ONSOLVE®

2023

OnSolve Global Risk Impact Report

onsolve.com

Table of Contents

“Up to 10 physical threats **can occur every minute**.”

— 2023 OnSolve Global Risk Impact Report

Introduction

A **tropical storm’s high winds** cause power outages that bring operations to a sudden halt. Dips in voltage damage a manufacturing plant’s controllers and work in progress, which creates a faulty product. Work-from-home employees face internet outages from the storm and customer support goes offline.

A **blizzard** on a major national highway halts traffic, stranding drivers in freezing temperatures for more than 20 hours. Travelers are unable to reach their destinations, many are at risk of hypothermia and medical emergencies as they run out of fuel and rescue teams are unable to reach them.

A **protest** a few blocks from a bank’s headquarters worries onsite HR teams and employees feel unsafe leaving the office.

Physical threats such as these are becoming more common and more interconnected, according to the latest OnSolve® research.

Physical threats also cost many organizations millions of dollars. According to the National Oceanic and Atmospheric Administration, damage from weather and climate disasters rose nearly 10 percent, from $156 billion in 2021 to over $171 billion in 2022, with numbers continuing to climb.

In support of this year’s Global Risk Impact Report, data was analyzed from OnSolve Risk Intelligence stemming from more than nine million global events from January 1, 2021, to December 31, 2022, that had the potential to impact customers worldwide. The analysis illustrates trends and identifies both known and emerging issues organizations face from physical threats.

Our risk intelligence data reveals a significant increase in infrastructure and technology failures, transportation accidents and extreme weather events in 2022 compared to 2021.

The growing frequency of physical threats and their devastating impact creates a renewed sense of urgency for every organization — but urgency alone isn't enough. Our report reveals how finance, staffing and operations are all negatively impacted when hit with a crisis. Getting ahead of the increasing ripple effect from these risks requires a proactive approach to planning, mitigation and response.

This proactive approach must be a C-suite conversation. In the same way senior executives were involved in responding to the COVID-19 pandemic, which impacted all aspects of the business, leaders are now asking for more insight into, and involvement in, crisis mitigation for other physical threats.

Despite the renewed sense of urgency, our data highlights that most organizations remain unprepared. To better understand how business leaders are dealing with increasing volatility uncovered by the risk data, OnSolve, in partnership with Censuswide, a leading global research company, surveyed 250 CEOs in the United States.

The survey found that even though nearly every participating CEO has dealt with a recent physical threat, most lack the knowledge, budget or strategic approach to manage them. Despite lessons of the past, evidence of the impact and pressure from a range of stakeholders, including boards of directors, most organizations are struggling to prioritize risk mitigation and crisis response.

> “Data reveals a **significant increase** in infrastructure and technology failures, transportation accidents and extreme weather events.”
>
> — 2023 OnSolve Global Risk Impact Report

Three Critically Rising Threats and Dynamic Risk

To properly prioritize physical threats, leaders need to know where to direct their attention. Our data shows that from 2021 through 2022, physical threats rose at an alarming rate across three key risk categories globally — infrastructure and technology, transportation accidents and extreme weather.

Threats by Percentage (2021 to 2022)

Risk Categories	U.S. Threats	Global Threats
Infrastructure and Technology	+807%	+688%
Transportation Accidents	+296%	+211%
Extreme Weather	+42%	+72%
Fire	+65%	+43%
Civil Unrest	-71%	+28%
National Security	-55%	+14%
Crime	-62%	-37%
Shootings	-64%	-48%
Public Health	-80%	-54%

When threats in these three risk categories materialize, business assets, employees and operations suffer. And it's not only the immediate consequences that are problematic. Every physical threat has the potential to cascade throughout (and devastate) an organization's operations, broader supply chain and market ecosystem.

In reality, the consequences of threats are often as unpredictable as the threat itself. These risks are dynamic, meaning the ultimate resulting harm (i.e., consequence) is different from the initially expected harm. This unexpected ripple effect can be one of the most challenging aspects of crisis preparation and management.

