



10TH EVENT IMPACT MANAGEMENT REPORT

WITT O'BRIEN'S

2023 EDITION

ambipar 
response

CONTENTS

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

DISCLAIMER

The data included in this report was provided directly by participants to BC Management's 10th Edition Event Impact 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 on the employees as well as estimated financial losses. In addition, there is an assessment on how organizations prepare for different events and use lessons learned to advance resilience management strategies. An overview of the data findings along with a correlation to program maturity highlights several differentiating factors to obtain operational resiliency. The data highlighted throughout this report was gathered in BC Management's 10th Edition Event Impact Management Study between December 8, 2022 through February 21, 2023.

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 [BCM Event 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 August 30, 2023 via our [online study](#). Our dashboards highlight a tremendous amount of data points that are not included within this complimentary report.

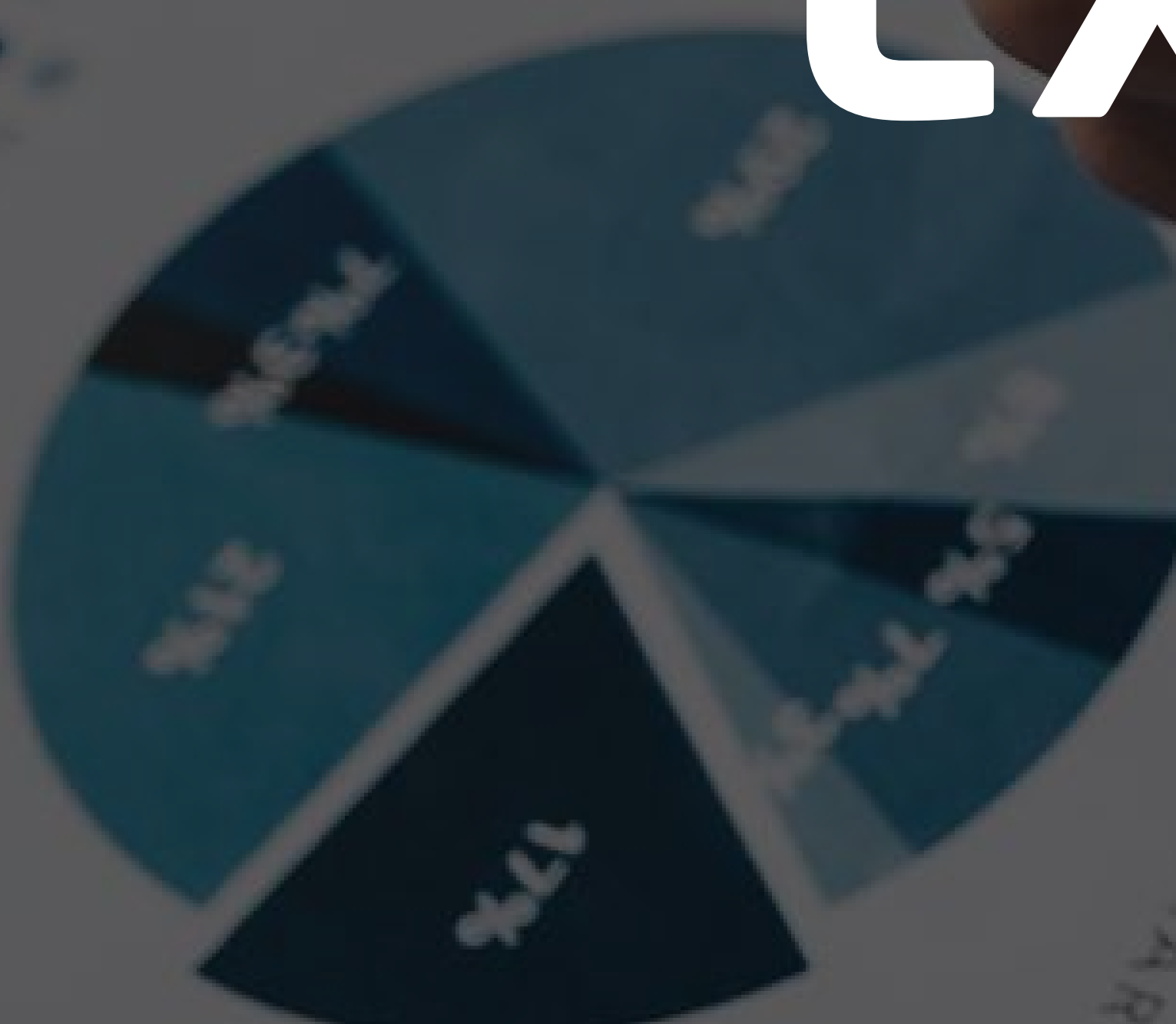
Like our research analytics?

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 find this information useful.

WITT O'BRIEN'S

ambipar[®]
response

EXECUTIVE SUMMARY



No.	Payment Date	Payment Due
0	1/1/2013	
1	1/2/2013	
2	1/3/2013	
3	1/4/2013	
4	1/5/2013	
5	1/6/2013	
6	1/7/2013	
7	1/8/2013	
8	1/9/2013	
9	1/10/2013	
10	1/11/2013	
11	1/12/2013	
12	1/13/2013	
13	1/14/2013	
14	1/15/2013	
15	1/16/2013	
16	1/17/2013	
17	1/18/2013	
18	1/19/2013	
19	1/20/2013	
20	1/21/2013	

Company B	Company C
\$ 301,218	\$ 585,842
\$ 404,879	\$ 484,829
\$ 508,372	\$ 505,555
\$ 608,130	\$ 747,459
\$ 808,248	\$ 828,214

(Unit: million)

BUDGET VS. ACTUAL

Enter your budget for each category in the Summary By Category table. The actual spending compares to your budget.

Top Trends

PRE-EVENT PLANNING

67% of organizations indicated they are either "extremely prepared" or "prepared" for events, but under half (**48%**) noted that they have prevented a disruption in the past based on their preparedness efforts.

TOP EVENTS & CRISIS 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 5 crisis impact ratings from the top 10 events in 2022.

- Pandemic/Disease (**65**)
- Cyber Attack (**54**)
- Supply Chain Disruption (**51**)
- War or Insurrection (**46**)
- Network/Communication Outage (**44**)

Executive Summary

The Event Impact Management Report is designed to provide a summary of the wealth of data collected from our 10th edition of this study assessment. This report highlights how different crises impact organizations from organizational losses, downtime, impact on the employees as well as financial losses. We've also included an assessment on how organizations prepare for crisis management and use lessons learned to advance their resilience management strategies. Before you get into the details and insights highlighted throughout this report, here are some key findings we wanted to share with you.

Gaps in Pre-Planning - Being prepared is key and while **67%** of organizations indicated they were either "extremely prepared" or "prepared" for events, the data told a different story.

- Organizations are least prepared for a disgruntled employee (**37%**), supply chain disruption (**38%**), or workplace violence (**38%**), while only about half of organizations address supply chain disruption (**54%**) or workplace violence (**48%**) in the scope of their program.
- **33%** of all organizations use a standard definition of 'Crisis' to ensure the appropriate level of response and management. Additionally, only **24%** of all organizations document all areas of executive risk acceptance and perform annual reviews.
- Using a mobile phone was the top method (**86%**) to communicate throughout an event, but only **64%** noted that their plans are accessible in a mobile format.
- The top challenges noted for corporate-level crisis management teams are: 1) Agreement on the level of transparency in crisis communications, 2) clarity on when a crisis management team is notified and activated, and 3) inability to focus on the strategic 'what' to do versus devolving into the operational 'how' to do it.

Top Events & Crisis Impact Ratings - This year we took a different approach to assess not only the top recent events 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 this report, but here are the most notable insights.

- Fortunately, the effect from COVID-19 eased in 2022, but organizations continued to work through the lingering challenges. Pandemic/disease received the highest crisis impact rating (**10**) in each of the following categories: employee impact, geographical scope, critical systems impacted, and business resumption timeframe.
- Cyber attack received the 2nd highest crisis impact rating with a score of 8 in the following: full activation, least advanced warning, employee impact, critical systems impacted, and business resumption timeframe.
- Although supply chain crises were the 9th most common event to recently hit organizations, their impact definitely registered in the last year with a rating of 10 for frequency and estimated financial losses and a score of 9 for geographical scope.

Top Trends

IMMATURITY & POTENTIAL LOSS

13% of all organizations noted \$1M in financial losses for an individual event, while **17%** of all organizations with "immature" programs indicated the same.

FUTURE PROGRAM ENHANCEMENTS

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

- Cyber Response **69%**
- Integration with Risk Disciplines **67%**
- Program Metrics (Ability to Resonate & Drive Continual Improvements) **60%**

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

- Software Automation **50%**
- Technology to Improve Resilience **44%**
- Situational Awareness & Threat Intelligence **38%**



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

A Correlation Between Program Maturity & Potential Financial Loss - In assessing the respondents who noted \$5M+ in estimated losses for an individual event, we noticed a marked immaturity with less tenured programs.

- **14%** noted "very immature" (reactive - chaotic/ad hoc) programs compared to **8%** of all respondents indicating a \$5M+ in estimated financial losses for an individual event.
- A majority of programs have been in existence for less than 4 years: Pandemic Planning (**57%**), Business Continuity (**43%**), Crisis Management (**43%**), Disaster Recovery/IT Service Continuity (**43%**), and Supply Chain Resilience (**33%**).
- **57%** do not have plans accessible in a mobile format compared to **33%** of all respondents.

Cyber & Technology are a Top Focus for Program Enhancement Strategies but is it Enough? - It shouldn't come as a surprise that cyber and technology investments are top of mind. Cyber attack not only received the 2nd highest crisis impact rating score (behind pandemic/disease), but it is a very real threat that companies are grappling with in addition to keeping up with the ever-changing threats. Couple a potential cyber attack with archaic systems and applications that desperately need updating, and it becomes a scenario of not "if" but "when" something will happen.

Being truly "resilient"; however, involves a holistic approach. Organizations are balancing technology advancements in addition to elevating their organizational resilience management posture by integrating with other risk disciplines, driving program metrics, and increasing governance. But let's look behind the proverbial curtain. Resilience management encompasses seeking out every potential organizational vulnerability. The data also highlighted that a very small pool of respondents expects to improve the program response strategies for liquidity issues (**6%**) and credit issues (**4%**). Now one can quickly assume that this is likely under a financial risk officer, but at the same time respondents also noted that they were "prepared"/"extremely prepared" for a financial market disruption (**78%**). This leads us back to crisis management pre-planning and how vital every aspect is.

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 a [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 demographics but also its an opportunity to create a roadmap for your program based on effective peer-based models and supporting data.

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.



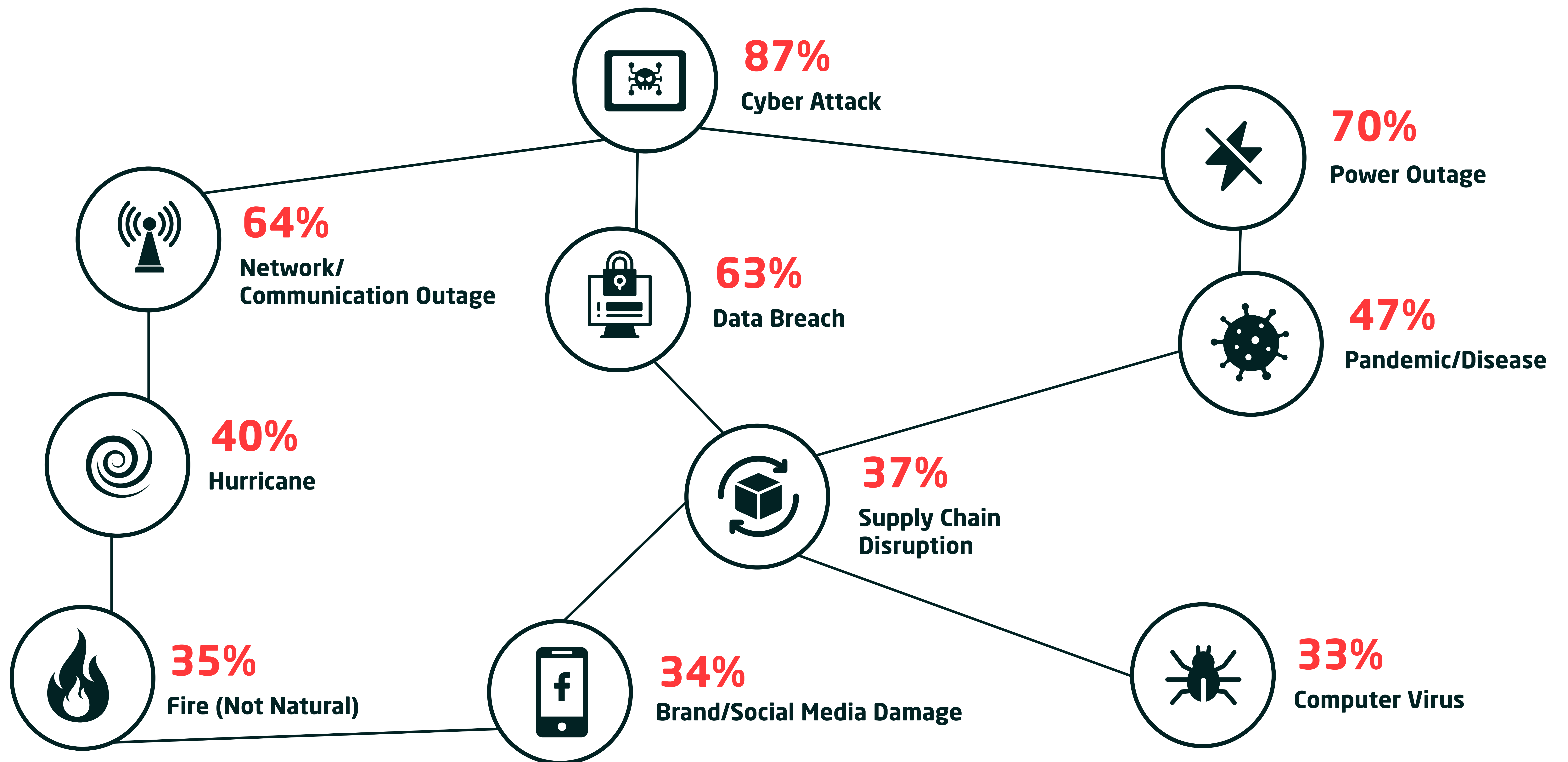
PRE-EVENT PLANNING

What Events are Organizations Most Concerned About?

Participants chose the top 5-10 events out of a list of 50+ different accidents, human/business, natural, and technical disasters. Sum exceeds 100% due to multiple selections.

Organizations are most concerned about **Human/Business Disasters (39%)**, **Technical Disasters (37%)**, followed by **Natural Disasters (24%)**, and **Accidents (19%)**.

TOP 10 Events Most Concerned About



TOP 5 Events Least Prepared For

Percent of respondents indicating prepared or extremely prepared.

37%

Disgruntled Employee

63%

Terrorist Activities

52% Prepared

Respondents indicated they were **15%** extremely prepared, **25%** neutral, **6%** unprepared, and **1%** extremely unprepared for events.

38%

Supply Chain Disruption

64%

Earthquake

38%

Workplace Violence

TOP 5 Events Most Prepared For

Percent of respondents indicating prepared or extremely prepared.

92%

Pandemic/Disease

80%

Power Outage

82%

Fire (Not Natural)

78%

Health/Safety Issue

81%

Hurricane

78%

Financial Market Disruption

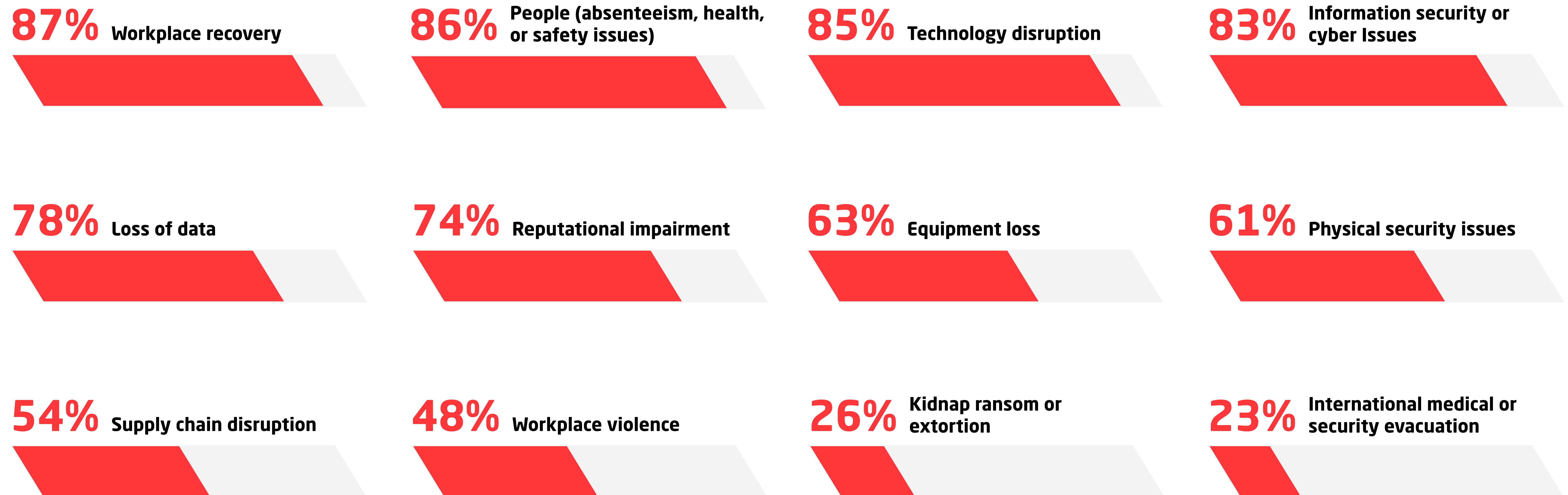
INSIGHTS

Although organizations indicated that they were most concerned about various technical crises as highlighted on the previous page (cyber attack, network/communication outage, and data breach), they seemed to be moderately prepared for them in comparison to several different human/business disasters (disgruntled employee, supply chain disruption, workplace violence, or terrorist activities) that topped the list of being least prepared for. Additionally, **78%** of organizations believe they are prepared for a financial market disruption but only **6%** and **4%** are improving liquidity and credit issues, respectively (as noted on page 29 within this report).

Supply chain disruption was the 7th potential crisis organizations were most concerned about while in previous years it never made the top 10 list. Shortly after the COVID pandemic hit though, supply chain disruptions were quickly showing gaps in resiliency programs and only **38%** of organizations believe they are prepared for such an event.

