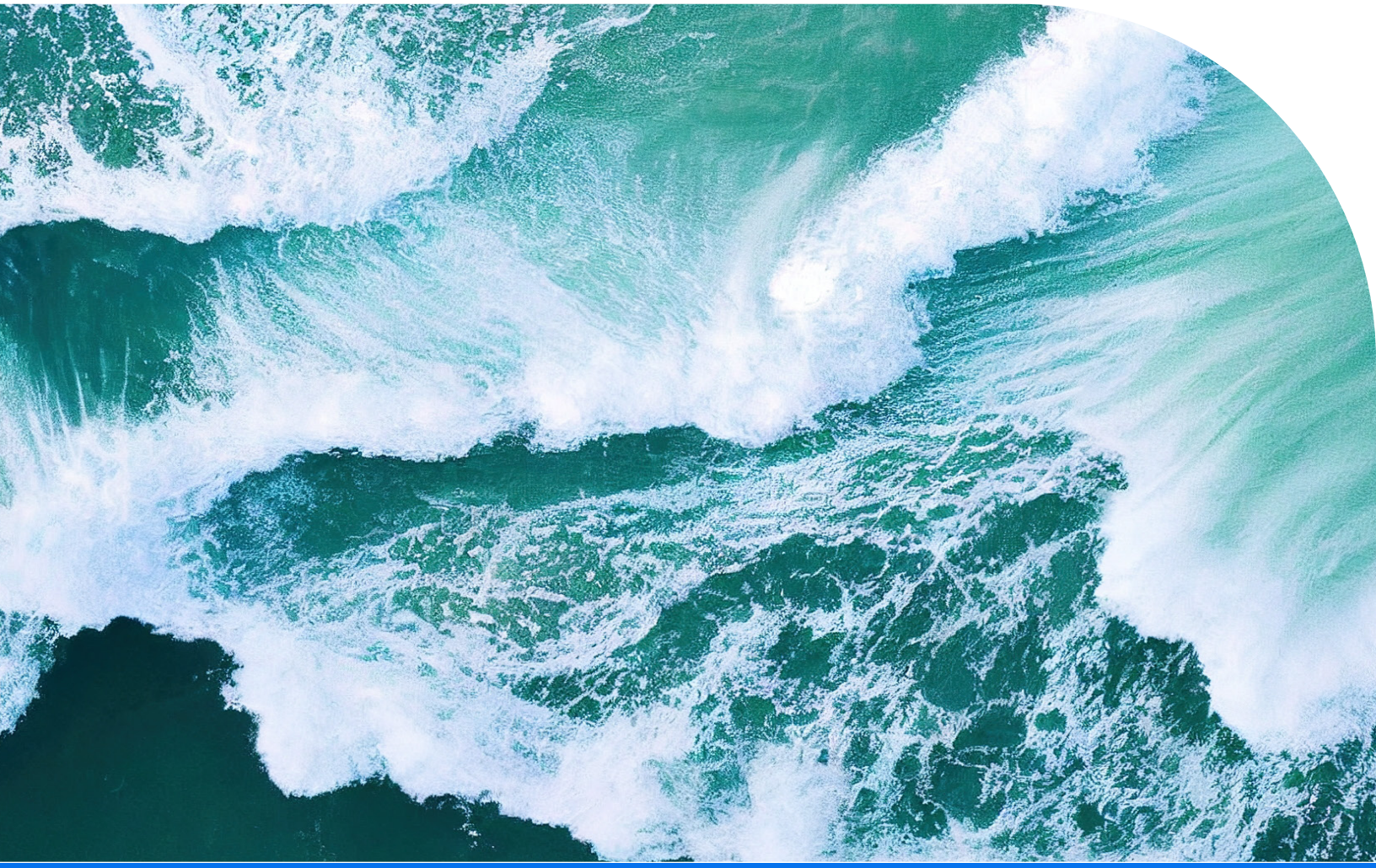
infiniteblue



2024

Global Enterprise Resilience Report:

When Forces Collide

infiniteblue.com

Introduction.

