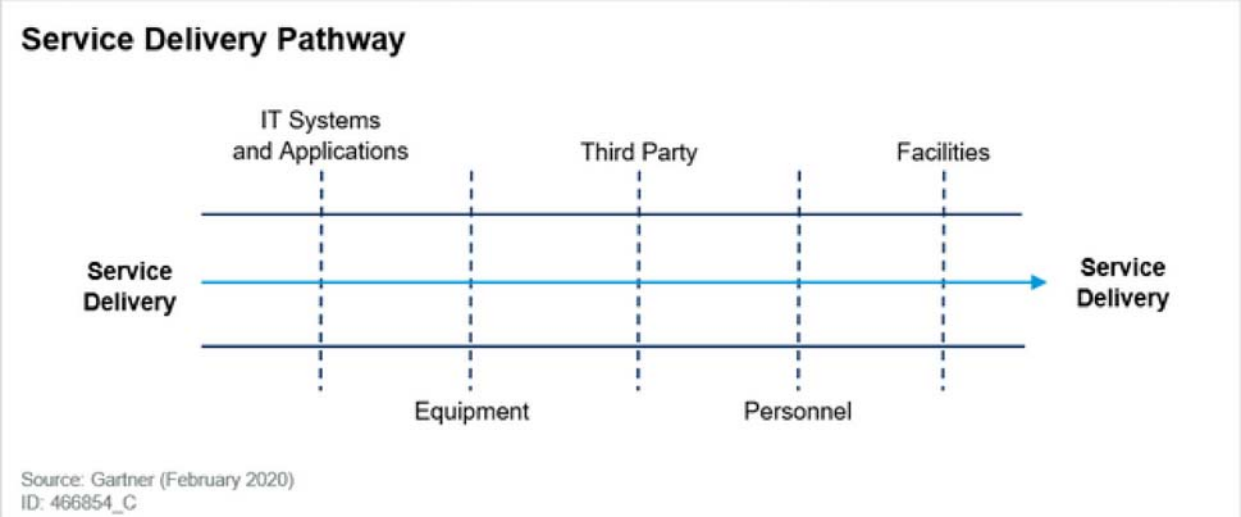
Figure 7. Top Supplier Risk Events



The risk landscape will continue to grow in volume and velocity, with threats becoming harder to predict, mitigate and control. In addition, external partners will frequently be exposed to similar threats, creating risks of failure, as well as valuable experience, intelligence and knowledge related to these risk exposures.

Therefore, SRM leaders will need to take an end-to-end service delivery approach (see Figure 8) and develop their resilience strategies, together with their key suppliers, to minimize and manage supply chain disruption.

Figure 8. Service Delivery Pathway



Dependencies should be considered as joints in the service delivery pipeline. If a joint fails, service delivery will be disrupted or will stop completely. Each point of failure that could disrupt service delivery will be subject to a risk management action plan to reduce the likelihood of the risk occurring or manage the impact of failure.

Third parties that support the most-critical activities, are vulnerable to failure or would have the greatest impact on critical service delivery should be invited to participate in joint contingency operations.

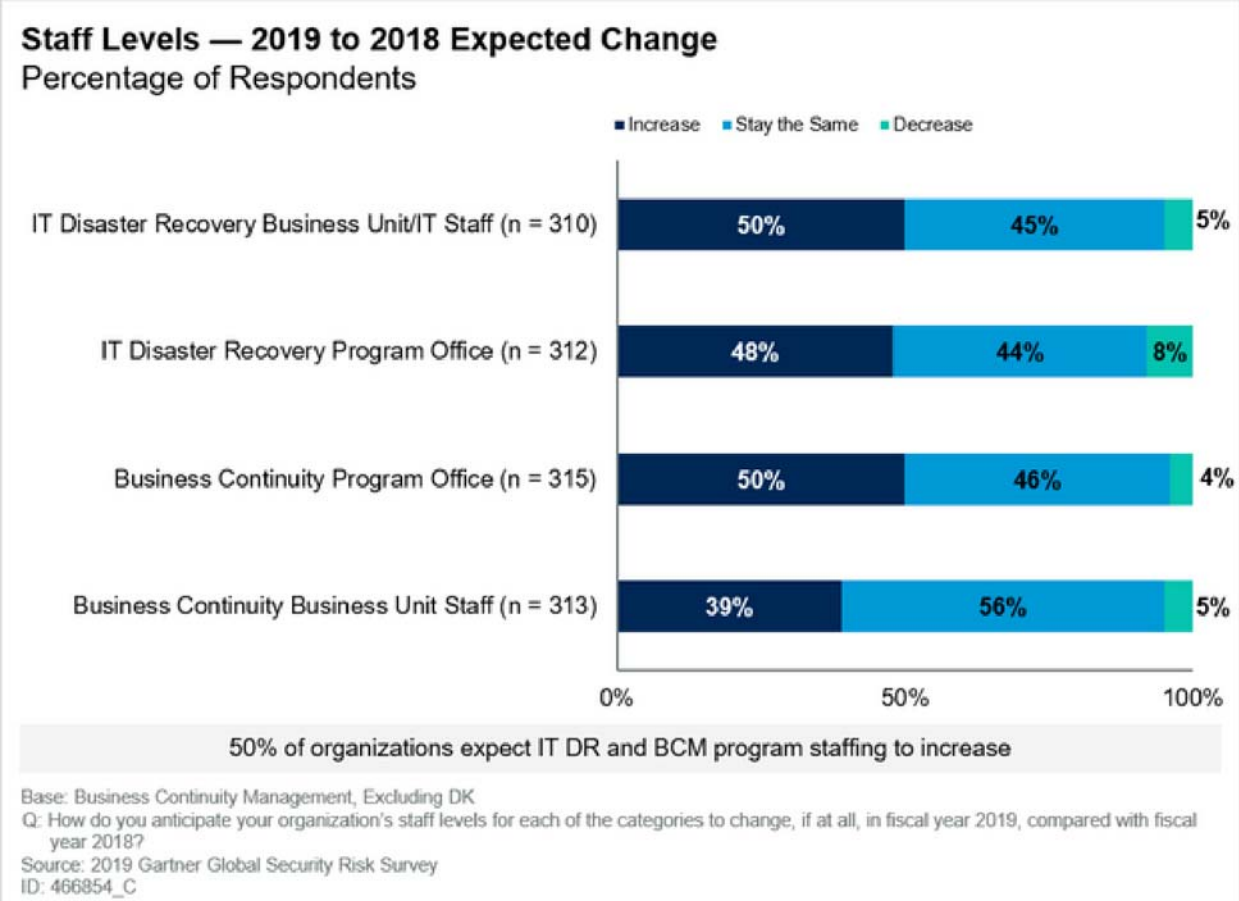
Organizations Will Need a Resilience Culture

