

2023 Strategic Business Resilience Report

.....
Position your organization to assess,
prepare for and adapt to evolving risks



Global instability, societal shifts and technological advances have ushered in a new era of risks for business leaders to address. Recent advances in generative AI demonstrate how quickly change can occur, with government and business leaders racing to simultaneously leverage the technology and protect against its potential exposures. Meanwhile, geopolitical, economic, cybersecurity, social and natural risks continue to evolve.

As business leaders confront this uncertain landscape of emerging exposures and imminent disruptions, the need to develop sound resilience strategies is paramount. CNA's **2023 Strategic Business Resilience Report** provides an overview of the current risk environment and provides timely considerations for advancing an organization's ability to mitigate and manage disruptive events.



**Key factors for
building resilience:**

01 UNDERSTAND
THE EVOLVING
RISK LANDSCAPE

02 IMPLEMENT
STRATEGIC INSURANCE
COVERAGES

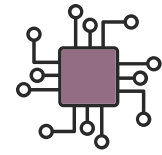
03 BUILD AND ADVANCE
OPERATIONAL
RESILIENCE



01 UNDERSTAND THE EVOLVING RISK LANDSCAPE

The threats facing today's businesses are more complex and interconnected than ever before, and every organization must grapple with myriad challenges to its ability to operate. To agilely manage potential impacts, it's essential to recognize risks early.

Business leaders should consider a variety of questions as they plan for disruptive scenarios. For example, how might regulatory shifts, technological advancements or workforce trends affect the organization's trajectory? Would these business risks emerge gradually, giving the company time to prepare and adjust? If not, how would the organization deal with a sudden disruption that required an immediate response? Recent years have brought enormous changes to the risk landscape, challenging businesses to prepare for impacts across all aspects of operations.



Artificial Intelligence

The potential impact of artificial intelligence is hard to overstate. AI will contribute an estimated \$15.7 trillion to global economic growth by the year 2030,¹ and many companies are already harnessing its capabilities to reduce costs and gain a competitive edge. OpenAI’s ChatGPT tool, which businesses are using to streamline processes and elevate customer support, gained a record-breaking 200 million active users in a two-month period in early 2023. Revenues from the application are expected to exceed \$1 billion in 2024.

Despite its transformative promise, the under-regulated AI landscape also poses significant risks. Computer scientist, Dr. Geoffrey Hinton, hailed as the “godfather of artificial intelligence,” asserts that ChatGPT embodies a 100-fold increase in knowledge compared to a single human brain, enabling the generation of diverse content (e.g., application code, text, images and videos) with unparalleled precision and efficiency.²

In early 2023, Dr. Hinton resigned from his position to freely address his apprehensions regarding the machine capabilities he had played a key role in developing. In an interview with *The New York Times*, Dr. Hinton shed light on the potential risks tied to this technology, including the proliferation of misinformation on the internet, job displacement for roles such as help desks, personal

assistants and translators, and the potential exploitation of AI by nefarious entities seeking criminal, political or national security advantages.³

The gravity of these concerns prompted the Future of Life Institute to rally support from more than 1,000 computer scientists in March 2023, urging all AI labs to implement an immediate pause of at least six months. Their collective assertion underscored the transformative impact advanced AI could have on the future of life on Earth, emphasizing the imperative to implement thoughtful controls, regulations and oversight, with adequate resources, in a timely manner.

The EU parliament is working to implement the first comprehensive AI laws by the end of 2023 to establish

AI contribution to global economic growth

\$15.7 trillion



\$1 billion
(ChatGPT only)



2024

2030

controls, reporting and oversight capability. The regulations focus on ensuring “AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly. AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes.”⁴

Given AI’s exponential growth, varied use cases by business leaders and the potential impact of impending legislation, corporate oversight is paramount. Companies using AI technology see their top risks as cybersecurity, data privacy, liability, legal compliance, reliance on 3rd parties for AI algorithm, lack of regulation, reputation, bias and physical safety.⁵

(Note: In a real-world demonstration of AI’s utility, ChatGPT was used to enhance the content quality of this report.)