For resilience professionals, this is a watershed time that requires a new way of looking at the challenges ahead and what we can do to help our companies and communities prepare.

This new era is being driven by at least two global forces. First, the world is becoming increasingly interconnected and interdependent. Communications, supply chains, manufacturing, transportation, healthcare, financial services, government, public safety, and media are all a part of a sophisticated, tightly connected web.

Although this phenomenon has been evolving over the past several decades, recent advances in the Internet of Things, telehealth, e-commerce, geographic information systems, and dual-use (civilian and military) technologies, among others, have rapidly accelerated the transition.

While this level of interconnectedness brings many benefits, such as greater efficiency, lower costs, and economic growth, it has changed the risk landscape for public and private sector organization. Today, with very little warning, one disruption may have a domino effect across sectors, nations, and geographies.

Second, the volume and severity of incidents is increasing furiously. Consider:

- In September, the number of ransomware attacks was 153% greater than the year prior.
- In the last three years, the U.S. experienced an average of 20 billion-dollar disasters annually, up from 12.8 billion-dollar disasters per year in the 2010s and 6.7 billion-dollar disasters per year in the 2000s.
- 2023 is poised to be the hottest year in human history, breaking a record set in 2016.
- The world is experiencing a surge in civil unrest, with global incidents rising 3% in the past year to 30,376.
- As the U.S. approaches the 2024 election, the risk of significant unrest in many parts of the country will increase and, according to one survey, a growing number of Americans support political violence in an effort to save the United States.
- Workplace violence is on the rise. Forty percent of healthcare workers experienced violence on the job in the last two years.
- According to the Congressional Research Service, since 2000, the annual average of acres burned by wildfires has doubled since the 1990s.

As these two forces collide, the challenge for enterprise resilience professionals is growing more complex. In particular, organizations no longer have the luxury of planning for individual incidents. They must now prepare for multiple concurrent or cascading business disruptions.

Some refer to this as "layered" crises, or "polycrises," where the "shocks are disparate, but they interact so that the whole is even more overwhelming than the sum of the parts."

For example, as COVID took hold in 2020, supply chains broke, the economy faltered, civil unrest spread over racial tensions, 58,258 forest fires charred more than 10 million acres, and cybercriminals attacked Marriott, Twitter, and more than 1,000 other organizations.

Was this a bad year? Or a new normal?

The evidence suggests that we must plan for the latter.

To achieve true resilience in this environment, organizations must focus less on what can go wrong and more on building a flexible approach that will allow them to respond to anything. This entails at least two prerequisites:

- Highly accurate data about its people, operations, finances, vendors, and other assets.
- A clear understanding of the interconnections within an organization – how when one part of the organization is disrupted, other functions are impacted.