Integrating resilience as a cultural norm will be an essential requirement for future resilience management. SRM leaders will be working against a backdrop of perpetual change, and must be able to bridge the gap between the tactical and operational resilience planning needs and the strategic business requirements. They will need to ensure that the whole organization is working as one to implement and maintain the resilience strategies to ensure the stability and sustainability of critical operations.

Senior management will need to drive resilience as a value-added activity and organizational leaders will need to take a long-term approach to resilience. Traditional BCM will need to be able to operate at a more strategic level, working with management and teams as a trainer, mentor, facilitator and enabler to ensure that resilience strategies become an integrated, good management practice. Resilience methodologies will need to become “second nature” to managers, so they can practice it on a dynamic basis, as part of ongoing change management.

To achieve this, future leaders will need to be trained and educated in the principles and methodologies of BCM, so that they are equipped to approach organizational resilience from a corporate, strategic perspective. Organizational culture will play an imperative role in retaining talent against a backdrop of a growing staff requirements. Gartner research confirms that 50% of organizations expect IT DR and BCM staffing levels to continue to increase (see Figure 9).

Figure 9. IT DR and BCM Staffing

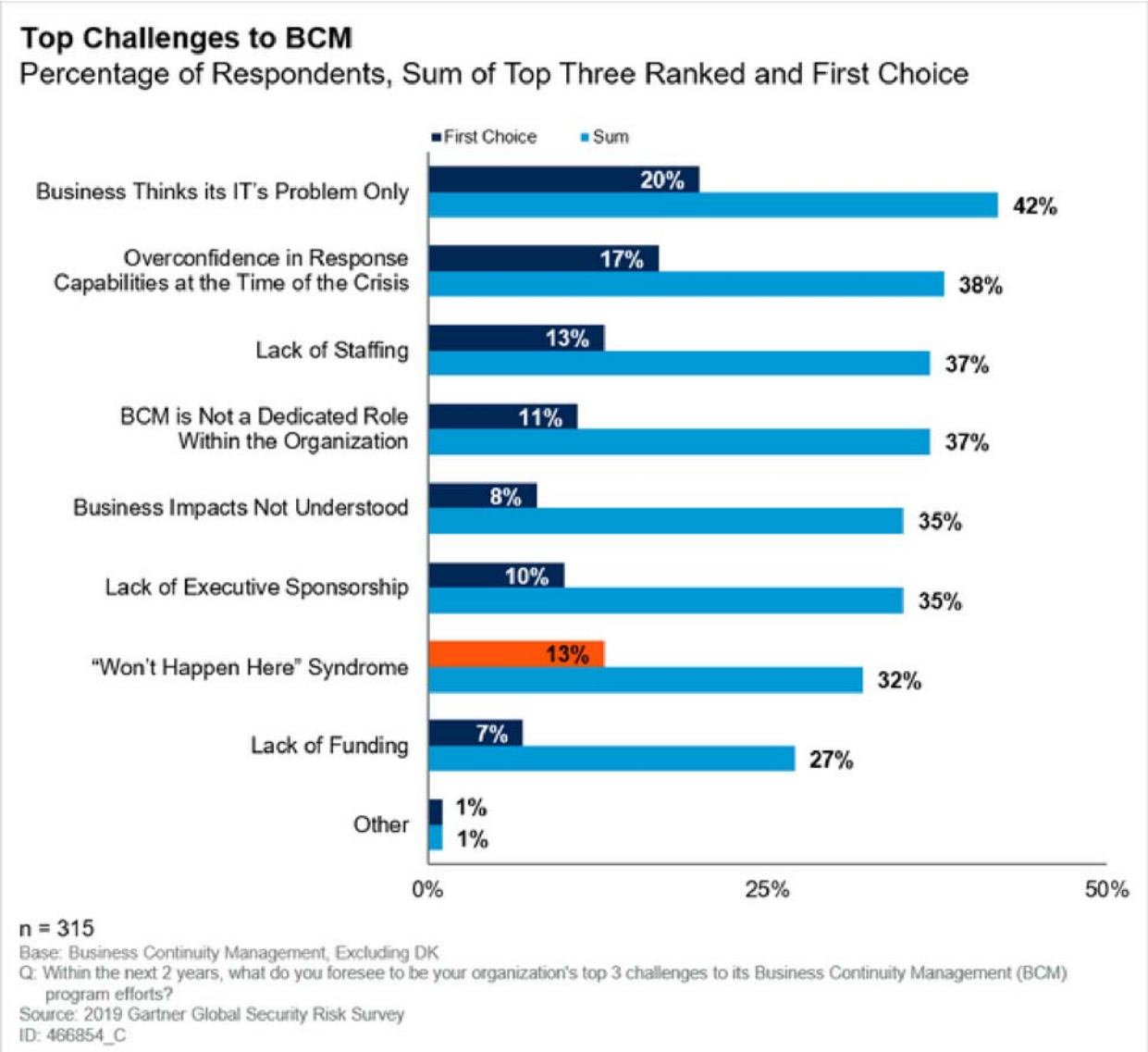


Therefore, organizations will need to ensure that the culture is one in which staff members are able to grow and develop so that key knowledge and skills are retained. Failure to do so will lead to a further knowledge drain, resulting in uncertainties and delays when responding to and recovering from serious disruptions, thereby increasing their impact.

BCM Cannot Be Considered an IT-Only Issue

Gartner research confirms that organizations do not take their resilience planning seriously enough (see Figure 10).

