

11TH CRISIS MANAGEMENT REPORT

2024 EDITION

WITT O'BRIEN'S

ambipar^a
response

CONTENTS

- 04** Executive Summary
- 07** Pre-Crisis Planning
- 15** Top 10 Crises & the Impact to Organizations
- 27** Future Program Enhancements
- 30** Program Characteristics
- 33** Participant Characteristics
- 39** BCM Research Overview
- 41** International Research Advisory Board
- 46** Distributing Organizations
- 48** About Witt O'Brien's
- 50** About BC Management

DISCLAIMER

The data included in this report was provided directly by participants to BC Management's 11th Edition Crisis Management Study. This report may be viewed as a representation of the companies and organizations that elected to participate in this survey.

About the Report

This report focuses on how different crises impact organizations from organizational losses, downtime, impact to the employees as well as estimated financial losses. In addition, there is an assessment of how organizations prepare for different crises and use lessons learned to advance resilience management strategies. An overview of the data findings and a correlation to program maturity highlight several differentiating factors to obtain operational resiliency. The data highlighted throughout this report was gathered in BC Management's 11th Edition Crisis Management Study between May 30, 2024 through September 4, 2024.

This report is available as a complimentary report.

As a thank you to all of our study respondents, we provided each participant with a complimentary, customized [Crisis Management Peer Data Dashboard](#), of which all study participants could choose their top three preferences by either industry sector or by organizational revenues. If you haven't participated in this study and you'd like to receive a customized dashboard, you may still participate before February 28, 2025 via our [online study](#). Our dashboards highlight a tremendous number of data points that are not included in this complimentary report.

Like our research analytics?

Be sure to visit our website to download other [complimentary reports](#) and sign up for our study alerts. All study participants will receive customized peer dashboards for the corresponding studies they contribute to. Please feel free to direct any inquiries to info@bcmanagement.com. We hope you enjoy this report.

WITT O'BRIEN'S

ambipar 
response



EXECUTIVE SUMMARY

Executive Summary

The Crisis Management Report offers a comprehensive summary of the extensive data collected in the 11th edition of our study. It examines the effects of various crises on organizations, including operational downtime, employee impact, organizational losses, and financial damage. Additionally, the report assesses how organizations prepare for crisis management and use lessons learned to strengthen their resilience strategies. Before diving into the detailed insights, here are some key findings we'd like to share with you.

Gaps in Pre-Planning - Being prepared is key and while **71%** of organizations indicated they were either "extremely prepared" or "prepared" for crises, the data told a different story.

- Organizations are least prepared for a supply chain disruption (**38%**), financial market disruption (**46%**), or disgruntled employee (**64%**). While organizations have broadened the scope of their programs, with significant increases in addressing specific risks such as supply chain disruptions (**+18%**) and workplace violence (**+12%**) from 2023 to the present, only **9%** and **5%** of organizations anticipate improvements in liquidity and credit issues, respectively.
- **26%** of all organizations use a standard definition of 'Crisis' to ensure the appropriate level of response and management. Additionally, only **30%** of all organizations document all areas of executive risk acceptance and perform annual reviews.
- Using a mobile phone was the top method (**91%**) to communicate throughout a crisis, but only **71%** noted that their plans are accessible in a mobile format.
- The top challenges noted for corporate-level crisis management teams are 1) Clarity on when a crisis management team is notified and activated, 2) inability to focus on the strategic 'what' to do versus devolving into the operational 'how' to do it., and 3) agreement on the level of transparency in crisis communications.

Top Crises & the Impact Ratings - This year we continued with the same assessment to not only highlight the top crises recently impacting organizations, but we also assigned a crisis impact rating based on the frequency, full activation rating, advance warning, impact on employees, geographic scope, percent of critical systems impacted, business resumption period, and the estimated financial losses. The full details are included within the report, but here are the most notable insights.

- Technology disasters had a greater impact on organizations compared to natural, accident, or human/business disasters, as three out of the top five crisis impact ratings were attributed to technology-related incidents (software issues, cyber attacks, and network/communication outages).
- Software issues surpassed other crises in impact, receiving the highest ratings with a score of 10 for employee and geographical impact, and a score of 9 for frequency, full program activation, and impact on critical systems.
- Cyber attacks ranked as the second most impactful disaster, receiving a score of 10 for minimal advance warning and estimated financial losses, and a score of 9 for geographical impact scope and recovery time to normal business operations.

Top Trends

PRE-CRISIS PLANNING

71% of organizations indicated they are either "extremely prepared" or "prepared" for crises, but just over half (**52%**) noted that they have prevented a disruption in the past based on their preparedness efforts.

TOP CRISES & DISRUPTION IMPACT RATING

Crises were assigned a rating based on 8 different impact categories. Each category was scored between 1 (lowest impact) to 10 (highest impact) for a total potential impact rating varying between 8 - 80.

Here are the top 10 crises impacting organizations in the last year by impact rating.

- 1) Software Issues (**62**)
- 2) Cyber Attack (**59**)
- 3) Network/Communication Outage (**49**)
- 4) Ice Storm/Winter Weather (**49**)
- 5) Power Outage (**42**)
- 6) Flood (**41**)
- 7) Supply Chain Disruption (**39**)
- 8) Hurricane (**33**)
- 9) Water-Main Break, Loss, or Failure (**33**)
- Fire-Natural (**33**)

Estimated Financial Losses following a Crisis - On average, **57%** of respondents reported difficulty in estimating financial losses after a crisis. However, for those who were able to calculate the loss, the data revealed the following.

- Cyber attacks led to the highest estimated financial losses for organizations, followed by network/communication outages, ice storms/ winter weather, and supply chain disruptions.
- **83%** of organizations reported that their executives were highly involved in managing crises that resulted in estimated financial losses of over \$5 million.
- All organizations that experienced a crisis resulting in estimated financial losses exceeding \$5 million reported being affected operationally and/or by supply chain disruptions impacting product or service delivery.

Balancing Technology & Elevating Organizational Resiliency - Being truly "resilient" requires a holistic approach. Organizations are stretched thin as they strive to balance technological advancements while enhancing their resilience management by integrating with other risk disciplines, improving supply chain resilience, and driving program metrics. Given that technology disasters had the highest impact ratings on organizations, it's no surprise that more are increasing investments in technology improvements and software automation.

People remain the greatest asset in building resilience; however, fewer organizations plan to increase full-time, permanent staff next year, down **12%** from 2023. In contrast, more organizations expect to maintain current staffing levels, up **11%** from last year. While uncertain markets may lead to a hiring slowdown, the work still needs to get done. As a result, there has been a slight uptick in the use of third-party consulting services to support resilience management strategies.

How can this report benefit your program and organization? This report is a broad analysis of a segment of the data, illustrating how the Resilience Management profession is viewed and what we can learn from these study results. Although this is simply a baseline of the trends in our industry, we hope you leverage this report to present data findings to your executive management to increase the visibility and commitment of your program. Enclosed you will find a great deal of data, though it is impossible to display everything, which is why **customized dashboard reporting** specific to your organization is essential to obtain a clear understanding of other "similar" organizations. A feature of the customized dashboards is providing a detailed analysis specific to your industry or by organizational revenues, which not only allows you to benchmark your own program specific to your demographic, but also its an opportunity to create a roadmap for your program based on effective peer-based models and supporting data. Our customized dashboards will be made available to professionals who confidentially participated in the **11th Edition Crisis Management Study**.

Since 2001, we've been conducting data research to increase the understanding of the analytical underpinnings of our profession. As we continue our efforts to advance the knowledge, insights, and value our business provides to the maturity of our profession, we know that to that end, the understanding of how to increase resiliency and better understand how the profession is evolving is of key importance. Thank you to all who responded to this survey, our advisory board, and to Witt O'Brien's team for their efforts in developing this valuable report. We hope you enjoy this report, and we are available to discuss customized versions to meet your needs.

Top Trends

ESTIMATED FINANCIAL LOSSES

Technology disasters—such as cyber attacks, data breaches, and network/communication outages—accounted for **83%** of crises affecting organizations with estimated financial losses exceeding **\$5 million**.

FUTURE PROGRAM ENHANCEMENTS

Organizations anticipate increasing the strength of their resilience management program by addressing the following top items in the next year:

- Integration with Risk Disciplines **69%**
- Third-Party Resilience **67%**
- Program Metrics (Ability to Resonate & Drive Continual Improvements) **61%**
- Cyber Response **61%**

Top investment strategies (increase) in the next year include:

- Technology to Improve Resilience **45%**
- Software Automation **42%**
- Situational Awareness & Threat Intelligence **39%**



Cheyene Marling, Hon MBCI
Managing Director,
Witt O'Brien's
cmarling@wittobriens.com

An overhead view of a business meeting around a wooden table. Several people in business attire are gathered, looking at documents and a laptop. The table is covered with various business charts, including bar graphs, pie charts, and line graphs. A laptop in the foreground displays a dashboard with a 3D bar chart and performance metrics. There are also two mugs of coffee on the table. The scene is dimly lit, with a dark blue overlay and bright yellow decorative shapes in the corners.

PRE-CRISIS PLANNING

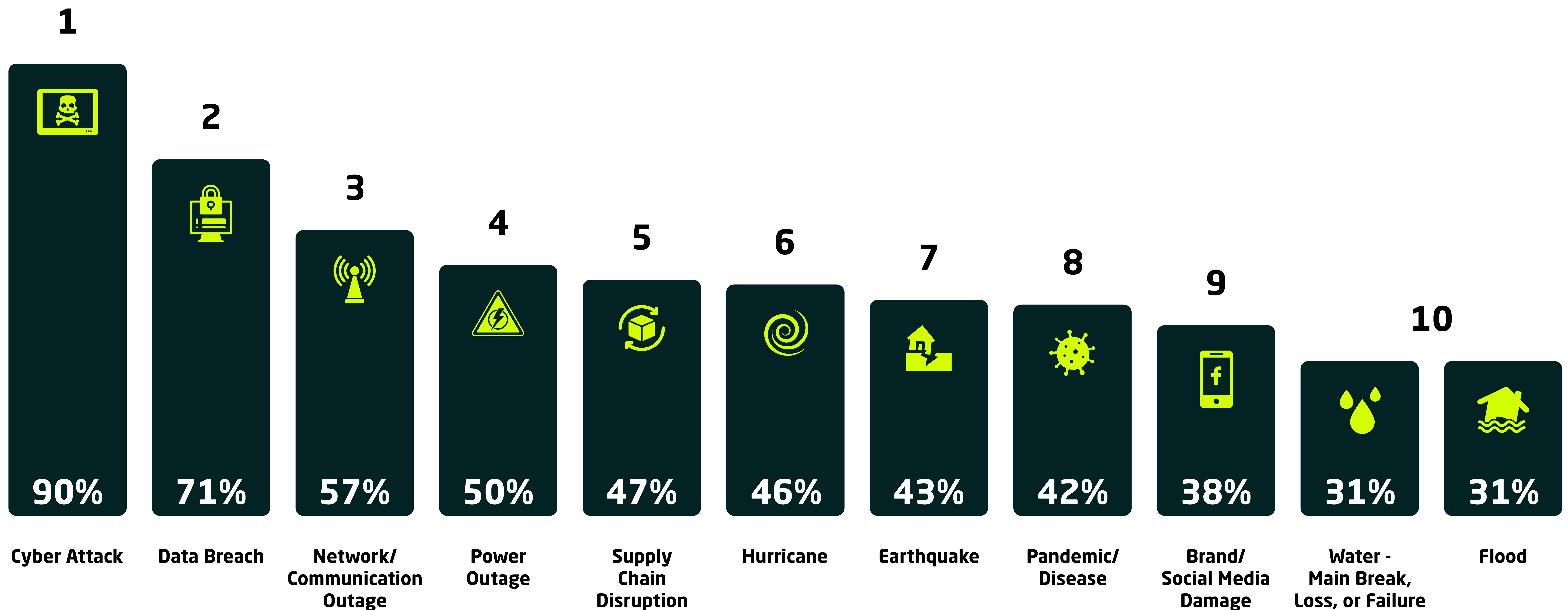
What Crises are Organizations Most Concerned About?

Participants chose the top 5-10 crises out of a list of 50+ different accidents, human/business, natural, and technical disasters.

Organizations are most concerned about **Human/Business Disasters (37%)**, followed by **Technical Disasters (29%)**, **Natural Disasters (20%)**, and **Accidents (14%)**.

Top 10 Crises Organizations are Most Concerned About:

Sum exceeds 100% due to multiple selections.



52% Prepared Respondents indicated they were **19% extremely prepared**, **26% neutral**, **3% unprepared**, and **0.5% extremely unprepared** for crises.

Top 5 Crises Least Prepared for:

Percent of respondents indicating prepared or extremely prepared. Only crises with 25%+ of respondents noted as being concerned about the crisis were included below.

38% Supply Chain Disruption	46% Financial Market Disruption	62% Server Issues	64% Disgruntled Employee	64% Software Issues
--	--	-----------------------------	---------------------------------------	-------------------------------

Top 5 Crises Most Prepared for:

Percent of respondents indicating prepared or extremely prepared. Only crises with 25%+ of respondents noted as being concerned about the crisis were included below.

92% Ice Storm/ Winter Weather	91% Health/ Safety Issue	90% Power Outage	88% Pandemic/ Disease	85% Fire (Not Natural)
--	---------------------------------------	----------------------------	------------------------------------	-------------------------------------

INSIGHTS

Despite organizations expressing significant concern about technical crises such as cyber attacks, data breaches, and network/communication outages (as highlighted on the previous page), they appear to be moderately prepared for these crises. In contrast, they seem **far less prepared for various human and business-related disasters**, such as supply chain disruptions, financial market disruptions, disgruntled employees, and workplace violence, which ranked highest on the list of crises they are least prepared to handle.

Supply chain disruption, in particular, has become an increasingly pressing concern. Before COVID-19, it did not even rank among the top 10 crises, but by 2023 it had risen to #7, and this year it is listed as the #5 most concerning crisis. Additionally, organizations reported being least prepared for a supply chain disruption. There is also a **growing sense of vulnerability regarding potential financial market disruptions**, with the percentage of organizations feeling prepared dropping from 78% to 46%.

Which of the Following does the Scope of the Program Address?

Sum exceeds 100% due to multiple selections.



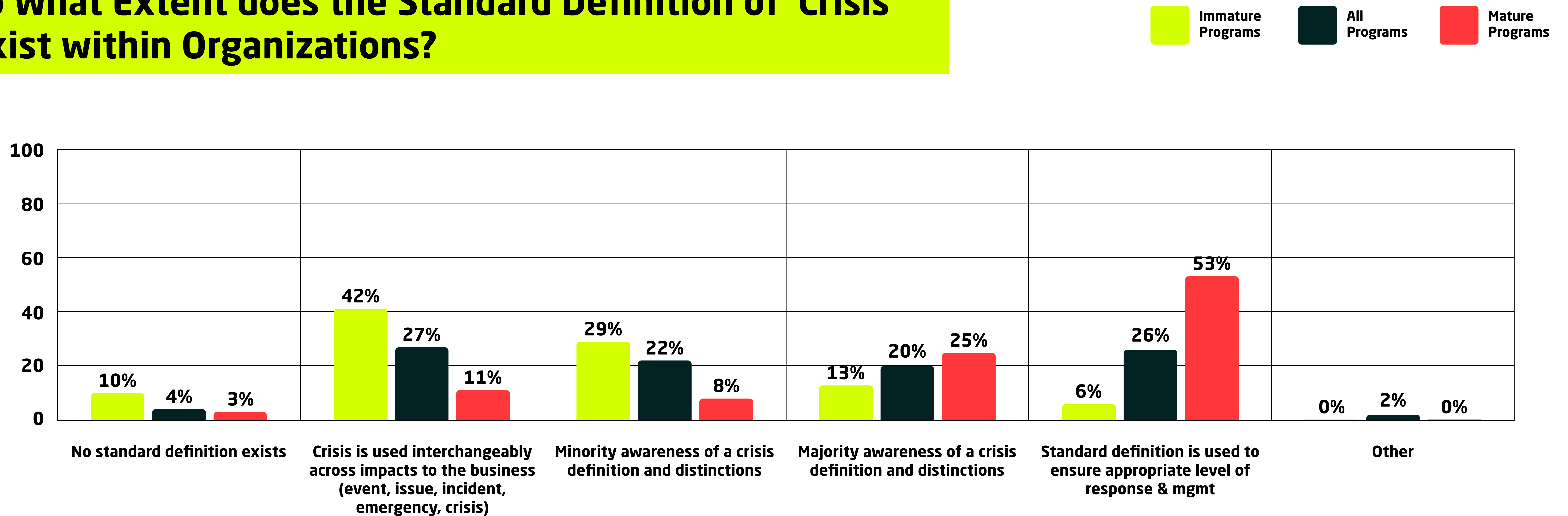
INSIGHTS

The data reveals that while a vast majority of organizations (**over 90%**) include technology-related risks in their programs, such as data loss, technology disruptions, and information security or cyber issues, **significantly fewer organizations (less than 40%)** address **human and business-related** risks. These under-addressed areas include product issues, international medical or security evacuations, kidnapping, ransom or extortion, and travel security, highlighting a critical gap in preparedness for several human/business crises.

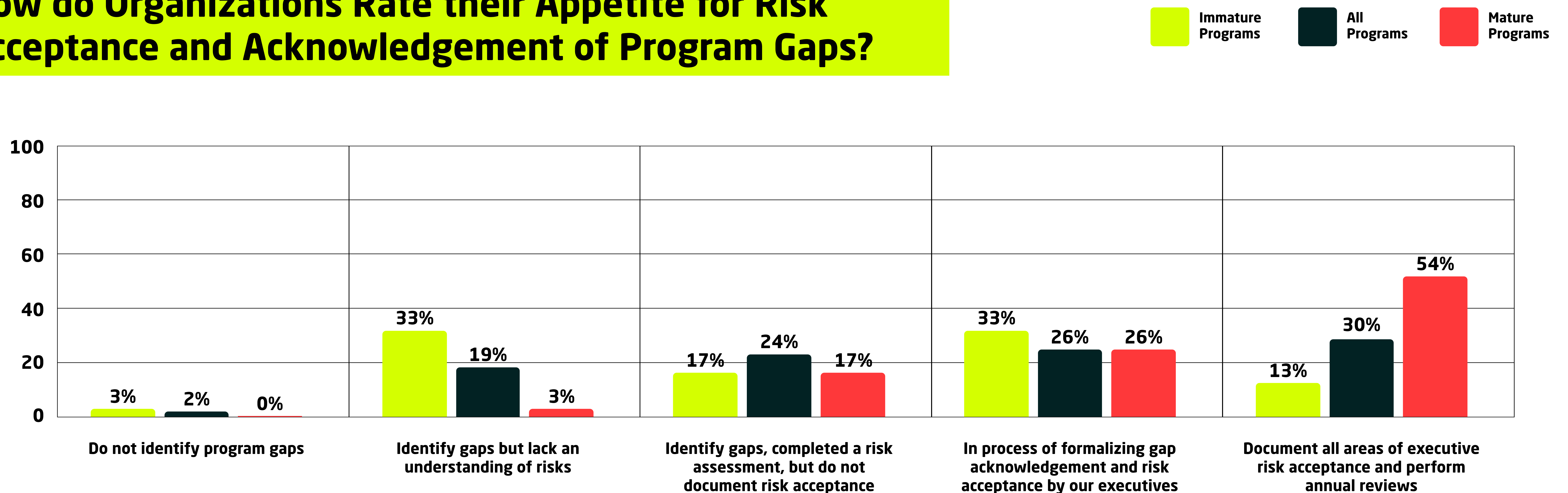
Organizations have expanded the scope of their programs, with notable increases in the inclusion of certain risks: supply chain disruptions (+18%), data loss (+15%), workplace violence (+12%), and physical security issues (+10%) from 2023 to the present.