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

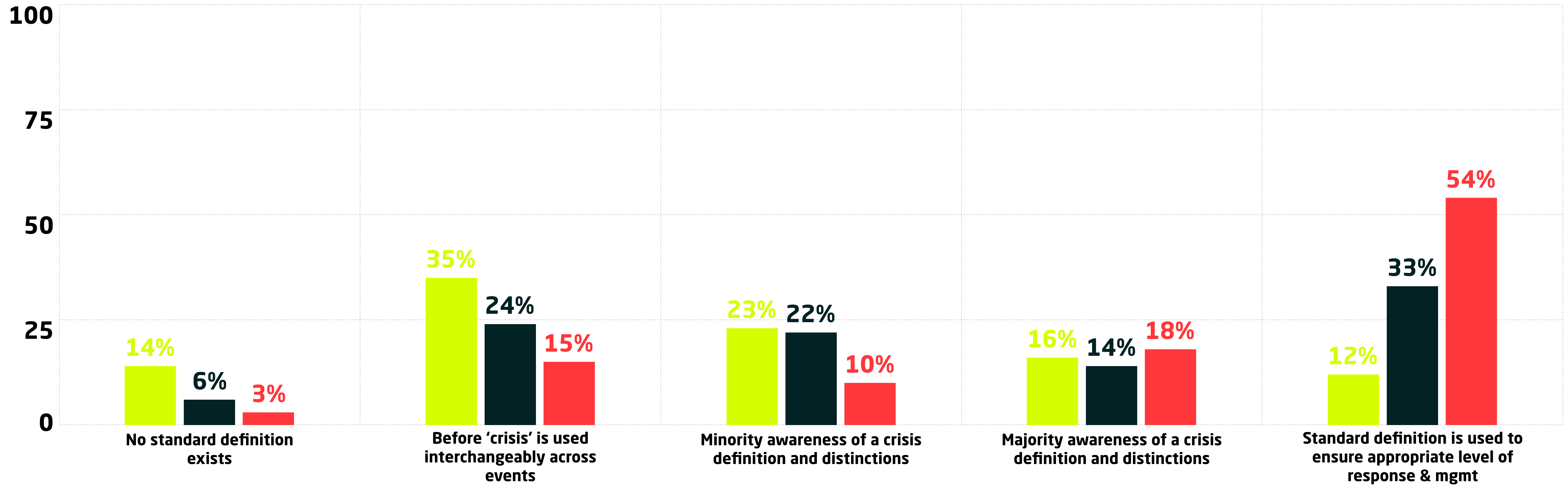
Sum exceeds 100% due to multiple selections.



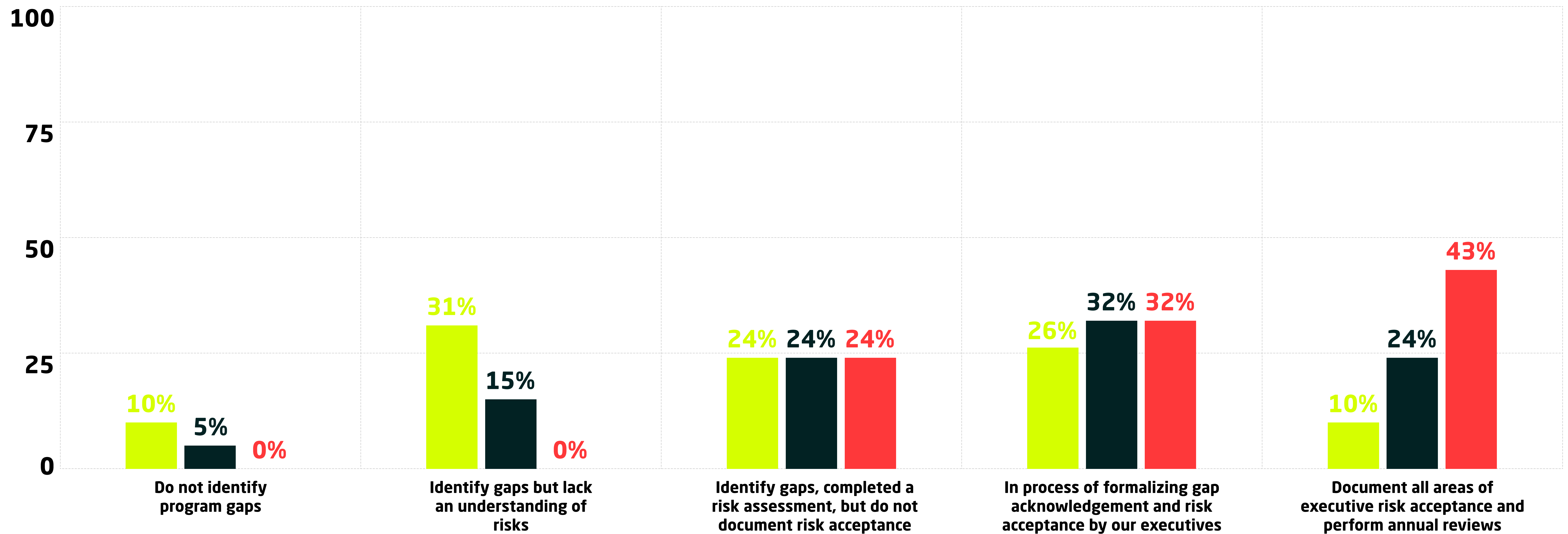
INSIGHTS

The data highlights that a majority of organizations address technology issues within their program (85% technology disruption, 83% information security or cyber issues, and 78% loss of data), while human/business disasters were less likely to be addressed within the program (54% supply chain disruption, 48% workplace violence, 26% kidnap ransom or extortion, and 23% international medical or security evacuation). This is certainly a gap when the previous page highlighted that organizations were least prepared for several human/business disasters with a few noting being prepared for a disgruntled employee (37%), workplace violence (38%), and a supply chain disruption (38%).

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



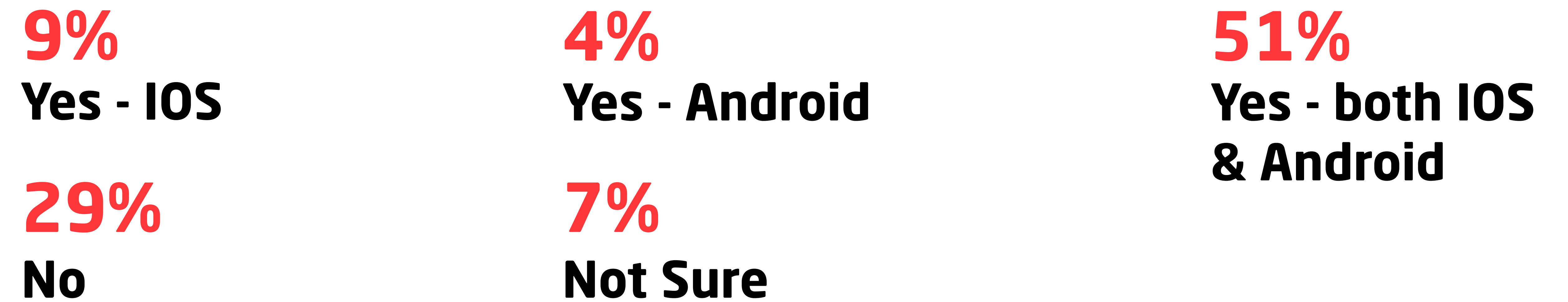
How do Organizations Rate their Appetite for Risk Acceptance and Acknowledgement of Program Gaps?



INSIGHTS

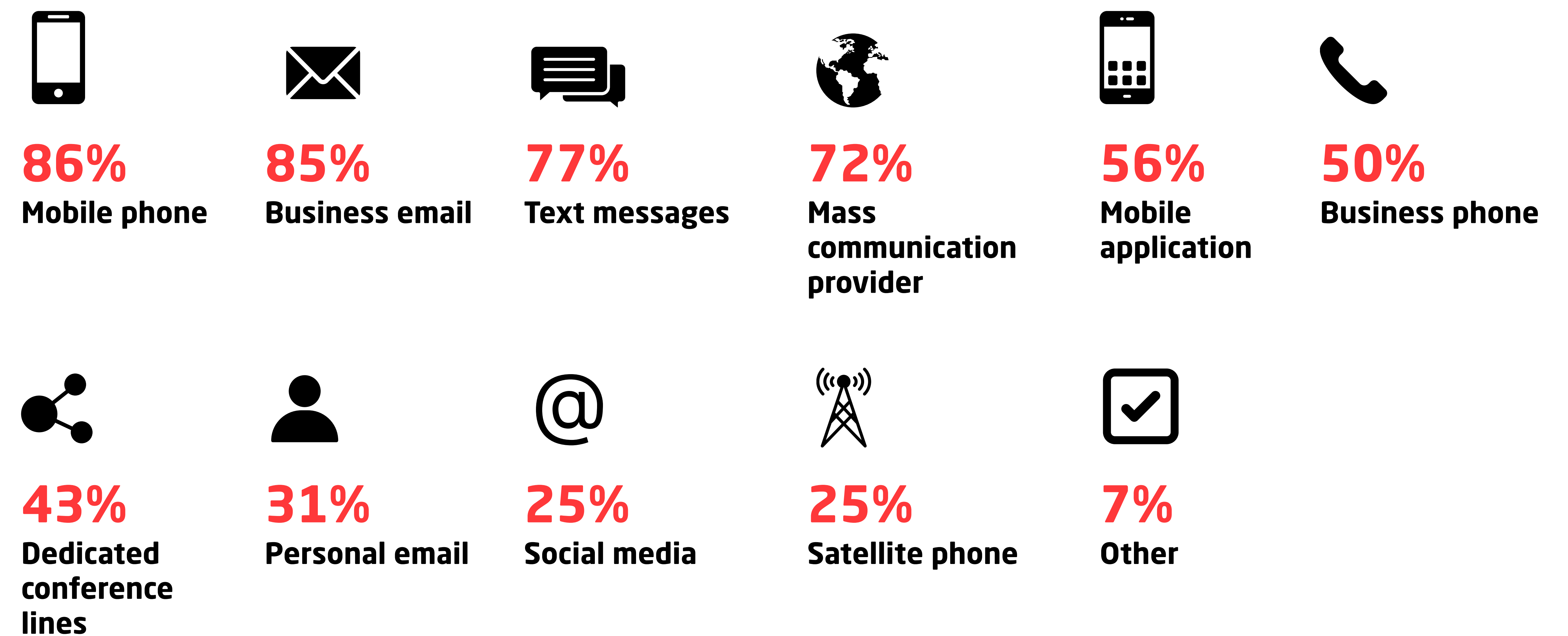
In today's technological landscape, **13%** of "mature" or "very mature" companies do not have their plans available in a mobile format. The percentages are higher for "immature" or "very immature" companies, coming in higher than half (**56%**). Yet, when selecting multiple options for how they would communicate throughout an event, **86%** of respondents indicated that they planned to communicate on a mobile phone; **77%** via text messages. Having mobile versions of plans could ensure access to plans if company systems are down; enable functions and business lines to review the checklists they have already organized so action steps are not overlooked; and the process for analyzing the impacts, setting a strategy, and assigning work streams is followed by those managing the response.

Are Plans Accessible in a Mobile Format?



How do Organizations Plan to Communicate Throughout an Event?

Sum exceeds 100% due to multiple selections.



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



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

13% Unsure

37% No

49% Yes

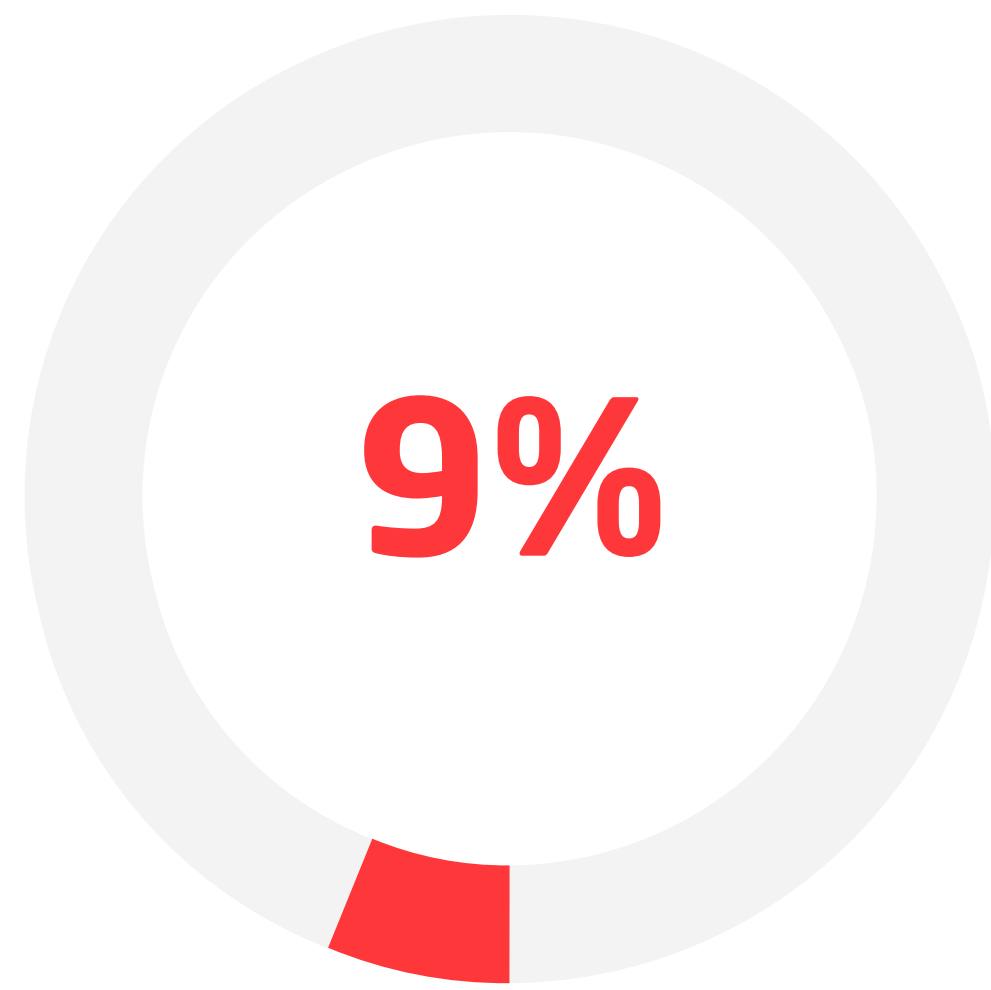


61%
Mature or Very
Mature Programs

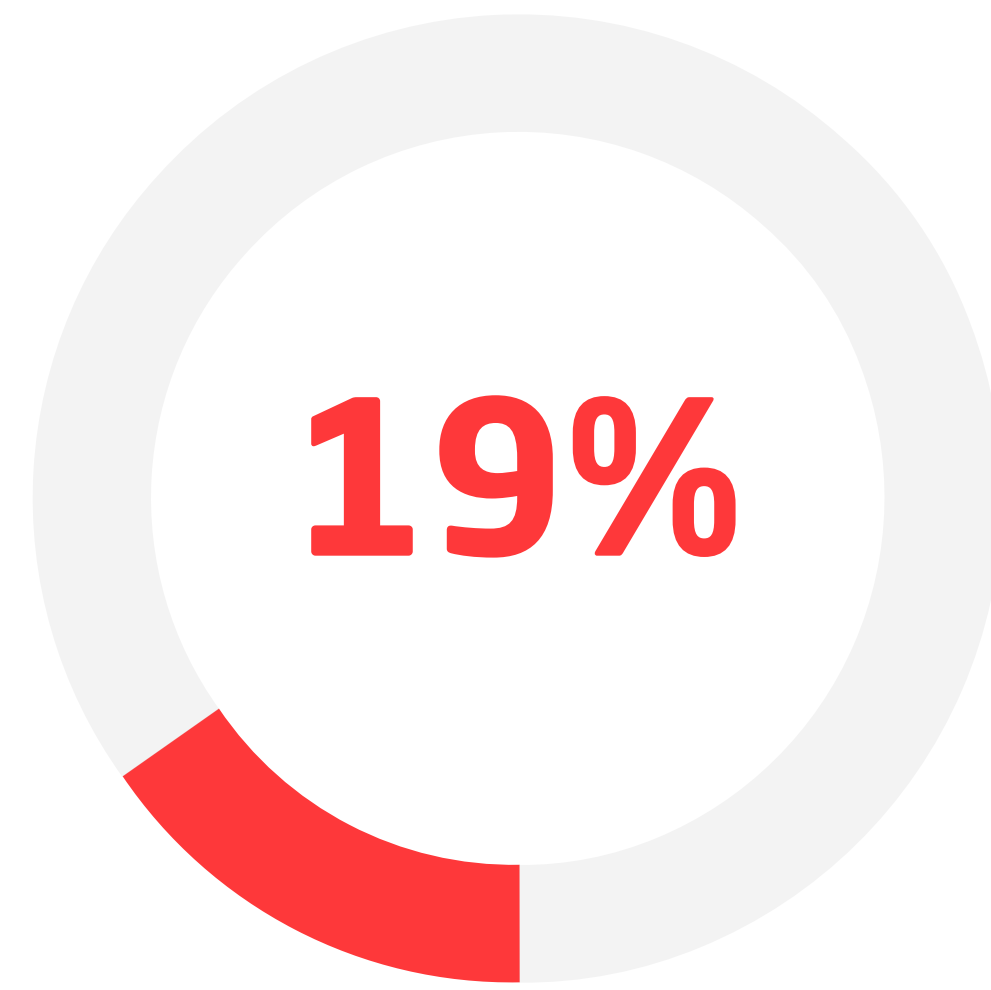


38%
Immature or Very
Immature Programs

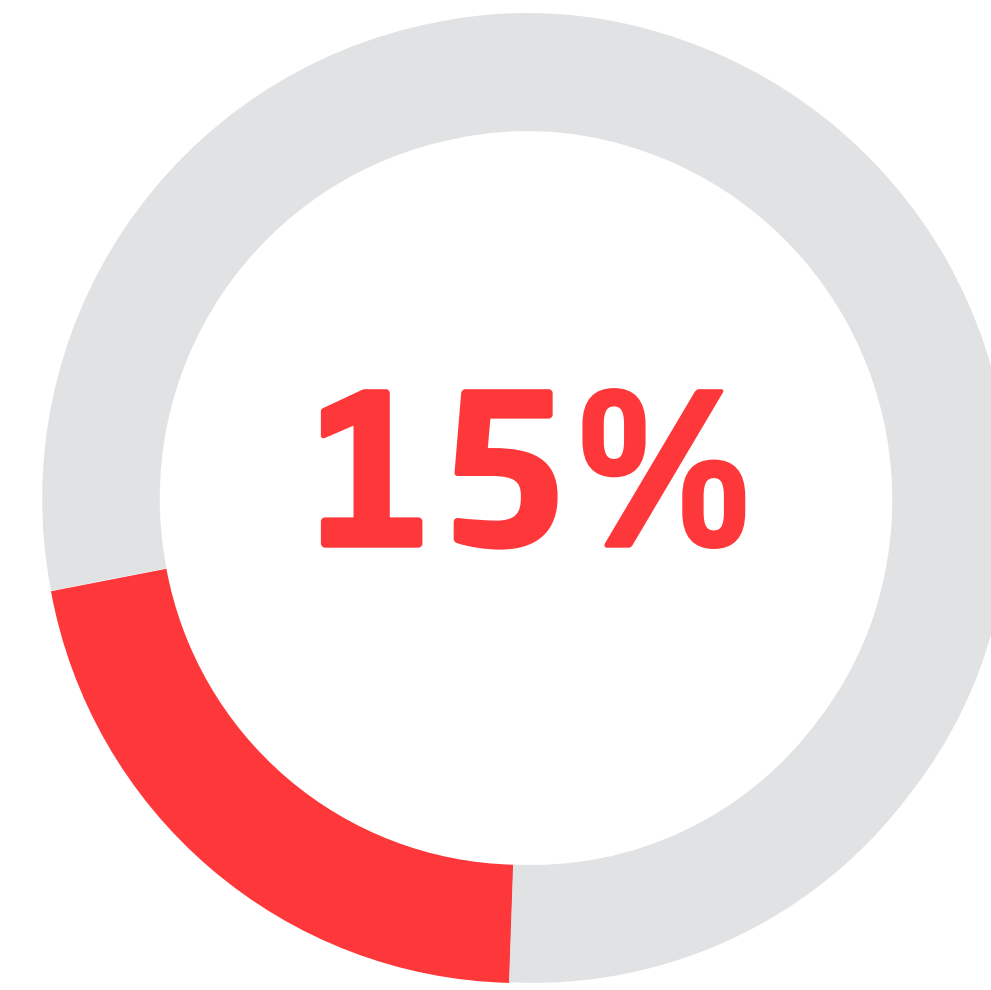
Importance of Business Continuity Software to Organizations in terms of the Ability to Identify Event-Driven Risks to Critical Processes in Real-Time.