For example, a major nationwide retail chain experienced multiple arson attacks between 2020 and 2022. The fires immediately destroyed infrastructure and inventory, causing a two-week store closure — per store — and an estimated $2 million in lost revenue. Some of the locations contained pharmacies, creating a secondary impact. What began as primarily property damage cascaded into a scenario in which people couldn't get vital medicine. Millions in revenue were lost from the downtime, and pharmacy customers faced the difficult decision of sourcing medicine elsewhere.

We see similar situations in all three critically rising risk categories: Infrastructure and technology, transportation accidents and extreme weather. Each threat presents specific risks on its own. However, they're often interconnected.

Extreme Weather

Extreme weather such as floods can impair operations, disrupt supply chains and destroy company property. It also impacts employees' wages, as employees may be unable to get to work. Logistical and distribution disruptions are other common consequences. From 2021 to 2022, extreme weather events were up 42 percent in the U.S. and 72 percent globally. In the U.S., winter storms and blizzards were up 216 percent, while tsunamis (221 percent), flash floods (52 percent) and severe storms (138 percent) all increased in frequency.

Extreme weather in particular can have a catastrophic ripple effect in a very short period of time. In 2022, Hurricane Ian damaged thousands of homes and businesses in Florida, North Carolina and South Carolina. Reports at the time estimated that more than two million homes and businesses lost power. Many roadways were impassable, a causeway collapsed and, sadly, lives were lost.

Smaller storms can also have a significant impact, often leading to loss of productivity and business downtime. An isolated winter storm in Buffalo, N.Y., for example, caused nearly a week-long driving ban in December 2022, keeping employees from going into work and halting deliveries.

Extreme Weather Event by Global Percentage

Type of Extreme Weather Event	U.S. 2021 to 2022	Global 2021 to 2022
Earthquake	+945%	+1964%
Winter Storm/Blizzard	+216%	+303%
Tsunami	+221%	+166%
Severe Storm	+138%	+86%
Flash Flood	+52%	+49%
Tornado	+11%	+36%
Landslide	-59%	+22%
Flood	+24%	+20%
Volcano	+22%	+6%
Cyclone	-41%	-14%
Avalanche	-41%	-27%
Wildfire	-58%	-40%

Infrastructure & Technology

From 2021 to 2022, infrastructure and technology failures (including power outages) soared 807 percent in the U.S. (688 percent globally). This is an issue that is expected to increase.

"An estimated 70 percent of the nation's transmission lines are over 25 years old, and this aging infrastructure makes American communities, critical infrastructure and economic interests vulnerable," according to the White House.

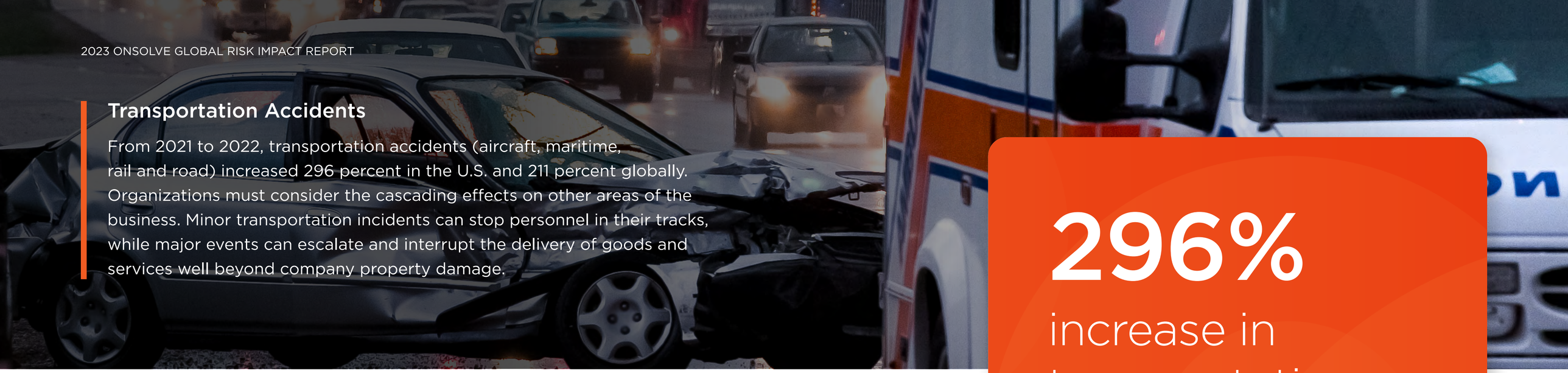
807%

increase in infrastructure and technology failures in the U.S.