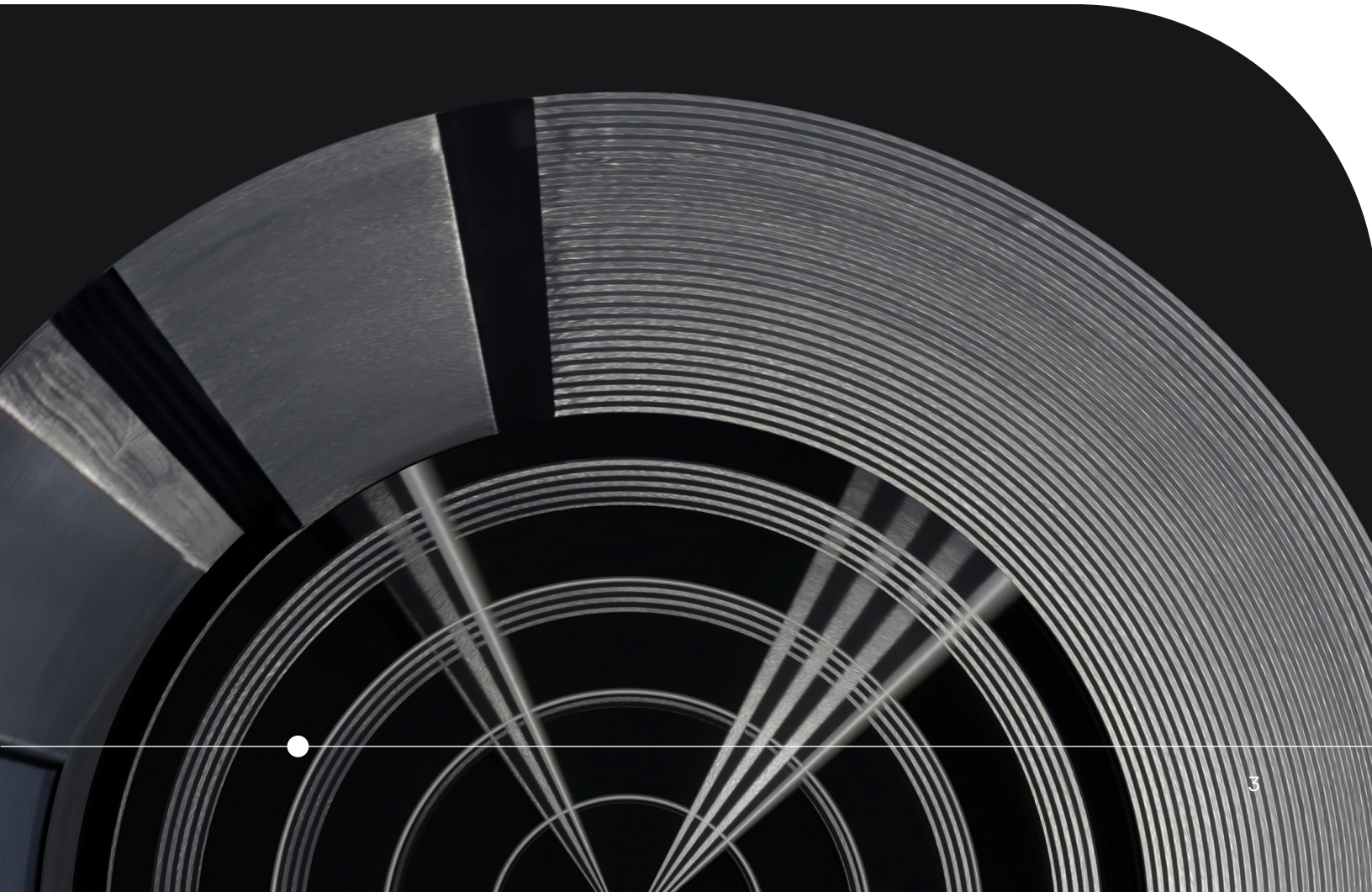
If these are met, when an incident does occur, resilience and security teams will immediately know all downstream impacts and how to respond to mitigate or avoid harm.

Are we ready?

To benchmark the industry's level of preparedness for polycrises, resource allocation, and outlook for the future, Infinite Blue conducted a survey of 130 resilience professionals. Survey respondents held senior roles in their companies and were generally experienced leaders. Twenty percent were VP level or higher and 60 percent had more than 10 years in business continuity and disaster recovery (BC/DR) roles.

And although they represented more than 20 industries, 68 percent agreed that they expect more disruptions over the next 24 months than the previous period.

Although they cited a variety of disruptions, 44 percent ranked an economic downturn and/or market disruptions as their greatest threat. Roughly one quarter (23.4%) said natural disasters were their top concern, followed by supply chain disruptions (15.6%).



infiniteblue

Buy in.

According to the survey, organizations generally recognize that they must make investments to successfully navigate this environment. Sixty-one percent of respondents either strongly agreed (36%) or agreed (25%) that their “organization understands the importance of BC/DR and resilience programs.” Similarly, 53 percent of respondents said they either strongly agreed (29%) or agreed (24%) with the statement that their “organization is investing the necessary resources to develop and maintain programs to prepare you in the event of a significant business disruption.” In fact, only four percent strongly believed that the necessary resources were not being committed.

Missed opportunities.