Additionally, four new risk categories were introduced this year: loss of site (office or production), threat monitoring/assessment, travel security, and product issues (recalls, quality, or delivery).

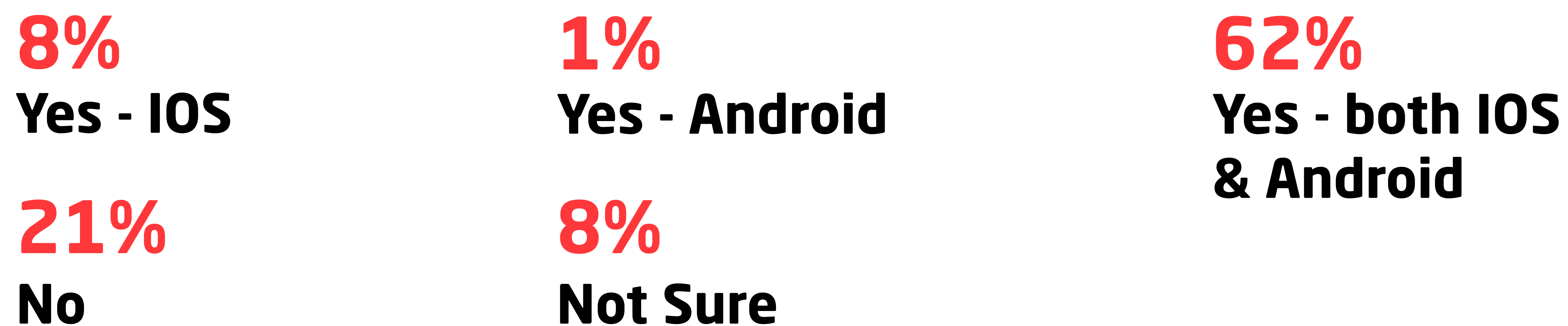
To What Extent does the Standard Definition of 'Crisis' Exist within Organizations?



How do Organizations Rate their Appetite for Risk Acceptance and Acknowledgement of Program Gaps?

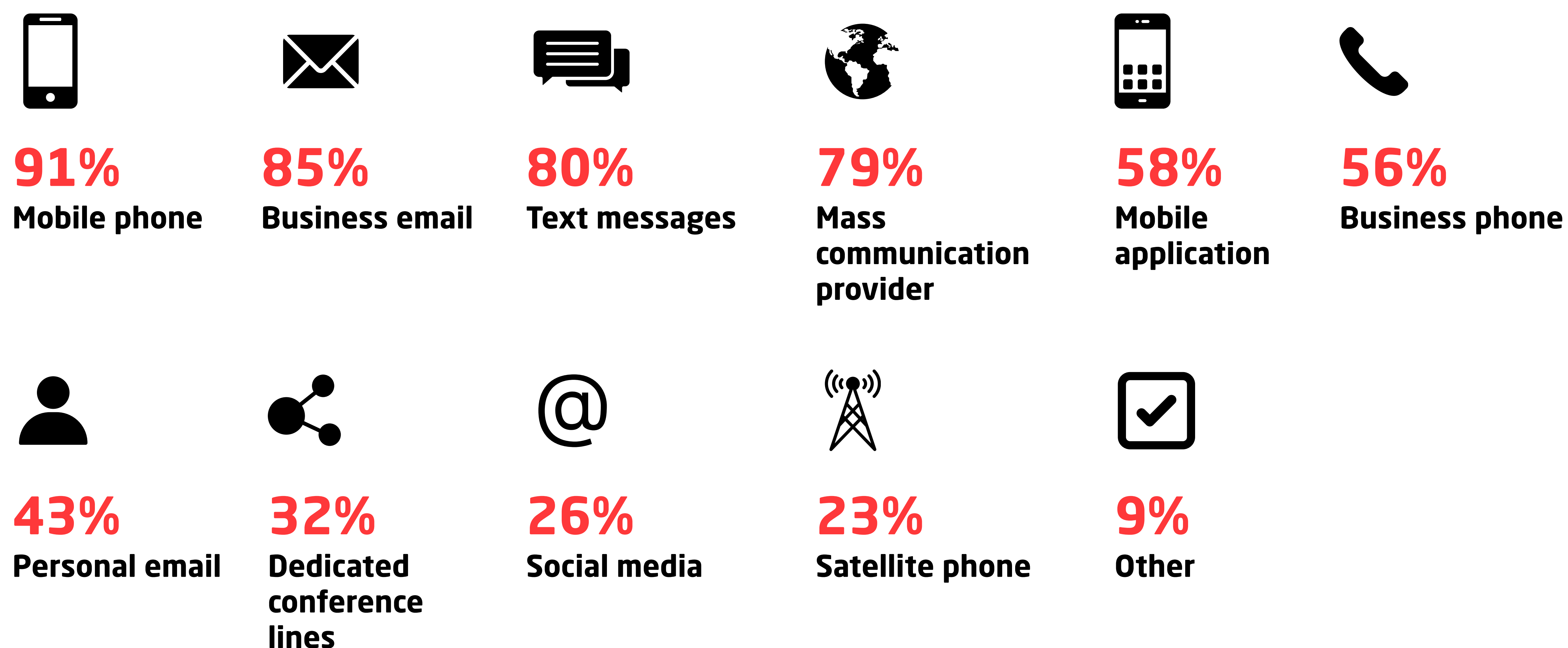


Are Plans Accessible in a Mobile Format?

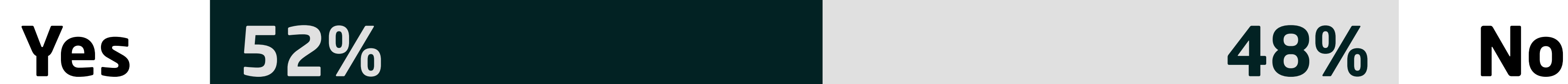


How do Organizations Plan to Communicate Throughout a Crisis?

Sum exceeds 100% due to multiple selections.



Based on Preparedness Efforts, has a Disruption been Prevented in the Past?



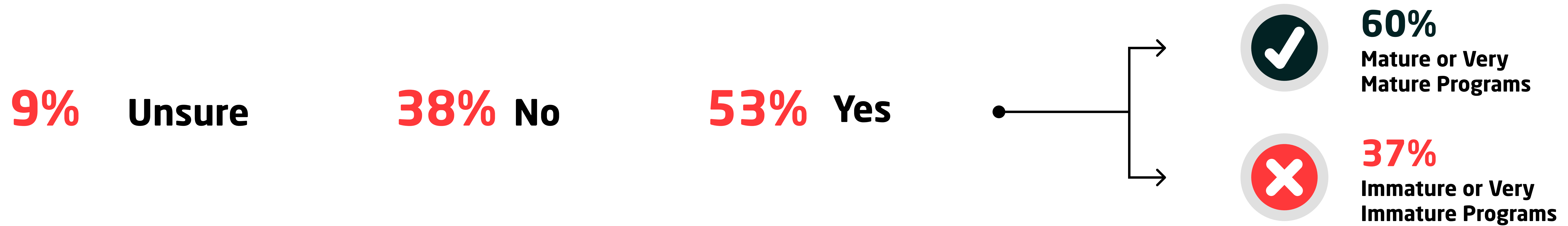
INSIGHTS

In today's tech-driven environment, **14%** of organizations with "mature" or "very mature" programs still lack mobile accessibility for their plans. This percentage is even higher among all respondents (**21%**) and rises to **29%** for organizations with "immature" or "very immature" programs. Despite this, when asked how they would communicate during a crisis, the majority of respondents reported using mobile phones (**91%**), text messaging (**80%**), and mobile applications (**58%**). Ensuring plans are available in mobile formats could provide critical access if company systems go down, allow teams to follow pre-organized checklists to avoid missed steps, and ensure proper analysis, strategy-setting, and task assignment during a crisis.

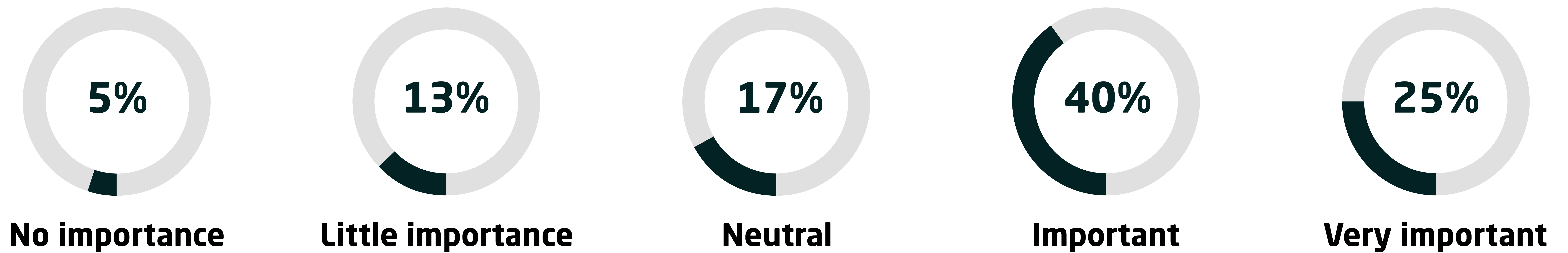
Overall, organizations have made progress in improving mobile accessibility by offering plans on both iOS and Android platforms, with adoption increasing from 51% in 2023 to 62%. Additionally, more organizations are using personal email addresses for communication, with usage rising by **12%** to **43%**.

After a more detailed analysis of the data, we found that **95%** of respondents opted for multiple communication methods. Among those who selected just one method, **40%** preferred a mass communication provider, while another **40%** chose mobile phones. Furthermore, **63%** of respondents reported using between 5 and 8 different communication methods during a crisis.

Ability for Real-Time Reporting (Software or Other) to Executive Leadership on Crisis-Driven Risks to Critical Processes.



Importance of Business Continuity Software to Organizations in terms of the Ability to Identify Crisis-Driven Risks to Critical Processes in Real-Time.



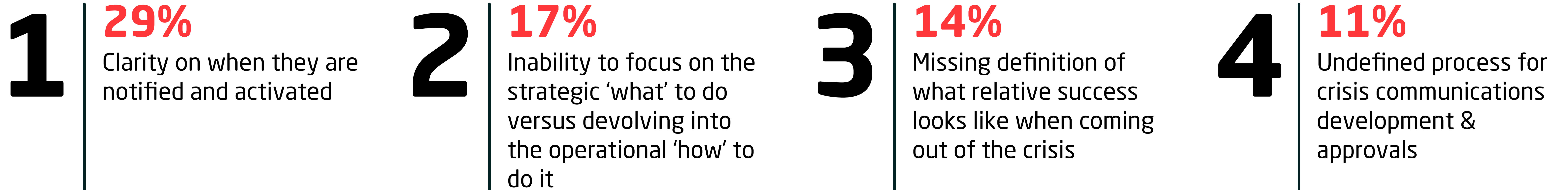
Do Organizations have a Defined, Corporate-Level Crisis Management Team?



Top 4 Greatest Challenges

Mature or Very Mature Programs

Percent of respondents indicating significant challenge or somewhat of a challenge.



Immature or Very Immature Programs

Percent of respondents indicating significant challenge or somewhat of a challenge.



INSIGHTS

"It is very clear that the biggest challenge is the lack of a structured approach that is well rehearsed. The key is to ensure you have the basic crisis management model sorted - with teams assigned for:

- 1. Strategic - Big Picture:** Highest decision-making body- at management board/ExCo level (CEO/COO/Heads of Businesses & Functions). Makes strategic decisions based on inputs from tactical Team's inputs.
- 2. Tactical - Middle Management:** Business and Functional Representatives - deals with actual business impact, consequence management, and key actions
- 3. Operational - Technical/ Experts/Practitioners:** who are actually dealing with the "fire". They should not be disturbed while they try to fix the problem, and get the organisation/systems back and running. Tactical teams need to shield them from senior management intervention directly.

Depending on the complex nature of the business and size, there could be multiple operational teams. Most importantly, this setup is rehearsed/tested as part of crisis management exercises and everyone knows their roles. Some organisations call this a GOLD, SILVER, and BRONZE setup, but I prefer Strategic, Tactical, and Operational."

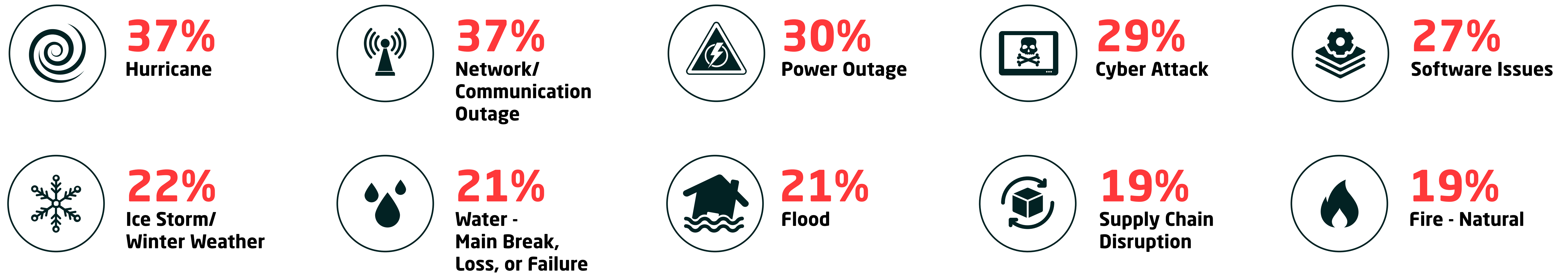
- Jayaraj Puthanveedu (Advisory Board)



TOP 10 CRISES & THE IMPACT TO ORGANIZATIONS

Top 10 Crises Leading to Employing a Response/Recovery in 2024

Sum exceeds 100% due to multiple selections.



Organizations employed a response/recovery team more often for Technical Disasters (**31%**) and Natural Disasters (**30%**) followed by Human/Business Disasters (**21%**) and Accidents (**17%**).

In Comparing the Top Crises from 2020 to 2022 to 2024 We Noticed the Following:

Ice Storm/Winter Weather continually increased from **20%** to **32%** to **37%**

Civilian unrest/Political instability continually decreased from **29%** to **8%** to **6%**

Pandemic/Disease continually decreased from **79%** to **50%** to **6%**

Protest continually decreased from **21%** to **12%** to **10%**

Supply Chain Disruption increased from **13%** to **21%** and then decreased slightly to **19%**

Software issues stayed consistent at **17%** to **17%** and then increased to **27%**

War or Insurrection increased from **2%** to **24%** and then decreased to **14%**

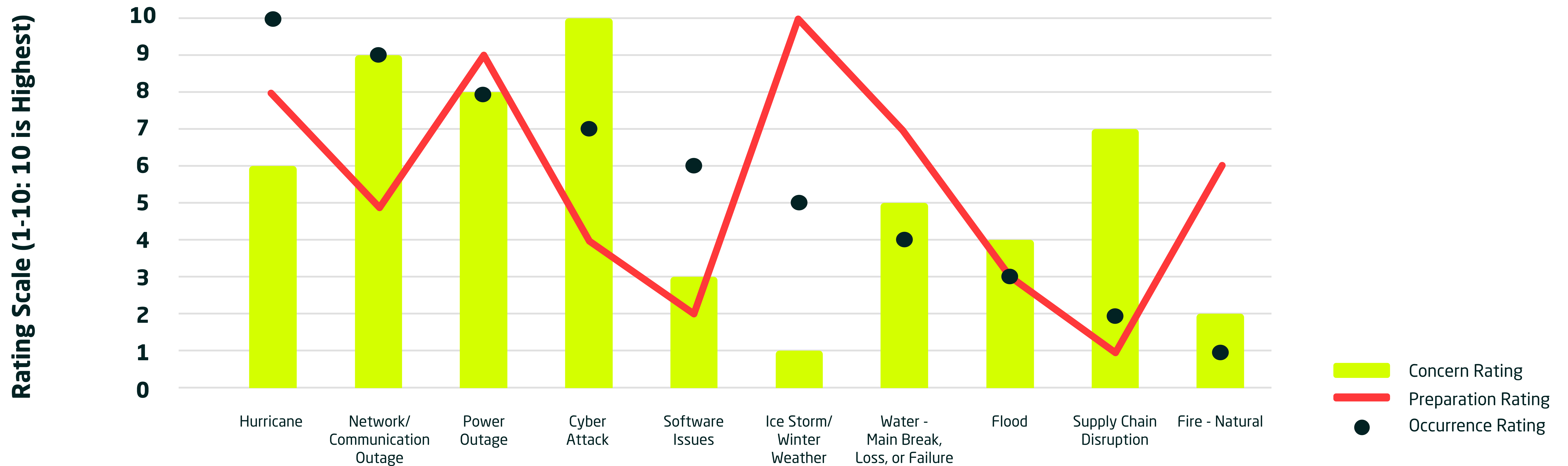
INSIGHTS

Over two-thirds of organizations encountered a crisis or disaster in the past year that required them to activate their response and recovery teams. These high-impact disruptions have included global supply chain breakdowns, a surge in cyber-attacks, severe weather storms (Hurricane Helene and Milton), escalating geopolitical tensions, and a global outage caused by CrowdStrike. While each year presents new challenges that test resilience management strategies—such as the COVID-19 pandemic from 2020 to 2022, civil unrest and political instability in 2020, and a spike in supply chain disruptions in 2022—certain crises remain persistent. **Long-standing challenges that continue to impact organizations include power outages, water infrastructure failures, hurricanes, floods, tornadoes, and, increasingly, cyber-attacks.**

In 2024, notable issues like software failures, network outages, and cyber incidents have come to the forefront, further underscoring the importance of robust crisis management systems.