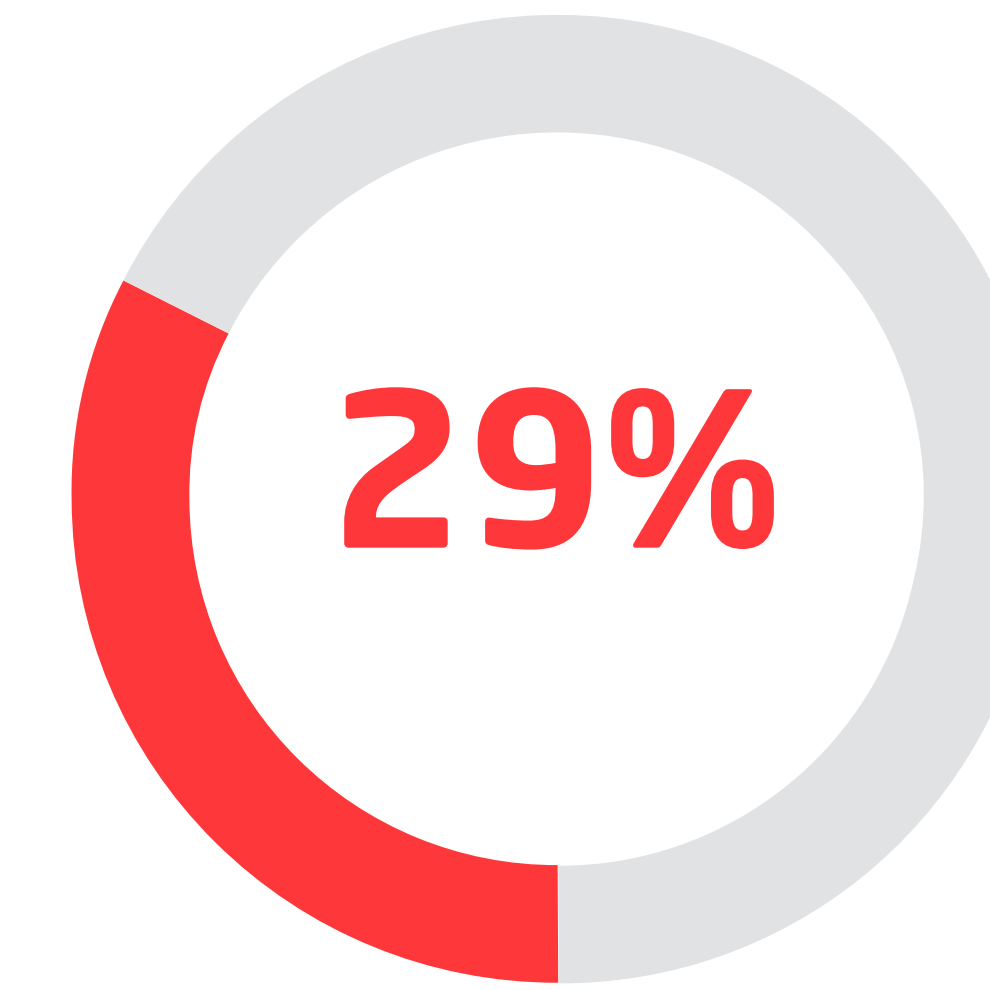
No importance



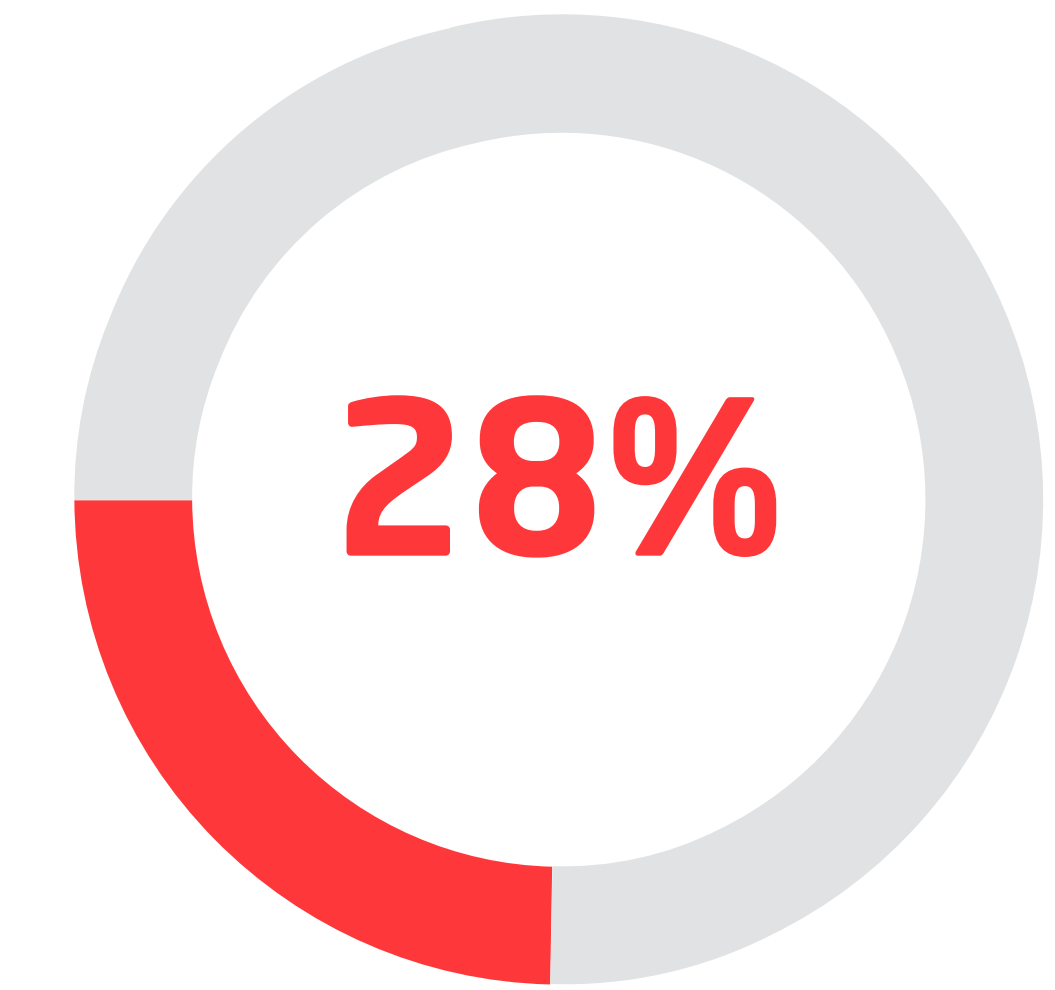
Little importance



Neutral



Important



Very important

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

8%

No defined corporate-level crisis management team, we assemble business as usual and executives manage a crisis

9%

Yes, but no pre-defined 'crisis leader'

27%

Yes, but we only have 'primary' roles identified and filled

55% - All Programs

Yes, we have both 'primary' and 'alternate' roles identified and filled



68%
Mature or Very
Mature Programs



33%
Immature or Very
Immature Programs

TOP 4 Greatest Challenges

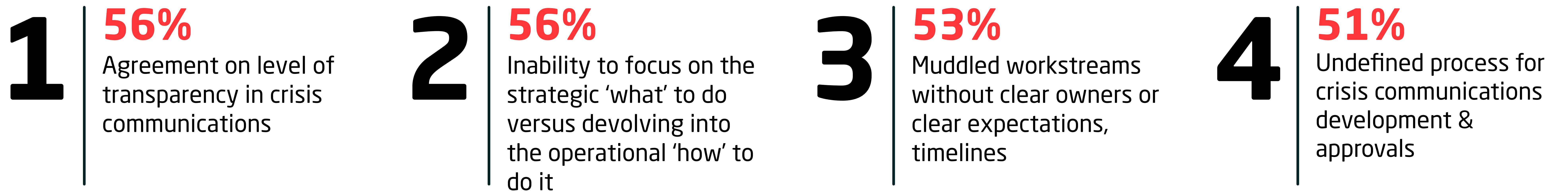
Mature or Very Mature Programs

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

“Regardless of maturity, programs identify “agreement on level or transparency” and “undefined process for crisis communications” during an incident in their top-4 greatest challenges. Both issues can be simultaneously workshopped during a tabletop or exercise involving senior management, the crisis management team and the group(s) responsible for internal and external communications (including PR) by practicing responses to an event, both internal and external, given a varied set of scenarios.”

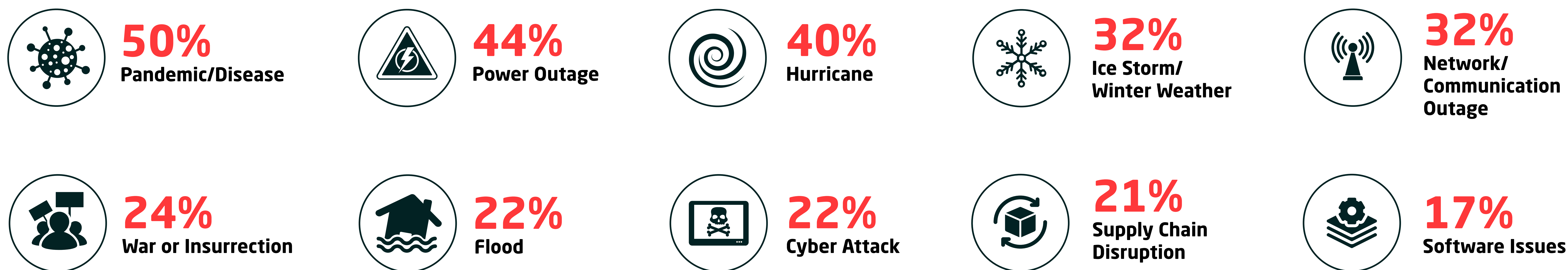
Kevin M. Cunningham, MS, CEM, CBCP (Advisory Board)

A hand is shown typing on a laptop keyboard. The background is a dark blue gradient with a blurred image of a computer screen displaying code. The code includes lines like '#include', 'main', 'stdarg', 'varargs', and 'gcc'. The text 'TOP 10 EVENTS & THE IMPACT TO ORGANIZATIONS' is overlaid in the center in a large, white, bold, sans-serif font. The image has a diagonal split with a bright yellow-green color on the top-left and bottom-right corners.

TOP 10 EVENTS & THE IMPACT TO ORGANIZATIONS

Top 10 Events Leading to Employing a Response/Recovery

Sum exceeds 100% due to multiple selections.



Organizations employed a response/recovery team more often for Human/Business Disasters (36%), Natural Disasters (27%), followed by Technical Disasters (22%), and Accidents (15%).

In Comparing the Events from 2020 to 2022 we Noticed the Following:

War or Insurrection increased from 2% to 24%
Ice Storm/Winter Weather increased from 20% to 32%
Supply Chain Disruption increased from 13% to 21%

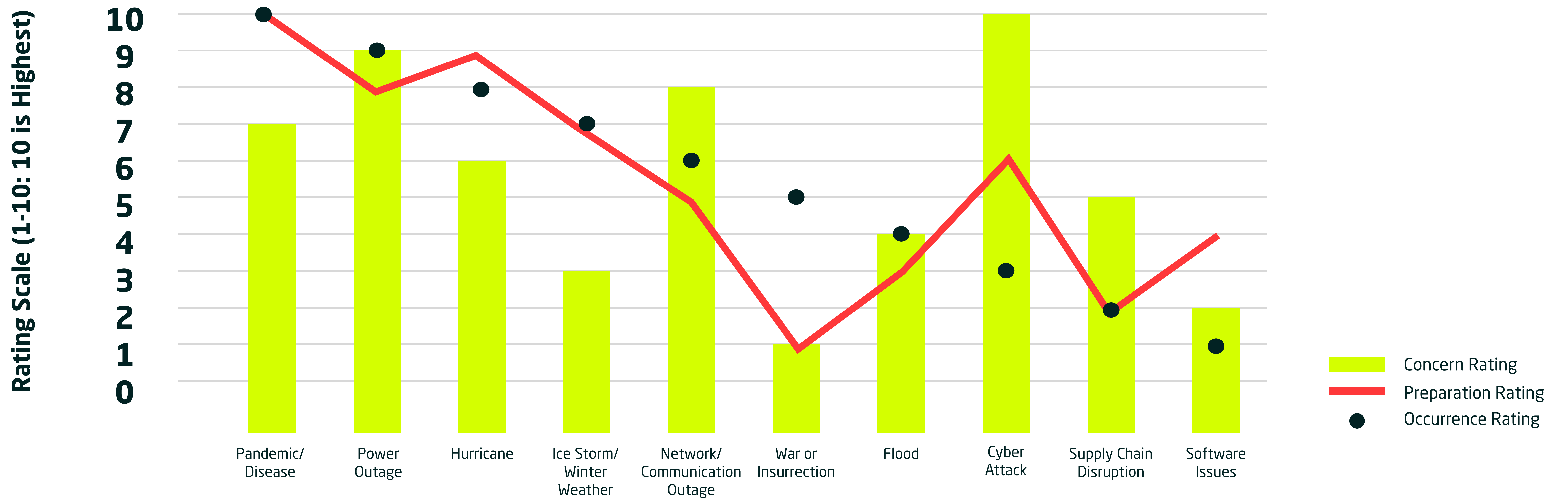
Pandemic/Disease decreased from 79% to 50%
Fire (Natural) decreased from 35% to 11%
Civilian Unrest/Political Instability decreased from 29% to 8%

INSIGHTS

More than **2/3** of organizations experienced an event, crisis, or incident in which they had to employ a response/recovery team in the last year. High-impact disruptions have ranged from global supply disruptions, the increasing prevalence of cyber-attacks, severe weather emergencies, geopolitical conflict, a billion-dollar airline meltdown, a pandemic, and the most consequential financial crisis since the Great Recession that's still potentially unfolding. And while each year is marked with crises that have tested resilience management strategies (pandemic since 2020, war or insurrection and supply chain disruptions topped the list for the first time in 2022, and civilian unrest/political instability and protests in 2020), the crises that have continued to challenge organizations for years include power outages, hurricanes, ice storms/winter weather, network/communication outages, floods, and cyber attacks.

An Assessment of the Top Crises Leading to a Response/Recovery Effort in 2022 and the Ratings of Concern and Preparation for each Event in the Future.