Despite the level of corporate buy-in for resilience initiatives, the effectiveness of these investments and programs varied. In particular, three areas of concern emerged:

Engaging vendors. Although nearly every organization relies on third parties for supply chains, information technology, call centers, fulfillment, logistics, or other essential services, only 21 percent of respondents said they fully engage critical vendors and suppliers in planning and exercises. A quarter said they didn't involve vendors in these activities at all.

Predicting impacts. As soon as an incident is detected, effective resilience programs are able to predict potential impacts. When the National Weather Service determines that a hurricane or tornado is likely to make landfall, it issues a cone of impact, also referred to as a cone of concern. This shows the likely path of the storm and allows communities to prepare, issue evacuation orders, preposition supplies, minimize impact, and respond more effectively.

Corporate resilience programs should strive to have the same ability to predict likely impacts for all types of disruptions. This allows resilience professionals to manage incidents, not react to them. Yet, fewer than half of respondents (45%) said their programs enabled them to see and understand downstream and upstream impacts of incidents before they occur.

Collaborating across the enterprise. Security and resilience departments cannot effectively operate in a silo. Teams across the enterprise must be engaged in planning for and responding to incidents. Although corporate leadership may see the value in BC/DR investments, fewer than half of all respondents (48%) said that "people and departments across the organization are properly engaged in BC/DR and resilience planning." Despite buy-in and resources, this type of compartmentalized program often leads to less-than-optimal responses.

It's tough to prepare for everything all at once. You need to change your mindset regarding what actually touches the organization.

Jeff Reider
VP, Global Threat and Crisis Management, Paramount

Rethink resilience.

Organizations seeking to adapt to today's threat landscape should consider adopting the following strategies:

Adopt All-Asset/All-Hazard Thinking. Organizations that have been diligent about drafting plans and testing scenarios must now shift their thinking toward a **comprehensive and flexible framework that can be applied to various types of disruptions – individually or concurrently. It involves setting roles of individuals and departments that would apply during any type of incident, a well-defined strategy for communications and alerts, exceptional data management, and dynamic processes.**

But here's what they must avoid: Increasingly complex plans that attempt to account for every eventuality. These frustrate teams during an incident and are frequently set aside. Plans used for an exercise or simulation are often not relevant in a crisis – or polycrisis.

Shift your mindset from prevention to resilience. In the past, business continuity personnel focused on risk identification and prevention: "How can we prevent it from happening?" This was soon followed by planning: "How will we respond once it happens?"

Today, however, it is no longer possible to identify and plan for every event – or every combination of events. As such, organizations must focus on resilience: "How can we prepare, absorb, recover, and bounce back quickly from any event, and adapt so we are more equipped for the future?"

> **The goal of crisis management is not to not have any crises. It's to be effective at responding to them.**
>
> *Jason Veiock*
> *Security and Resilience Expert*

From a whole society perspective, [resilience] is about public and private [sectors] working together and taking a strength-based approach to planning rather than planning in silos.

Joel Thomas
CEO, Spin Global

Collaborate at all levels. A resilience program cannot function effectively in a silo. It takes the coordinated engagement of teams and departments enterprise-wide, as well as critical vendors.

However, in an environment of multiple concurrent incidents, internal collaboration alone is not enough. Engaging in community planning efforts – and establishing local and regional connections – is essential. This must be done in peacetime. Effectively establishing lifelines beyond your organization **will lead to resource and information sharing and more coordinated, comprehensive, and effective responses.**

Consider, for example, how a significant weather event not only impacts businesses in the storm's path but also the homes of employees and customers and local infrastructure. By working together, businesses, government entities, and community organizations can develop strategies that build long-term resilience to recurring and emerging threats to the community or region.

Look beyond traditional sources. While interviewing resilience practitioners to conduct research for this report, one experienced professional highlighted how ChatGPT and other public artificial intelligence platforms can help a company conduct research for business plans, understanding changing regulatory requirements, identifying potential downstream impacts, and for other purposes that can save time and money and improve responses. However, because these technologies are still in their infancy and the problem of "hallucinations" has not yet been fully resolved, these sources should be considered a starting point.