An Assessment of the Top Crises Leading to a Response/Recovery Effort in 2024 and the Ratings of Concern and Preparation for each Crisis in the Future

Top Crises in 2024: Future Concern & Preparation Rating

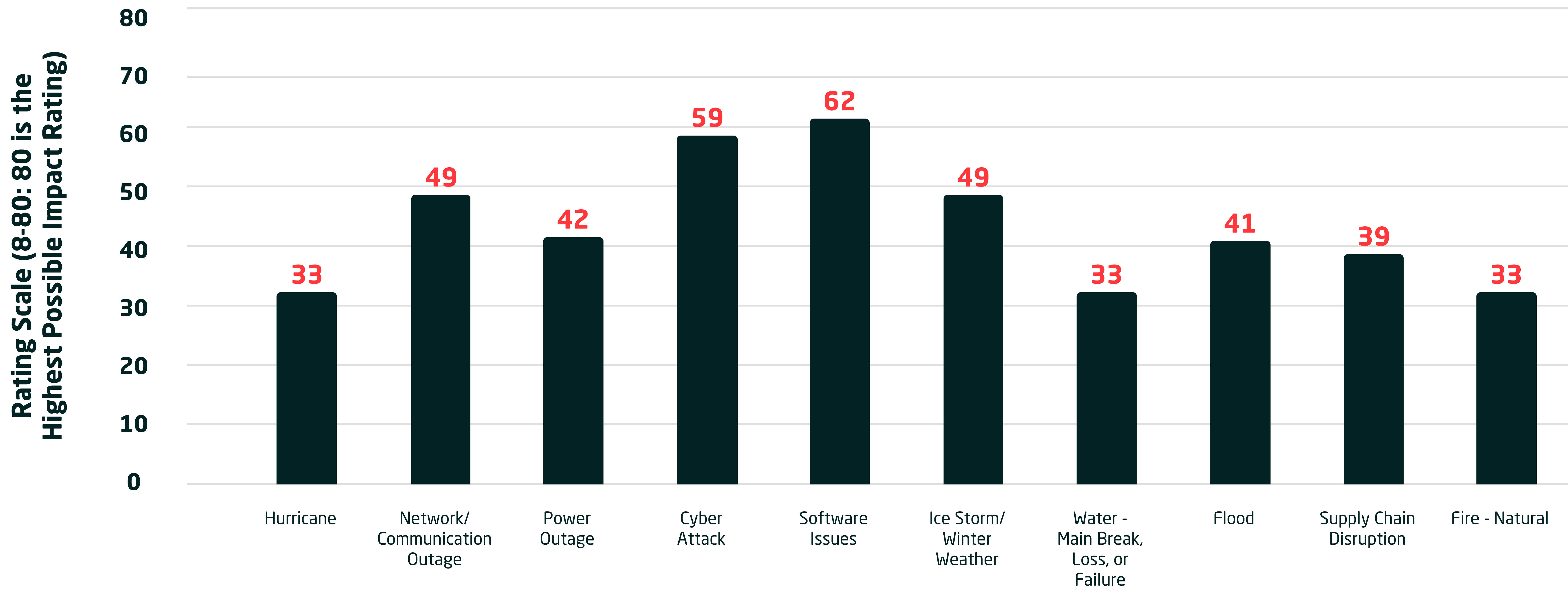


Top Crises Leading to Employing a Response/Recovery in 2024

Rating scale from 1 to 10 with 10 being the highest and 1 being the lowest.

	Occurrence Rating	Concern Rating	Preparation Rating
Hurricane	10	6	8
Network/Communication Outage	9	9	5
Power Outage	8	8	9
Cyber Attack	7	10	4
Software Issues	6	3	2
Ice Storm/Winter Weather	5	1	10
Water - Main Break, Loss, or Failure	4	5	7
Flood	3	4	3
Supply Chain Disruption	2	7	1
Fire - Natural	1	2	6

Crisis Impact Rating for Top Crises in 2024



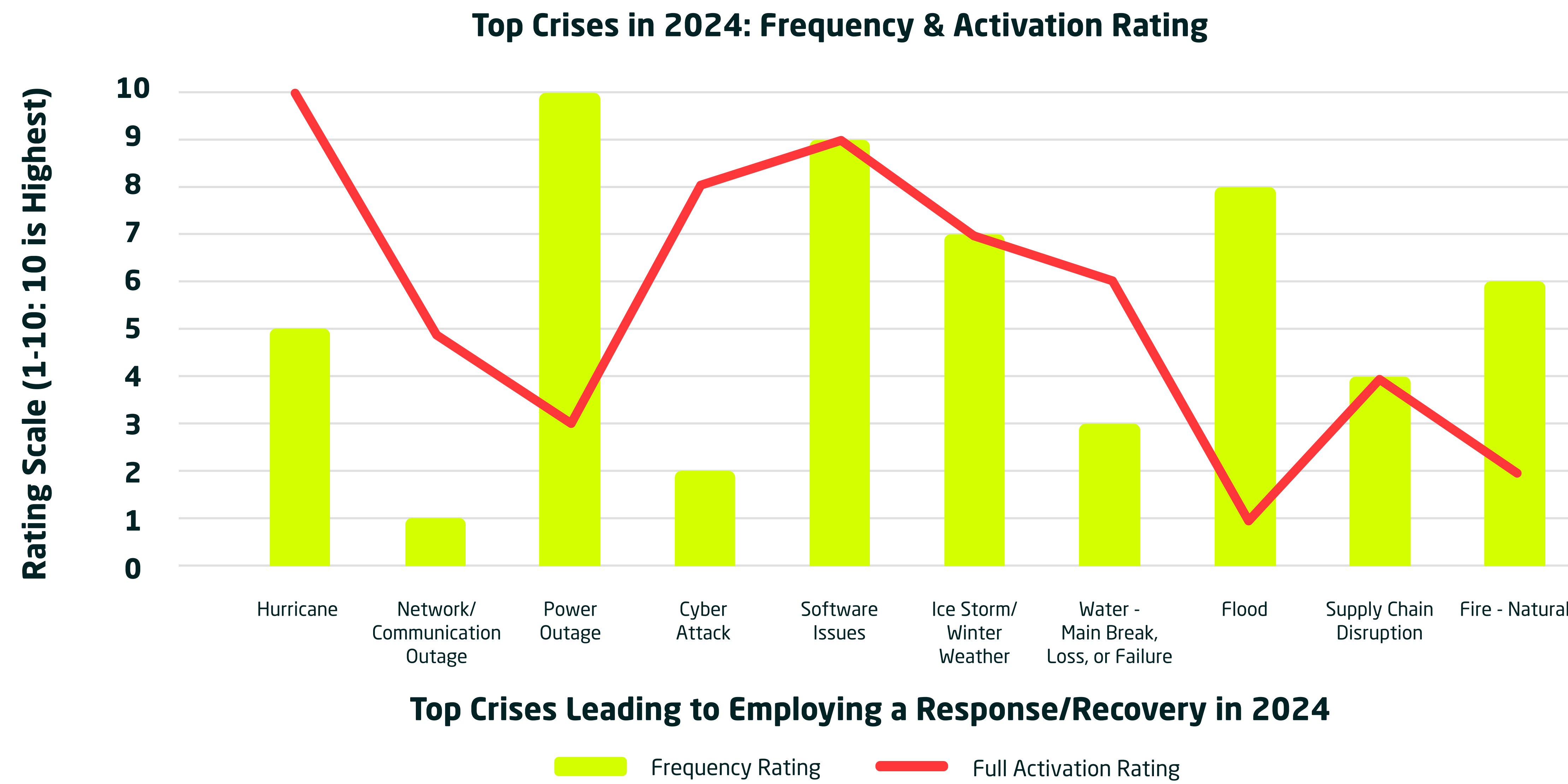
Top Crises Leading to Employing a Response/Recovery in 2024

INSIGHTS

This year, we continued our evaluation of the most significant recent crises affecting organizations, assigning each a crisis impact rating based on several factors: frequency, full activation of response teams, advance warning, employee impact, geographic scope, percentage of critical systems affected, business resumption time, and estimated financial losses. **The analysis revealed that software issues had the highest impact, receiving a crisis impact score of 62, followed by cyber attacks (59), network/communication outages (49), and ice storms/winter weather (49).**

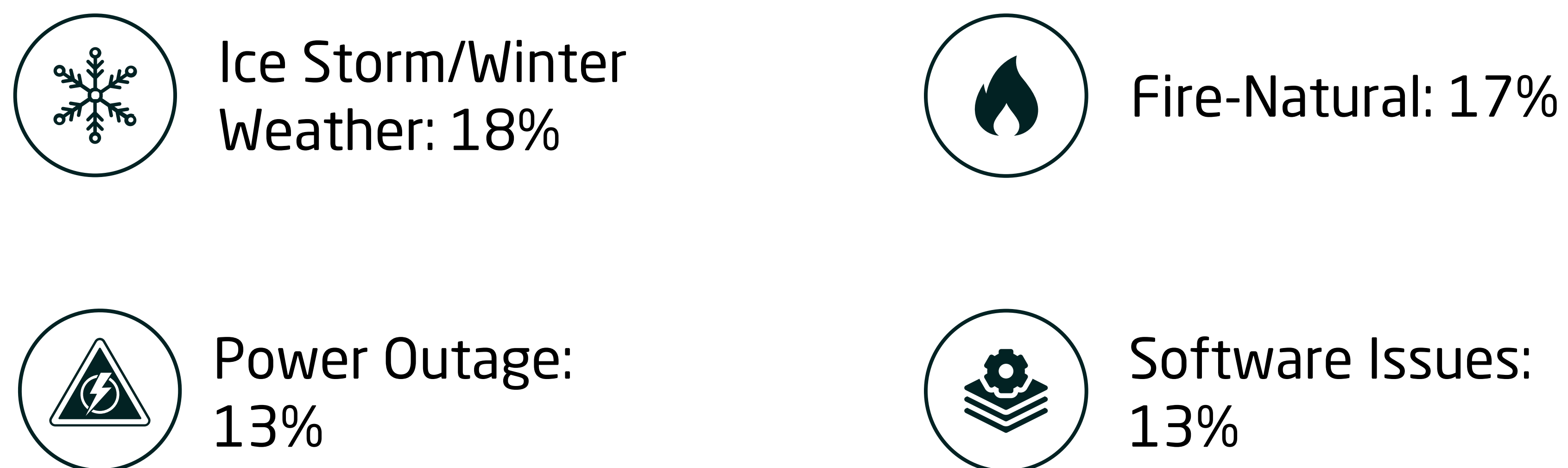
The following sections detail how each crisis affected organizations based on the mentioned criteria. Each crisis was evaluated with a rating system ranging from 1 (lowest impact) to 10 (highest impact) across eight categories, resulting in total potential impact scores between 8 and 80.

Frequency and Activation Rating for the Top Crises Leading to a Response/Recovery Effort in 2024

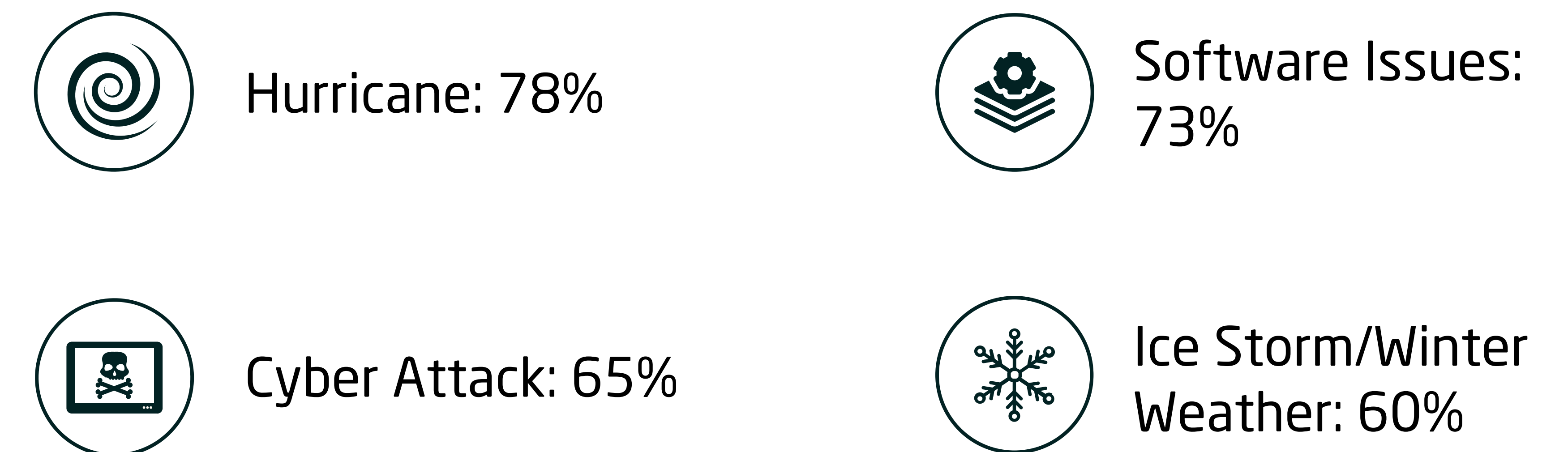


	Frequency Rating	Full Activation Rating
Hurricane	5	10
Network/Communication Outage	1	5
Power Outage	10	3
Cyber Attack	2	8
Software Issues	9	9
Ice Storm/Winter Weather	7	7
Water - Main Break, Loss, or Failure	3	6
Flood	8	1
Supply Chain Disruption	4	4
Fire - Natural	6	2

Percent of Respondents indicating a Crisis Occurring 10+ Times



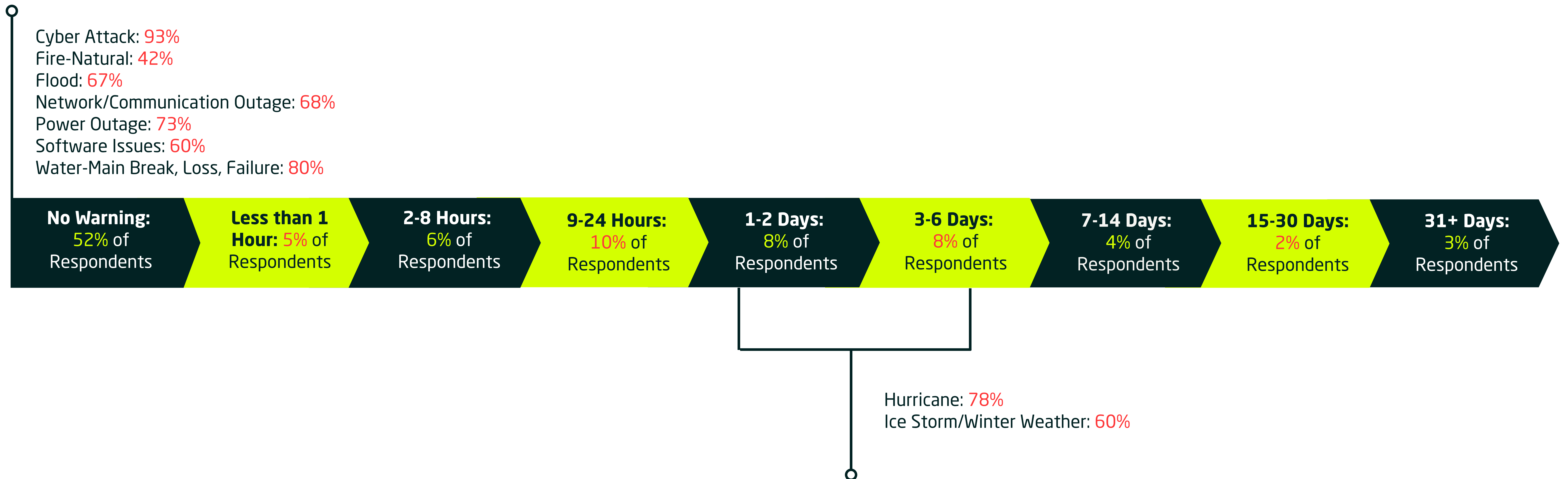
Percent of Respondents indicating Full Activation by Crisis



The data also highlights that **software issues** and **ice storm/winter weather** were most likely to occur at high frequency and lead to a full activation.

Note: Study participants ranked the frequency of each crisis from occurring 1 time to 10+ times in addition to ranking the level of activation from pre-vent alert and preparation to full activation.

Advance Warning for the Top Crises Leading to a Response/Recovery Effort in 2024



INSIGHTS

Most organizations (52%) had to quickly invoke a response/recovery effort in response to a crisis due to receiving no warning before a disaster hit and 26% of organizations received 9 hours to 6 days advanced warning. It's not surprising that such weather related crises (hurricanes and ice storm/winter weather) provided some advanced warning of 1-6 days while accidents and technical disasters provided no warning at all.

"While the vast majority of incident-type gave no warning at all, some incidents (particularly weather events) have some advanced warning to varying degrees. It is important to plan for and exercise both no-notice events as well as those that may develop over days and ensure your surveillance and intelligence tools are able to best position the organization for an effective response."

- Kevin Cunningham (Advisory Board)

Recovery/Response Activated for the Top Crises Leading to a Response/ Recovery Effort in 2024

Sum exceeds 100% due to multiple selections.

Business Recovery (Work Area)

Call Center Recovery

Cyber Incident Response

Emergency Operations Center (EOC)

Hot-Site Activation

Mobile Recovery

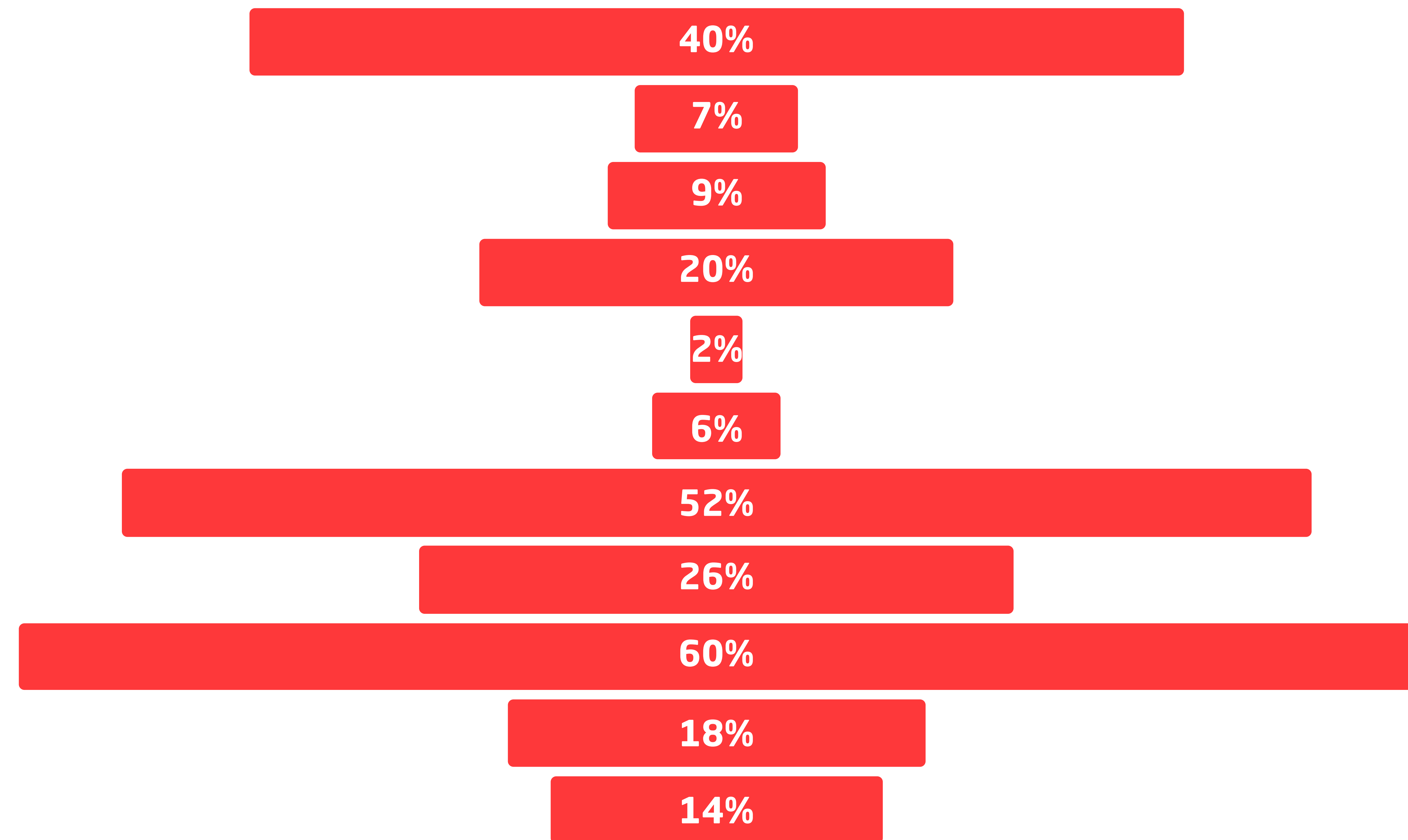
Notification System

Technology Recovery

Local/Regional Crisis Management Team

National Crisis Management Team

Global Crisis Management Team



INSIGHTS

The data reveals that **crisis management teams are the most frequently activated in response to a crisis, followed closely by the use of notification systems and business recovery (work area)**. This underscores the critical importance of pre-planning for crisis management within an organization. However, it's especially concerning that only 26% of organizations have a standardized definition of "crisis" to ensure a consistent level of response and management, as noted on page 11 of the report.