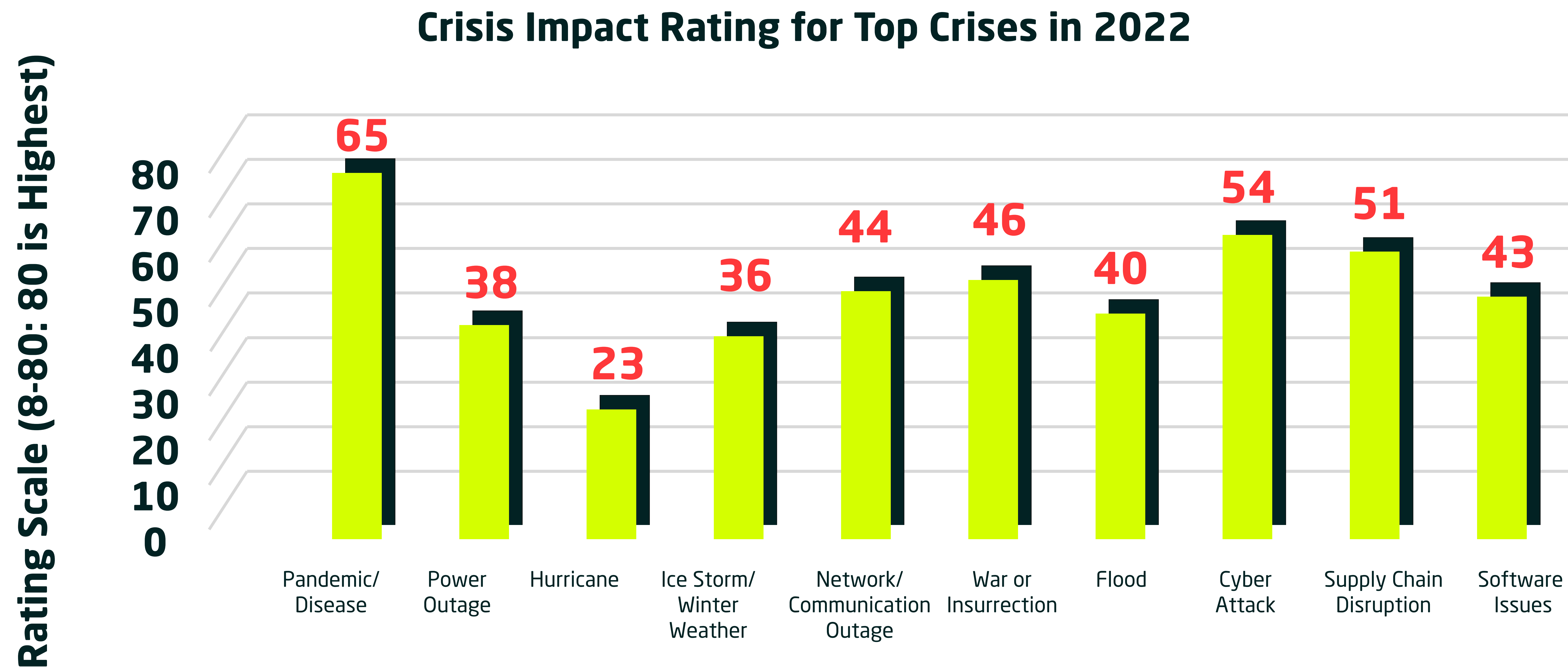
Top Crises in 2022: Future Concern & Preparation Rating



Top Events Leading to Employing a Response/Recovery in 2022

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

	Occurrence Rating	Concern Rating	Preparation Rating
Pandemic/Disease	10	7	10
Power Outage	9	9	8
Hurricane	8	6	9
Ice Storm/Winter Weather	7	3	7
Network/Communication Outage	6	8	5
War or Insurrection	5	1	1
Flood	4	4	3
Cyber Attack	3	10	6
Supply Chain Disruption	2	5	2
Software Issues	1	2	4



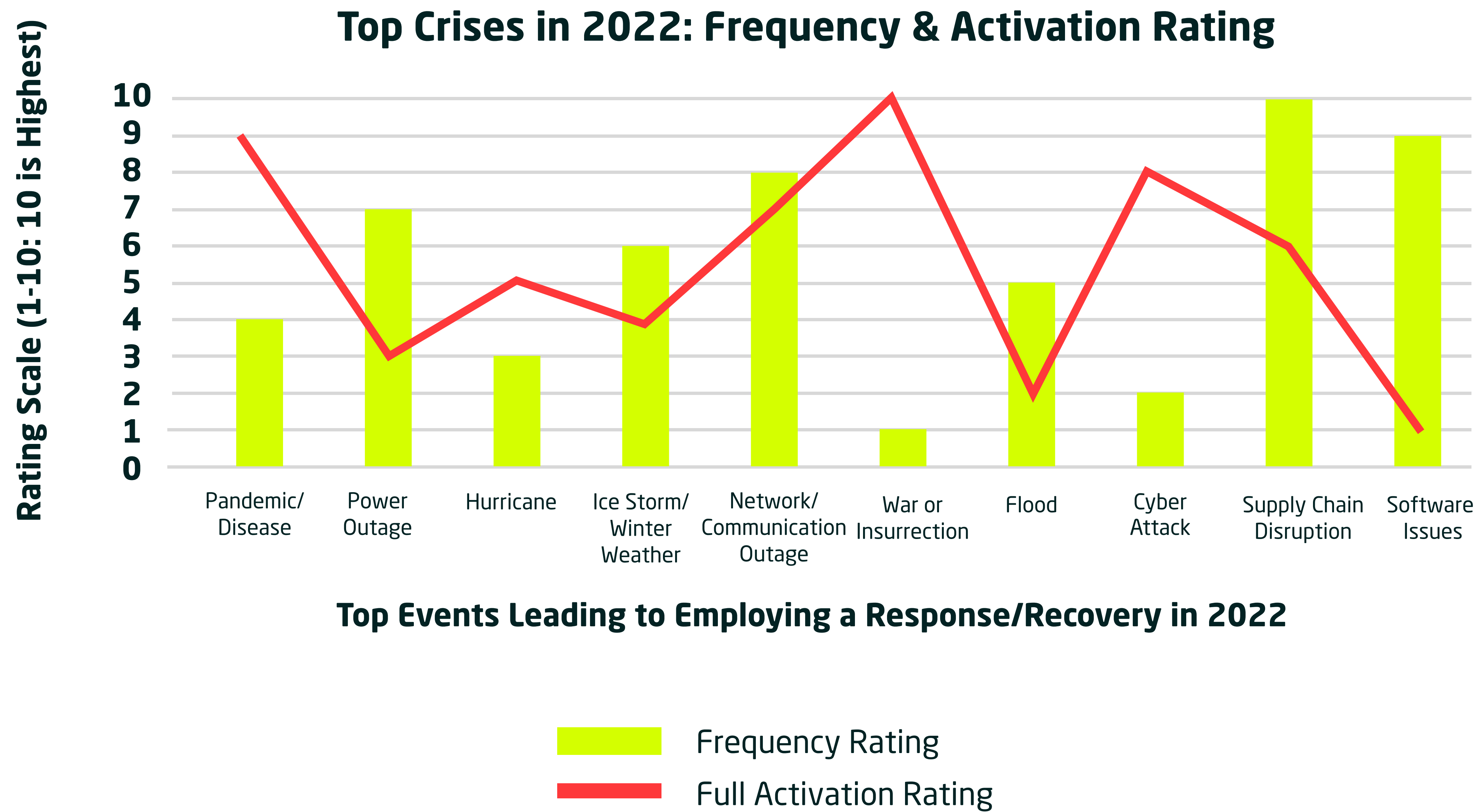
Top Events Leading to Employing a Response/Recovery in 2022

INSIGHTS

This year we took a different approach to assess not only the top recent events impacting organizations, but 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. In this assessment, the data indicated that pandemic/disease continued to challenge organizations more than other crises receiving the highest crisis impact rating of **65** followed by cyber attacks (**54**) and supply chain disruptions (**51**). The following pages highlight how each crisis impacted organizations.

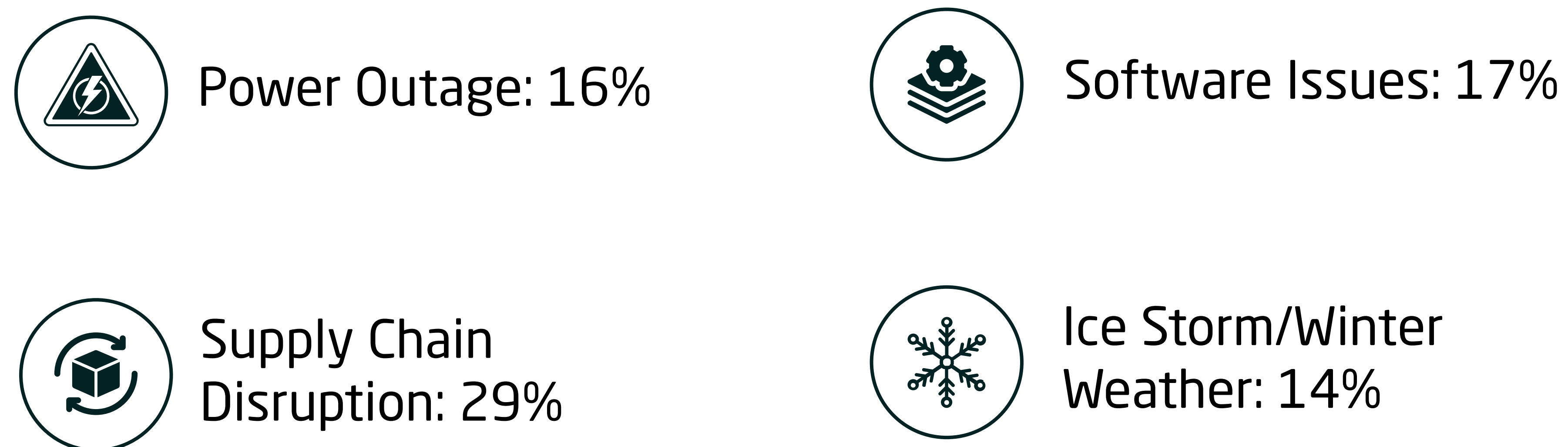
Note: Each crisis was rated based on the frequency, full activation rating, advance warning, impact on employees, geographic scope, percent of critical systems impacted, business resumption period, and estimated financial losses. For each impact, crises were assigned a rating between 1 (lowest impact) to 10 (highest impact) with a total potential impact rating varying between 8 to 80.

Frequency and Activation Rating for the Top Crises Leading to a Response/Recovery Effort in 2022



	Frequency Rating	Full Activation Rating
Pandemic/Disease	4	9
Power Outage	7	3
Hurricane	3	5
Ice Storm/Winter Weather	6	4
Network/Communication Outage	8	7
War or Insurrection	1	10
Flood	5	2
Cyber Attack	2	8
Supply Chain Disruption	10	6
Software Issues	9	1

Percent of Respondents indicating a Crisis Occurring 10+ Times



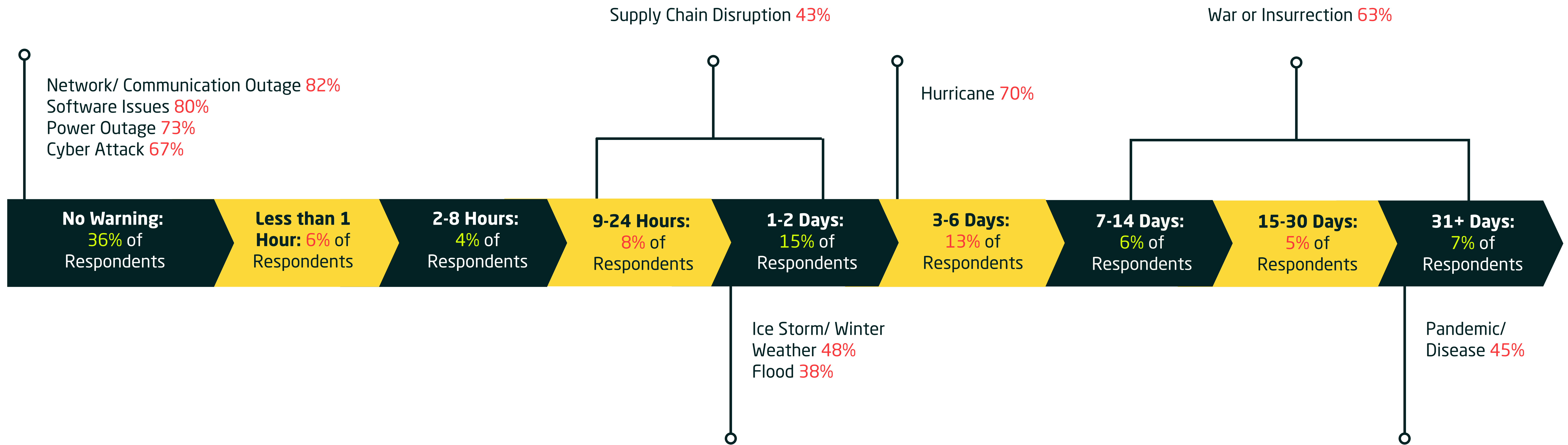
Percent of Respondents indicating Full Activation by Crisis



The data also highlights that **supply chain disruptions** and **network/communication outages** were most likely to occur at high frequency and lead to a full activation.

Note: Study participants ranked frequency of each event from occurring 1 time to 10+ times in addition to ranking 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 2022



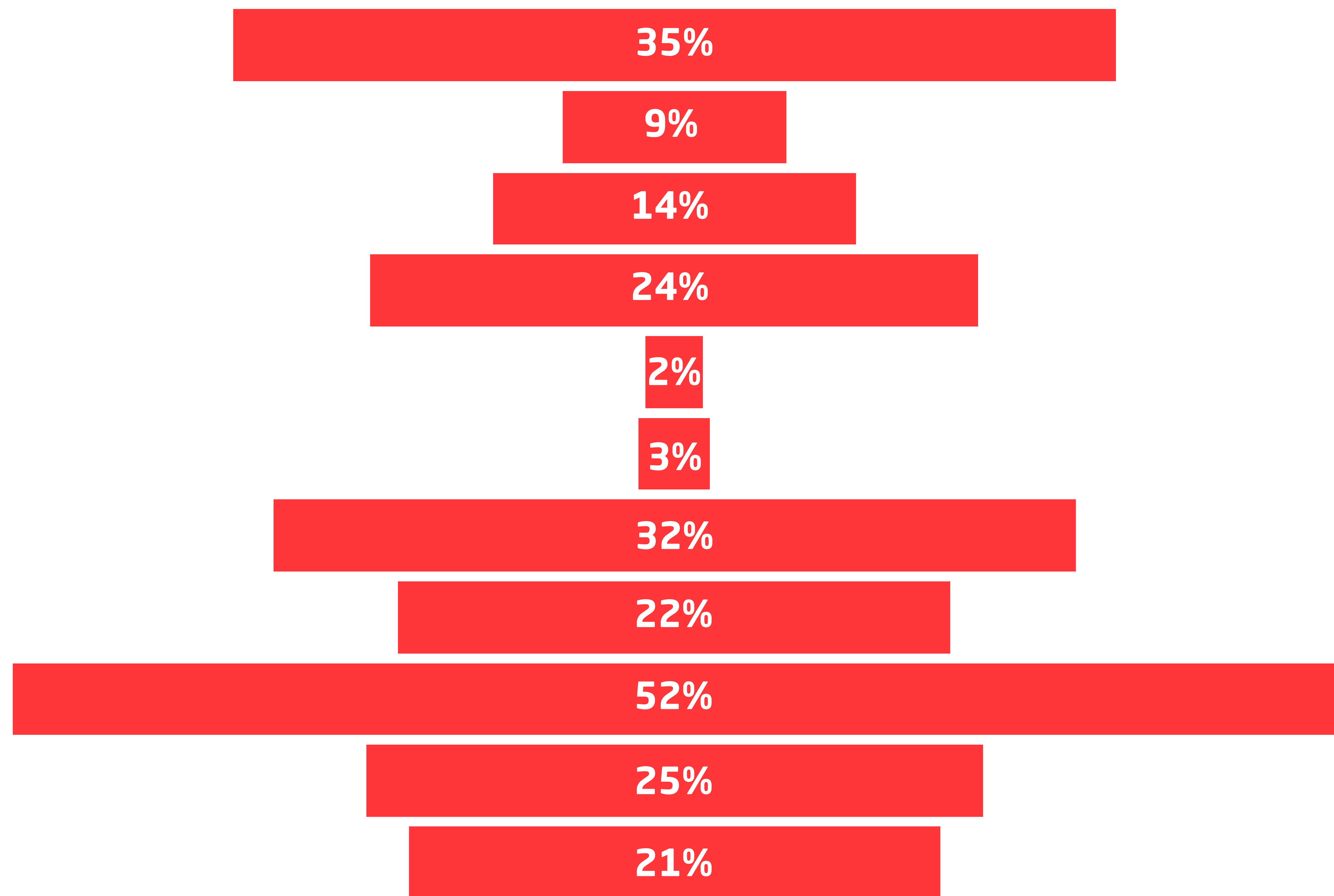
INSIGHTS

While most organizations (**36%**) indicated no warning before a crisis hit an equal amount (**36%**) noted an advance warning between 9 hours to 6 days. The technical crises commonly came with no warning (**82%** of network/communication outages, **80%** of software issues, and **67%** of cyber attacks) while human business disasters provided the most advance warning (**63%** impacted by war/insurrection noted 7+ days advance warning). Organizations were typically alerted to natural events within 1 to 6 days. Interestingly enough, page 23 highlights the business resumption period and human/business disasters noted the longest recovery time with **33%** noting a business resumption time of 7 to 30 days for a supply chain disruption and **47%** and **38%** noting 121+ days respectively for pandemic/disease and war/insurrection. **29%** of all organizations impacted by a crisis in the last year noted a business resumption period of over a week.

Recovery/Response Activated for the Top Crises Leading to a Response/Recovery Effort in 2022

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

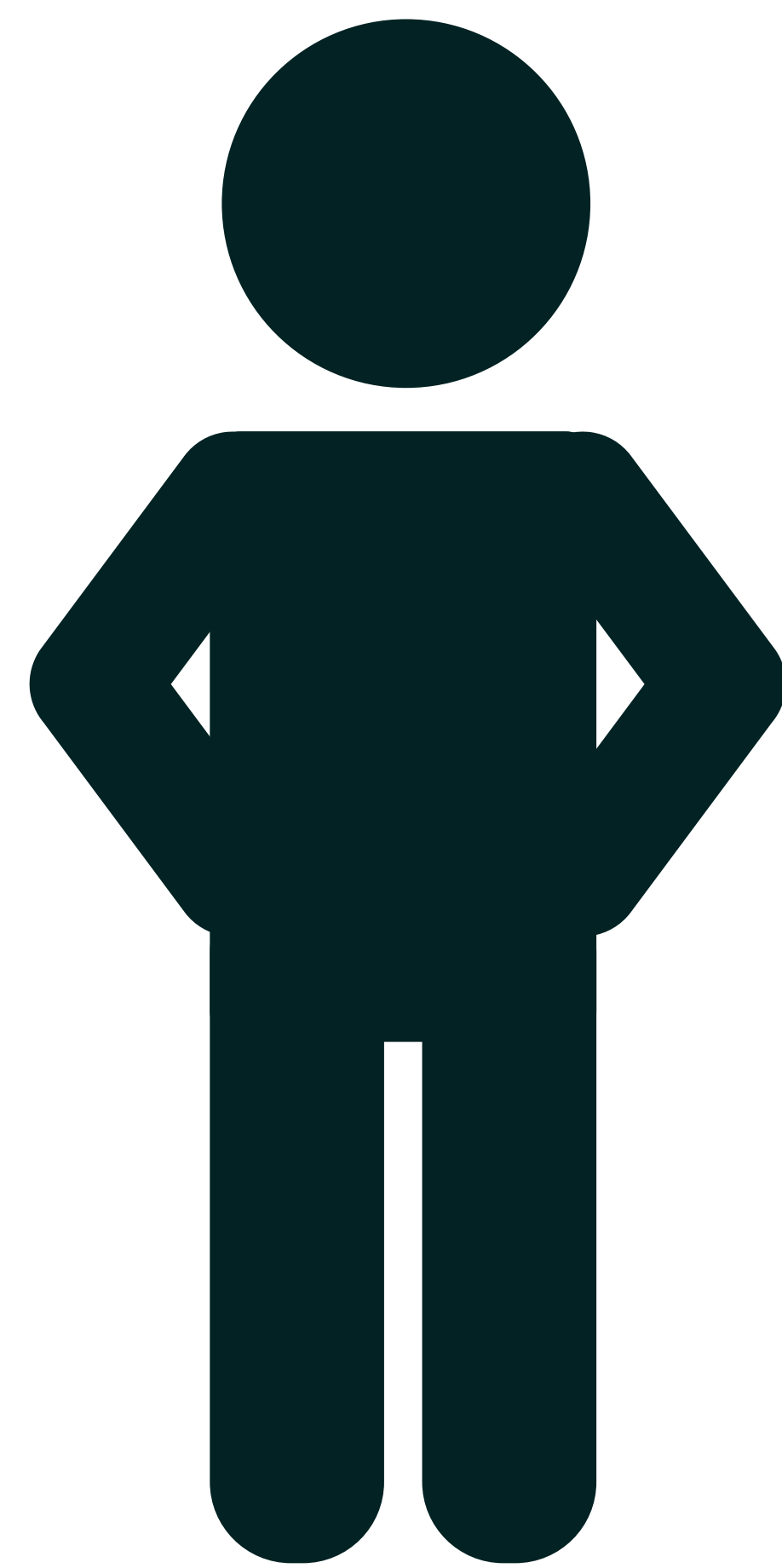
The data indicated that crisis management teams are the most likely to be activated in recovery/response to an event followed by business recovery (work area) and notification systems. This highlights how imperative crisis management pre-planning is for an organization and why it is especially concerning that only **33%** of all organizations have a standard definition of 'crisis' in place to ensure an appropriate level of response and management (as highlighted on page 11). Furthermore, earlier in this report on page 14, the data indicated several challenges in crisis management pre-planning from clarity on when to notify and activate, wrong person in a leadership role, an undefined process in crisis communications, agreement on the level of transparency, and muddled workstreams without clear owners or clear expectations, timelines.

