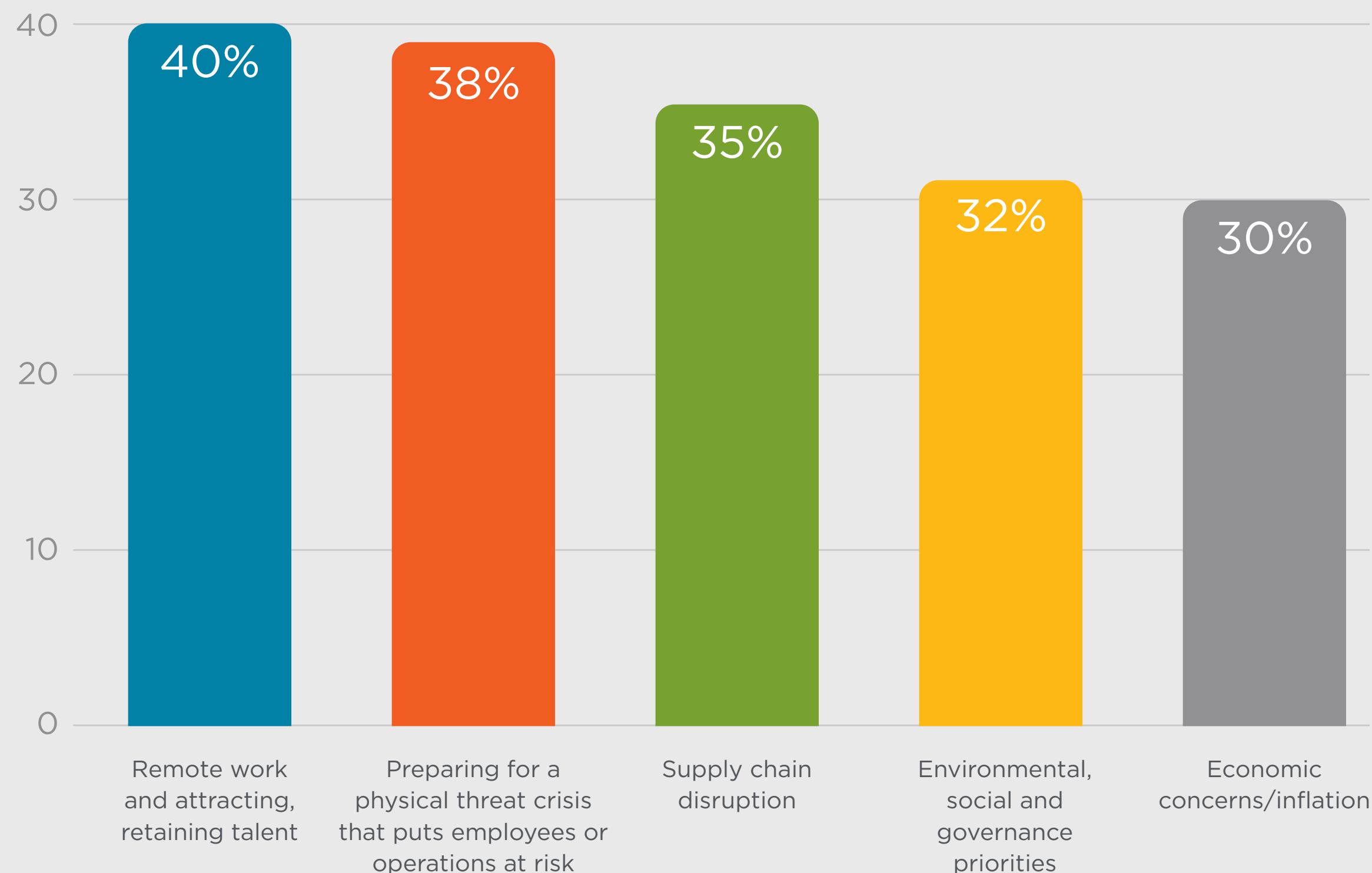


Today's Leaders Acknowledge the Reality of Physical Threats

Almost every CEO surveyed has dealt with at least one physical threat in the last three years, and none believe their organization will avoid one in 2023. Perhaps that's why more CEOs have noted that preparing for them is now a top priority (38 percent) — even more than those prioritizing economic inflation (30 percent).

The question is: How are they preparing, and do they have enough resources to prepare adequately?

Top 2023 Priorities of CEOs Surveyed



Leaders Need to Be More Involved in Mitigation Strategies

While most CEOs say they had some strategy in place when a crisis hit, 62 percent reported it had only some or little to no effect on mitigating the impact, and only 42 percent had a plan and updated it after an incident occurred.