Moreover, on page 14, the data outlines several challenges organizations face in their crisis management pre-planning. These include ambiguity about when to initiate notifications and activate crisis response, a lack of defined processes for crisis communication, difficulty in maintaining focus on the strategic "what" needs to be done rather than getting bogged down in the operational "how" to execute it, and confusion around workstreams, which often lack clear ownership, expectations, and timelines. These gaps in preparedness can significantly hinder an organization's ability to respond effectively in times of crisis.

Percent of Employees Impacted for the Top Crises Leading to a Response/Recovery Effort in 2024

Negatively Impacted

75% + of Employees

- Network/Communication Outage: 25%
- Software Issues: 20%
- Cyber Attack: 17%
- Fire-Natural: 8%

25-50% of Employees

- Flood: 18%
- Supply Chain Disruption: 10%
- Ice Storm/Winter Weather: 9%
- Water-Main Break, Loss, or Failure: 9%

Displaced

75% + of Employees

- Water-Main Break, Loss, or Failure: 9%
- Power Outage: 7%

25-50% of Employees

- Flood: 18%

10-15% of Employees

- Ice Storm/Winter Weather: 9%
- Fire-Natural: 8%

Placed at Recovery Site

25-50% of Employees

- Hurricane: 6%

20-25% of Employees

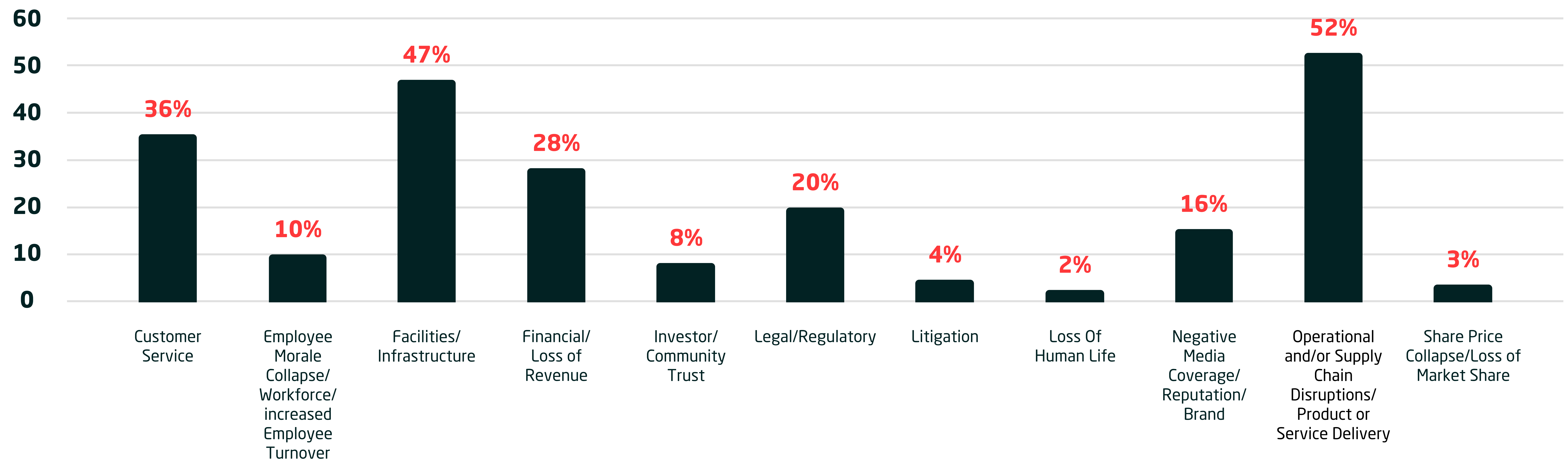
- Fire-Natural: 8%
- Power Outage: 7%

10-15% of Employees

- Flood: 9%
- Water-Main Break, Loss, or Failure: 9%

Impact to the Organization for the Top Crises Leading to a Response/Recovery Effort in 2024

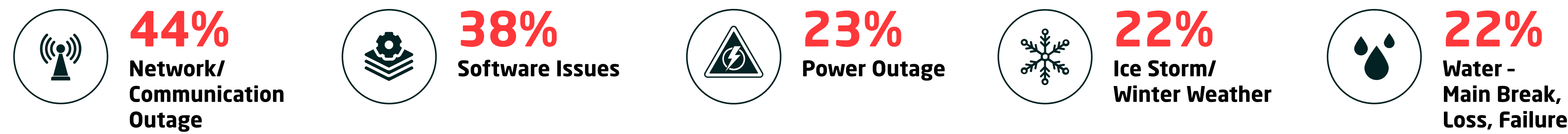
Sum exceeds 100% due to multiple selections.



19% of Organizations Indicated that More than 25% of Critical Processes were Impacted while Responding/Recovering to the Top 10 Crises in 2024.

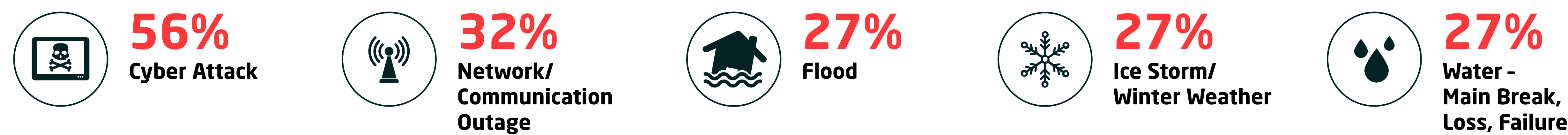
Five of the Top 10 Crises Compromised Critical Processes More.

Percent of respondents noting 25%+ critical processes impacted for the following five crises.



Executive Leadership Involvement for the Top Crises Leading to a Response/Recovery Effort in 2024 - More than 1/3 of Executives were Very Involved Regardless of the Crisis

The crises that triggered the most active executive leadership are (indicated below as "very involved"):

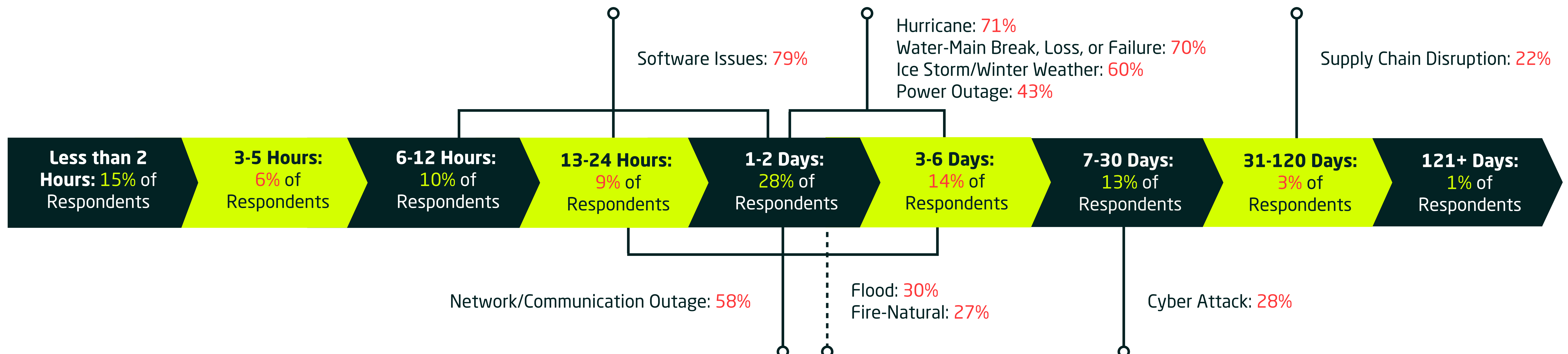


INSIGHTS

Geographical Scale of Impact for the Top Crises Leading to a Response/Recovery Effort in 2024

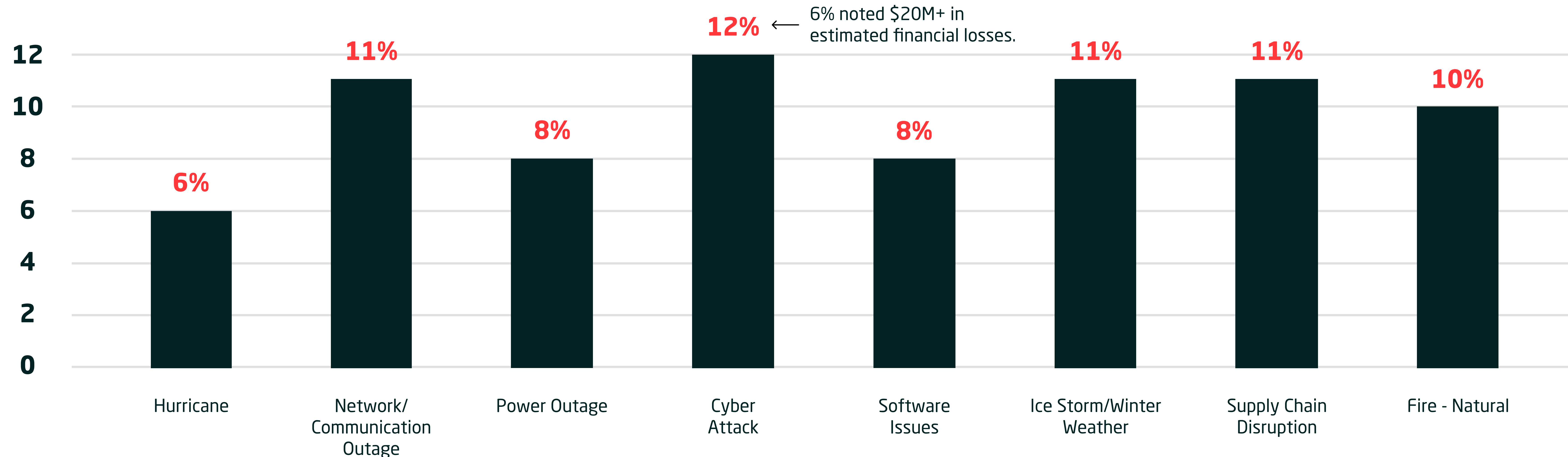
- Global: 5%
- National: 10%
- Regional: 19%**
- City Wide: 6%
- Multiple Buildings: 5%
- Complete Building: 13%
- Partial Building: 5%
- Multiple Business Units: 24%**
- Business Unit: 13%

Business Resumption for the Top Crises Leading to a Response/Recovery Effort in 2024



Percent of Respondents Noting Over \$1,000,000 USD in Estimated Financial Losses for the Top 10 Crises in 2024

Sum is not meant to equal 100%.



On average **57%** of all respondents indicated it was difficult to calculate the estimated financial losses.

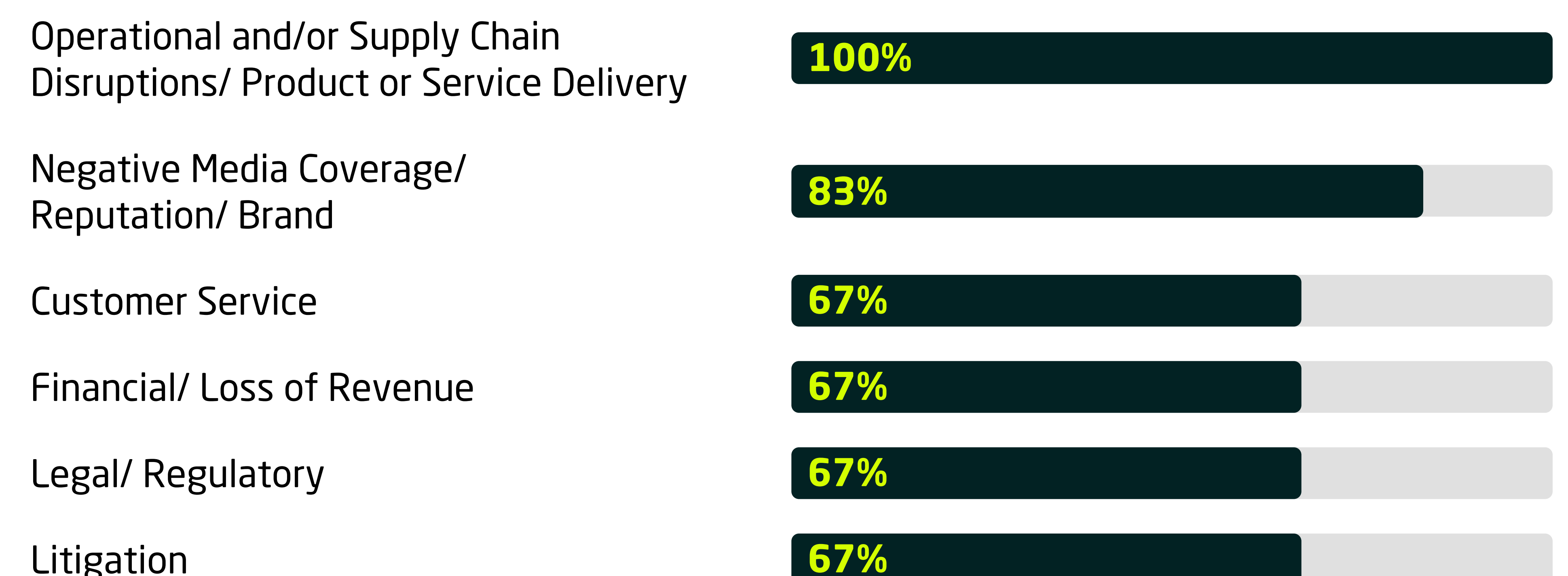
Assessing Respondents Who Noted \$5M+ USD in Estimated Losses for an Individual Crisis

83% of crises were technology disasters (cyber attacks, data breaches, and network/communication outages).

33% of respondents experienced a business resumption period of 121+ days before being back to normal business operations.

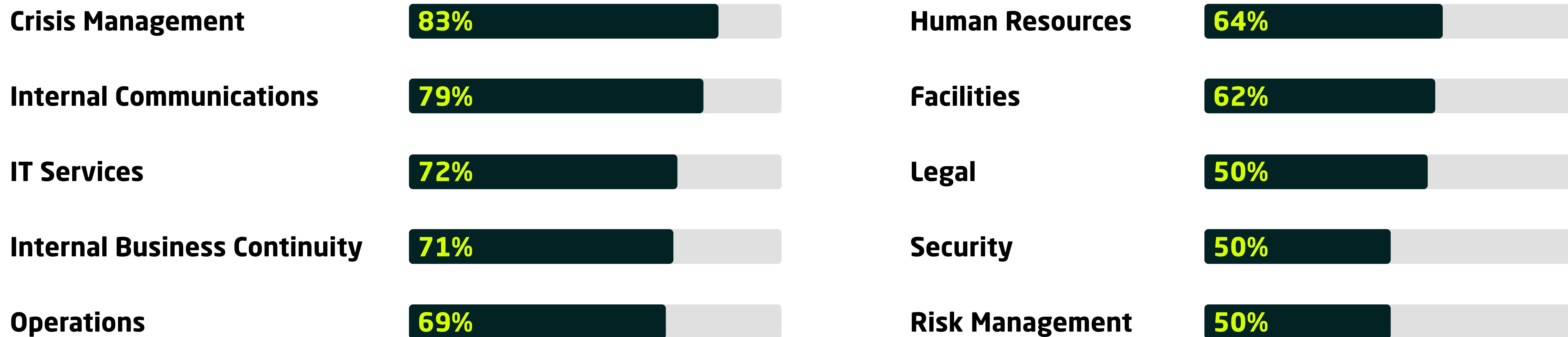
83% of respondents noted that their executives were very involved.

How did these crises with \$5M+ in estimated financial losses impact organizations?



Who or What was Included While Recovering/Responding to a Crisis?