"Business Recovery (Work Area) - In Singapore, due to the COVID19, the demand for work area has reduced tremendously, as most organizations plan for staff to work from home instead of subscribing to business recovery work area. And many organizations are now planning for hybrid model for business as usual, i.e., staff will be rotated to work from office and home as part of their business continuity planning."

Wong Tew Kiat, CBCP, FBCI, CITBCM(S), CITPM(S), COMIT(S), Fellow of Singapore Computer Society (Advisory Board)

Percent of Employees Impacted for the Top Crises Leading to a Response/Recovery Effort in 2022

Negatively Impacted



75% + of Employees

- Pandemic/Disease: 45%
- Cyber Attack: 13%
- Power Outage: 9%

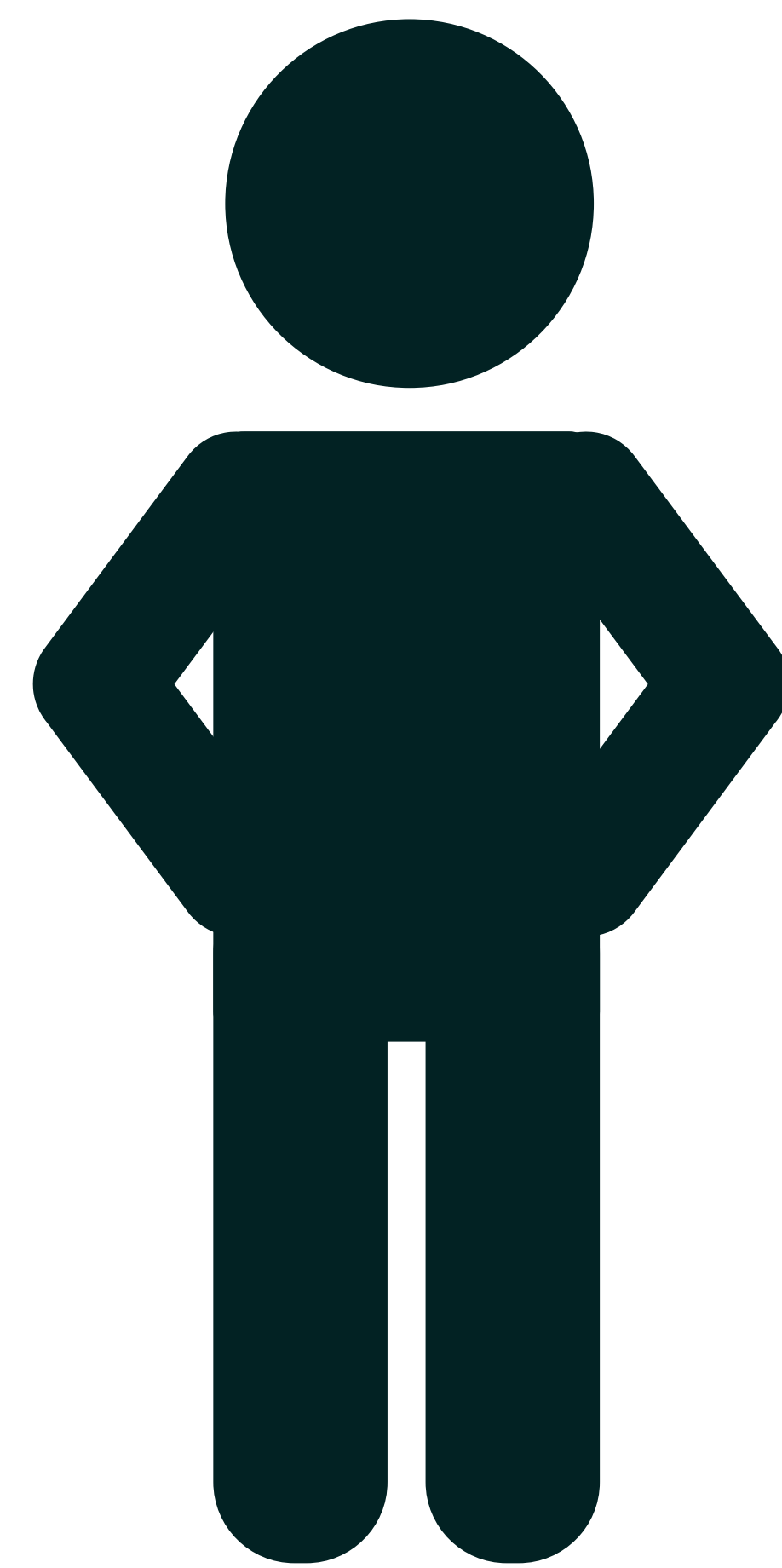
50-75% of Employees

- Network/Communication Outage: 18%

25-50% of Employees

- Software Issues: 17%

Displaced



75% + of Employees

- Ice Storm/Winter Weather: 5%

25-50% of Employees

- Hurricane: 4%

Less than 10% of Employees

- Supply Chain Distribution: 40%

Placed at Recovery Site



50-75% + of Employees

- Flood: 7%

10-15% of Employees

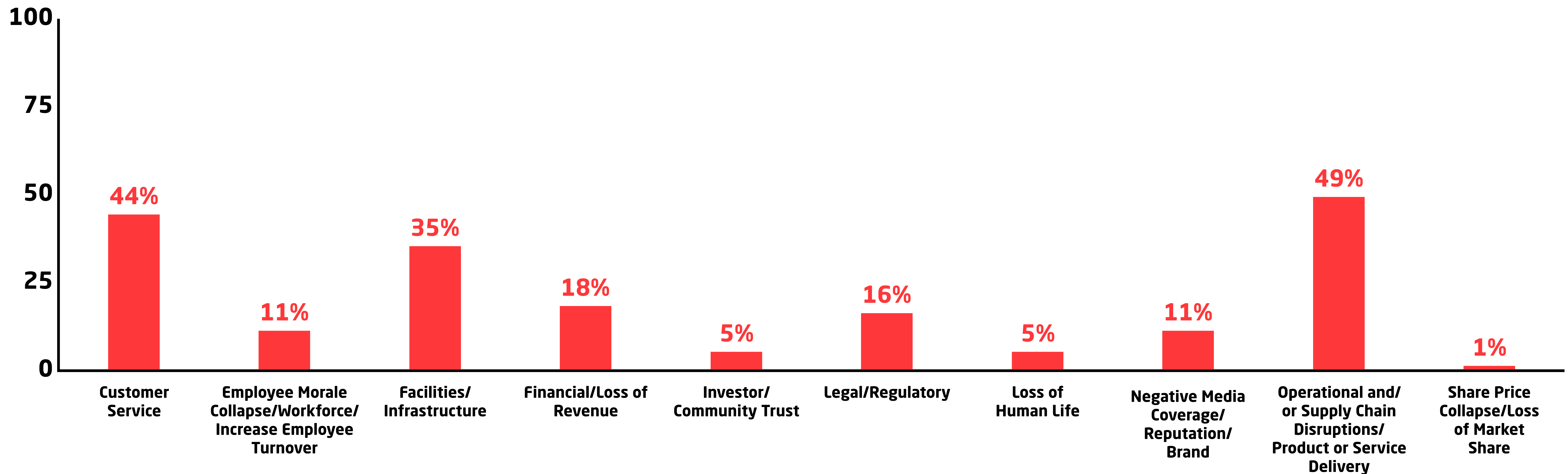
- Ice Storm/Winter Weather: 9%

Less than 10% of Employees

- War or Insurrection: 53%

Impact to the Organization for the Top Crises Leading to a Response/Recovery Effort in 2022

Sum exceeds 100% due to multiple selections.



INSIGHTS

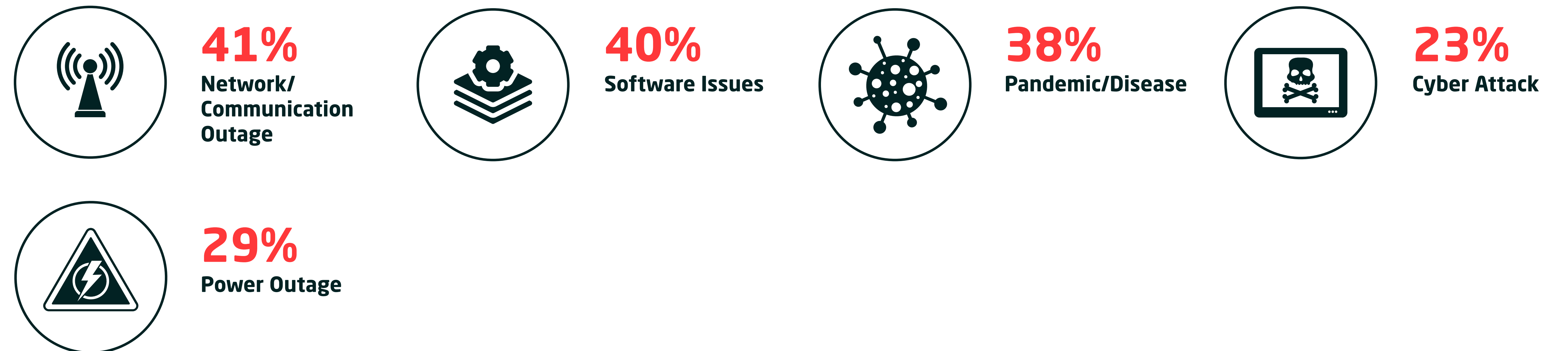
Geographical Scale of Impact for the Top Crises Leading to a Response/Recovery Effort in 2022

- Global (21%)
- Regional, (18%) Multiple Business Units (18%)
- Business Unit (14%)
- National, (10%) Multiple Buildings (10%)

22% of Organizations Indicated that **More than 25%** of Critical Processes were Impacted while Responding/Recovering to the Top 10 Crises in 2022.

Five of the Top 10 Crises Compromised Critical Processes More

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

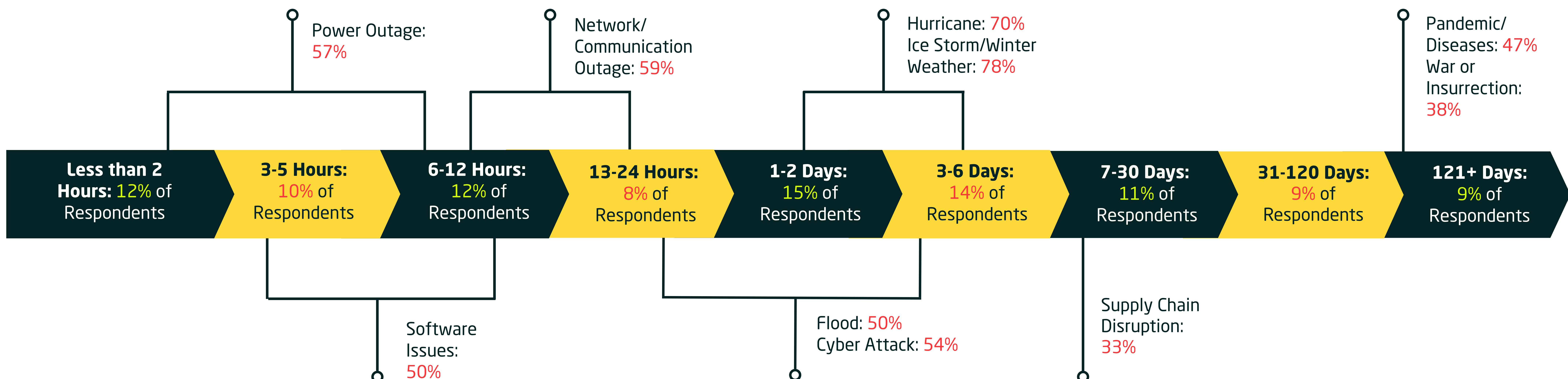


Executive Leadership Involvement for the Top Crises Leading to a Response/Recovery Effort in 2022

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

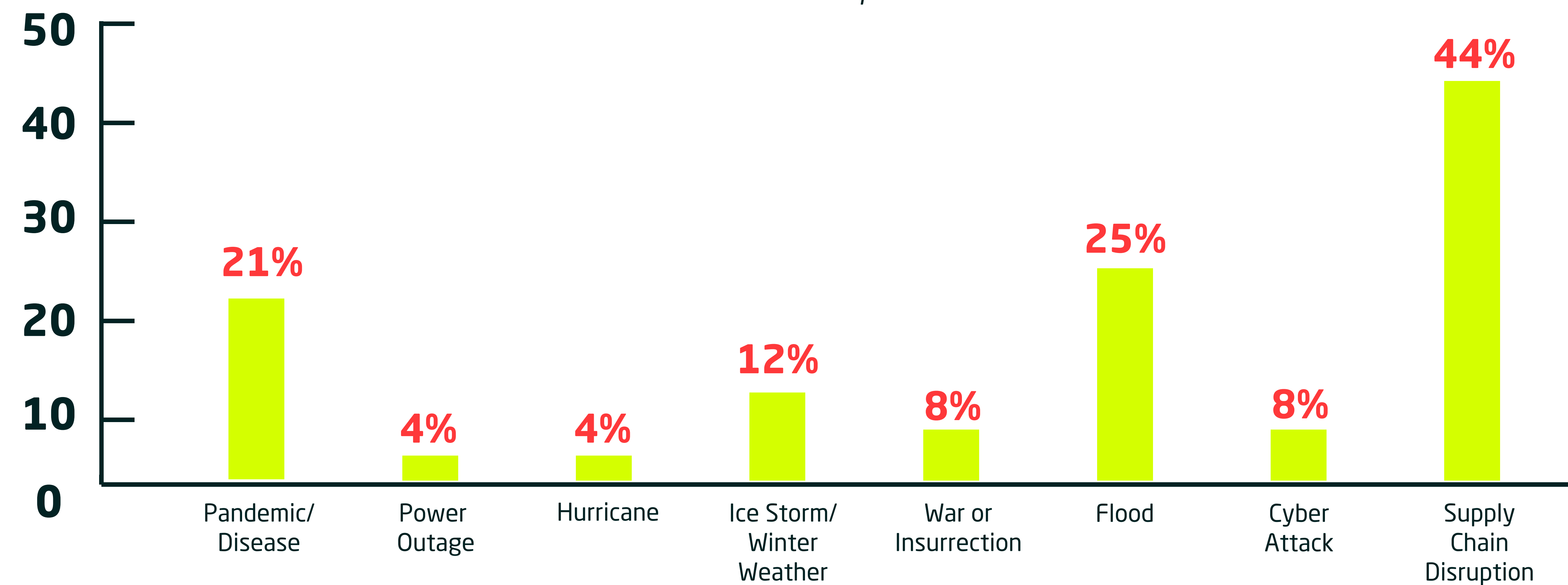


Business Resumption for the Top Crises Leading to a Response/Recovery Effort in 2022



Percent of Respondents Noting Over \$1,000,000 USD in Estimated Financial Losses for the Top 10 Events in 2022

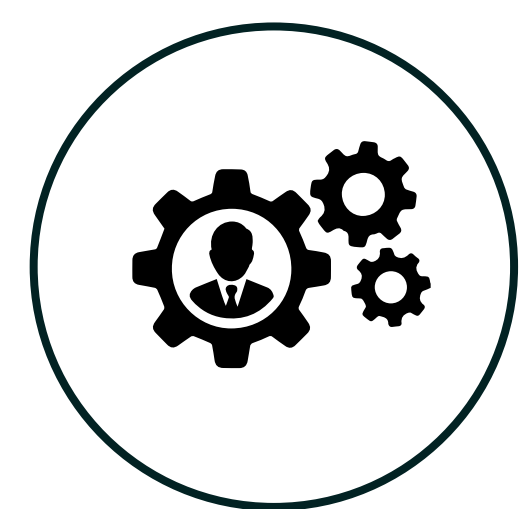
Sum is not meant to equal 100%.



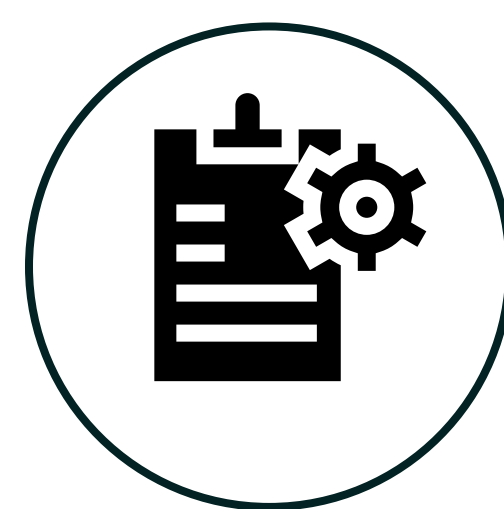
On average, 53% of all respondents indicated it was difficult to calculate the estimated financial losses.