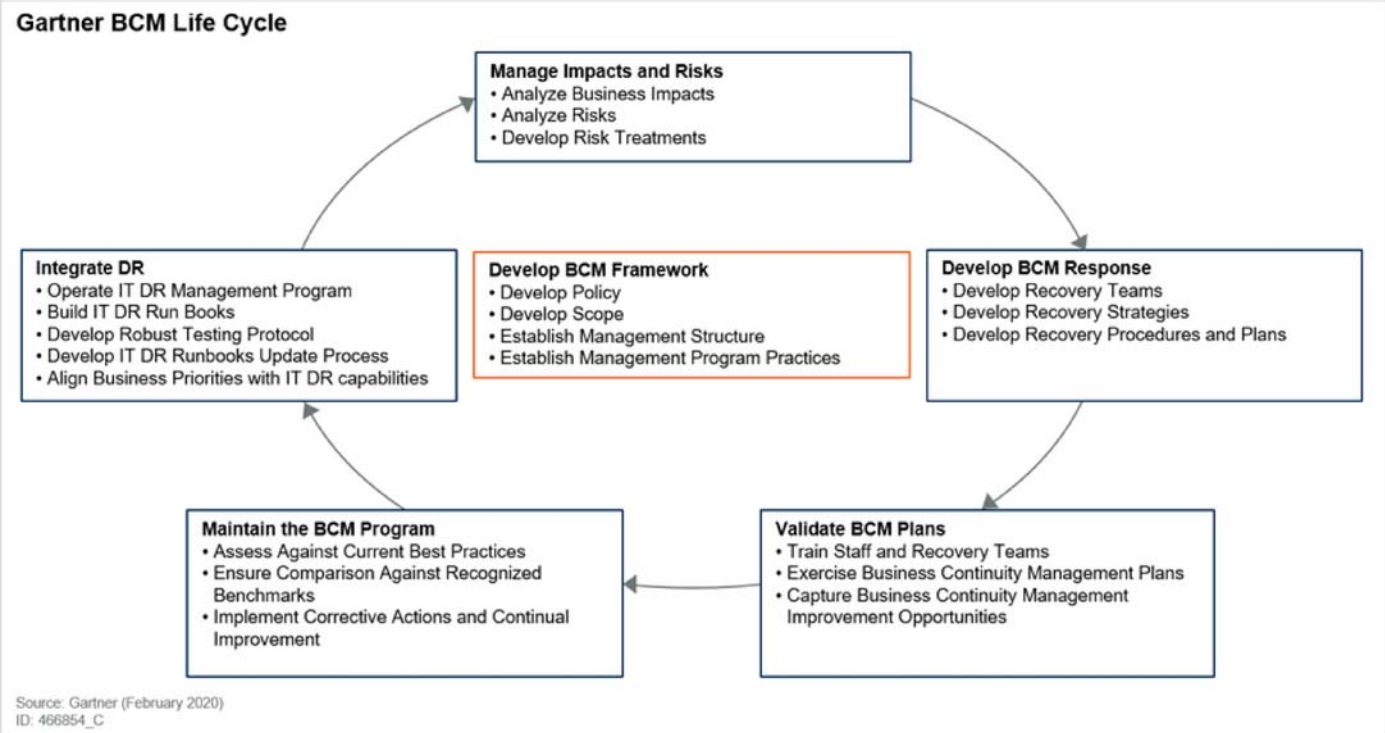
Figure 10. Top Challenges to BCM



The increasingly complex risk landscape, coupled with the dynamic pace of organizational change, will require business leaders to ensure that the business is equipped to respond, recover and restore operations, regardless of the nature and cause of the disruption. With the exception of some known key risks, it is already impossible to predict every eventuality that could befall the digital business. Organizations that continue to view BC as simply an IT DR issue are playing a dangerous game of "Russian roulette" with their organizations future sustainability, should a serious disruption occur.

SRM leaders will need to look beyond IT failures to ensure that resilience structures are in place to enable the implementation of a response that is appropriate to the nature of the disruptive event. In the future, it will be imperative that the digital business develops resilience from an integrated perspective with IT DR strategies developed as a critical dependency to the delivery of key corporate activities. The Gartner maturity assessment sets this out (see Figure 11).

Figure 11. Gartner BCM Life Cycle



Current State

BCM Is Seen as a "Must Do" as a Result of Fear, Uncertainty and Doubt

The current method for demonstrating the value of a BCM program relies heavily on practitioners presenting a negative perspective based on fear, uncertainty and doubt. Discussions are often based on the assumption that something bad will happen, and we must be prepared to deal with it. In most cases, this engenders a mindset committed to doing only the "bare minimum" that's required.

Another fundamental flaw in this approach is that it leads to the "it will never happen here" response. This is the result of managers and leaders being unable to directly conceptualize the nebulous concept of bad things happening. This prevents them from seeing the value of investing in something that doesn't directly relate to their current reality.

Unless you're in the business of responding to major incidents (e.g., an emergency service) or you're in a high-risk area (such as a flood-risk or severe weather zone), most businesses will require a full BC response only a handful of times during a manager's career. Therefore, to counter this mindset, it's important to relate the BCM program to the ongoing delivery of the corporate objectives. This is accomplished by understanding the service delivery pathways, ensuring their resilience, and discussing the capabilities and resources required to recover these within agreed-on recovery time objectives (RTOs).