¹ <https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence.html>

² ‘Godfather of AI’ Geoffrey Hinton: Tech will get smarter than humans | Fortune

³ <https://www.nytimes.com/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html>

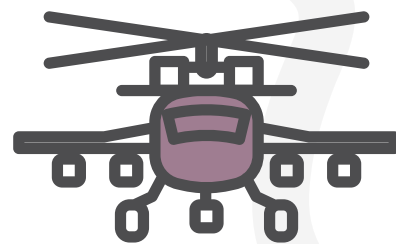
⁴ EU AI Act: first regulation on artificial intelligence | News | European Parliament (europa.eu)

⁵ [aisurveypptfinalmarch20222.pdf \(bakermckenzie.com\)](https://www.bakermckenzie.com/ai-survey-ppt-final-march-2022-2022.pdf)



Conflict and Geopolitical Instability

Tensions and mistrust between the U.S. and China are a growing concern. *The New York Times* observes that the two countries “jockey for influence beyond their own shores, compete in technology, and maneuver for military advantages on land, in outer space and in cyberspace.”⁶ Given the reliance on international trade and business partnerships, further deterioration could significantly affect the state of global commerce.



In key nations, military spending has increased:

- | | |
|--------------|---------------------|
| U.S. | Russia |
| China | India |
| Iran | Saudi Arabia |

These tensions have led to a modern-day arms race. In a reversal of a 15-year demilitarization trend prior to 2022, military spending has increased among global and regional powers such as the U.S., Iran, Russia, India, China and Saudi Arabia. In addition, support for Ukraine’s war effort by NATO’s 31 member countries will likely reach 7% of GDP if all members meet their target spending.⁷

Although the pace of development, volume and trend towards more precise attack weapons will be difficult to control without transnational collaboration, nations tend to focus on their own resources and security interests. Furthermore, increases in local, regional and global military investment are diverting resources needed to maintain and improve infrastructure and trade.

The Russian invasion of Ukraine has caused economic hardship far from the conflict zones, triggering great migrations, inflation and supply route closures. In July 2023, Russia announced its withdrawal from a wartime agreement that had allowed Ukraine to export wheat, corn, sunflower seeds and vegetable oil through the Black Sea, as profitability was increasing for those exports.⁸ Unfortunately, that decision means that vulnerable countries in the Middle East and Africa will be at higher risk for long-term food insecurity while the transport passages are blocked.⁹

To mitigate potential business disruptions, business leaders must diligently track global trends and prepare to swiftly adapt their operations and supply chains.

⁶ U.S.-China Relations: What to Know - The New York Times (nytimes.com)
⁷ <https://intelligence.weforum.org/topics/a1Gb0000000pTDXE2> , World Economic Forum, Global Risks, Security, July, 2023
⁸ <https://www.nytimes.com/2023/07/17/world/europe/ukraine-grain-deal-russia-war.html>
⁹ Ibid



Climate Change

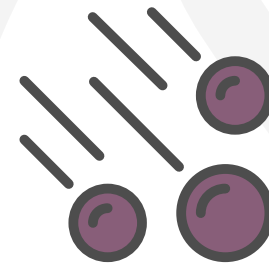
The effects of climate change are already upon us – and will likely continue to escalate without global collaboration and collective action. The United Nations Intergovernmental Panel on Climate Change (IPCC) states that “Global warming will continue to increase in the near term (2021-2040) ... in nearly all considered scenarios and modelled pathways. Risks, projected adverse impacts, related losses, and damages from climate change escalate with every increment of global warming (very high confidence).”¹⁰

Rising temperatures are associated with widespread changes in weather patterns, including an increase in severe weather events. During the first six months of 2023, severe convective storms resulted in estimated insured losses of at least \$35 billion. These perils included at least 812 confirmed tornadoes in the U.S., but the primary cause of damage was hail. NOAA recorded at least 729 instances of hailstones larger than two inches (5.1 centimeters) in diameter. Although the U.S. accounted for 76% of worldwide insured losses related to natural hazards, it was far from the only country to face severe weather events. In Germany and France, for instance, June thunderstorms resulted in over a billion dollars of insurance costs.¹¹

In the first half of 2023, the U.S. had

76% of all natural hazard-related insured losses worldwide.