What are **THREE things that the Respondents Who Noted \$5M+ USD in Estimated Losses for an Individual Event have in Common?**

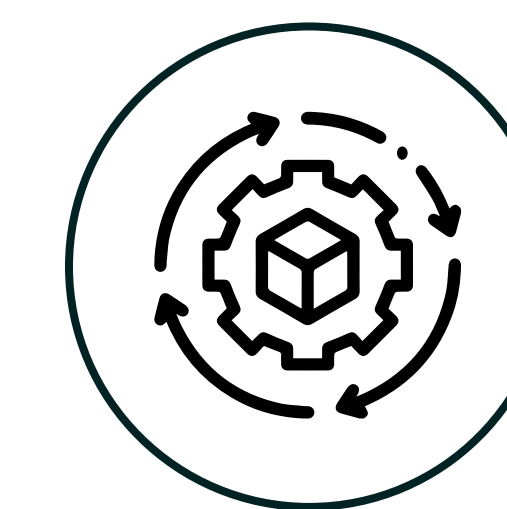
- **Very Immature:** 14% self-rated their program as Very Immature (Reactive - chaotic/ad hoc) compared to 8% of all respondents who noted the same.
- **Plans are not accessible in a mobile format:** 57% of respondents compared to 33% of all respondents
- **Newer Programs:** A majority of programs have been in existence for less than 4 years.



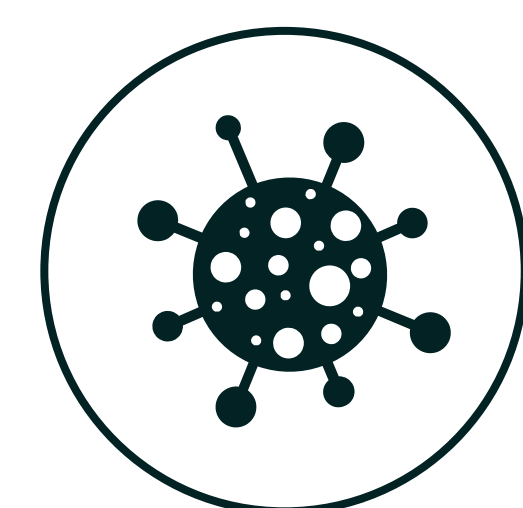
Business Continuity: 43%



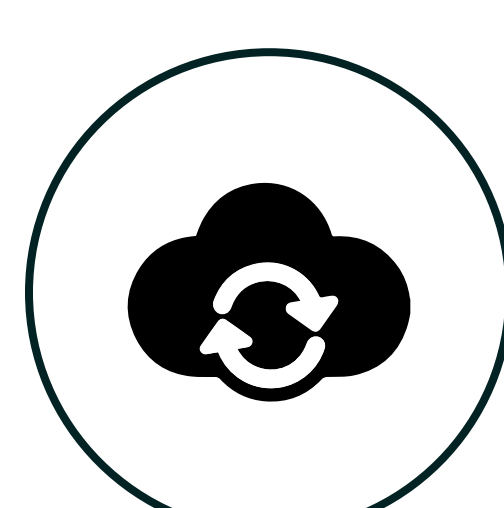
Crisis Management: 43%



Supply Chain Resilience: 33%



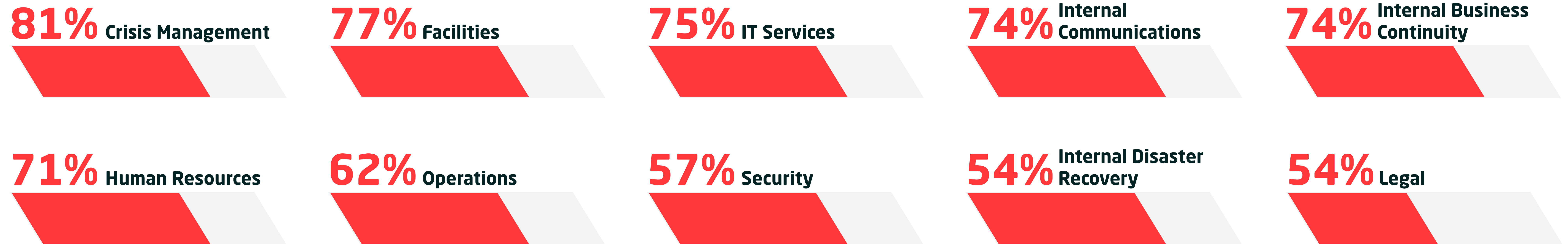
Pandemic Planning: 57%



Disaster Recovery/IT Service Continuity: 43%

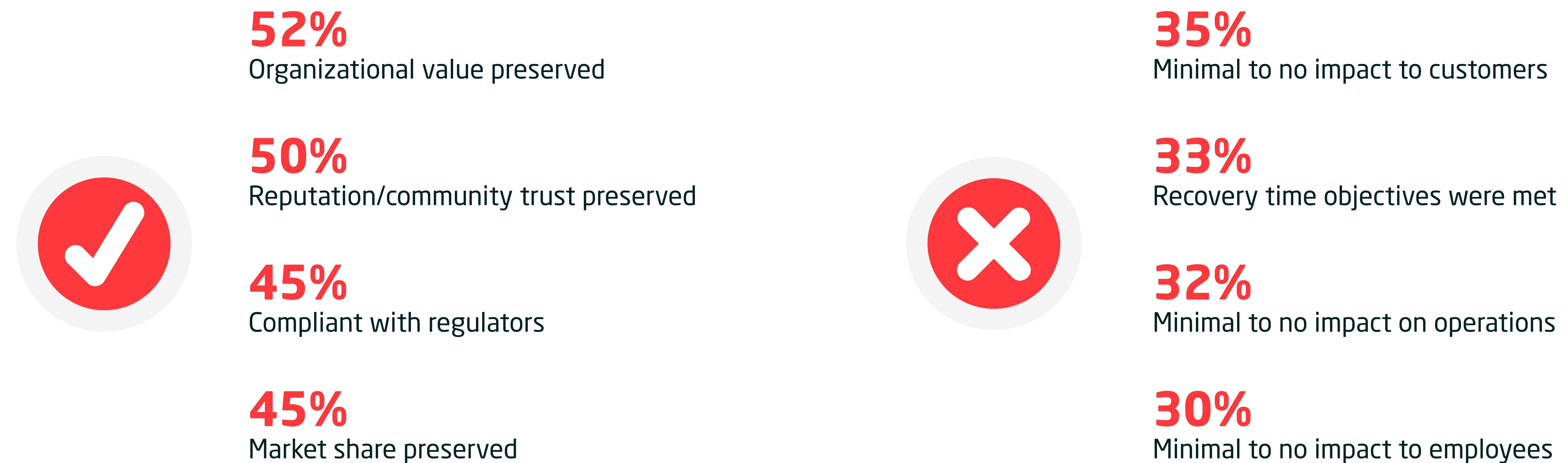
Who or What was Included While Recovering/Responding to a Crisis?

More than 50% of respondents indicated:



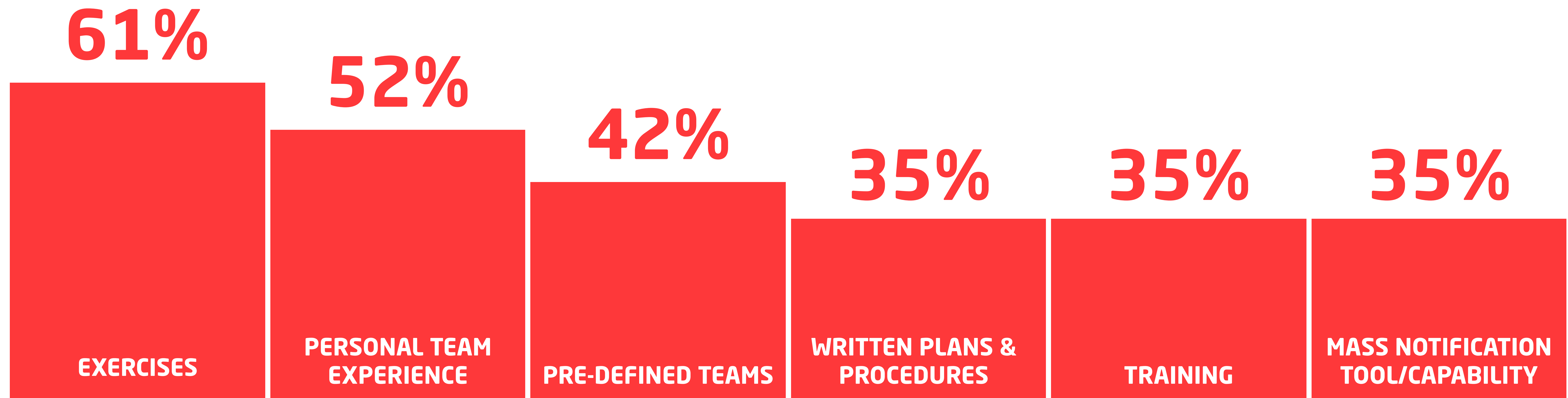
What Outcomes Were Noted as Successful as a Result of Employing Resilience Capabilities Following the Onset of a Business Disruption or Crisis?

Percent of respondents indicating "very successful".



Most Beneficial During a Response

Sum exceeds 100% due to multiple selections.



INSIGHTS

We can see from these answers that the most beneficial thing during a response is exercise. Additionally, if we consider that training is a type of exercise, it becomes doubly important with respect to the other aspects mentioned in this chart. Not surprisingly, exercises are the key to effective and prompt mitigation and recovery of operations in any type of disaster.

In my experience, we can make the best business continuity plans and response protocols and procedures, but if employees have not exercised what we have designed the plan will not help much. Two examples of the above. In an earthquake, if the city has a seismic alert, you have 40 to 60 seconds to carry out evacuation procedures, only the first 2 or maximum 3 floors per set of stairs may descend. Since an earthquake lasts an average of 45 seconds, no attempt should be made to evacuate higher floors. But this must be trained if we want to save lives since we will not be able to give instructions of this type in seconds.

Another example, in a cyber-attack, the affected systems or networks must be detected, mitigated, and isolated to prevent the dispersion of the attack to other systems and networks. The reporting, disconnection, and isolation of infected PCs could be executed by the user or by the system, but if we have not trained the users and tested the equipment, our response will not be as effective or fast enough and the impact to the organization will be greater.

In terms of business continuity, we must therefore invest time, effort, and budget with a high emphasis on exercises. We can summarize the benefits of exercises with the following Chinese Proverb: "I hear, I forget. I see, I remember. I do, I understand!"

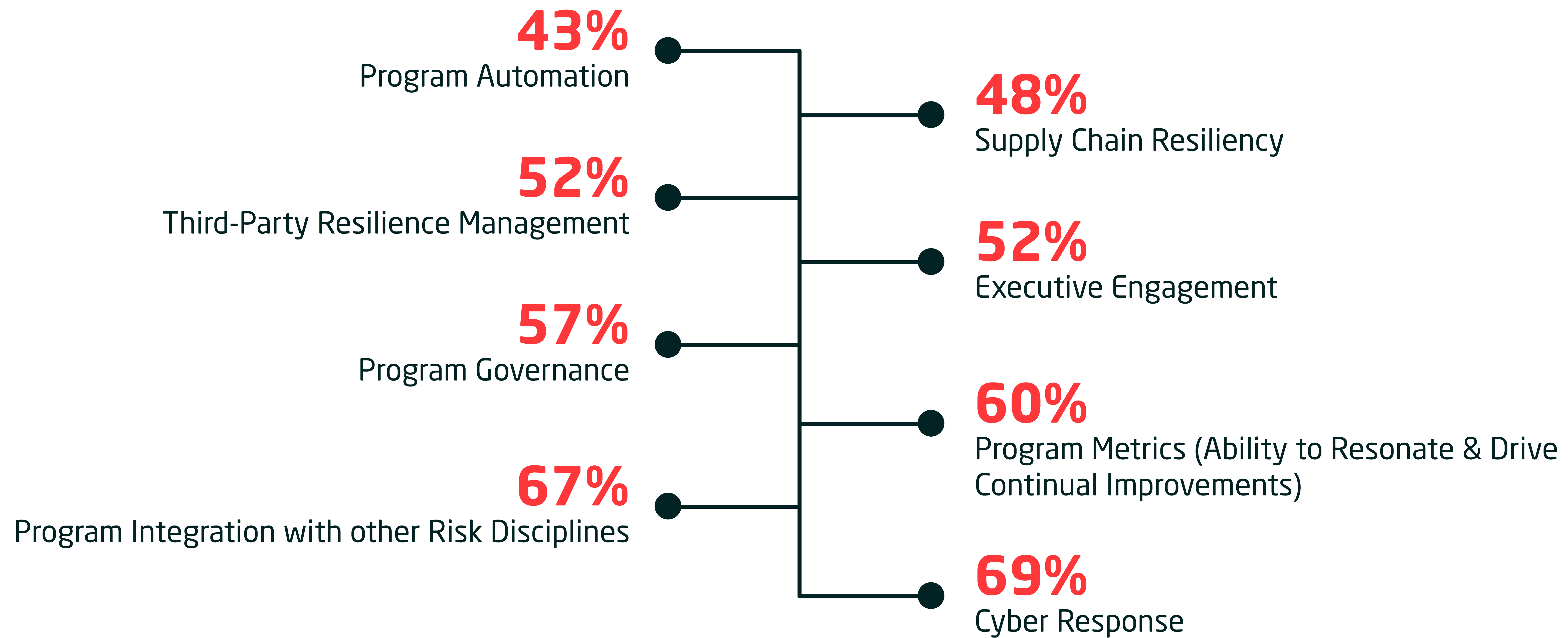
Ing. Jorge Escalera, MBA, RM-3100, MBCP, CCRP, LA 22301 (Advisory Board)



**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.

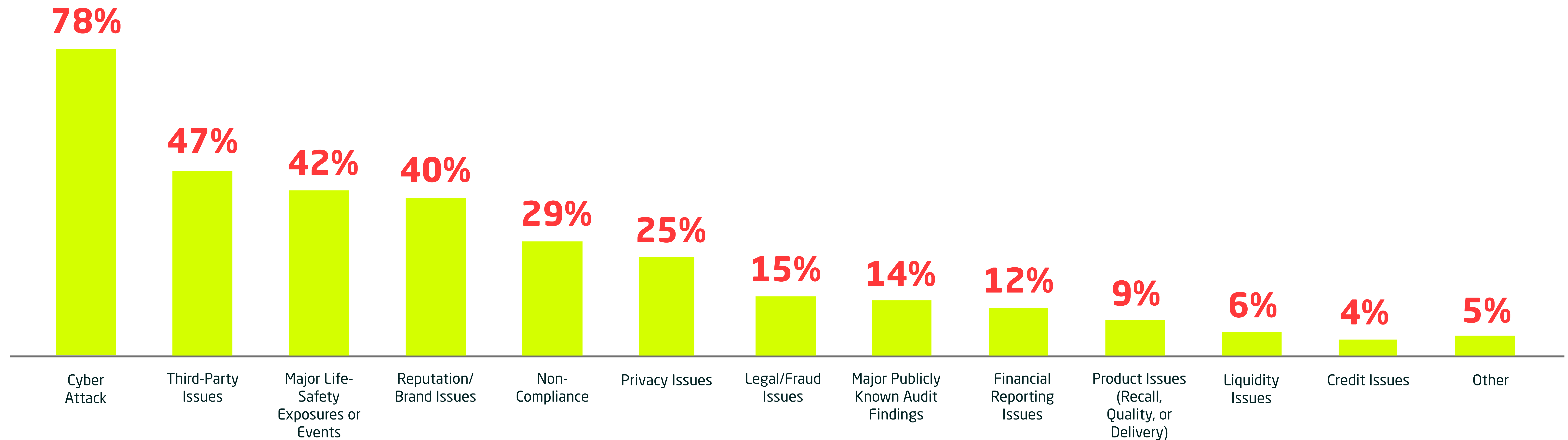


How are the Investment Strategies in Your Program Evolving in the Next Year?



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

“With the rapid rise of cloud adoption around the world, there is a significant amount of attention being paid by regulatory authorities around third party risk management and potential cloud concentration risks. While there is no agreement yet on what we mean by concentration risk, there are several factors to consider. Firstly, for business continuity planners, it is important to reduce geographic concentration risks by ensuring that primary and backup systems are geographically dispersed such that a single catastrophic event (**e.g., power outages, natural disasters et al**) does not impact both systems.

Secondly, there are systemic concentration risk concerns around the use of a single provider whose failure could cause widespread damage to multiple firms within a sector or across multiple sectors. To partially mitigate these risks, when outsourcing to the cloud or any third-party, planners should conduct thorough due diligence to ensure the cloud service provider has adequate controls around cyber security, data protection, business continuity and IT infrastructure that meet or exceed firm and regulatory requirements for operational resilience.”