50%+ of respondents indicated:



What Outcomes Were Noted as Successful as a Result of Employing Resilience Capabilities Following the Onset of a Business Disruption or Crisis



46% Organizational value was preserved

45% Compliant with regulators

45% Preserved reputation/community trust

43% Market share was preserved

42% Profitability levels continued

42% Revenue was preserved



38% Minimal to no legal exposure

32% Minimal to no impact to customers

25% Minimal to no impact to employees

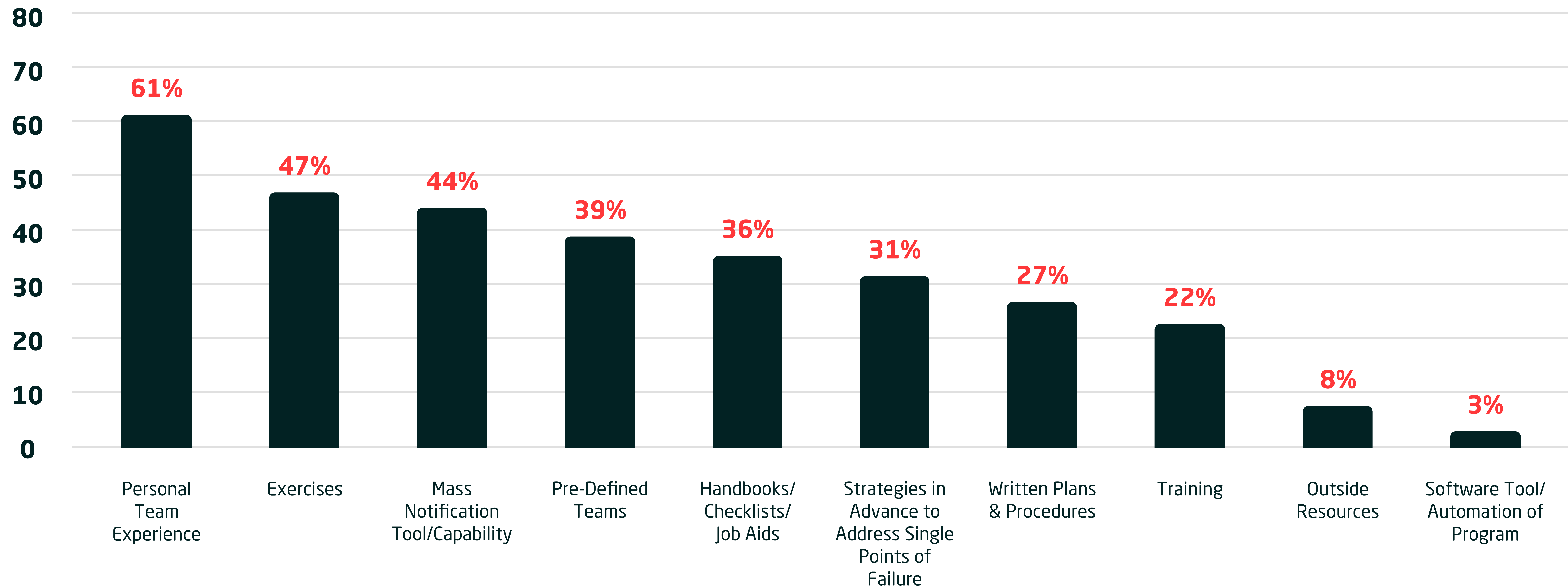
25% Minimal to no impact to partners

21% Minimal to no impact to operations

20% Recovery time objectives were met

Most Beneficial During a Response

Respondents chose their top 3 choices. Sum exceeds 100% due to multiple selections.



INSIGHTS

"In this 11th Edition Crisis Management Report 2024 the results to this question show that "Personal team experience" increased to be the number 1 benefit, displacing "exercises" which is now number 2. It is noteworthy that "mass notification tool" ranked last in 2023 and now, in 2024 occupies the number 3 benefit during a response (a huge increase in importance!).

My interpretation is that now, in 2024, respondents place greater importance on having these three elements (of similar importance) for an event response: "experienced personnel", "exercises" and "mass notification". There is no doubt that with these three elements we will be more effective in responding to an event.

However, in my opinion, this implies that we are relying more on people and/or systems, (which are "external" elements to our own responsibility), than on our own capabilities. Therefore, I recommend continuing to reinforce the "exercises" and "training"; in this way, we will build greater organizational resilience."

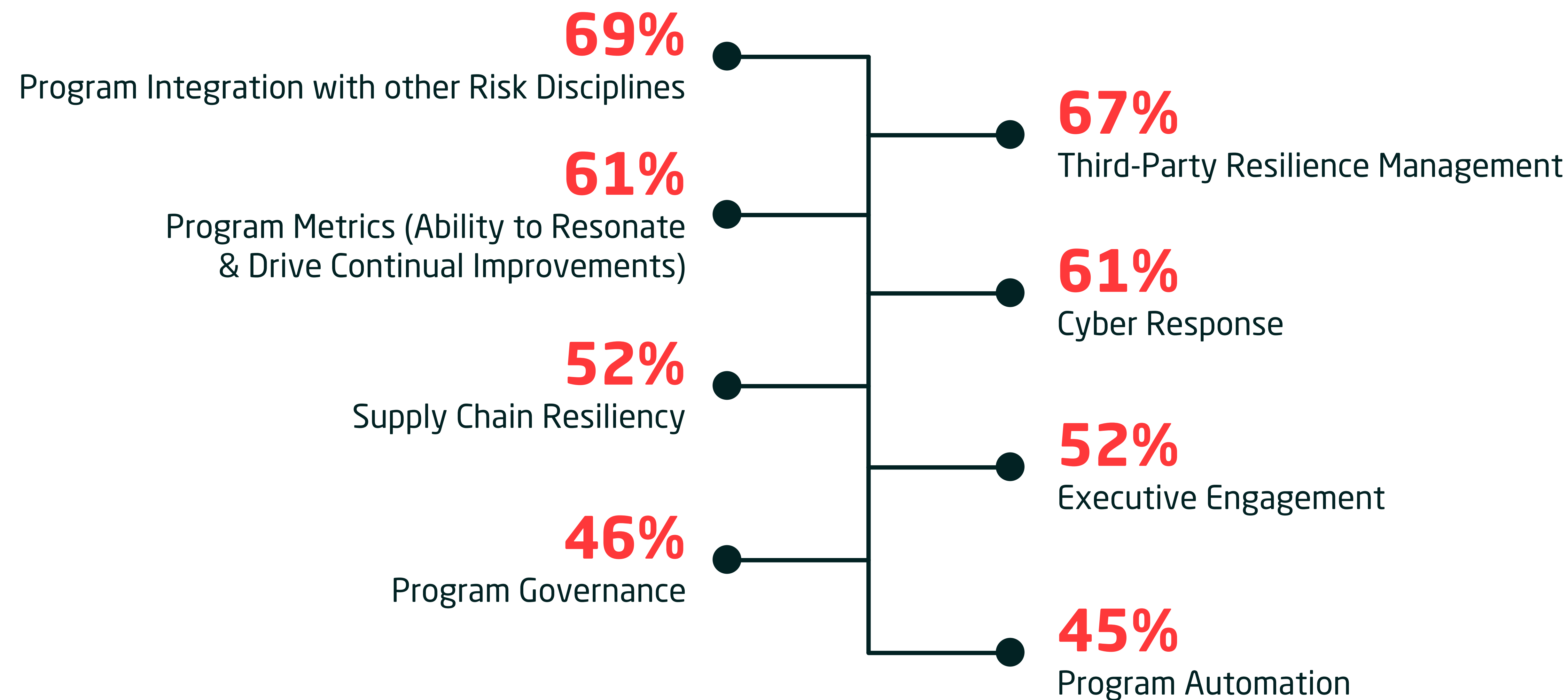
- Jorge Escalera Alcázar (Advisory Board)

A photograph of three business professionals in a meeting. A woman is seated at a table, pointing at a document. Two men stand behind her, looking at the document. The scene is dimly lit with a blue tint. A bright yellow curved shape is in the top-left corner, and another is in the bottom-right corner. The text 'FUTURE PROGRAM ENHANCEMENTS' is centered in white, bold, uppercase letters.

FUTURE PROGRAM ENHANCEMENTS

How will the Strength of Your Resiliency Program Change in the Next Year

Percent of respondents noting an **increase** in resiliency program initiatives.

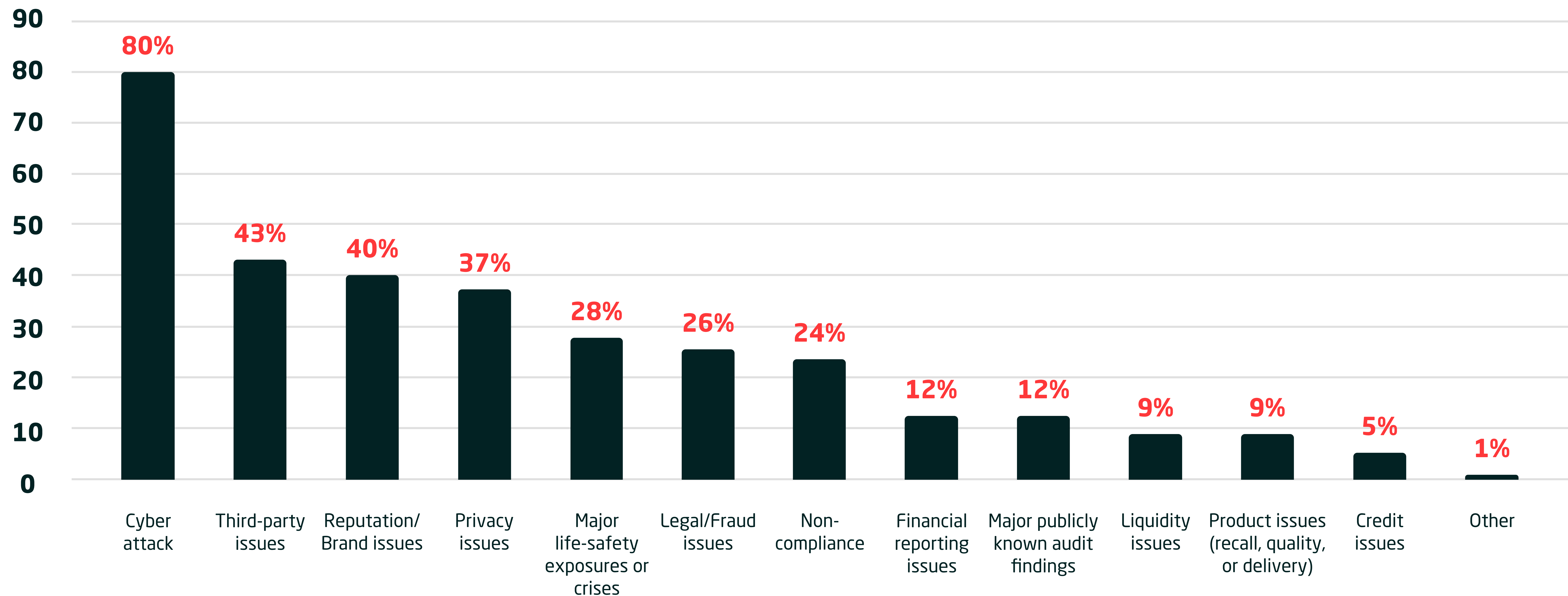


How are the Investment Strategies in Your Program Evolving in the Next Year



Which of these Potential Issues, when Impact Exceeds Day-to-Day Management Control, do You Expect to Improve Your Program Response Strategies in the Next Year

Sum exceeds 100% due to multiple selections.




INSIGHTS

A review of last year's data revealed that companies are increasingly focused on strengthening program responses for the coming year to address potential privacy (+12%) and legal/fraud issues (+11%) that may exceed day-to-day management control, while significant life safety incidents have declined by 14%.

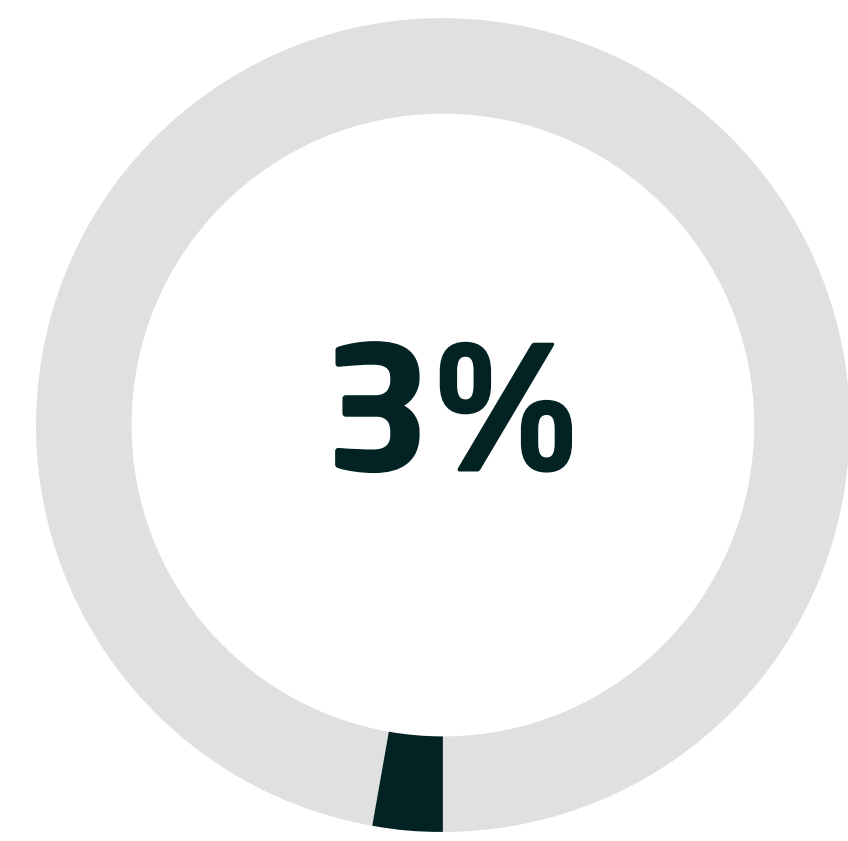
"In today's complex environment, companies face increasingly intricate and interconnected crisis events. To enhance both effectiveness and efficiency in coordinated responses, it is crucial to ensure linkage, training, and exercises with key response teams. Adopting an "all hazards" approach strengthens the company's ability to manage events that expand beyond the intended scope of existing plans and teams."

- Jennie Clinton (Advisory Board)

A person is sitting at a desk, working on a laptop. The laptop screen displays various data visualizations, including bar charts and pie charts. The person's hands are visible, one holding a pen and the other near a calculator. The background is slightly blurred, showing a desk with a cup and some papers. The overall scene is dimly lit, with a dark blue overlay. Two bright yellow shapes are present: a large curved shape in the top-left corner and a smaller curved shape in the bottom-right corner.

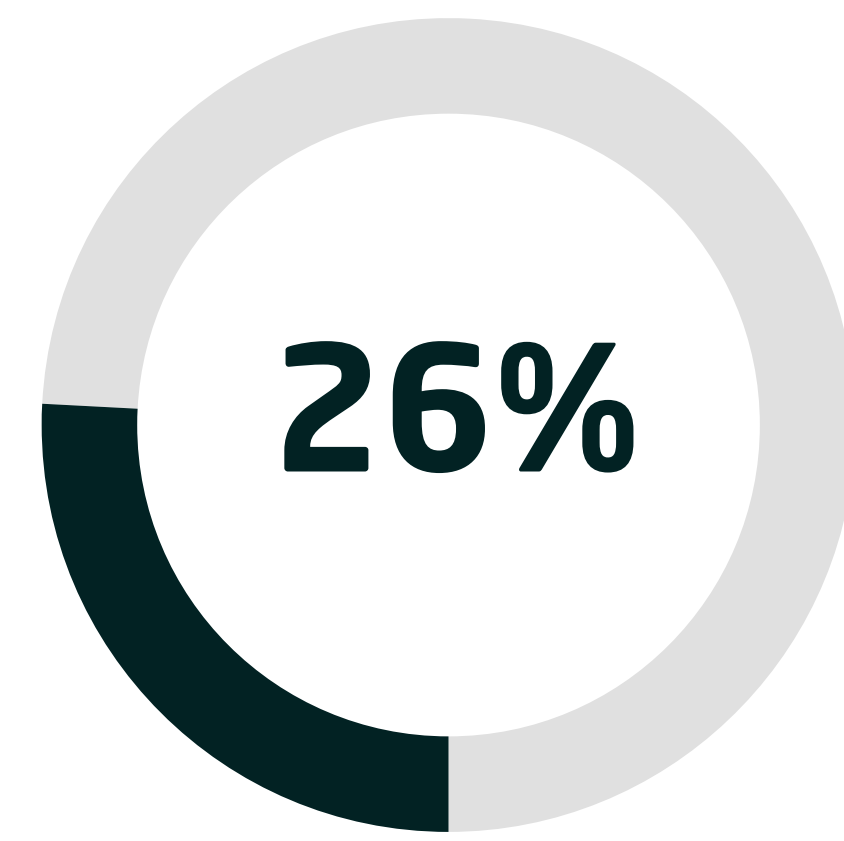
PROGRAM CHARACTERISTICS

Program Maturity (Self Rating)



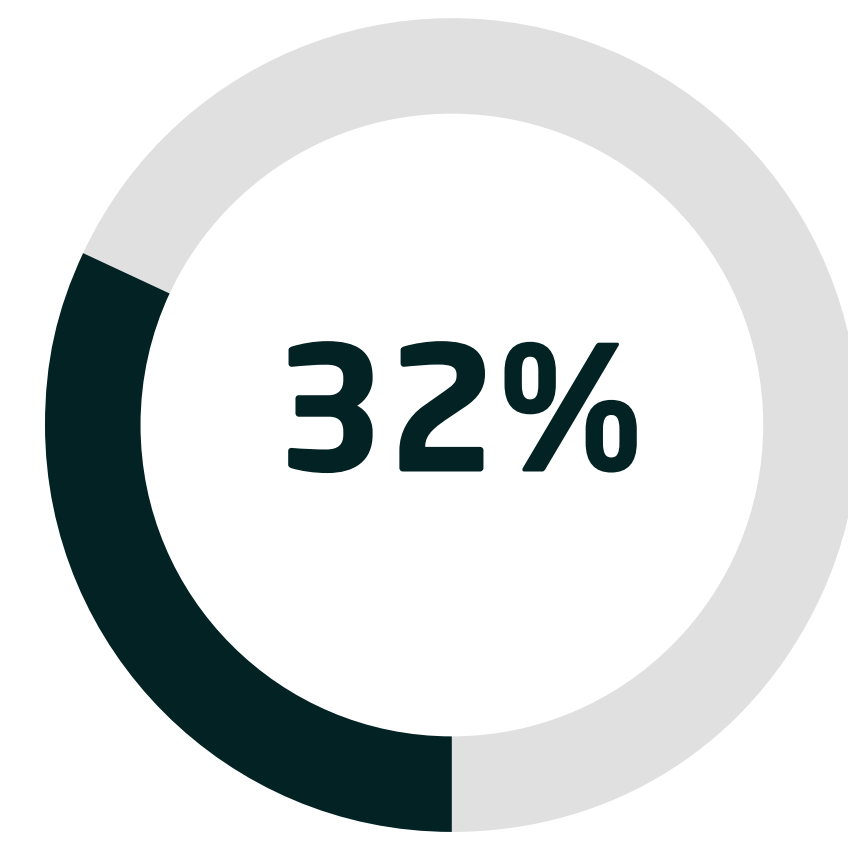
Reactive

(chaotic, ad hoc, individual heroics) The starting point for the use of a new or undocumented repeat process.