Hail was the primary cause of damage.



Droughts driven by record high temperatures have plagued North America and Europe, creating ripe conditions for wildfires across many countries. While the connection between droughts and increased wildfire risk is well known, droughts can exacerbate existing water scarcity, requiring local governments to take significant measures to restrict or prohibit water use to conserve resources for essential functions, such as firefighting, healthcare and drinking water. In many cases, local jurisdictions will restrict the testing of fire protection equipment, such as fire sprinkler systems and booster pumps, that is critical to maintaining reliability and identifying problems in these fire and life safety systems.

Intensified by rising temperatures, severe weather events will continue to threaten the operations and supply chains of businesses, and leaders should plan accordingly.

¹⁰ [AR6 Synthesis Report: Climate Change 2023 — IPCC](#)

¹¹ <https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/natural-catastrophe-report-2023-h1.pdf>



Cybersecurity

Each day, cyberattacks grow more frequent, more complex and more expensive. Organized crime groups, state and individual bad actors continue to benefit, often without consequence. About a quarter of these cybersecurity incidents involve ransomware, with email, desktop sharing software and web applications as the top three action vectors.¹² Bad actors continually seek new ways to attack and monetize vulnerable organizations, finding complex and creative methods for obtaining credentials or social engineering an email to route funds to a criminal account.

“ While some adversaries (hackers) use advanced tools and techniques, most take advantage of unpatched vulnerabilities, poor cyber hygiene or the failure of organizations to implement critical technologies like MFA (multi-factor authentication). Sadly, too few organizations learn how valuable MFA is until they experience a breach. ”

Jen Easterly, Director of the U.S. Cybersecurity and Infrastructure Security Agency

1/4 of cybersecurity incidents involve **ransomware**. The top action vectors are:



Email



Desktop Sharing Software



Web Applications

The aim of cyber attackers is not necessarily to steal data but to stop businesses from being able to function, holding their data or resources hostage until a ransom is paid. Cryptocurrencies are one factor that enables these attacks to achieve their goal, as they are difficult to trace and don't respect international borders or banking laws. As of August 2023, there were over 9,500 cryptocurrencies with a total market capitalization of more than \$1 trillion.¹³

Regulatory action to curb this illegal cyber activity and ransom payments has not impeded the proliferation of

cybercrime. Legislators have made strides in requiring cryptocurrency exchanges to comply with OFAC and anti-money laundering laws in some nations. The U.S. Congress and some individual states have proposed restrictions on ransomware payments to improve cyber reporting to identify, capture and shut down the criminal networks that are enabling these attacks to continue with limited or no punitive risks.¹⁴

As the threat of cybercrime continues to increase and evolve, all businesses are at risk – regardless of their size, location or industry.

¹² <https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf>

¹³ [Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap](https://www.coinmarketcap.com/price) (accessed 8/10/23)

¹⁴ <https://www.csoonline.com/article/3622888/four-states-propose-laws-to-ban-ransomware-payments.html>



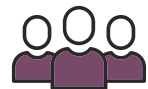
Environmental, Social and Governance (ESG) Expectations

Investor, customer and workforce interests continue to favor companies that provide information on how they are managing risks and developing business strategies to address ESG issues.

These include:



Environmental topics related to how organizations manage carbon emissions, natural resources, pollution and waste management, and make use of green technology and construction.



Social topics, such as how organizations manage labor and supplier labor standards, provide human health and safety (employees, consumers, communities), support local and global health and nutrition.



Governance topics, such as sharing how organizations support ethics, compliance, anti-corruption, tax and accountability.

EU and U.K. agencies are carefully progressing regulatory mandates to standardize ESG disclosure reporting to promote responsible business practices, corroborate ESG claims and allow for more informed consumer/investor decisions. The EU commission adopted the Corporate Sustainability Reporting Directive (CSRD), which will require large entities to provide a standard ESG report in January 2025 on 2024 data.¹⁵ ESG information will be required in annual reports, with specific form, timing and reporting principles and assurance provided through an external audit.¹⁶ Attempts to regulate ESG in the U.S. are trailing EU and U.K. efforts.