BC Plans Are Scenario-Based Response Plans

One traditional method for developing BC plans is to base them on a range of risk-based

outlined above, building the entire BC program on this premise is likely to lead to failure, because of two fundamental flaws:

- It is impossible to predict and, therefore, plan for every scenario
- When the plans do not fit the disruptive scenarios, delays and indecision will lead to an ineffective and disjointed response

Instead, develop response procedures that will enable response, recovery and restoration procedures, regardless of the nature and scale of the disruptive event.

Senior Management Acceptance, Sponsorship and Engagement Depends on Individual Viewpoints

The level of engagement and maturity of an organizational BC program often depends on the individual viewpoint of a senior executive. In situations where the executive understands the value of BCM, there is likely to be more support for resilience planning. This motivation will be driven by several key factors, including:

- Previous experience responding to a major disruption without a plan in place
- Customer requirements
- Statutory obligations
- Previous resilience background

When this motivation does not exist, it is invariably more difficult to implement and maintain a BCM program. Therefore, future managers need to be educated early in their careers on BCM's value for delivering corporate agendas, so they accept it as part of good management practice and a cultural norm.

Business Leaders View BCM as an IT/DR Activity

In a 2019 Gartner survey, participants said that, "The business is still not taking recovery seriously, with 20% reporting that the business think recovery is IT's problem only." In addition, the survey shows a rise in BCM reporting to the CISO, ranking fourth in 2019, which is an improvement from sixth in 2017. These trends are driven by several factors, including requirements such as the NIST Cybersecurity Framework 1.1, the drive toward digital business and the realization that cyberattacks can have far-reaching impacts.