Despite there being some kind of strategy in place, more than half (60 percent) of CEOs have no plan to address all the most severe physical threats to their business. For almost half (46 percent), this lack of preparation means they have identified and planned for only some of the threats to their organizations. That means their businesses are at risk.

For instance, only 37 percent said they have a plan for extreme weather. Only 29 percent have a plan for infrastructure failure, and the number drops even lower to 25 percent for a plan to handle transportation accidents. These are the same critically rising threats our data revealed for 2022, bringing to light the gap between the level of risk and proactive preparation.

“An effective crisis mitigation strategy begins well before a crisis actually occurs. The real work is in the preparation and planning that happens beforehand. At Banc of California, it’s critical that our executive leadership team stay in lockstep with our risk management and business continuity teams from the very start of the risk planning process. With physical threats on the rise, we are deeply focused on ensuring our employees and clients remain safe and prepared for anything that comes our way.”

- Joe Arnett

Senior Vice President, Business Continuity Planning, Banc of California



60%
of CEOs have no plan to address all the most severe physical threats to their business.

What physical threats are top of mind for business leaders across industries and regions of the U.S.?

Around the country, CEOs from different industries highlighted top concerns — from infrastructure failure and public health to extreme weather and crime.

Top Perceived Threats: Industry Breakdown

Industry	Threat	Percentage of CEOs
Financial Services	Infrastructure Failure, Public Health	44%
Healthcare	Extreme Weather, Public Health	39%
Legal Services	Crime, Transportation Accidents	39%
Manufacturing	Infrastructure Failure	36%
Retail/Wholesale	Public Health	48%
Utilities	Extreme Weather	60%

Top Perceived Threats: U.S. Regional Breakdown

Region	Threat	Percentage of CEOs
Northeast	Extreme Weather	36%
Midwest	Infrastructure Failure	53%
South	Crime	52%
West	Public Health	49%

Lack of C-suite Urgency, Despite Employee and Board Concerns

The varied states of physical threat crisis planning, or lack thereof, aren't going unnoticed outside the C-suite.


Employees are concerned. Just over half of CEOs surveyed (51 percent) said their employees share more concerns about physical security since the onset of the COVID-19 pandemic. However, in a 2022 OnSolve study of more than 600 employees across industries ranging from healthcare to finance to retail, most respondents only felt minimally confident in their employer's ability to keep them safe.

Forty percent of CEOs said remote work and attracting and retaining talent are top priorities. To accomplish this goal, executive leaders must pay attention to employee concerns and appropriately prepare for physical threats.

Additionally, corporate boards are on high alert about physical threats and their cascading implications on the business. Almost all (99 percent) boards have asked their top executives about plans to combat physical threats.

While it was not surprising that a majority of CEOs (78 percent) delegate crisis management responsibilities, 18 percent admitted they don't have anyone in the C-suite overseeing physical security and duty of care. Of those CEOs who indicated they have a plan, 23 percent indicated they have not personally reviewed it.

The ownership gap needs to be filled.



51%
of employees are more concerned about physical security since the COVID-19 pandemic.



Disclosing risks has been a longstanding practice for both public and privately traded organizations. In the past several years, there has been a heightened focus on what happens beyond exposure. **Never before have organizations been more focused on their ‘duty of care’ to the business and shareholders.** Geopolitical, cyber and physical threats pose potential and actual financial exposure and create an interruption in an organization’s ability to execute. This has created a heightened expectation for understanding, preparedness and readiness around corporate risks and structures. It’s no wonder why managing physical threats has now become a boardroom priority. To create trust and instill confidence across their broad business ecosystem, leaders must prove they have strong prevention plans in place and show how they are prepared to mitigate the impact of all categories of risk.”

– Mike Mayoras

Board of Director at EPAM Systems Inc. (NYSE:EPAM), Softeon and OnSolve

Proactive Preparation Is a Competitive Advantage

Given the potentially devastating effects of physical threats, proactive crisis planning creates a competitive advantage. Achieving this edge will take rethinking traditional Return on Investment (ROI) in favor of seeing threat mitigation as Return on Resilience Investment (RORI).

CEOs often sanction investments based on a tangible financial return. If they believe a threat is unlikely to happen, they're less likely to dedicate a portion of the budget to planning and mitigation. However, with physical threats rising in multiple categories, what once may have been unlikely is now inevitable.

RORI measures the ability of an organization to anticipate, absorb and recover from hazardous events. For example, if executives prioritize investing in a strong backup generator, when the power goes out, their business won't experience operational downtime. If they invest in alternative supply chain modes or routes, their customers won't experience significant delays in deliveries should a storm impact a supplier's production or a major logistics route.