Build the capability to predict impacts. Now more than ever, it is essential to see the cone of concern as soon as an incident is detected. When concurrent incidents emerge, understanding the potential overlap will allow the most efficient allocation of resources to respond.

At the earliest indication of an event, resilient companies seek to answer:

- What does this mean for our customers?
- What must we do to protect employees?
- Can we reposition assets and employees to avoid damage and enable us to recover faster?
- What organizations in our community should we engage?
- What regulatory considerations can we get ahead of?

These are all questions that can be answered sooner – and to greater effect – if an organization has the ability to foresee how an incident will impact its people and operations.

Conclusion.

According to the survey of resilience professionals conducted by Infinite Blue in November 2023, 43 percent cited economic factors as the greatest risk to their enterprise. In the subsequent weeks, the economic news has been increasingly positive, and the Federal Reserve has indicated that, after months of interest rate increases, a soft landing appears more likely. Twenty-three percent of respondents rated natural disasters as their highest concern, and 15 percent cited geopolitical risk.

And while each of these incidents have the potential to disrupt organizations, communities, and governments, the likelihood remains that many companies will face a polycrisis scenario with compounding impacts.

Although companies have been designing, implementing, and refining BC/DR programs for at least three decades, today's challenges require new thinking.

Operating models have evolved. Organizations are more global, workforces are more diverse and dispersed, supply chains are more complex, and we are much more technology dependent.

Threats have also become increasingly severe, frequent, and, in many instances, impossible to prevent. A single bad actor on the other side of the globe can now disrupt a business or the economy of a city or region in the U.S.

Planning for every potential crisis or polycrisis is no longer feasible, and building higher castle walls is not effective. Disruptions are inevitable and unpredictable, and organizations must have a flexible, dynamic approach that enables them to respond to anything and, in doing so, achieve true enterprise resilience.

Potential Incidents, 2024-2025	Likely Impacts	
Geopolitical tensions In Ukraine, Middle East, the South China Sea, or Korean Peninsula; potential large-scale migrations.	• Supply chain disruptions • Market closures • Manufacturing disruptions	• Loss of life • Cyberattacks
Economic event or downturn Including asset bubble burst, bank failures, or real estate market shock	• Supply chain disruptions • Market closures • Financial pressures	• Workforce challenges • Cyberattacks
Domestic political upheaval Potentially related to the 2024 election or a variety of pending legal proceedings involving public figures.	• Supply chain disruptions • Loss of life • Market closures	• Manufacturing disruptions • Workforce challenges • Cyberattacks
Weather events Particularly in the Gulf states.	• Supply chain disruptions • Loss of life • Market closures • Manufacturing disruptions	• Loss of power or comms infrastructure • Workforce challenges
Forest fires Most prevalent in the west.	• Supply chain disruptions • Loss of power or comms infrastructure • Loss of life	• Market closures • Manufacturing disruptions • Workforce challenges
Cyber incidents Across all industries, particularly healthcare and financial services.	• Brand harm • Loss of data or systems • Supply chain disruptions • Loss of life	• Market closures • Manufacturing disruptions • Workforce challenges
Act of terrorism Most likely in a major urban area.	• Supply chain disruptions • Loss of power or comms infrastructure • Loss of life	• Manufacturing disruptions • Workforce challenges • Cyberattacks
Disruption to the nation's infrastructure Including the energy grid, communications network due to a cyber or terrorist attack.	• Supply chain disruptions • Manufacturing disruptions	• Workforce challenges
Localized civil unrest Due to mass shootings, police violence, or racial tensions.	• Supply chain disruptions • Loss of life • Market closures	• Workforce challenges • Cyberattacks

About Infinite Blue

For more than a decade, Infinite Blue's team of innovators and experts in risk, technology, business continuity and disaster recovery, supply chain, and operations have been helping organizations not just weather storms but also to emerge more informed and synchronized than ever. Today, 4 of the Fortune 10 and other respected companies worldwide trust Infinite Blue's total enterprise resilience solutions.

infiniteblue

infiniteblue.com