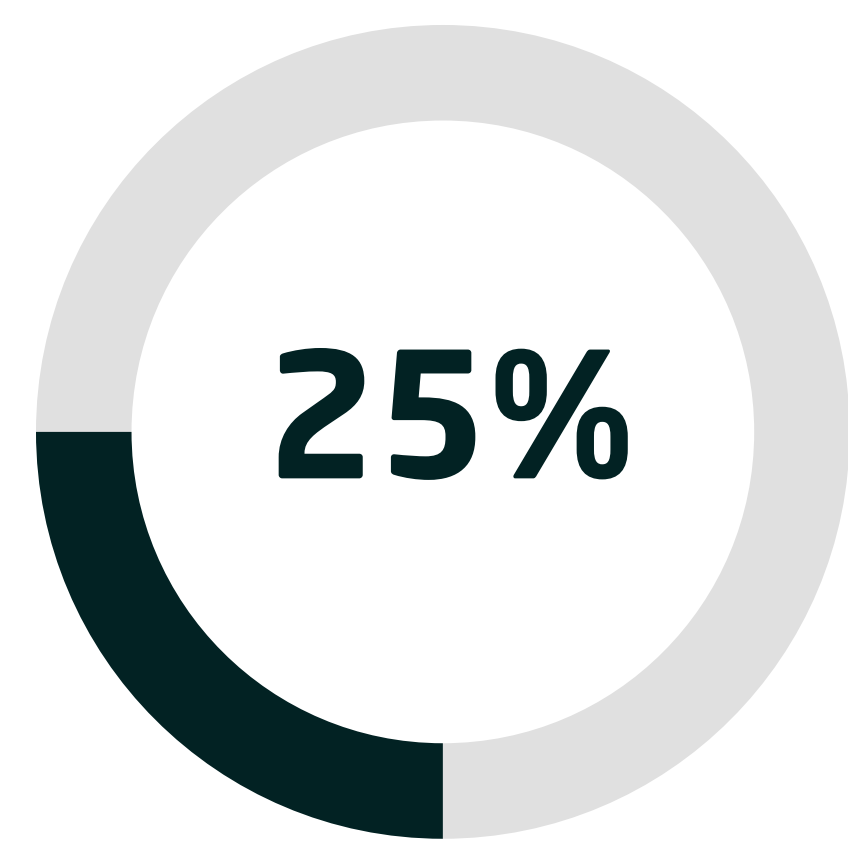
Developing

The process is at least documented sufficiently such that repeating the same steps may be attempted.



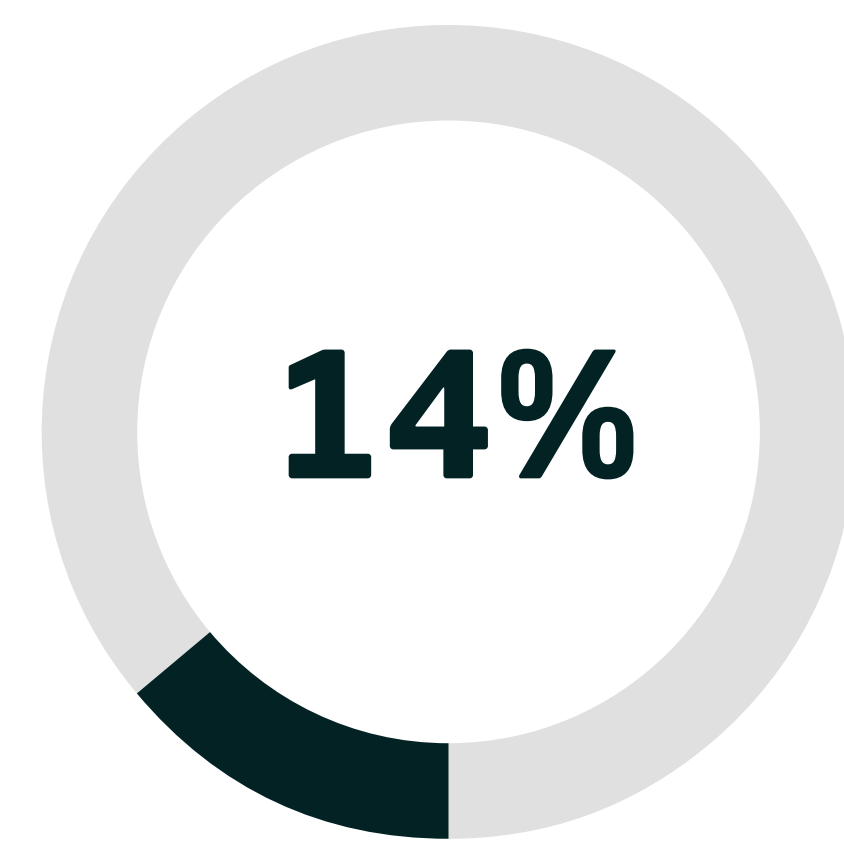
Sustaining

The process is defined/confirmed as a standard business processes.



Evolving

The process is quantitatively managed in accordance with agreed-upon metrics.



Capable

Process management includes deliberate process optimization/improvement.

Program Focus (Manage or Work Within)

Completely Focused on
2% IT Processes
14% Business Processes

More Focused on
10% IT Processes
42% Business Processes

Equally Focused on
32% IT & Business Processes

INSIGHTS

In our study, respondents were asked to self-assess the maturity of their programs, ranging from reactive (the starting point for using new or undocumented repeat processes) to capable (focused on deliberate process optimization and improvement). **Although the ratings were self-reported, the data revealed several key distinctions between "immature" and "mature" programs.**

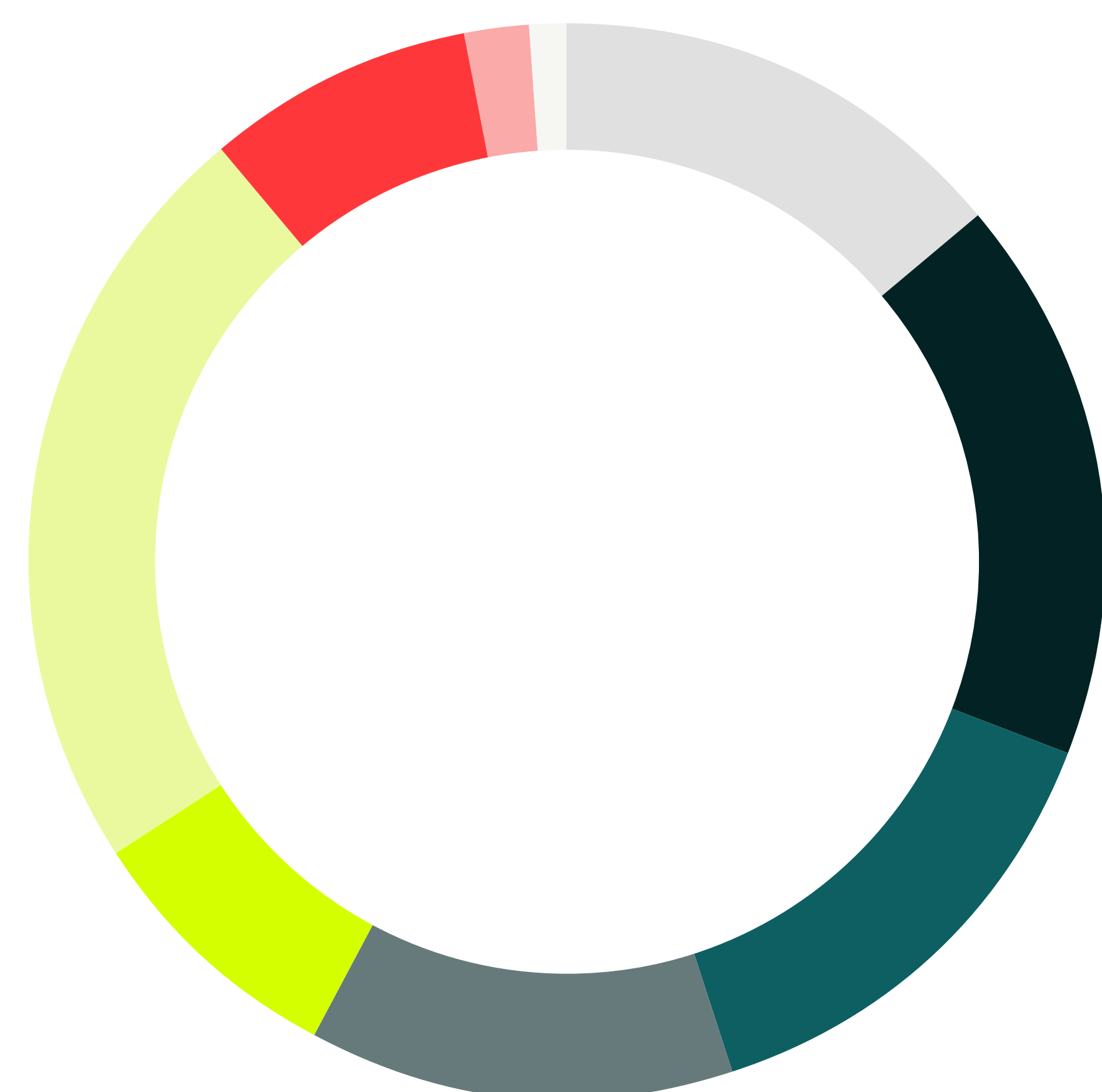
Programs with higher levels of maturity were significantly more likely to have a standardized definition of 'crisis' in place to ensure an appropriate response and management (**53%** compared to **6%** of immature programs). Additionally, mature programs were more likely to document all areas of executive risk acceptance and conduct annual reviews (**54%** compared to **13%** of immature programs).

Organizations with mature programs also demonstrated greater capability for real-time reporting to executive leadership on crisis-driven risks to critical processes (**60%** compared to **37%** of immature programs). Furthermore, they were more likely to have established corporate-level crisis management teams with clearly defined "primary" and "alternate" roles (**80%** compared to **30%** of immature programs), ensuring readiness and continuity during a crisis. These differences highlight the critical factors that contribute to higher levels of preparedness in mature programs.

Length of Program Existence (With or Without Your Involvement)



Program End-to-End Review or Refresh



14% **Currently Developing the Program**

17% **Currently Reviewing the Program**

14% **Updates are on an as Needed Basis**

13% **Less than 6 Months**

8% **6 - 12 Months**

23% **1 - 2 Years**

8% **2 - 4 Years**

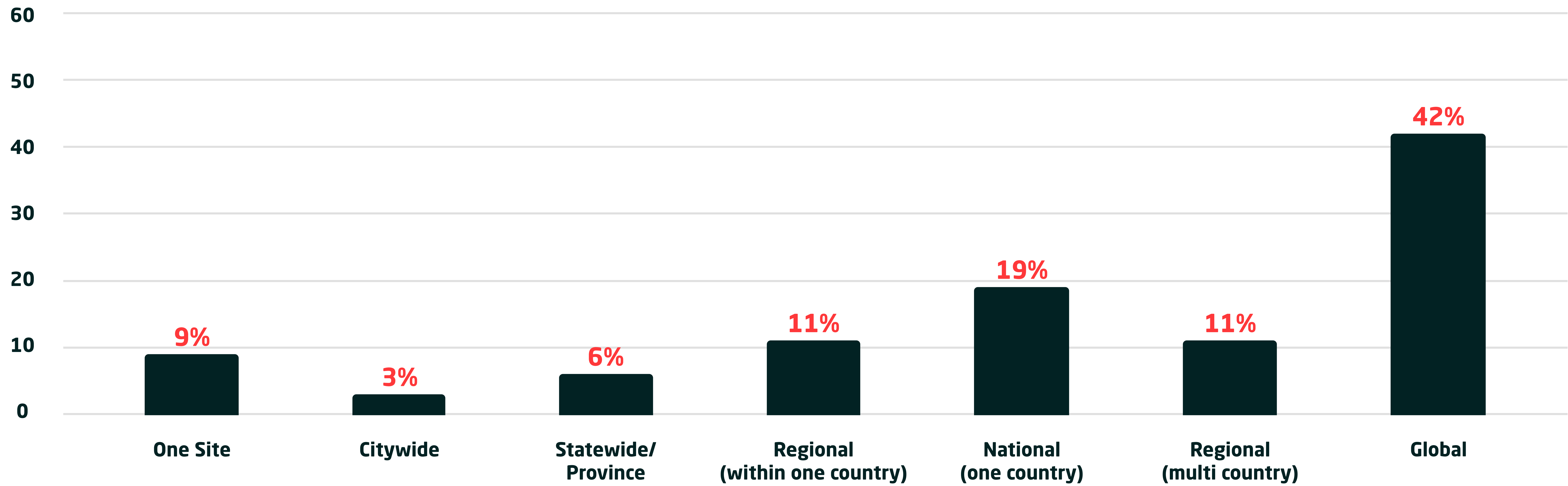
2% **4 - 8 Years**

1% **Over 8 Years**



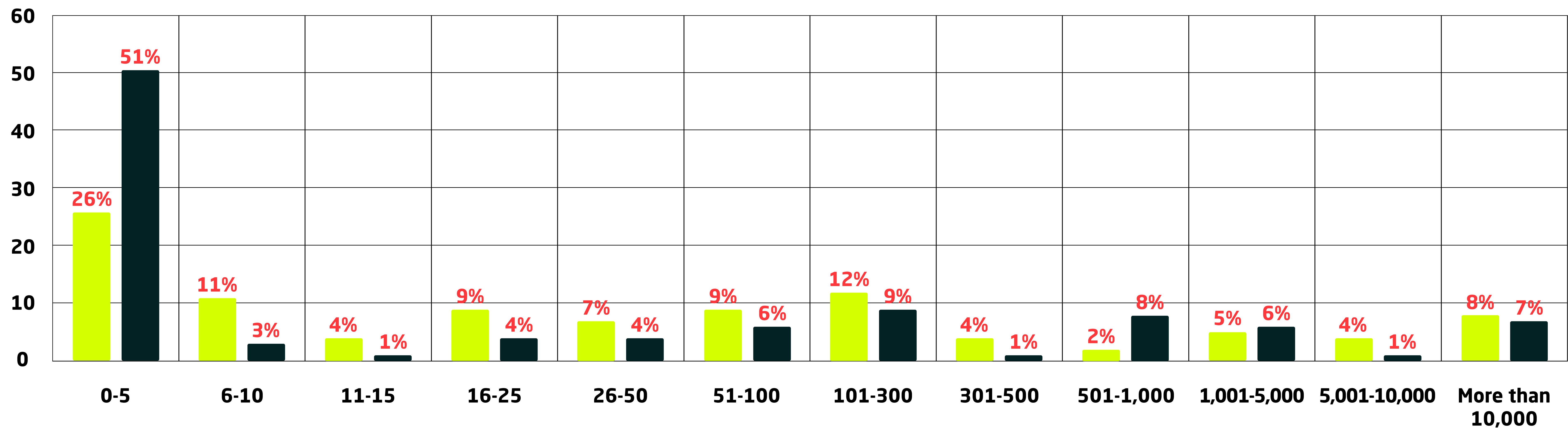
PARTICIPANT CHARACTERISTICS

Organizational Distribution



Number of Organizational Locations

■ Corporate/Operational Functions (Operational, Financial, Manufacturing Distributions)
 ■ Retail/Customer Interfacing (Outlets, Call Centers, Stores)



Industry - Top Industry Responses



30%
Financial



19%
Technology



17%
Insurance



9%
Consulting Services



6%
Government



6%
Utilities



5%
Healthcare/Medical

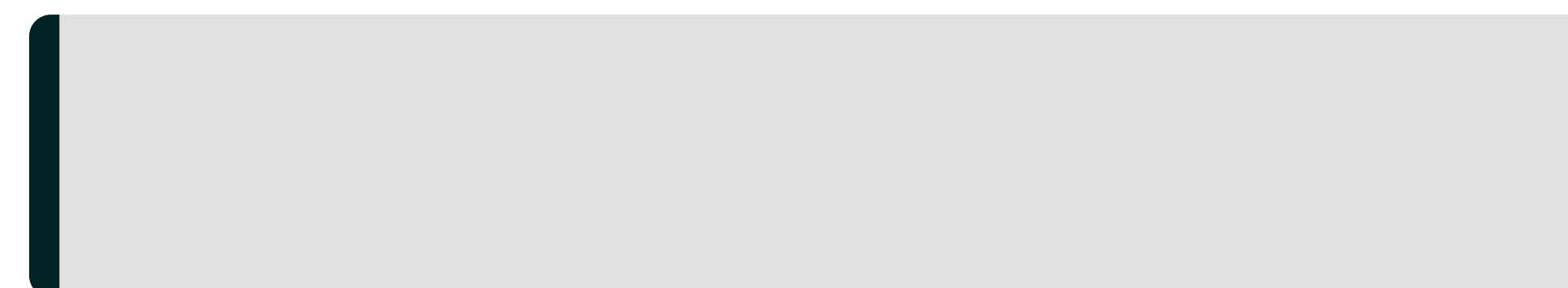
Organizational Classification

Sum exceeds 100% due to multiple selections.