Tom Wagner, CBCP, MBCI (Advisory Board)

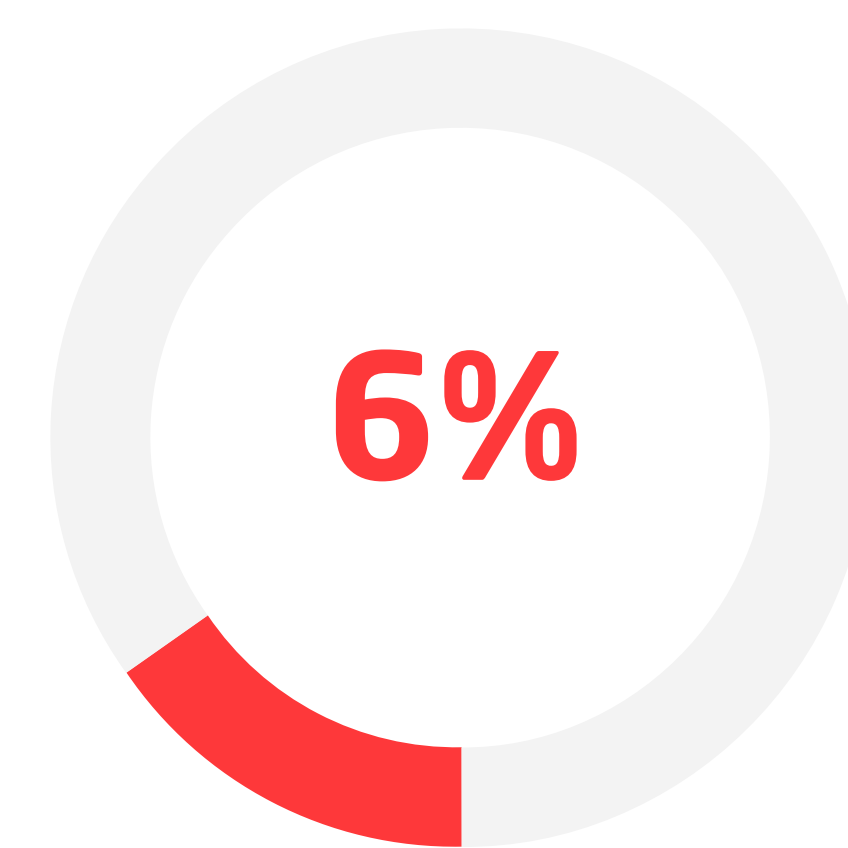


PROGRAM CHARACTERISTICS

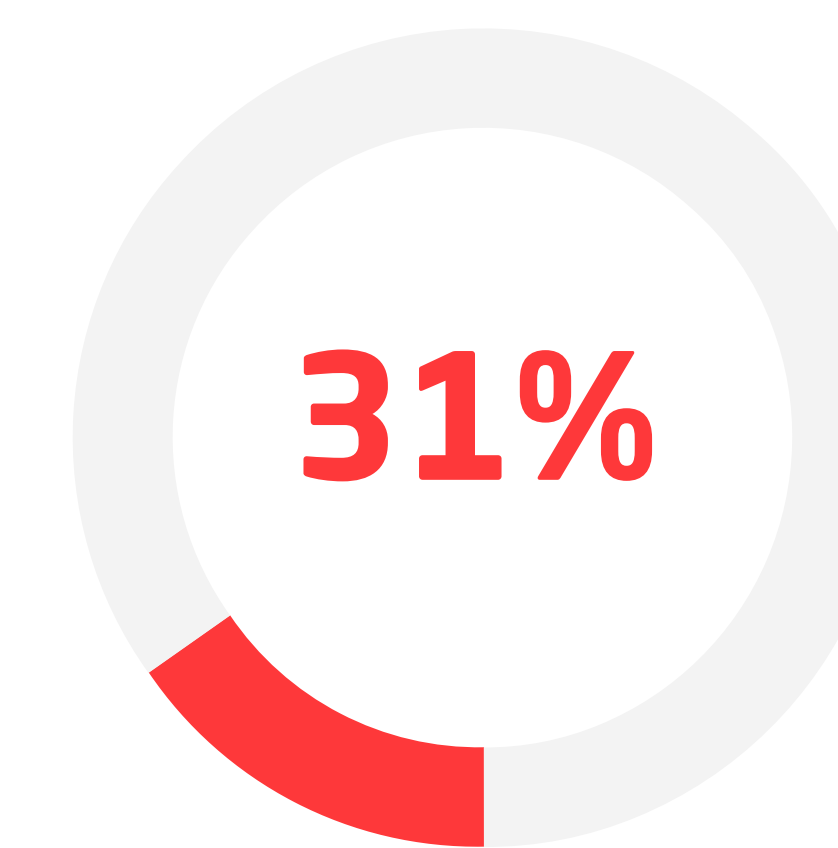
INSIGHTS

Respondents to our study were asked to self-rate the level of program maturity from reactive (a starting point for the use of new or undocumented repeat process) to capable (deliberate process optimization/improvement). And although this was a self-rating, the data highlighted several differentiating factors between programs that were "immature" and "mature". Programs with a higher-level program maturity tended to use a standard definition of 'crisis' to ensure an appropriate level of response and management (**54%** compared to **12%** of immature programs) in addition to documenting all areas of executive risk acceptance and performing annual reviews (**43%** compared to **10%** of immature programs). Organizations with mature programs were also more likely to have the ability for real-time reporting to executive leadership on event-driven risks to critical processes (**61%** compared to **38%** of immature programs) and they were more likely to have a defined, corporate-level crisis management team with both 'primary' and 'alternate' roles identified and filled (**68%** compared to **33%** of immature programs).

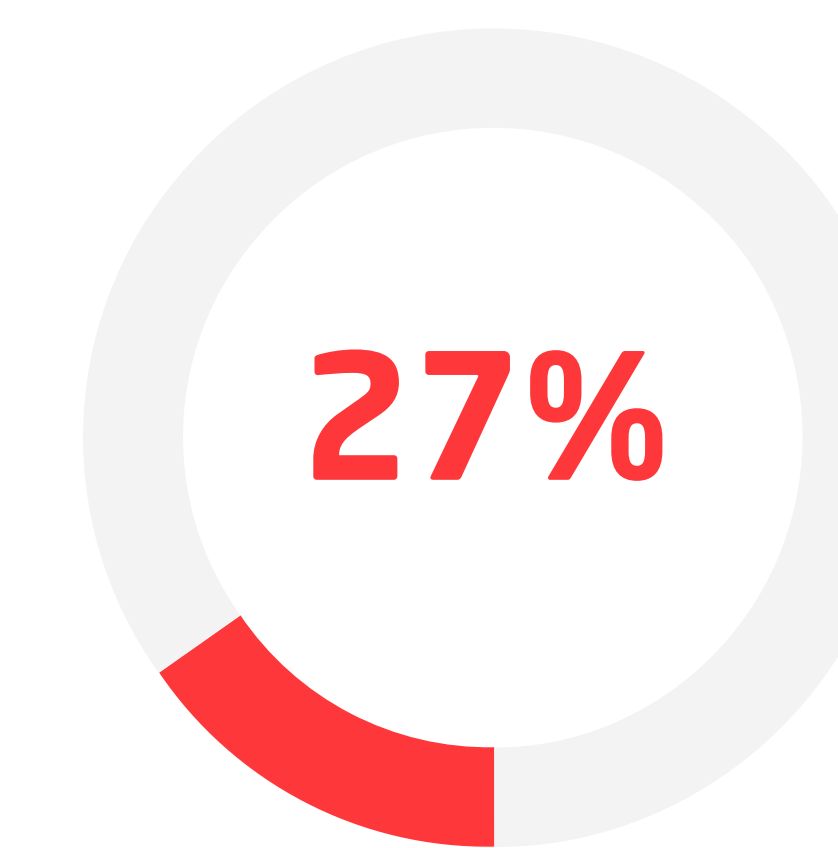
Program Maturity (Self-Rating)



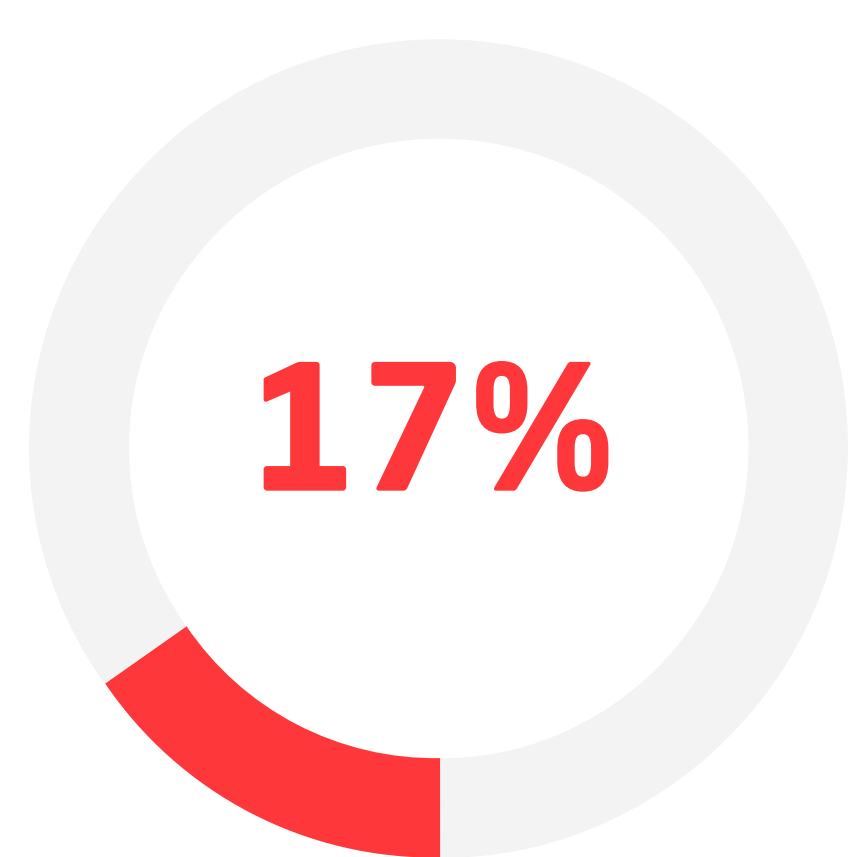
Reactive
(chaotic, ad hoc, individual heroics) The starting point for the use of a new or undocumented repeat process.



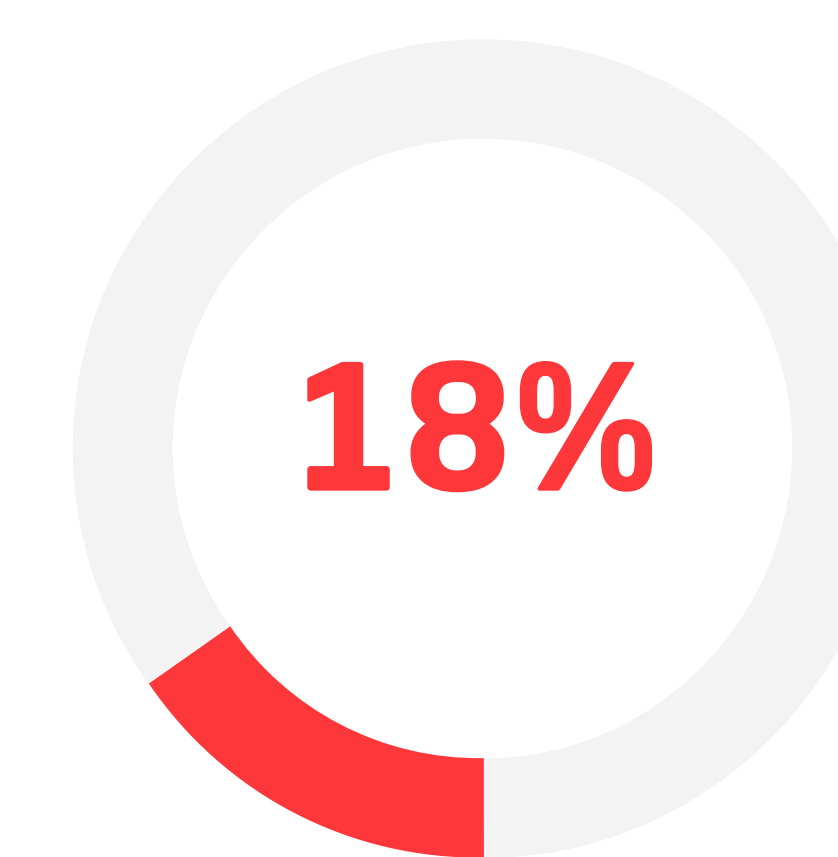
Developing
The process is at least documented sufficiently such that repeating the same steps may be attempted.



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

8%
Business Processes

More Focused on

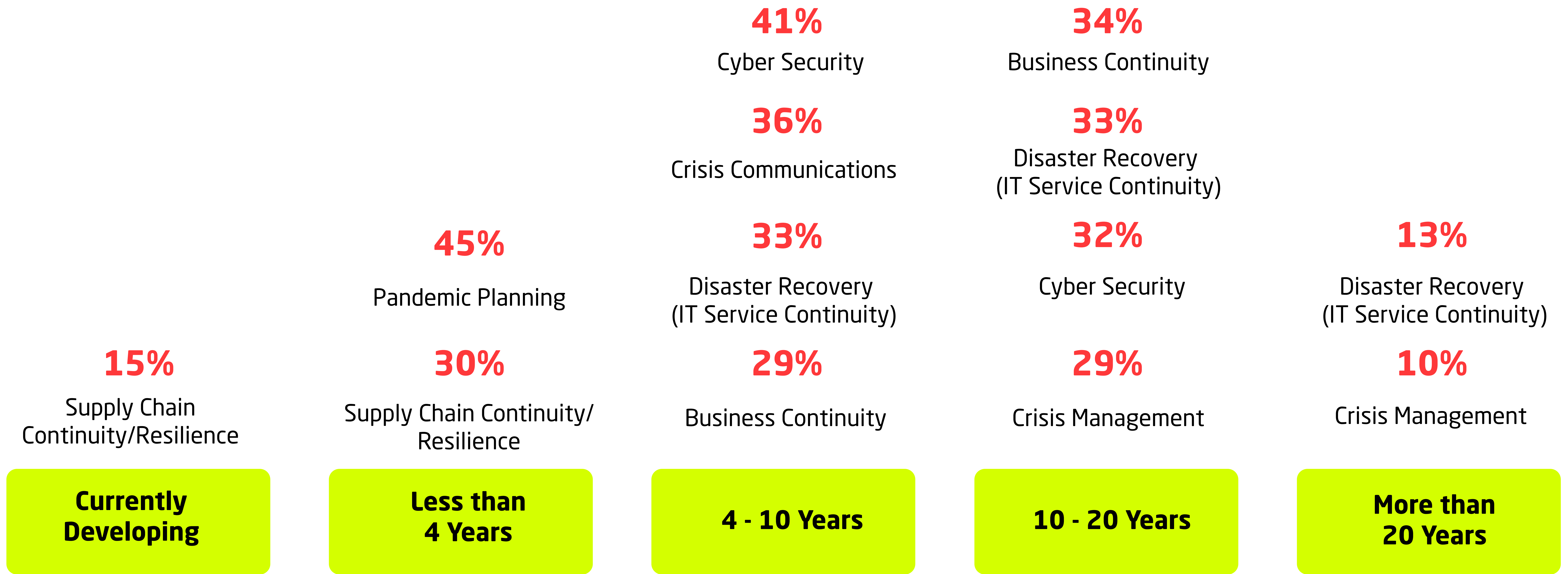
6%
IT Processes

41%
Business Processes

Equally Focused on

44%
IT & Business Processes

Length of Program Existence (With or Without Your Involvement)



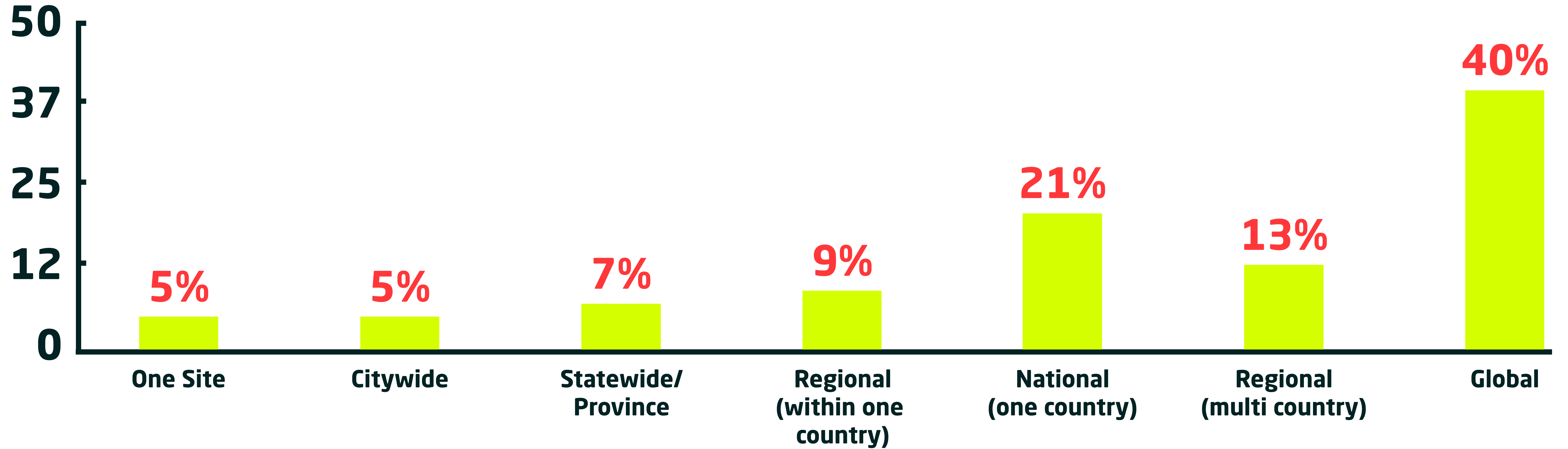
Program End-to-End Review or Refresh



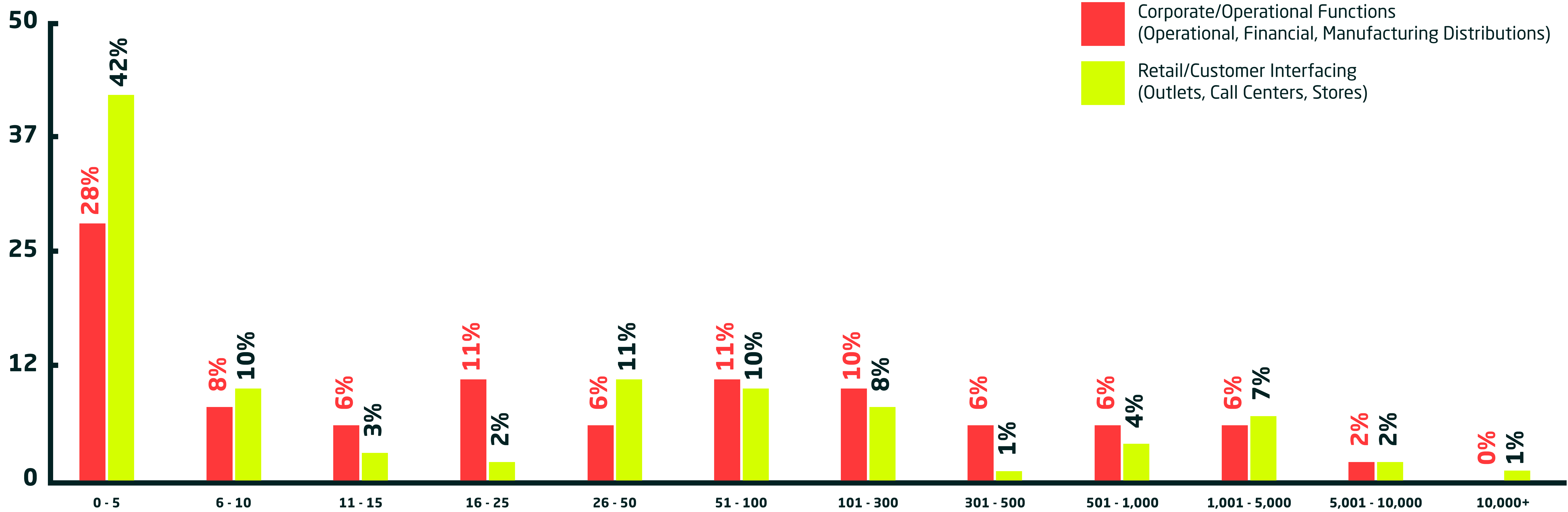
A woman with long blonde hair, wearing a white turtleneck and a black vest, stands in a meeting room, gesturing with her right hand as if presenting. She is smiling and looking towards the audience. In the foreground, the backs of several audience members' heads are visible, including a man in a grey suit jacket and a woman with long dark hair. The background is a plain white wall. The image is overlaid with a semi-transparent dark grey filter and features bright yellow diagonal accents in the top-left and bottom-right corners.