In its 2023 agenda, the U.S. Securities and Exchange Commission has set dates to finalize 29 rules and propose another 23 amendments related to ESG disclosure and reporting.¹⁷ State legislators have started developing their own regulations for or against

ESG reporting requirements. States with a Republican majority are moving to minimize or eliminate ESG considerations from state funding decisions, while states with a Democratic majority are designing pro-ESG policies. The Harvard Law School Forum on Corporate Governance expects state governments to continue to create ESG-focused laws as the 2024 U.S. presidential election approaches.¹⁸ As of March 2023, at least seven states have enacted laws or policy statements that seek to prohibit or discourage public entities from considering ESG factors when investing state resources.¹⁹

Since organizations subject to ESG reporting standards may face reputational risks if they don't comply in a timely manner, they should invest in resources to comprehend the changing requirements and provide accurate information.

¹⁵ <https://kpmg.com/nl/en/home/topics/environmental-social-governance/corporate-sustainability-reporting-directive.html>

¹⁶ Ibid

¹⁷ [The SEC Plans to Finalize ESG-Related Rules in 2023 | ACA Group \(acaglobal.com\)](https://www.acaglobal.com/news/the-sec-plans-to-finalize-esg-related-rules-in-2023)

¹⁸ [ESG Battlegrounds: How the States Are Shaping the Regulatory Landscape in the U.S. \(harvard.edu\)](https://www.harvard.edu/esg-battlegrounds-how-the-states-are-shaping-the-regulatory-landscape-in-the-u.s.)

¹⁹ Ibid



Evolution of Work

Workforce change and retention are paramount considerations for today’s business leaders. The COVID-19 pandemic led to increased early retirements and reduced immigration, creating a labor shortage in the U.S. The Chamber of Commerce estimated that there are 1.9 million fewer U.S. citizens participating in the labor force compared to February 2020.²⁰

Some households have adapted to a single-income lifestyle given the inflated costs for childcare, food and utilities.²² In June 2023, there were 10.1 million vacant roles in the U.S. and just over half that many (5.7 million) people that may have needed work.²³

Three quarters of Americans plan to look for new work in 2023, according to a recent Gallup survey, and their considerations may differ from workers of the past. A Gallup poll found that millennials and Gen Z members are more focused on quality of life and well-being, and that over half of U.S. workers had made moves that equaled or lessened their income to improve their lifestyle and career.²⁶

Labor force shortage by industry (July 2023)²¹



Today’s “remote work” professional landscape is very different from the pre-pandemic workplace. Many organizations that have tried to mandate a return to the office have met with employee revolts.²⁴ City office towers used to be the hub of activity, but commerce has shifted from downtown areas to neighborhoods. This leaves many office towers with significant vacancy rates and reduced values for their properties.²⁵

In the highly competitive landscape of recruitment and retention, companies will need to consider innovative HR strategies to retain their existing workforce and attract qualified candidates. At the same time, vacancy increases may support real estate and overhead reduction.

²⁰ America Works Data Center | U.S. Chamber of Commerce (uschamber.com)
²¹ Ibid
²² Ibid
²³ Get Ready for the Full-Employment Recession - WSJ
²⁴ A New CEO Says Employees Can't Work Remotely After All, and They Revolt - WSJ
²⁵ Distress in Office Market Spreads to High-End Buildings - WSJ
²⁶ The New Rules of Success in a Post-Career World - WSJ

02 IMPLEMENT STRATEGIC INSURANCE COVERAGES

Helping businesses transfer risk and provide financial resilience after disruptive incidents, insurance is a vital component of any effective business resilience program. Intense competition for limited resources, combined with a challenging operational risk landscape, requires business to carefully consider many factors when determining insurance coverage choices.

A recent study of property appraisals revealed that – following pandemic-era inflation that reached a 40-year high – 68% of buildings valued from 2020 to 2021 were underinsured by at least 25%, and almost 90% of the buildings appraised were valued below their actual worth.¹ Businesses and insurance brokers work with insurance carriers like CNA to help businesses determine accurate property valuations, as well as assess and mitigate property, liability and cybersecurity exposures.