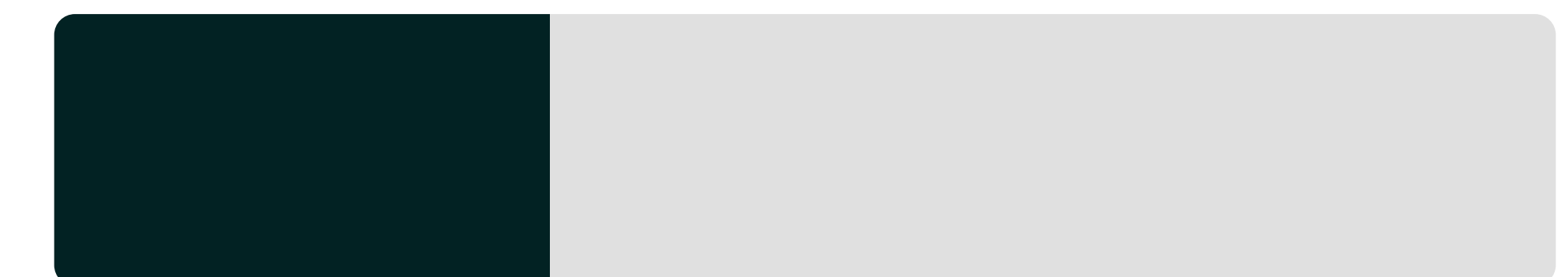
53% Publicly traded



2% Public, but not listed



33% Private



23% Regulated



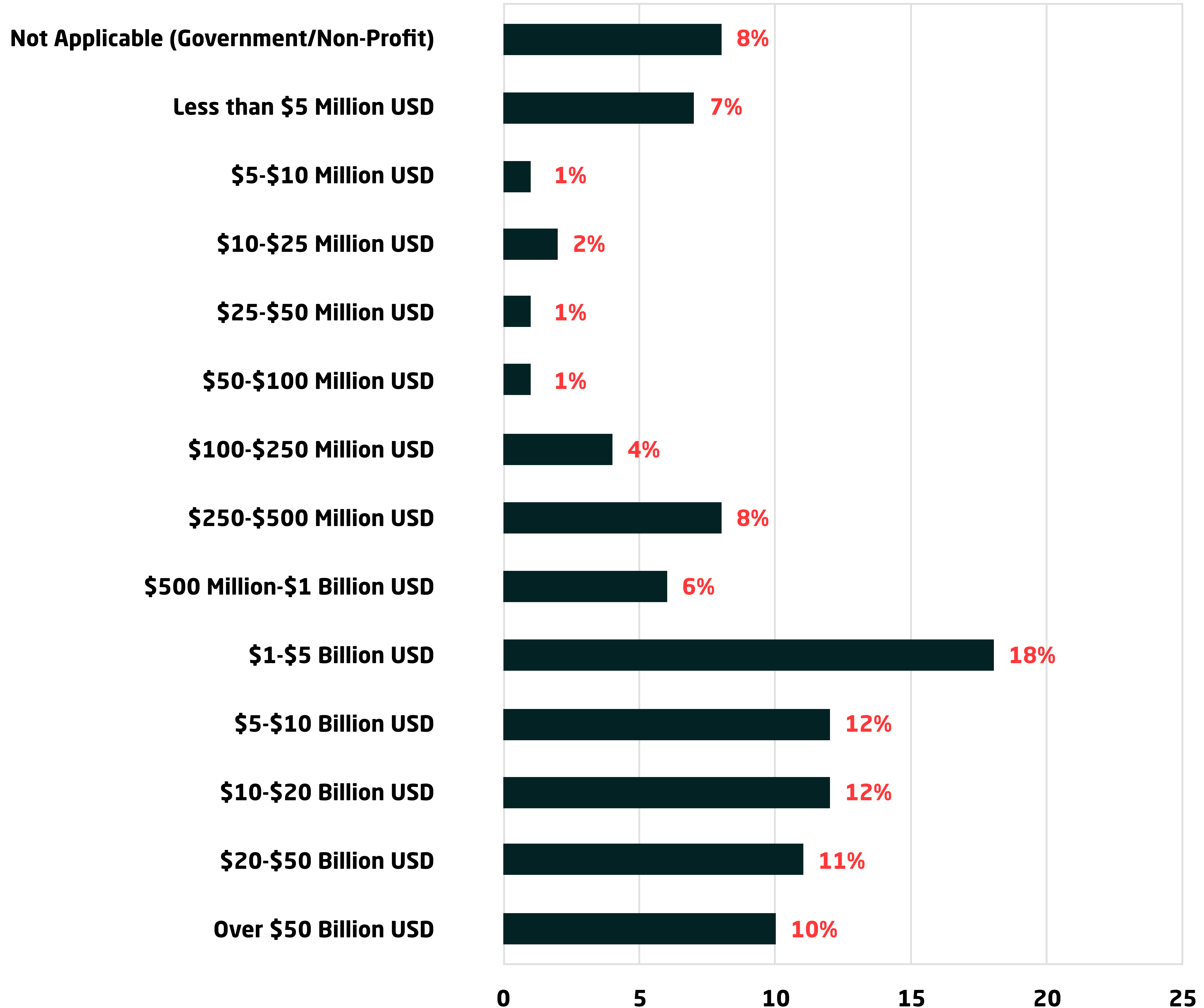
2% Unregulated



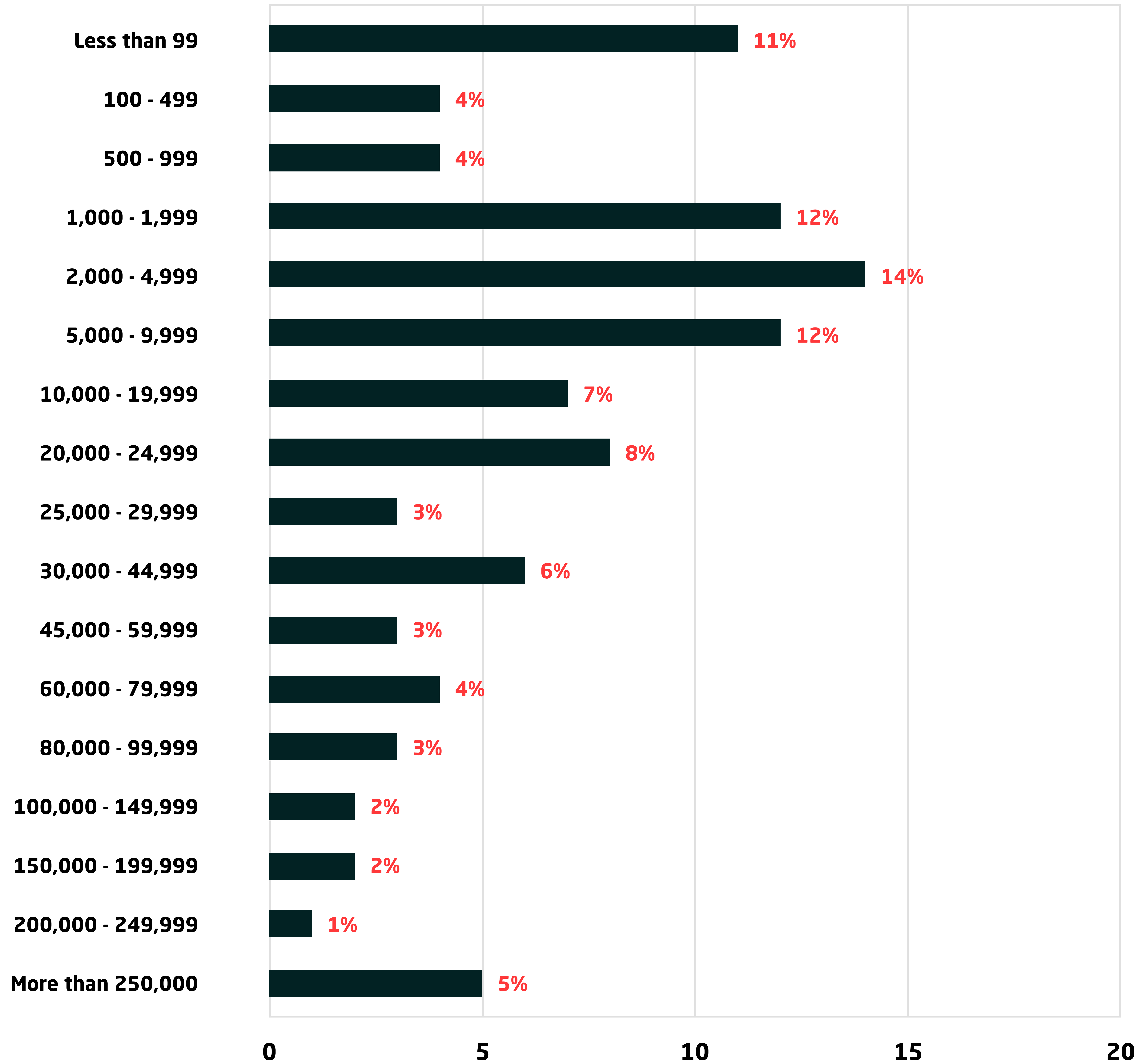
6% None of the above



Organizational Revenues (Annual Gross Revenues - USD)



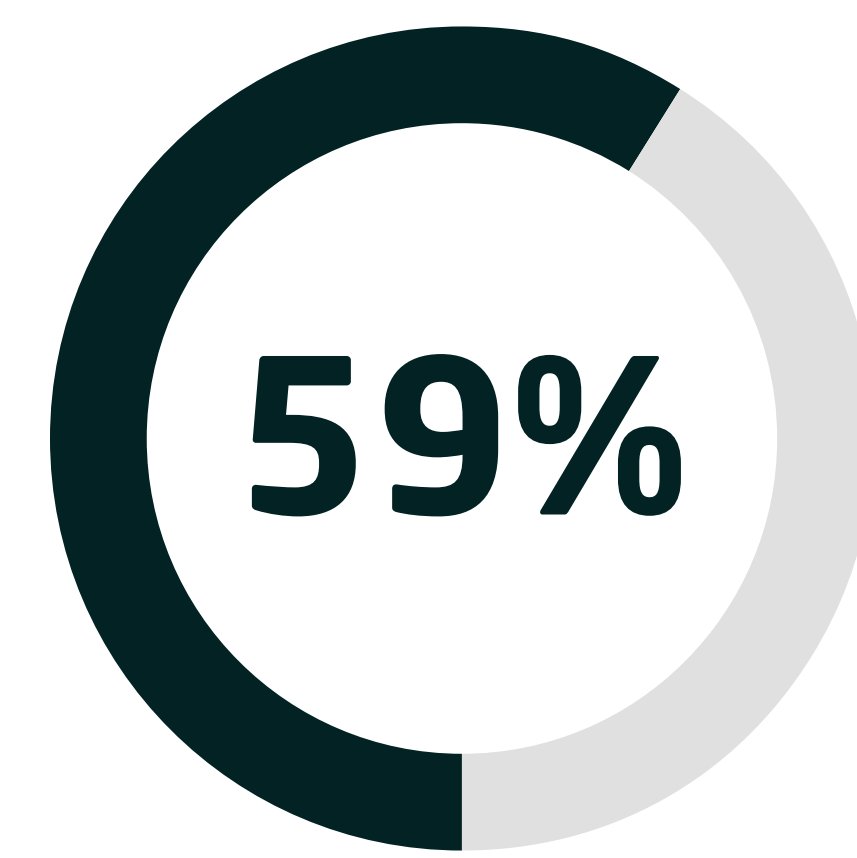
Number of Employees



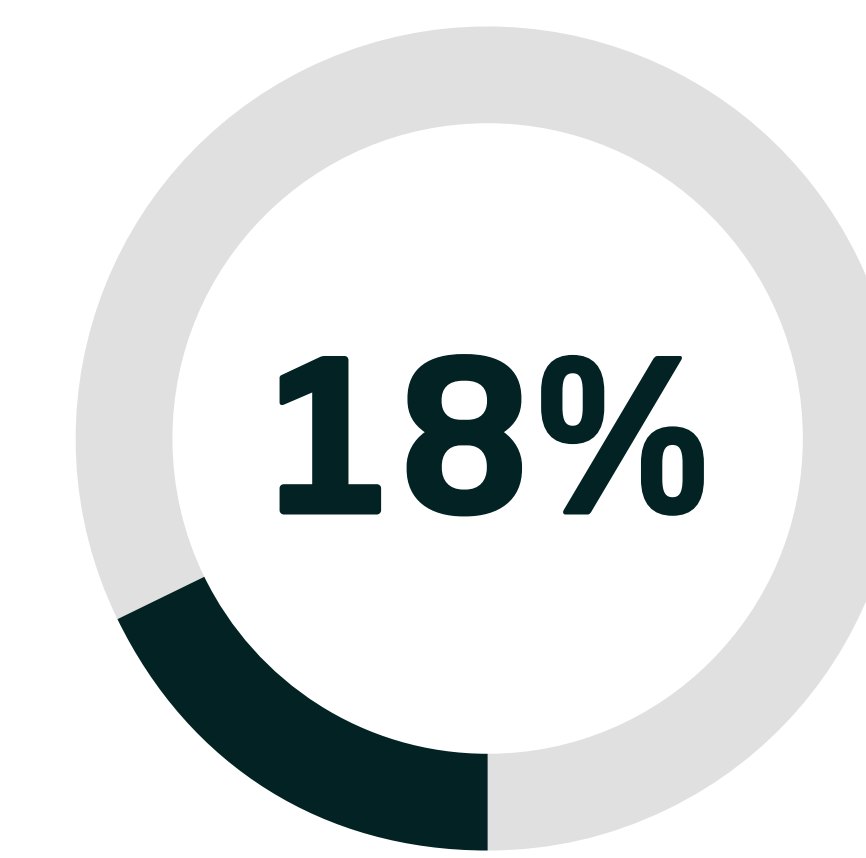
Current Role



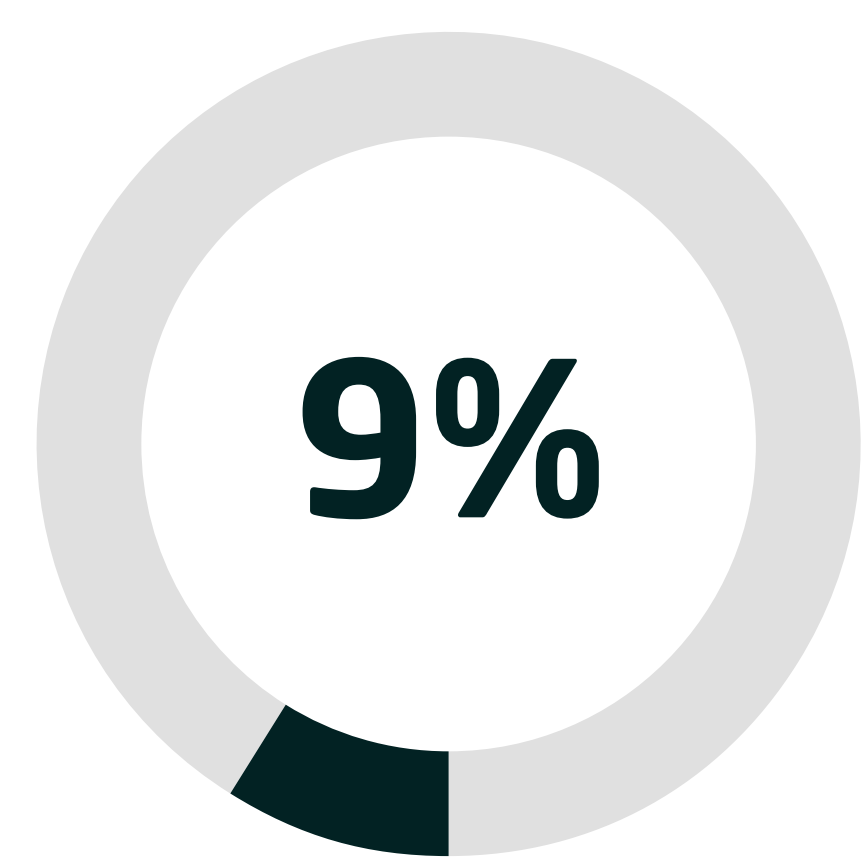
Executive Sponsor of the Program



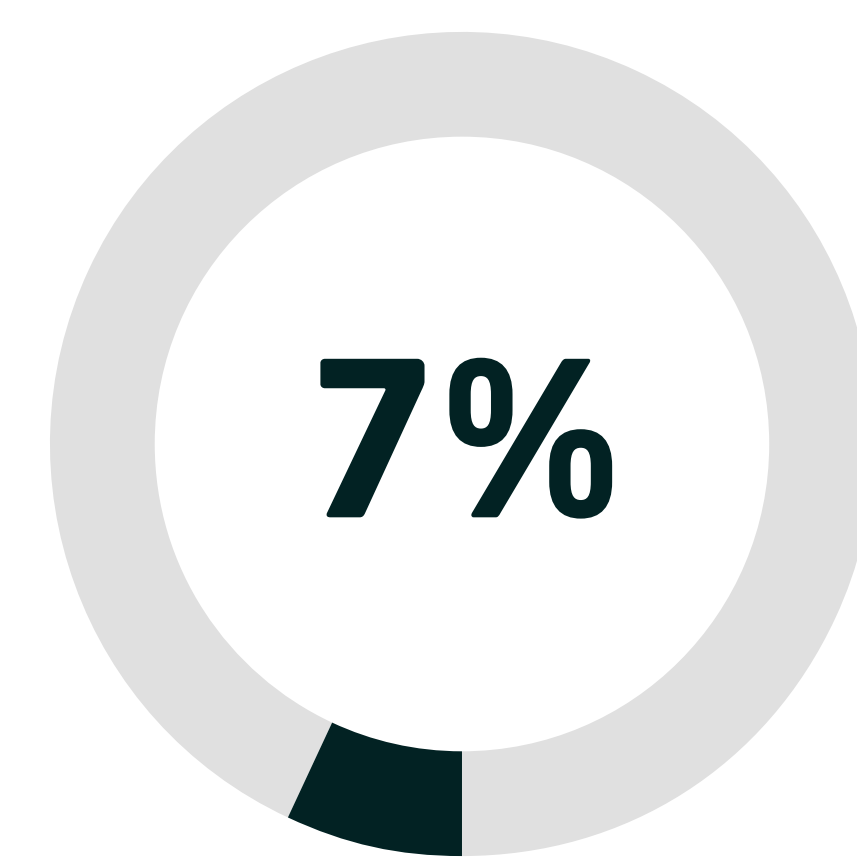
Leader or Manager with Accountability of a Program



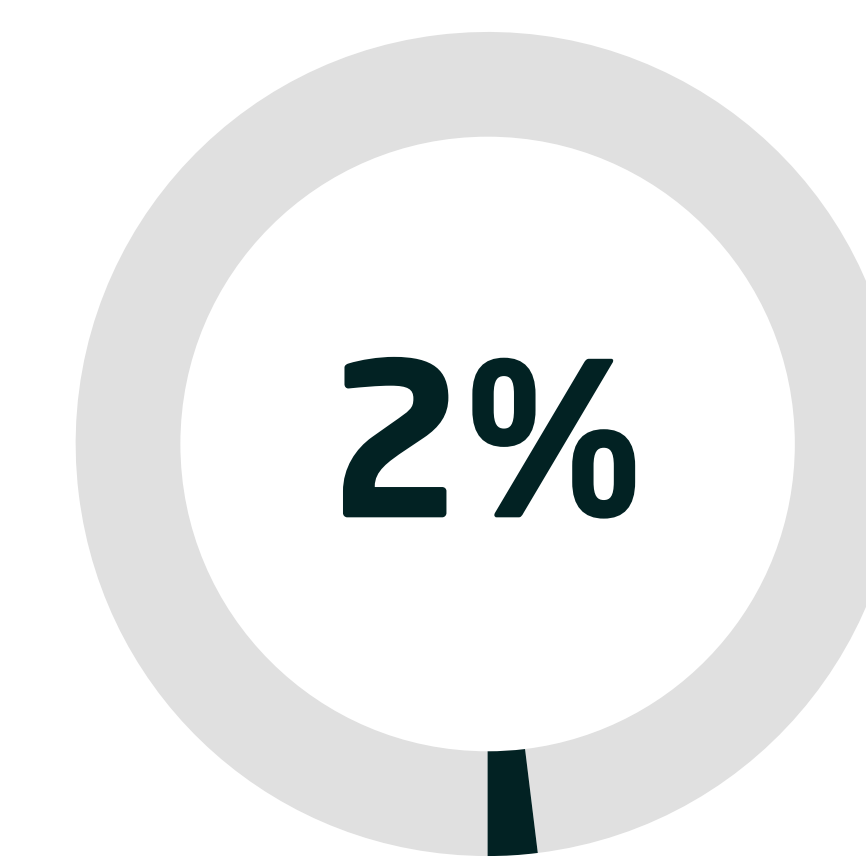
Subject Matter Expert Providing Input on Program



Member of Program Team



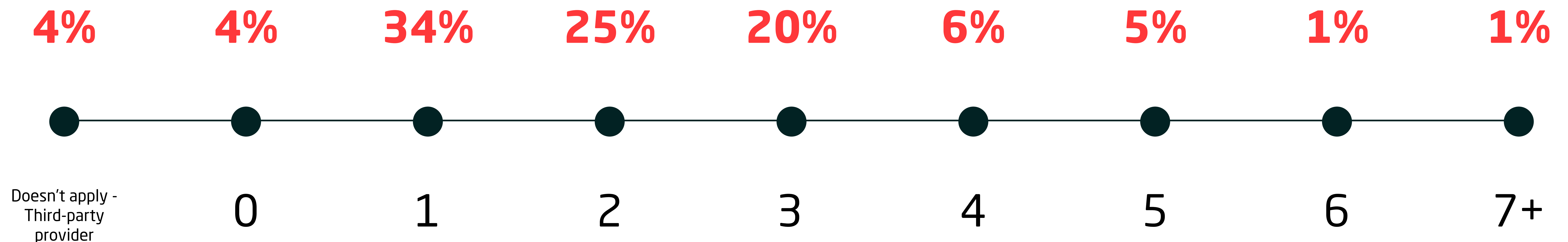
Third-Party Services Providing Advice on a Program



Other

Level of Separation from Executive Management

Number of people between you and the executive team.