PARTICIPANT CHARACTERISTICS

Organizational Distribution

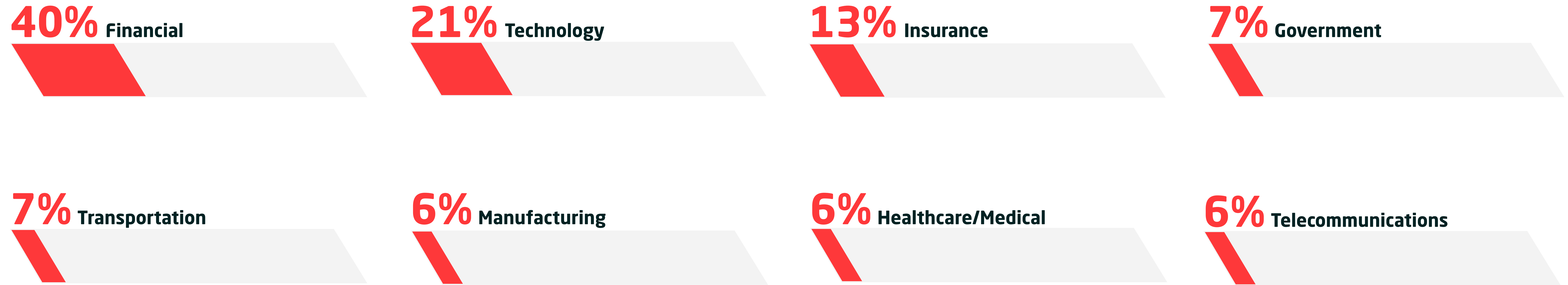


Number of Organizational Locations



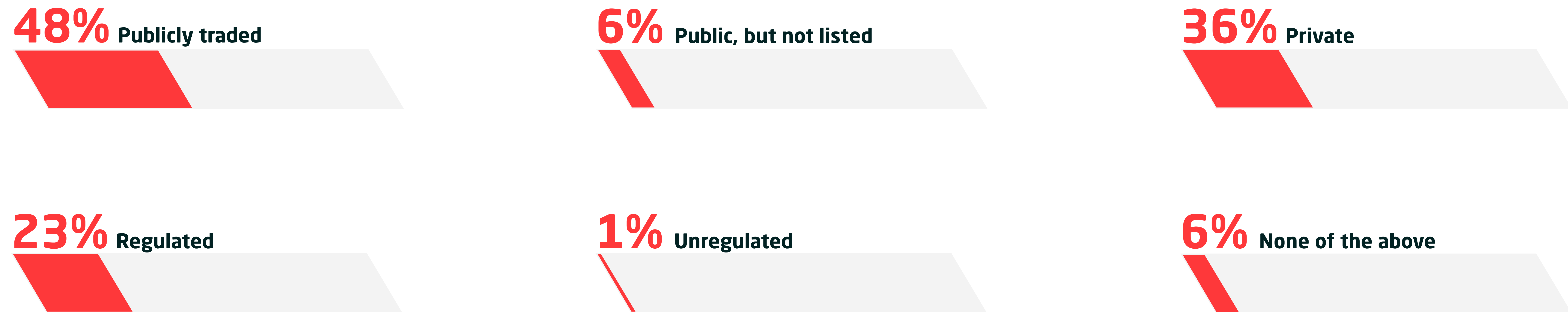
Industry - Top Industry Responses

Sum exceeds 100% due to multiple selections.

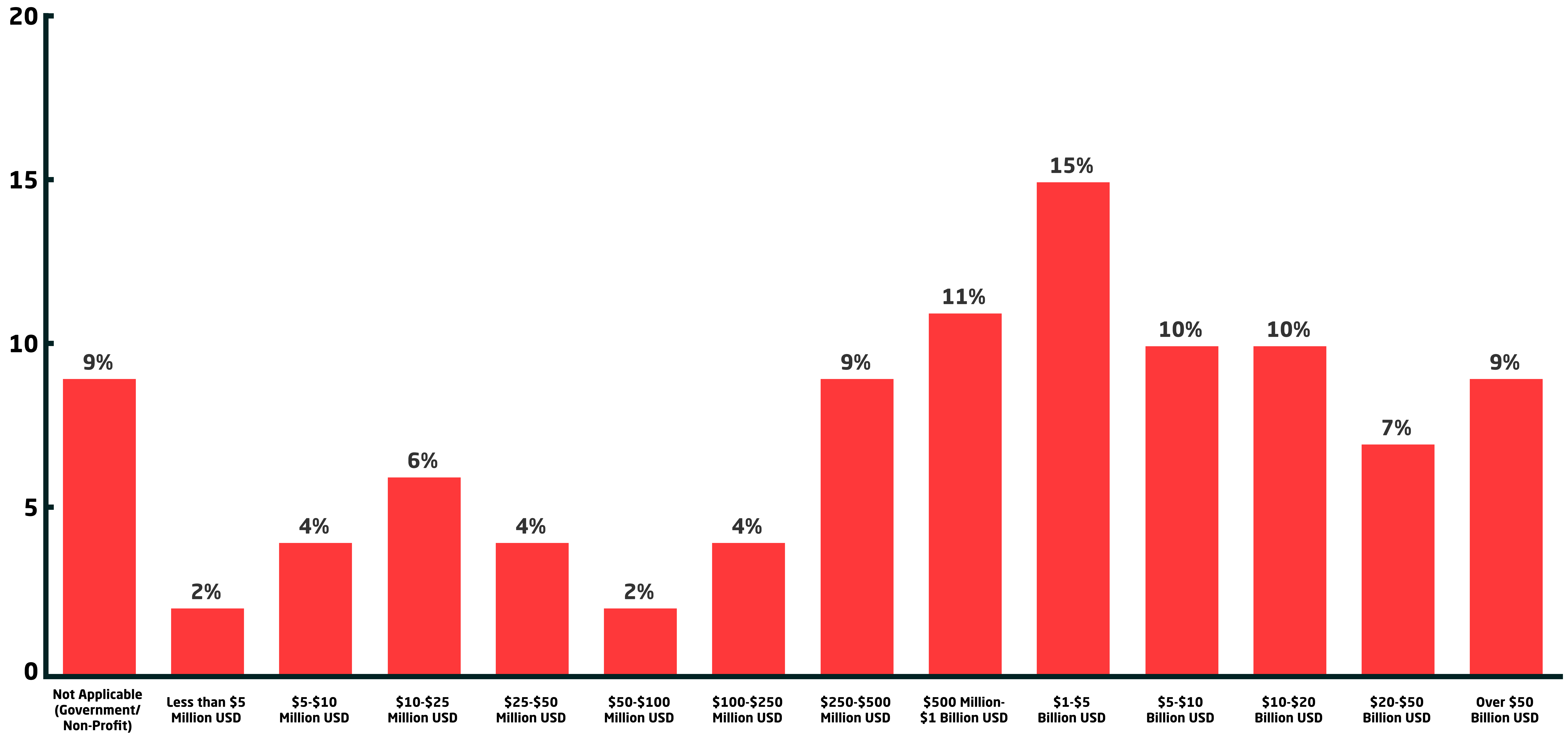


Organizational Classification

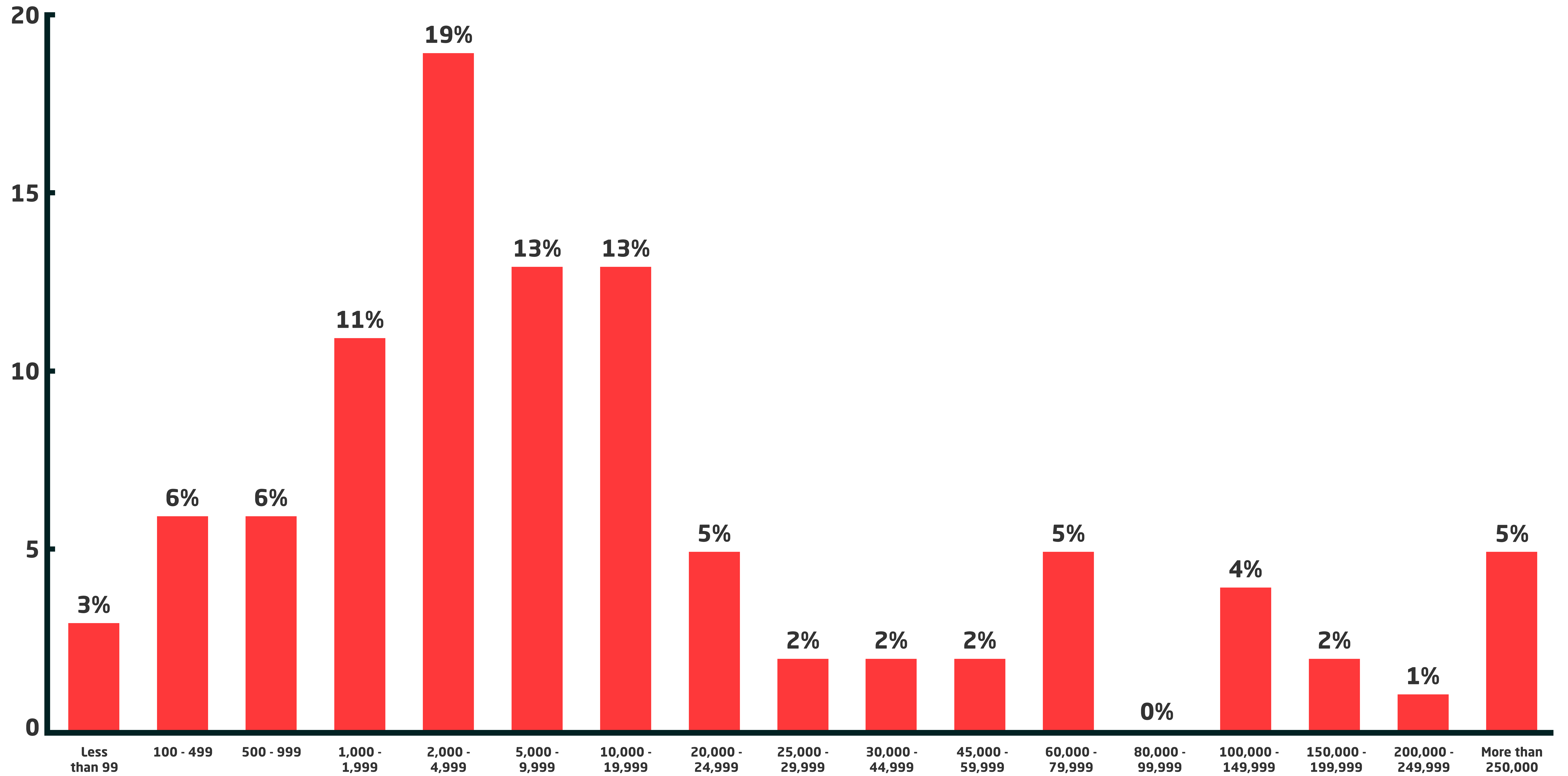
Sum exceeds 100% due to multiple selections.



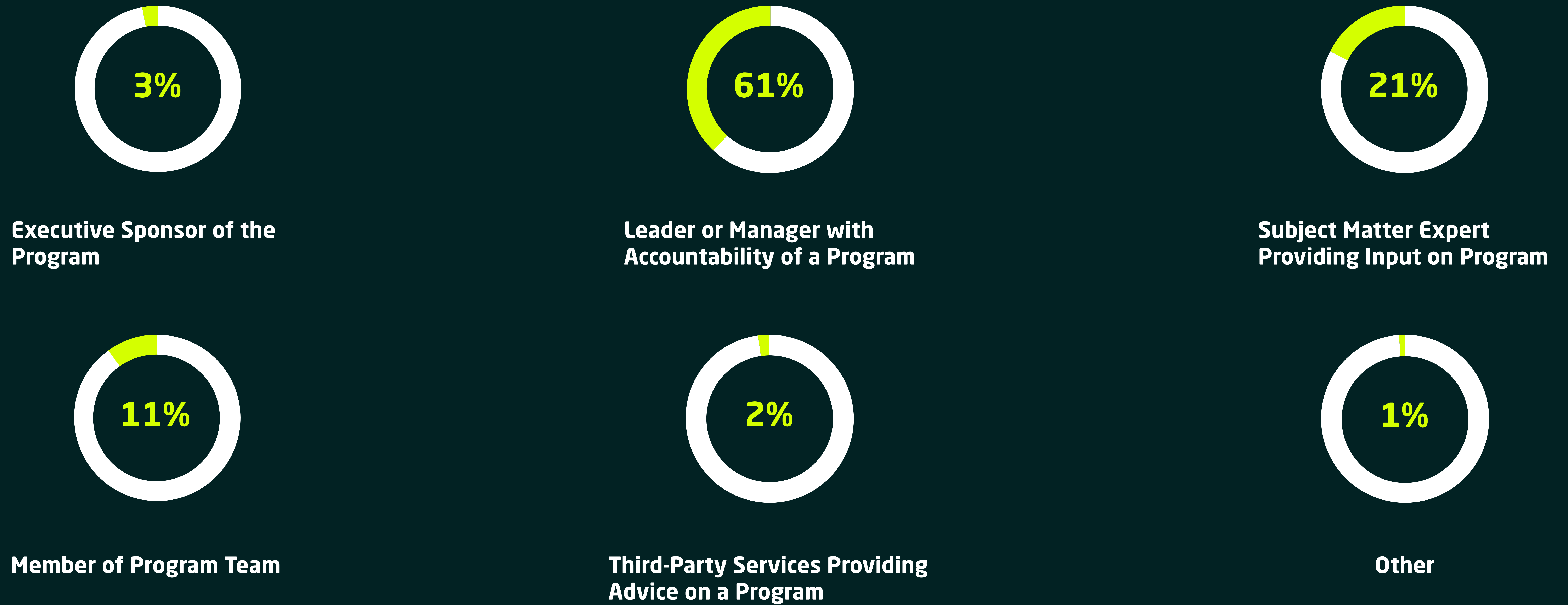
Organizational Revenues (Annual Gross Revenues - USD)



Number of Employees

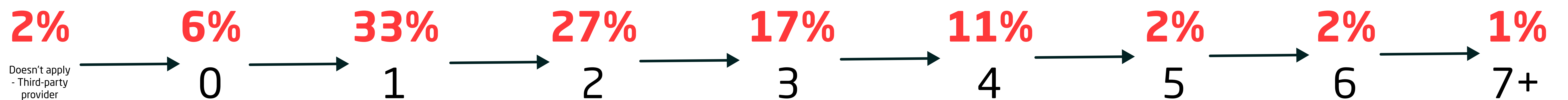


Current Role



Level of Separation from Executive Management

Number of people between you and the executive team.



A close-up photograph of a person's hands holding a silver pen over a financial report. The report features various charts, including a bar chart on the left and a pie chart at the bottom. The text 'BCM RESEARCH OVERVIEW' is overlaid in large, white, bold letters. The image is framed by a dark blue background with bright yellow diagonal accents in the top-left and bottom-right corners.

BCM RESEARCH OVERVIEW

Reporting History

Since 2001, BC Management has been gathering data on Business Continuity 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 Research Advisory Board. WorldAPP Key Survey, an independent company from BC Management, maintains the study and assesses the data collected. The study was launched on December 8, 2022, and it will remain open through August 30, 2023. 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

153

professionals participated in our 10th Edition Event Impact Management Study.

21

countries between December 8, 2022 to February 21, 2023. 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, **Canada (7%)**, France, Ghana, India, Indonesia, Ireland, Italy, Japan, Malaysia, Pakistan, Peru, Philippines, Saint Lucia, Saudi Arabia, Singapore, South Africa, Spain, United Arab Emirates, **United Kingdom (9%)**, and **United States of America (67%)**.

A top-down view of a meeting table with people, papers, charts, and sticky notes. The scene is dimly lit, with a bright yellow diagonal stripe running from the top-left to the bottom-right. The table is covered with various documents, including bar charts and line graphs. Several people are visible, some with their hands on the papers, suggesting an active discussion. There are also coffee cups, a laptop, and a smartphone on the table. The overall atmosphere is professional and collaborative.

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 (USA) - Director, Enterprise Resilience & Crisis Management, Microsoft

Jennie Clinton understands the unexpected. She has been involved in the business of risk management, business continuity and crisis management for more than 20 years. Jennifer is uniquely qualified in her field not only due to her diverse Fortune 500 experience, but from her hands-on involvement in managing teams during the crisis. She has successfully managed response efforts for COVID-19, major product recall, power outages, hurricanes, floods, and terrorist attacks across North America.

Jennie's expertise is the design, implementation and management of innovative and effective enterprise-wide programs related to risk management, disaster recovery and business continuity.

Jennie has a proven ability to customize risk management, crisis, and business continuity programs for a variety of industries with diverse corporate cultures and strategic imperatives. Her expansive theoretical and experiential perspective allows her to be masterfully adept at preparing organizations for the unforeseen. She is a frequently requested speaker at local and international conferences, as well as an active member of several government, risk management and business continuity boards and organizations.

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.

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.

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.

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 in front of a wall covered in sticky notes. The image is partially obscured by a bright yellow diagonal graphic element in the top-left and bottom-right corners. The text 'DISTRIBUTING ORGANIZATIONS' is overlaid in the center in a bold, white, sans-serif font.

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



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.



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.



The Hidden 60,000

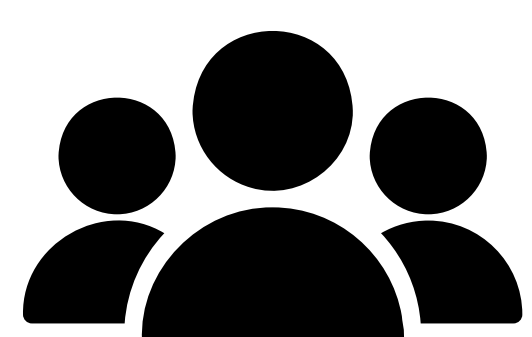
We have the largest network of passive resilience management candidates in the world! Many won't be found actively looking for a job or on LinkedIn.



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
CONTACT US



info@bcmmanagement.com