From 2021 to 2022, infrastructure and technology failures, including power outages, rose for certain states such as Kansas (683 percent), Oklahoma (649 percent) and South Carolina (1716 percent). Similar issues continued in 2023 as heavy snow and strong winds caused more than 100,000 residents and businesses to lose power for days across several other states.

Infrastructure and technology failures are heightened as extreme weather increases. This means the dynamic risk from a blizzard now has a greater chance of extending beyond road closures into lengthy power outages. The impact to both communities and critical operations, not to mention nearby businesses within the area, is significant.

In addition to storm-induced infrastructure issues, power grid attacks are also becoming more frequent. The North American Electric Reliability Corporation estimates that attacks rose 71 percent in 2022 compared to 2021 and are expected to continue to increase in 2023.



Transportation Accidents

From 2021 to 2022, transportation accidents (aircraft, maritime, rail and road) increased 296 percent in the U.S. and 211 percent globally. Organizations must consider the cascading effects on other areas of the business. Minor transportation incidents can stop personnel in their tracks, while major events can escalate and interrupt the delivery of goods and services well beyond company property damage.

296%

increase in transportation accidents in the U.S.

Consider the February 2023 train derailment in East Palestine, Ohio. It continues to affect an entire region. According to reports, the trains were carrying hazardous materials, such as vinyl chloride, that leaked after the crash and caught fire. When the weather and atmosphere changed a few days later, officials feared the chemicals would explode. Authorities were forced to do a controlled burn.

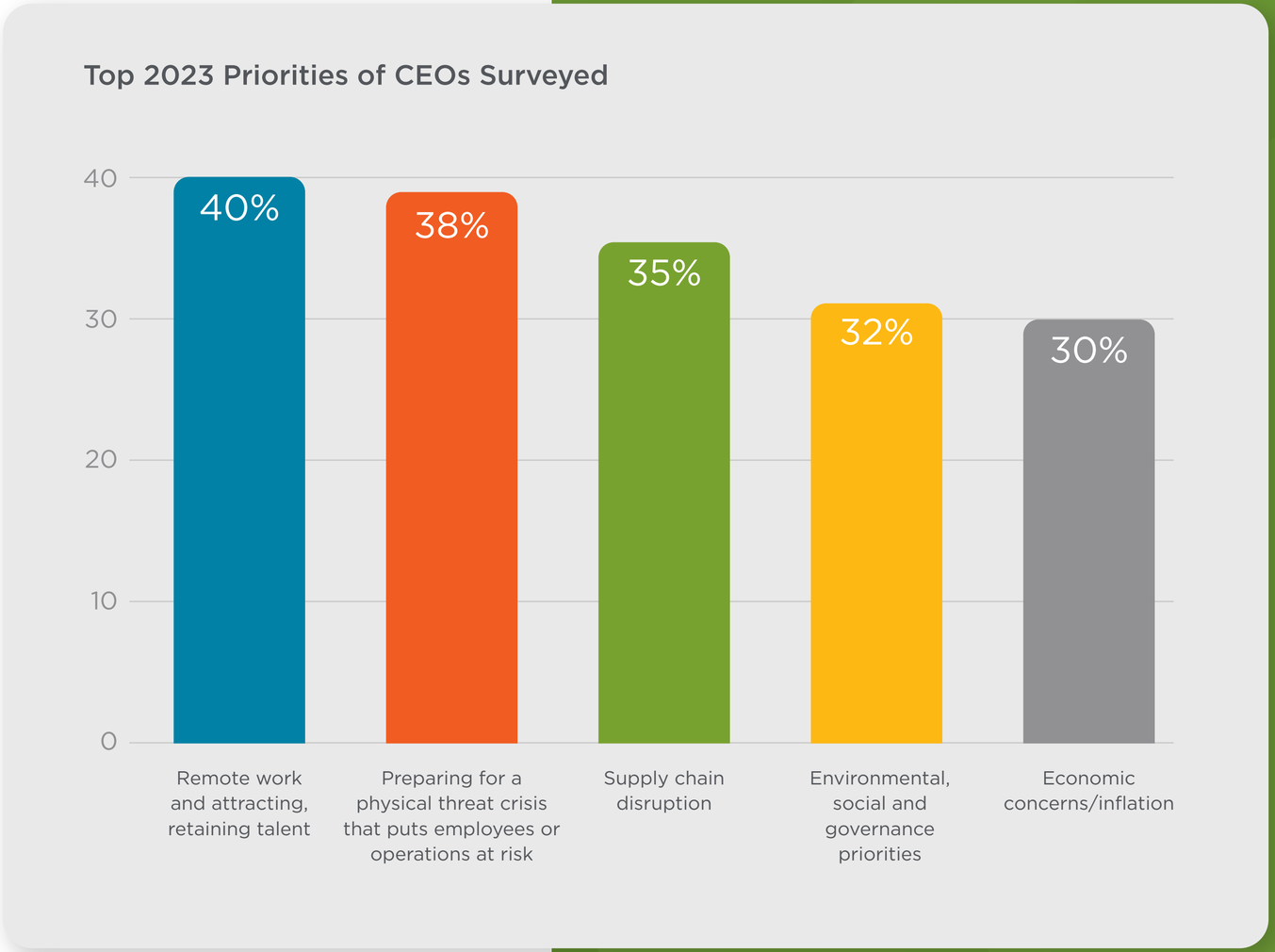
The cascading effects went beyond temporarily displacing residents due to harmful chemicals released into the atmosphere. Approximately 3,500 nearby fish died — spanning 12 species — bringing into question the water quality in the region. For residents and agricultural businesses in the area, a train that previously had no direct correlation to their business has now left lasting uncertainty.