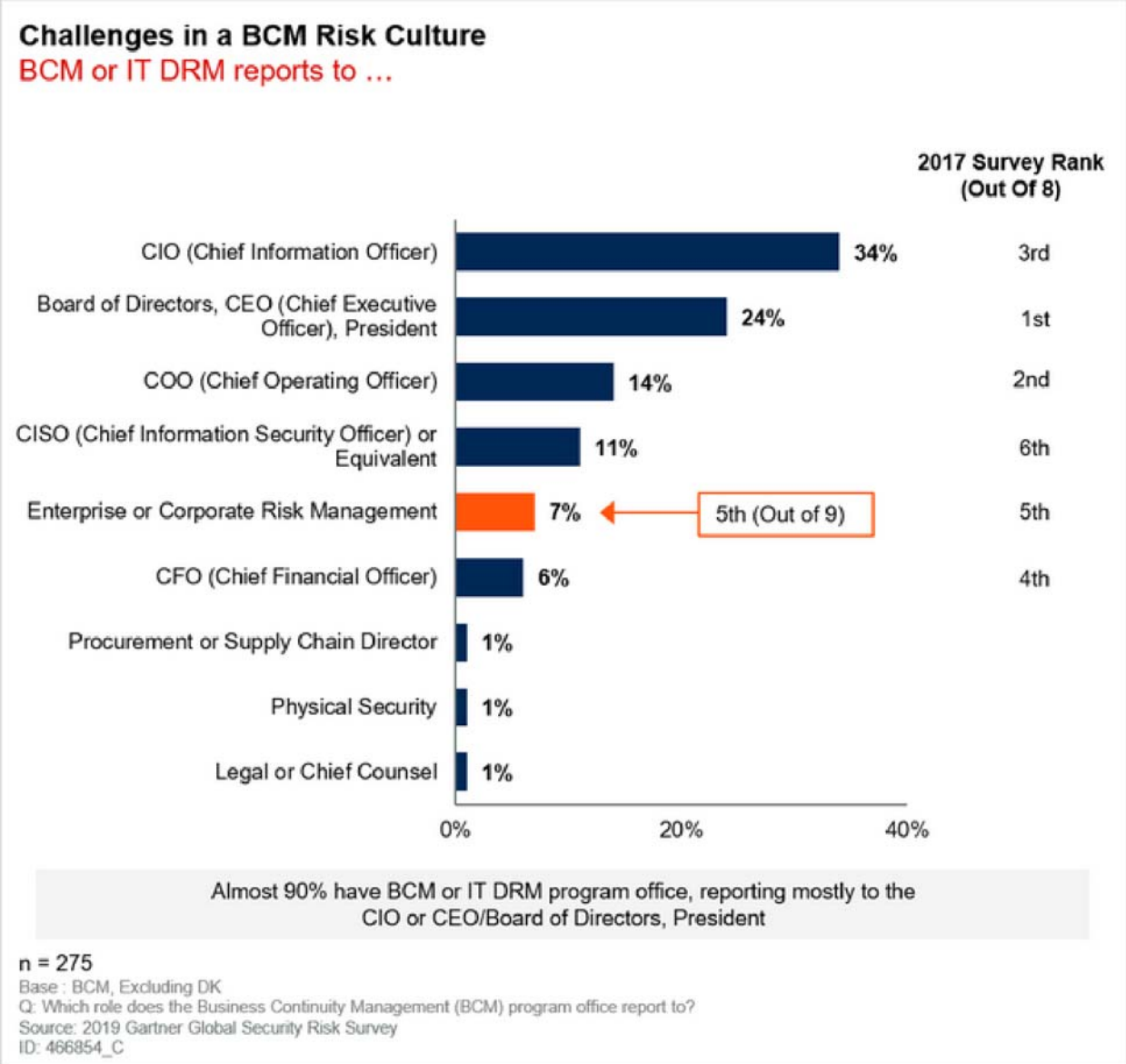
However, as businesses increasingly rely on digital infrastructures, the need to adopt an integrated approach to BCM will increase to ensure that the inevitable businesswide impacts of IT security events (e.g., a cyberattack) are sufficiently considered and addressed.

Organizations that are reluctant to fully adopt a BCM program will see this as an administrative function in which the BC lead uses Microsoft Word and Excel, as well as shared file resources, to keep plans up-to-date. This, in turn, makes the process difficult to manage, causing only partial ongoing maintenance and limited continuous improvement. In these situations, the implementation of a software support package can improve the day-to-day management of the BC program, thus freeing time to allow for more-strategic and continuous improvement approaches.

BCM Is Practiced in Organizational Silos With Fragmented Results

An ongoing silo mentality toward BCM will deliver only partial success. Ultimately, this will result in uncoordinated efforts, possible duplication of resources and a fragmented response to a disruption, leading to a slower recovery, greater impacts and increased costs. An integrated approach to the organization's BCM is the only way to effectively minimize business impacts and ensure a swift response. Gartner research confirms that this remains a challenge (see Figure 12).

Figure 12. Challenges in a BCM Risk Culture



However, BCM needs to be viewed as an all-enterprise initiative (see Figure 13) to ensure a robust framework, timely response and good crisis management.

Figure 13. BCM Is an All-Enterprise Initiative

BCM Is an All-Enterprise Initiative

BCM Program Discipline	Best-Practice Direct Management Responsibility
Governance and Program Management (BCM Program Office)	• Enterprise/Operational Risk Management • BCM Steering Committee Oversight
Crisis/Emergency Management	• Senior Management Executives • BCM Program Office Manager as Facilitator
Business Recovery/Continuity	• BCM Program Office in Conjunction With Business Units
IT DR/Service Continuity Management	• CIO Office
Supplier Risk and Contingency Management	• BCM Program Office in Conjunction With Procurement and the Business Units

Source: Gartner (February 2020)
ID: 466854_C

Time and Resource Commitments for Training/Exercising Remain a Challenge

Gaining management commitment for training and exercising continues to be difficult, especially when the organization doesn't see the value of a BCM program. Busy managers will not provide the necessary time or resources to participate in training and exercise sessions when BCM is seen as a must-do activity.