Ultimately, when CEOs take the lead to prioritize minimizing disruption — while setting their business up for recovery in the face of physical threats — the business will save time and resources, which results in a return on their investment. Also, they'll be one step ahead of competitors who are most likely inadequately prepared when a threat strikes.



When CEOs take the lead to prioritize minimizing disruption, the business **will save time and resources.**

The C-suite Should Take a Cue From Cybersecurity

Traditionally, business leaders have prioritized and planned for cyber threats. According to [Deloitte's 2023 Global Future of Cyber Survey](#), 70 percent of survey respondents said cyber was regularly on their board's agenda, either monthly or quarterly. In addition, 86 percent of respondents reported that cyber initiatives made a significant, positive contribution to at least one key business priority. This tells us that cybersecurity is already a C-suite dialogue and proves a safety strategy works when it comes from the top.

As physical and cyber threats continue to intersect, leaders need to invest in holistic planning, processes and technology. OnSolve data shows that 93 percent of CEOs believe technology would help protect their employees and operations from physical threats. However, only 26 percent of CEOs say they've invested in technology for that purpose (though an additional 48 percent are prioritizing such an investment this year).

In the same way cybersecurity leaders have leveraged technology to create better visibility into a cyber incident, AI-powered technology can predict the direct impact of an organization's physical threats and vulnerabilities, forecasting the cascading effects that could materialize.



93%
of CEOs believe
technology would
help protect
their employees
and operations.

The New CEO Mandate: Ensuring Crisis Ownership Across the C-suite

Today's risk landscape requires a new mandate for CEOs. They must take the lead in initiating the dialogue across the C-suite about crisis mitigation and ownership. Here are three steps for CEOs to stay ahead of today's evolving risk landscape.

STEP ONE

Broaden awareness of risk beyond cyber to physical threats.

Business leaders must understand that physical threats are increasing, the impact is significant and employees are concerned. Planning cannot be delegated or managed in silos. It should involve the entire executive team.

The consequences of any unchecked threat should raise the eyebrows of all executives: unexpected operational downtime, product loss, customer churn, reputational damage, broken vendor or supplier relationships, harm to employees and loss of investor or market confidence.

Understanding an organization's risk landscape is part of the prioritization process. CEOs and their C-suite counterparts should start a dialogue with their teams to identify the most prominent threats in each business function and assess how that risk could materialize and cascade.

STEP TWO

Work together to create a holistic mitigation approach.

Once top risks and impacts are at the forefront of C-suite priorities, leaders should create a strategy that includes prevention and mitigation plans. It's critical that executives have complete insight into the ripple effect from all threats across their businesses and that roles and responsibilities are defined.

Taking lessons learned from the COVID-19 pandemic and cybersecurity plans, CEOs must bring the C-suite to the table to create a dialogue on mitigation strategies.

As for a CEO's role in crisis mitigation plans, they should be involved in as many actions as possible that require their approval. For example, a CEO may be the only one in the company who can pre-authorize overtime or provide access to emergency funds. Identifying these situations in advance helps avoid bottlenecks when time is critical.

The crisis mitigation strategy must be as dynamic as the threat landscape itself. It should:

- Take into account dynamic risk and how one threat can quickly cause another.
- Consider today's hybrid work environment and tailor crisis plans accordingly.
- Incorporate time for debriefing sessions once the crisis has passed to ensure the strategy is updated.
- Set benchmarks for improvement.

Leaders need real-time data to stay informed of current and impending risk. Manual processes cannot keep up with today's risk environment.

STEP THREE

Invest in intelligent technology solutions.

Leaders need real-time data to stay informed of current and impending risks. Manual processes cannot keep up with today's risk environment. Modern risk intelligence solutions can optimize and centralize the data needed to keep leaders informed and mitigation strategies effective. Powerful artificial intelligence (AI) automatically sorts through risk information in real time, with minimal error and maximum relevance, to help determine when a contingency plan should be implemented.

Critical communications technology is also essential to delivering targeted alerts to specific groups and teams via mobile app, SMS, email, desktop and phone. A loss of communication in a crisis can leave employees, customers and teams vulnerable and in the dark.

With a technology solution that can more efficiently and expeditiously analyze risk, executives have a clearer, more accurate view of real-time threats to their business. They can avoid the expenditure of resources necessary for manual risk assessment. Also, with an accurate picture of their risk landscape, executives will realize ROI and RORI in the event of a crisis. As a result, they will minimize loss of productivity and customer impact, drive operational uptime and safeguard market reputation.