Now more than ever, organizations must sufficiently prepare for all physical threats and the dynamic risks that may follow. Readiness should start with action and planning in the C-suite. This could mean creating processes for expediting the release of emergency funds, ensuring staff members are trained in multiple disciplines, enabling remote work capabilities (if applicable) and keeping lines of communication open.

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?



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.

With up to 10 Threats Every Minute, the Time to Prepare Is Now

Our data shows that up to 10 physical threats can occur every minute. No organization can be risk-free, but all can be prepared. Safety must be a priority from the top. While board directors and the C-suite have a renewed sense of urgency, it's not enough. A holistic strategy with vested interest and prioritization from the C-suite is necessary to keep ahead.

Organizations must have protocols in place, from securing employees to maintaining uptime, protecting revenue and preserving reputation — all of which affect the bottom line. Business agility and, ultimately, competitive advantage depend on it.

Safety must be a priority from the top. While board directors and the C-suite have a renewed sense of urgency, it's not enough.

Appendix

Methodology

OnSolve CEO Survey

The research presented in this report is based on an OnSolve-commissioned CEO survey that took place in January 2023, conducted by Censuswide, an international market research consultancy. The CEO survey was executed across a sample of 250 U.S.-based CEOs with 100 or more employees.

OnSolve Risk Data

This research study outlines the top risks that have occurred as a percentage of all events OnSolve detected from January 1, 2021, to December 31, 2022, that had the potential to impact its customers worldwide. The data in this report was gathered using OnSolve Risk Intelligence, an AI-powered technology that monitors over 50 risk categories of physical threats across 159 countries in real time. OnSolve Risk Intelligence detected more than nine million global events, or physical threats, from 2021 to 2022, using AI and analyst-vetted information pulled from data sources that include local fire, police and emergency medical services departments; weather reports and alerts from government and non-government verified sources; federal government agencies such as the Federal Bureau of Investigation, Department of Homeland Security and other crisis management entities; local, national and international news; and critical event reports from verified social media feeds.