In these situations, making the link to the delivery of the organization's strategic objectives and demonstrating the value of the BCM program is imperative to achieve the management time commitment required. As a result, exercising the plans is invariably limited to component IT DR testing and departmental workshop-style desktop exercises. If developed and delivered appropriately, they can add value; however, opportunities to include the wider management teams and consider the wider business impacts of the disruptive scenario are often lost.

In most cases in which the BCM program lacks perceived value, little or no training to ensure that those named in the plan can carry out their roles will take place. Each of the factors highlighted above will cost time and money as a result of disjointed responses to a major disruptions. This will be because people will be unclear of their roles, unsure of what is expected of them and uncertain about "who is responsible for doing what."

When managers engage in training and exercising, the activities need to demonstrate a worthwhile ROI of time by ensuring that they're well-prepared and have relevant content. In addition, they need to be delivered and facilitated in a manner relevant to the audience.

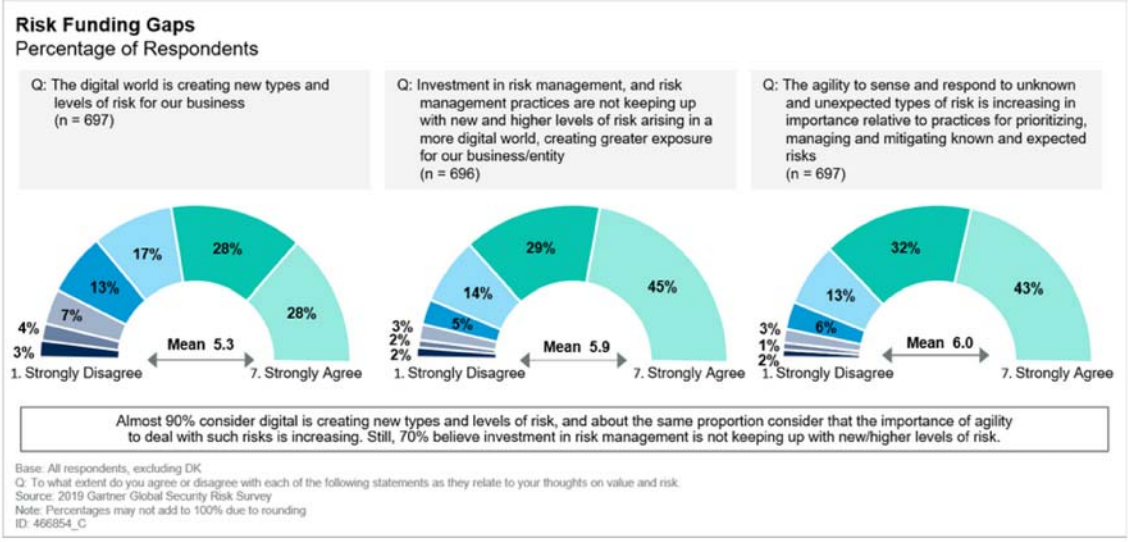
Organizations Lack Visibility Over Their Third Parties' Resilience

Therefore, organizations need to gain greater clarity over their third-party risks — both business- and IT-oriented — and collaborate with their third parties in the development of recovery plans. Any procedures implemented need to be prioritized in relation to the impact of a third-party disruption on the critical activities set by the organization and the agreed-on RTOs.