A blurred background image of a business meeting. Several people in business attire are seated around a table, looking at documents and charts. The image is overlaid with a dark blue gradient and two bright yellow decorative shapes in the top-left and bottom-right corners.

BCM RESEARCH OVERVIEW

BCM Research Overview

Reporting History

Since 2001, BC Management has been gathering data on resilience management programs and compensations to provide professionals with the information they need to elevate their programs. Each year our organization strives to improve upon the study questions, distribution of the study, and the reporting of the data collected.

Study Methodology

The on-line study was developed by the BC Management team in conjunction with Witt O'Brien's and the BC Management International Benchmarking Advisory Board. WorldAPP Key Survey, an independent company from BC Management, maintains the study and assesses the data collected. The study was launched on May 30, 2024, and it will remain open through February 28, 2025. Participants were notified of the study primarily through e-newsletters and notifications from BC Management, Witt O'Brien's, and from many other industry organizations. All participants are given the option of keeping their identity confidential.

Assessment of Data & Reporting

BC Management is continuously reviewing and verifying the data points received in the study. Data points in question are confirmed by contacting the respondent that completed that study. If the respondent did not include their contact information, then their response to the study may be removed. Data findings in many of the figures were rounded to whole numbers, thus the total percent may not equal 100%.

Participant Overview

148

professionals participated in our 11th Edition Crisis Management Study.

Responses were received from

14

countries between May 30, 2024 to September 4, 2024. Incomplete/partial study responses were included as appropriate within the report.

Responses were received from the following countries. The most significant responses are bolded and associated with a response. *Belgium, Brazil, **Canada (6%)**, Dominican Republic, Germany, **India (4%)**, Ireland, Japan, Malta, Mexico, Philippines, Singapore, **United Kingdom (3%)**, and **United States of America (76%)**.*



**INTERNATIONAL
RESEARCH
ADVISORY BOARD**

International Research Advisory Board

Thank you to BC Management's International Research Advisory Board

BC Management's International Research Advisory Board was instrumental in reviewing the study to ensure it focused on the topics that are of the greatest interest to resilience management professionals today. The goal was to develop a credible reporting tool that would add value to organizational resiliency.

Larry Chase

CBCP, CCRP Comp TIA A+ (USA) - Senior Vice President of Operational Risk Management for Enterprise Resilience, CitiGroup

Larry is the Director of Operational Resiliency Oversight in Citigroup's Operational Risk Management organization. An eight year United States Air Force veteran, Larry is a recognized and an industry leader in Enterprise Risk and Resiliency Management over the course of three decades. Credited with establishing global programs at Pfizer, Motorola, and most recently with Humana — His professional accomplishments include the 2017 BCI Continuity & Resiliency Team of the Year, 2015 DRI Program Leader of the Year, 2010 BCI Asia Group Excellence Award and the 2005 W.E Upjohn Award for Leadership. He spends a good portion of his free time as a professional musician around the Tampa Bay area and serving in different industry leadership roles; he is also credited as the co-founding of DRI Foundation's Veterans Outreach Program, providing scholarships to 700+ of our returning heroes.

Jennie Clinton

MBCP, MBCI (USA) - Sr. Director, Enterprise Resilience & Crisis Management, Microsoft

Jennie Clinton is the Sr. Director of Enterprise Resilience and Crisis Management program which enables Microsoft to anticipate, manage, and respond effectively to resilience risks, and crisis events.

Jennie has over two decades of experience in the business of risk management, business continuity and crisis management. She is uniquely qualified in her field not only due to her diverse Fortune 500 experiences, but from her hands-on involvement in managing teams during the crisis. She has successfully managed response efforts for COVID-19, geo-political conflicts such as the War in Ukraine, major product recall, power outages, hurricanes, floods, and terrorist attacks across North America. Her expansive theoretical and experiential perspectives allow her to be masterfully adept at preparing organizations for the unforeseen.

Kevin M. Cunningham

MS, CEM, CBCP (USA) - Director, Business Continuity Program Office, Equinix Inc.

Kevin is currently the Director of the Business Continuity Program Officer at Equinix Inc. Previously, he had spent 4 years as Vice President and Head of Global Business Continuity, Crisis Management and Emergency Services at NBCUniversal. Until May of 2013, he was Americas Regional Head of Business Continuity, Crisis Management for UBS AG. Prior to his tenure at UBS, Mr. Cunningham worked for the City of New York as a Preparedness Specialist for the New York City Office of Emergency Management.

Ing. Jorge Escalera

MBA, RM-31000, MBCP, CCRP, LA 22301 (Mexico) Director, RISK MEXICO, SA DE CV.

Jorge Escalera Alcazar is President of the Organization Resilience Institute (IRO), Practice leader of Enterprise Risk Management, Business Continuity Management Systems, IT Disaster Recovery, Risk Management, and Insurance. More than 25 years of experience. Consultant for private sector multinational corporations and public-sector institutions. Chemical Administrator Engineer from Tec de Monterrey. MBA from EGADE Business School. Master Business Continuity Professional (MBCP) and Instructor by Disaster Recovery Institute International. Certified Risk Management Professional and Trainer (RM-31000) by IRO. Former President of the Mexican Technical Committee ISO/TC262 Risk Management. Coordinator in Mexico of WG2 Business Continuity of ISO/TC292 Security and Resiliency. Convenor of the Spanish Translation Task Force of ISO TC262/STTF - Risk Management. First President and founder of the RIMS Mexico Chapter.

International Research Advisory Board

Robert Fucito

(USA) - Vice President, Enterprise Resiliency,
Security and Crisis Management, Leading Mortgage
Lender

Experienced executive with a demonstrated history of working in the financial services industry. Skilled in Crisis Management, Enterprise Risk Management, IT Service Management, and IT Strategy. Strong professional with a Certificate focused in Design Thinking & Problem Solving from Massachusetts Institute of Technology - Sloan School of Management.

Guy Gryspeerdt

AMBCI (USA) - Vice President, Global Head of
Business Resilience,
Honeywell

Guy Gryspeerdt BA (Hons), AMBCI, has a strong experience in aligning the risk, business resilience and crisis management functions to the organization's strategic business goals and managing both the change process and subsequent organizational systems. He is outcome focused and sees a robust resilience program as a key business enabler to deliver a competitive advantage to the organization and value to customers. He has worked internationally across industry sectors, managing risk, business resilience, crisis management and security in the financial, retail, manufacturing and government sectors and has managed high level projects in these areas for leading organizations globally. Organizations have included Ernst & Young, Goldman Sachs, Reinsurance Group of America, The Westfield Group and Bridgewater.

Gayle Hedgecock

(UK) - Business Continuity & Resilience Specialist,
Clifford Chance

Gayle has over 20 years of Business Continuity experience in Financial services and less than 6 months in legal services, covering the full continuity lifecycle from completing BIA's through to creating and implementing BC policies and everything in between. Gayle was the chair of the BCI London Forum for 4 years.

Evan Hicks

CBCP (USA)

Evan began his Business Continuity career in Blacksburg, VA implementing Emergency Notification Systems across the United States for local government agencies. Motivated by the events of the 2007 Virginia Tech shooting, Evan moved to New York City to pursue a Master's Degree in Emergency Management from John Jay College of Criminal Justice. While completing his graduate studies, Evan held positions at Goldman Sachs' Crisis Management Center and NYC OEM's Training & Exercise division. This unique experience in both the public and private sector, led him to Washington, DC where he held multiple roles across Fannie Mae's Corporate Incident Management Team, Business Continuity Office, Risk and Controls, and Credit Portfolio Disaster Relief Team. In 2016, Evan pursued an opportunity in Portland, OR to establish a Business Recovery program for Nike's world headquarters and global business operations. During his tenure with Nike, Evan elevated Business Continuity to the Board of Directors, authored the COVID-19 Return to Work Playbook, and implemented a global continuity planning process inclusive of incident management, third party risk, technology recovery, facility management, enterprise risk management, supply chain, HR and other enterprise partners. Today, Evan is applying his crisis management expertise to his community in Portland where he's helping local charities address and resolve the social vulnerabilities revealed by COVID-19 and the BLM movement.

Alberto Jimenez

PMP, CBCP (USA) - Director, MiaTomi

Alberto is a founder and director with MiaTomi, a provider of business continuity management consulting services. Alberto has over 20 years of cross-industry experience, helping clients meet their business continuity, risk, compliance, and IT transformation needs. Prior to founding MiaTomi, Alberto was a national practice director at Datalink, Senior Manager at SunGard, Associate Director at Protiviti, and technology manager at Accenture.

International Research Advisory Board

Sohail Khimani

MBA, MBCP, AFBCI, OSSNHS, ISO 22301 LA (UAE)
- Business Continuity Relationship Head,
Confidential

An award-winning risk and resilience luminary with over 16 years of experience in all facets of risk and resilience. He is considered as an expert in providing and implementing bespoke end-to-end risk solutions and is a qualified and well-versed risk and resilience thought leader assisting organizations survive and thrive in challenging times.

Nicola Lawrence

BCom, MBCI (UK) - Business Resilience Manager,
Marex

Nicola Lawrence a business continuity professional that has worked in the Banking and Finance industry for 18 years, involved all aspects of resilience from planning and implementing BCM program to developing training and awareness opportunities. She is an active member of both The Investing and Saving Alliance (TISA) and Investment Association (IA) Operational Resilience Working Groups with the purpose of developing guidance for its member firms and supporting them through transition phase of the Operational Resilience regulatory changes in the UK.

Jayaraj Puthanveedu

CISSP, MBCI, ISO Lead Auditor (UK) - Managing
Director - Cyber & Technology RISK & Global head
of Operational Resilience & Third Party Tech Risk,
BNP Paribas

Jayaraj is a Senior Executive with over 21 years of experience in Cyber Security, Risk Management and Resilience, primarily focused on helping board level and CXO stakeholders in Tier1 Financial Services institutions in shaping their digital strategy to improve their Cyber Security and Resilience posture. In his current role as the Managing Director in BNP Paribas, he is the Global Head for Cyber Fraud, Cyber Resilience, Third Party Tech Risk, Data Breach Management, Business Continuity, IT Resilience and overall Operational Resilience. Prior to this, he has held various leadership roles in Deutsche Bank, Goldman Sachs, Northern Trust etc. covering Operational Risk, Cyber & Technology Risk and Resilience areas.

Malcom B. Reid

FBCI, CBCP, CPP, CFE (USA) - Director, Global
Security Operations Center, Confidential Company

Malcolm is a globally recognized, risk and resiliency thought leader. Among his many accomplishments includes the national critical infrastructure assessment of one of the top Liquefied Natural Gas (LNG) exporting nations. He has also led enterprise business continuity, security and risk advisory engagements for large global organizations. Malcolm is a graduate of the United States Military Academy at West Point and holds Masters degrees from Norwich University, Webster University and the University of Reading. He is a Fellow of the Business Continuity Institute and is Board Certified in Security Management. Malcolm is a member of a number of industry and community based boards including that of the BCI-USA chapter and the 2020 global board of ASIS International.

Wong Tew Kiat

CBCP, Fellow of BCI, CITBCM(S), CITPM(S),
COMIT(S), Fellow of Singapore Computer Society
(Singapore) - Managing Director & Founder,
Organisation Resilience Management Pte Ltd

More than 30 years of experience in IT Infra, Data Centre Infrastructure & Operations, Business Continuity Management, Pandemic Preparedness, Crisis & Incident Response, IT Disaster Recovery, Emergency Management and Data Centre (DC) Risk & Health Check. Managed a 100,000sqft Data Centre for the 30 years. Currently appointed as Chairman for the Data Centre Special Interest Group (DC SIG) by Singapore Computer Society (SCS) as a national platform for DC professionals to network and sharing of research & innovative ideas to meet the changing trends of the DC landscapes. A CBCP by DRII(USA) since 1997 and Fellow of BCI-UK since 2005. Also a Certified IT Project Manager, Certified Outsourcing IT Manager and Certified ITBCM Manager (CITBCM) by SCS. He was the President for the Business Continuity Group, a chapter in SCS from 2005-2008 & 2010-2011. In addition, he chaired the CITBCM Resource Panel to develop the Body of Knowledge and also chairs the Board of Assessors and he is also the authorised training provider for this CITBCM Certification Course.

International Research Advisory Board

Gilberto Tiburcio Freire Junior

(Brazil) - Global Workplace Recovery Sales Director,
LATAM, IWG

More than 45 years of experience with solid business knowledge in Sales of IT Services, with experience in IBM Brazil, IBM United Kingdom and REGUS. More than 20 years working as People Manager leading Services Organization (Infrastructure Services, Business Resilience Services, Business Continuity, Disaster Recovery, IT Security). He was responsible to implement a Business Recovery Organization in a IBM Brazil, afterwards he was responsible for this Business in all Latin America for more than 10 years. He is currently responsible in REGUS (IWG Parental company) for Workplace Recovery services in Latin America since 2016.

Sanjiv Tripathy

(India) - Managing Director and Risk & Security
Leader, Confidential Financial Firm

Sanjiv is a senior Risk leader and has managed Resilience & BCM for a global banks India set up (RBS Technology) comprising of ~15000 headcount size distributed over multiple locations working with Senior management / Silver & Gold global Incident management teams, partnering with businesses such as Banking business, Operations, Financial services and Risk services for India wide organisation (~25000 team size). Conceptualized & implemented fit for purpose Business Resilience, BC and Disaster Recovery strategies, reviewed them and implemented improvements as part of major incident review and Regulatory review. Fostered strong stakeholder relationships, developed specialised team, managed Resilience & BC critical processes, reviewed BCM program framework and standards, assessed large global critical 3rd party service providers BCM capabilities, assessed organizations effectiveness of BC/ Resiliency and presented BCM preparedness to Internal audit, External auditor and Regulators.

Thomas Wagner

(USA) - Managing Director, Major Trade Association

Tom is a recognized expert and innovative thought leader in the Business Continuity Management space with over 25 years' experience as a practitioner, management consultant and technology executive in the financial services industry. Tom is currently the Managing Director for a major trade association and he previously served in senior BCM roles at HSBC, Marsh, Gartner, Booz Allen and the NYSE. While at Booz Allen, Tom consulted to the President's Commission for Critical Infrastructure Protection (PCCIP), the White House Critical Infrastructure Assurance Office (CIAO / Homeland Security) and Intelligence Communities where he conducted risk assessments and helped develop strategies to protect the financial services industry from terrorism and natural disasters. Tom is also a recognized thought-leader in the IT Controls and Risk Management space having served as a SME with ISACA ITGI for the on-going development of CobiT and the IT Risk and Governance frameworks.

Kiyoshi Yoshikawa

(Japan) - Sr. Manager - Confidential Company

Mr. Yoshikawa has been a BCM professional for over 15 years in the financial and manufacturing industries. He started his career as an IT network engineer and build backup data centers and sites. He brings a sound knowledge of the financial regulations of the APAC countries and understands the residual risks in the production lines and supply chain.

A photograph of two business professionals shaking hands, overlaid with a dark blue semi-transparent filter. The image is framed by bright yellow curved shapes in the top-left and bottom-right corners. The text 'DISTRIBUTING ORGANIZATIONS' is centered in white, bold, uppercase letters.

DISTRIBUTING ORGANIZATIONS

Distributing Organizations

Thank You Distributing Organizations

BC Management also greatly appreciates the efforts of those organizations that assisted in this global effort. Below is a list of participating organizations that assisted in distributing our annual study. The contribution of each individual organization does not indicate an endorsement of the study findings or the activities of BC Management. This is NOT a complete list of distributing organizations.





ABOUT WITT O'BRIEN'S

About Witt O'Brien's

1/3 of the Fortune **100** have entrusted Witt O'Brien's to assist with their resiliency programs. Our team is here to support you every step of the way to develop and implement an integrated program to make your organization more resilient.

We serve as strategic consultants to create detailed plans, and training in Crisis Management, Business Continuity, and Crisis Communications. Our experienced team is innovative, flexible, and experienced. We are here for you to design and implement customized programs that work.

WITH YOU WHEN IT COUNTS

info@wittobriens.com

T: +1 281 320 9796

F: +1 281 320 9700

Contact Us

WITT O'BRIEN'S

ambipar[®]
response

A group of business professionals are seated around a conference table in a modern office setting. The image is overlaid with a semi-transparent blue filter. Two large, bright yellow decorative shapes are positioned in the top-left and bottom-right corners. The text 'ABOUT BC MANAGEMENT' is centered in white, bold, uppercase letters.

ABOUT BC MANAGEMENT

About BC Management

BC Management (powered by Witt O'Brien's), founded in 2000, is a **staffing** and **research** firm solely dedicated to the resilience management, business continuity, disaster recovery, risk management, emergency management, crisis management, and security professions. With decades of industry expertise, our staff has a unique understanding of the challenges professionals face with hiring, benchmarking, and analyzing best practices within these niche fields.

WHY BC MANAGEMENT?



We're "In" Resilience Management!

We have 25+ years of dedicated experience. We understand the language and can identify the skills needed to be successful.



The Hidden 60,000

We have the largest network of passive resilience management candidates in the world! Many won't be found actively looking for a job or on LinkedIn.



We're Fast

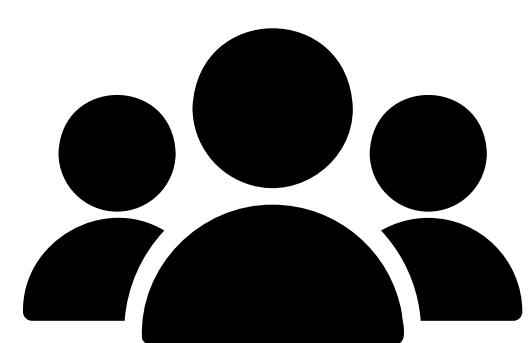
We have a proven process that gets results quickly. We also communicate frequently so you always know the status of your search.



Global Reach

From Detroit to Delhi - We have worked in dozens of countries.

OUR SERVICES



Global Staffing Services

Direct-Hire, Staff Augmentation, Contract-to-Hire, & Contractor-on-Demand



Complimentary & Customized Data Research

Crisis Management, Program Assessments, Trends, & Compensation



 BC Management

BC Management
CONTACT US

 info@bcmanagement.com