OnSolve Risk Intelligence monitors global physical threats that have an impact on its base of 30,000 customers, which consists of half of the Fortune 100, nearly half of the Fortune 500 and 10,000 communities across the U.S., including state, regional, local and federal entities. OnSolve programmatically maps events to locations worldwide, determining which part of an organization might be at risk.

This report aggregates to a country-level view year-over-year of the physical threats specific to our customers' people and operations across their offices, plants, warehouses and office locations, and while traveling worldwide. It highlights the most significant risks impacting businesses and governments when 2022 is compared to 2021.

Appendix *(continued)*

"Threats" include warnings of the event. OnSolve technology reduces the duplication of the threats reported across multiple data sources. The incidents detected by OnSolve Risk Intelligence are grouped into categories called "risk categories." These risk categories are defined below.

Risk Categories	Incidents Included in Category
Civil Unrest	Labor strike, protest, riot
Crime	Arson, assault, bombing, hijacking, homicide, hostage taking, mass shooting, sexual assault, shooting, theft
Extreme Weather	Avalanche, cyclone (hurricane), earthquake, flash flood, flood, landslide, severe storm, tornado, tsunami, volcano, wildfire, winter storm/blizzard
Fire	Fire, arson, explosion, gas leak, structure fire
Infrastructure and Technology	Power outage, explosion, structure collapse, technical disaster
National Security	Military action, bombing, terrorism
Public Health	Epidemic, pandemic
Transportation Accidents	Aircraft, maritime, rail, road

Works Cited

Deloitte, 2023 Future of Cyber Security (2022)
https://www.deloitte.com/content/dam/assets-shared/legacy/docs/gx-deloitte_future_of_cyber_2023.pdf.

NBC News. Hurricane Ian Knocks Out Power to 2 Million on Destructive Path Across Florida (September 2022).
https://www.nbcnews.com/news/us-news/hurricane-ian-barrels-florida-extremely-dangerous-major-hurricane-rcna49727.

NBC News. More Than 100,000 Without Power and Tornado Sirens Sound as Heavy Winds Hit Texas and the South (March 2023).
https://www.nbcnews.com/news/us-news/260000-power-tornado-sirens-sound-winds-hit-texas-south-rcna73210.

NOAA National Centers for Environmental Information (NCEI). U.S. Billion-Dollar Weather and Climate Disasters (April 10, 2023).
https://www.ncei.noaa.gov/access/billions/, DOI: 10.25921/stkw-7w73

NPR. A Nearly Week-Long Driving Ban is Lifted in Buffalo as Temperatures Rise (December 2022).
https://www.npr.org/2022/12/29/1145967684/winter-storm-buffalo-death-toll-driving-ban-lifted.

The Wall Street Journal. Power-Grid Attacks Surge and Are Likely to Continue, Study Finds (February 2023).
https://www.wsj.com/articles/power-grid-attacks-surge-and-are-likely-to-continue-study-finds-e7dfbc0b.

The Washington Post. What's Known About the Toxic Plume From the Ohio Train Derailment (February 2023).
https://www.washingtonpost.com/climate-environment/2023/02/15/ohio-train-derailment-toxic-chemicals/.

The White House. The Biden-Harris Administration Advances Transmission Buildout to Deliver Affordable, Clean Electricity (November 2022).
https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/18/fact-sheet-the-biden-harris-administration-advances-transmission-buildout-to-deliver-affordable-clean-electricity/.

ONSOLVE®

About OnSolve

OnSolve® is a leading critical event management provider that proactively mitigates physical threats, allowing organizations to remain agile when a crisis strikes. Using the most trusted expertise and reliable AI-powered risk intelligence, critical communications and incident management technology, the OnSolve Platform enables enterprises, SMB organizations and all levels of government to anticipate, detect and mitigate physical threats that impact their people, places and property.

With billions of alerts sent annually and proven support for both the public and private sectors, OnSolve is used by thousands of entities to save lives, protect communities, safeguard critical infrastructure and enable agility for the organizations that power our economy.

For more information, please visit www.onsolve.com.