Gap Analysis and Interdependencies

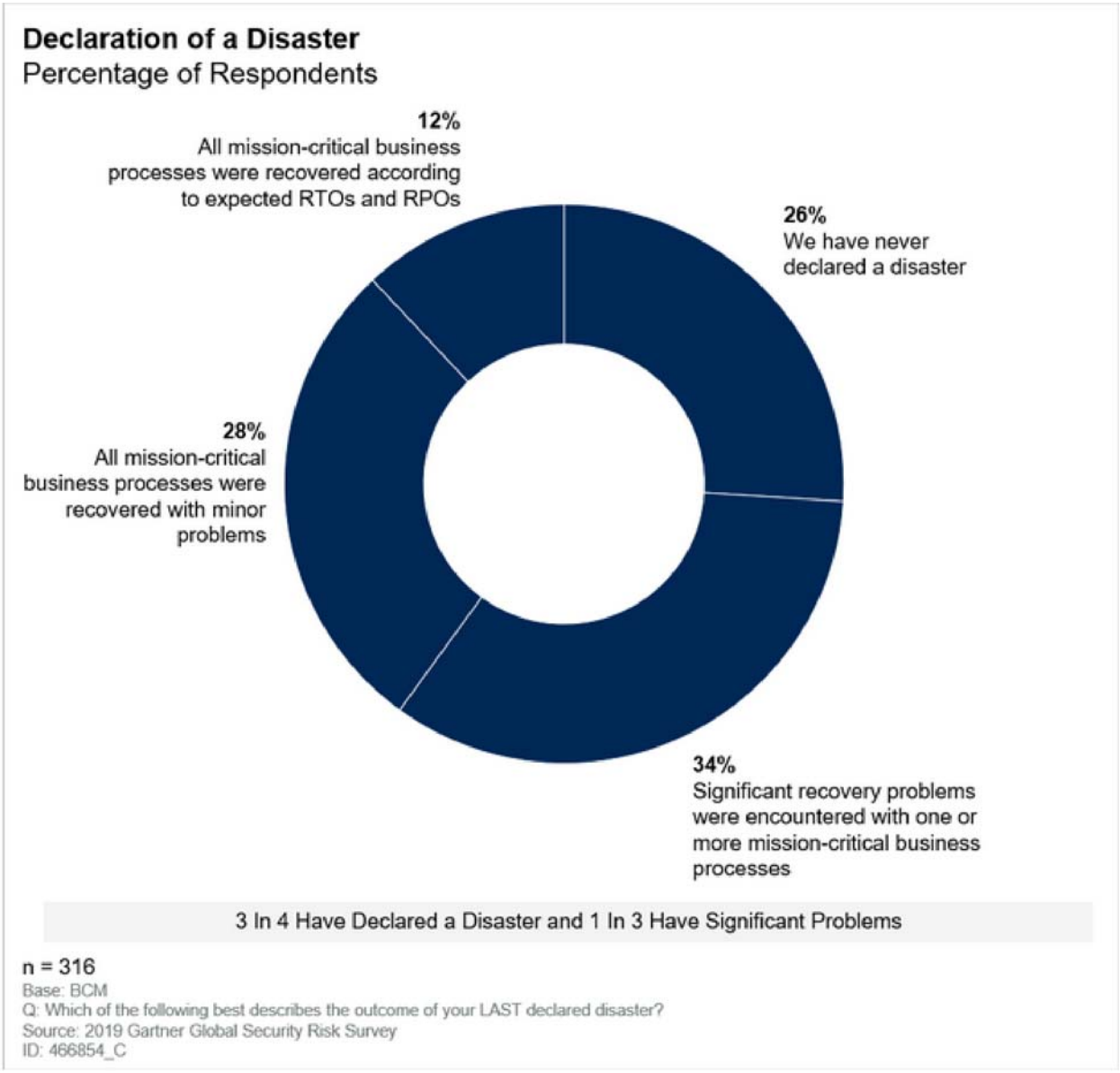
Achieving mature continuity of organizational operations by 2022 will be a significant, but challenging, achievement, and attaining organizational resilience will also be important. However, organizations will need to aspire to these goals to ensure future sustainability. Gartner's 2019 survey results confirm that almost 90% of respondents view the digital age as creating new types and levels of risks. About the same number agree it will be important to ensure agility to deal with these new risks; however, 70% believe investment in risk management is not keeping up with new and higher levels of risk (see Figure 14).

Figure 14. Risk-Funding Gaps



In addition, organizations continue to underestimate the threats to their organizations and overestimate their ability to recover. This is illustrated in Figure 15, from the latest Gartner survey.

Figure 15. Declaration of a Disaster

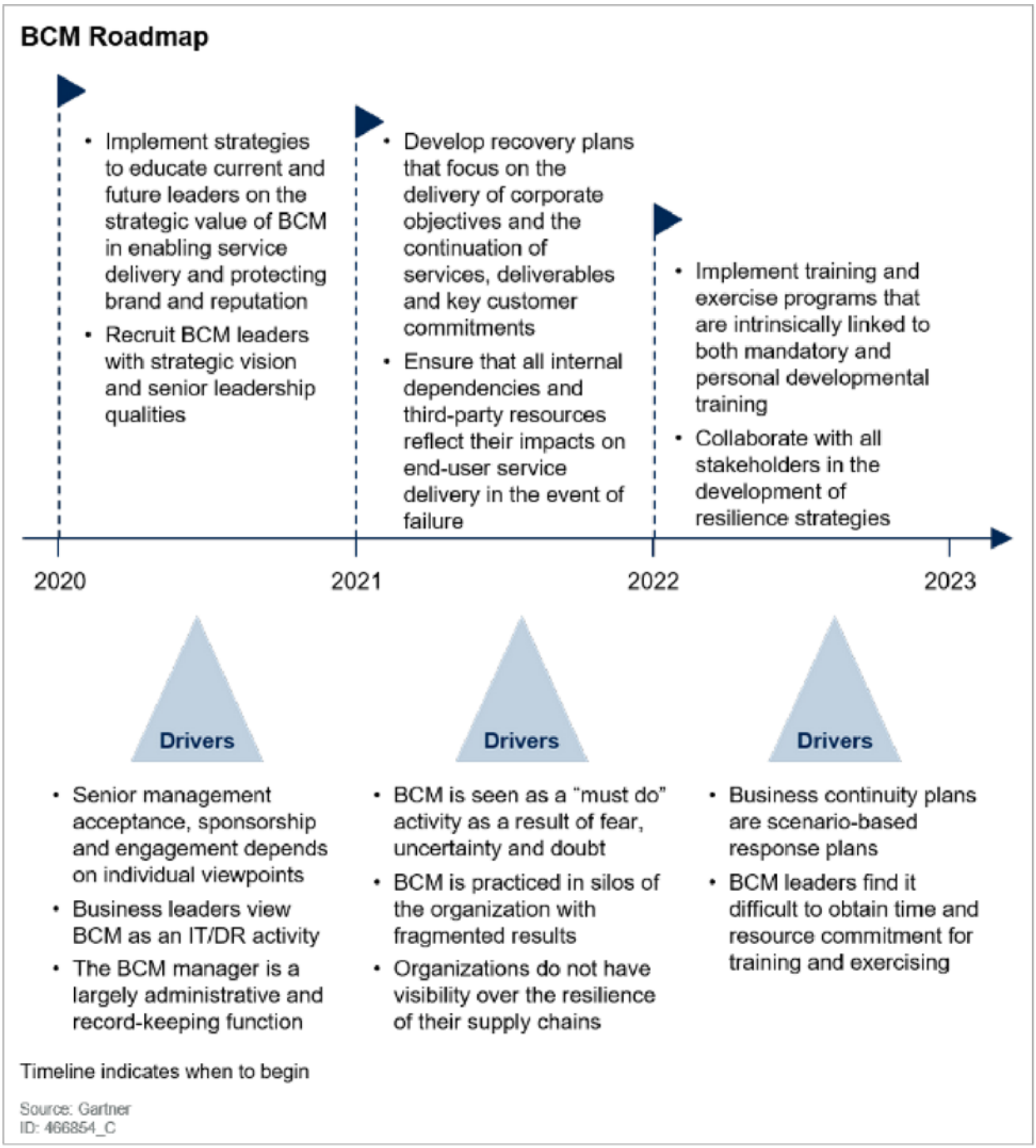


There is still not enough joined-up thinking in relation to BCM. Therefore, even partial success in the maturing of response, recovery and restoration procedures will make a fundamental difference, as long as they are business-focused and service-delivery-oriented improvements.

Migration Plan

The prioritized steps shown in Figure 16 will enable SRM leaders to move forward in their BCM planning.

Figure 16. BCM Roadmap



Higher Priority

SRM leaders should carry out the following actions by the end of 2021:

- Ensure that BCM program management is overseen by a cross-functional steering group that reports into a C-suite-level board. Once formed, this steering group should take an integrated, service-driven approach to BCM, and ensure that business impact analysis results link with the strategic outputs of the organization.
- Fully map the service delivery pathways of critical activities, as agreed to by the organization. Ensure that impact on service delivery in the event of dependence disruption is minimized by

- Create BCM program methodologies and frameworks that are flexible and adaptable to allow for organizational change. Develop the methodologies and frameworks and consider options for efficiently managing the day-to-day operations of the BCM program.
- Create a strong association with BCM as the enabler of the delivery of the strategic objectives by focusing efforts and activities on the two key principles of:
  - Making the organization more resilient
  - Ensuring that the organization can make the crisis management journey as effectively as possible

If no other component is created for BCM, a crisis management team must be established to handle all types of crisis events that the organization might experience.

Medium Priority

SRM leaders should carry out the following actions by the end of 2022:

- Recruit and/or develop BCM program leaders with knowledge and experience to take a strategic, rather than operational, approach to BCM in the organization.
- Educate staff at all levels to provide them with the appropriate level of understanding of the organization's BCM program and the role they can play in relation to this.
- Align BCM program responsibilities to performance management objectives for critical activity owners, BCM program leads and responding personnel.
- Establish an integrated BCM program that includes BR/BC, IT DRM, third-party risk management for availability, and crisis management

Lower Priority

By the end of 2022, SRM leaders should:

- Ensure that key stakeholders are engaged as partners in the organizational BCM program.
- Ensure that key stakeholders participate in an exercising and testing program.
- Ensure that the RTOs of mission-critical third parties are aligned with the recovery requirements of the organization.

Evidence

Data is taken from client inquiries, supporting Gartner research and IT Score survey data.

performed, especially in the following areas:

- SRM
- BCM
- Security compliance and audit management
- Privacy

The research was conducted online among 698 respondents in the following countries: Brazil (n = 138), Germany (n = 135), India (n = 140), U.S. (n = 142) and U.K. (n = 143).

Qualifying organizations must have at least 100 employees and $50 million (USD equivalent) in total annual revenue for FY18. All industry segments qualified, with the exception of agriculture, construction, IT services and software, and IT hardware manufacturing. Furthermore, each of the four technology-focused section of the questionnaire required the respondents to have certain job roles/category and have at least some involvement or responsibility with at least one of the technology domains we explored.

Interviews were conducted online and in a native language. The sample universe was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets and was reviewed, tested and administered by Gartner's Research Data Analytics team.

Sources: ISC2, Infosec Institute, Gartner