¹ <https://riskandinsurance.com/underinsured-properties-are-crushing-reinsurers-why-proper-valuations-will-be-a-focus-for-years-to-come/>

Business Interruption

Depending on impact severity and operational complexity, it could take weeks, months or even years to recover and restart operations after a disruptive incident. Business interruption (BI) coverage allows insured companies to sustain their financial path and cover ongoing expenses during recovery. Essential components of this coverage, per the policy terms, usually include the following:

Business income coverage aids in recouping net income plus continuing expenses, such as payroll, rent and utilities, throughout the period of restoration.



Actions to consider:

1. Conduct a pragmatic yearly evaluation of the anticipated changes in revenues and expenses for both 12-month and 24-month periods when deciding on your insurance coverages.
2. Assess the revenue impact for each location using a "complete loss" scenario to understand your organization's potential financial BI limits. This analysis will also identify specific site operations where risk management and business continuity planning can be prioritized and provide the most return on investment.
3. Examine your ability to pay and retain employees displaced during an extended period of restoration. Strongly consider including ordinary payroll as a continuing expense coverage to retain your workforce through an extended period of restoration.

Extra expense coverage allocates funds to lessen an organization's recovery time and the impact of losses during the restoration phase, as circumstances allow.



Actions to consider:

1. Estimate the funds each location will need to secure recovery resources (e.g., temporary relocation, warehouses for salvage, extra shipping costs) when an incident disables operations.
2. Estimate the contract or temporary labor requirements and their daily/weekly costs for supporting the recovery of affected operations. This includes additional staff required to aid in the recovery and restart of disrupted operations.
3. Consider the aforementioned points when estimating the appropriate time and revenue loss coverages.

Extended period of indemnity coverage offers financial support beyond the restoration period, providing for ongoing business income losses and aiding in recovery to the pre-loss sales capacity.



Actions to consider:

1. Identify sites where a prolonged property interruption could lead to substantial revenue loss related to your organization's services or products. For instance, consider a data center integral to enterprise functions or a primary manufacturing unit or warehouse where key equipment or finished products are housed.
2. Estimate, for each location, the time required for sales to return to pre-disruption levels after the impacted operation has been fully restored and is functioning at pre-incident levels again.
3. Consider the aforementioned points when estimating the appropriate time and revenue loss coverages.

Cyber

No organization is safe from cyber criminals. Even with strong controls to limit a security breach, the possibility remains that a network or data impact will occur. In 2022, there was a surge of 112% in the activities of criminal access brokers, who gain entry into organizations and then sell or offer this unauthorized access to other malevolent actors such as ransomware operators.²



Actions to consider:

1. Work with your insurance broker to establish the appropriate coverages such as network failure, dependent business income loss, wrongful collection, theft and social engineering.
2. Implement a cybersecurity framework to identify, protect, detect, respond and recover, as defined by the National Institute of Standards and Technology (NIST).



For additional insight into cyber trends and risk management approaches, [check out Season 3 of CNA's Risk Control e-Talks.](#)

Liability

Commercial liability insurance helps protect organizations from financial liability for injuries or property damage that occur during the course of daily business activities by paying for an organization's defense costs and indemnifying the organization for losses (subject to the terms of the policy). As liability exposure for companies worldwide continues to rise, there has been a notable increase in litigation and larger court verdicts.



Actions to consider:

1. Perform a risk assessment at the corporate level to understand your liability exposures and establish controls (e.g. secure access, snow/ice removal, etc.) to minimize incidents from occurring on your premises.
2. Work with your insurance broker to understand liability trends (e.g. emerging interests, damage and litigation monitoring services).³
3. Transfer risk as much as possible with contractual indemnification and insurance requirements for all third parties involved in supporting your operations.



² <https://riskandinsurance.com/underinsured-properties-are-crushing-reinsurers-why-proper-valuations-will-be-a-focus-for-years-to-come/>



Equipment Breakdown

Equipment breakdown insurance (as part of property coverages or as a standalone policy) provides coverage for physical damage repair/replacement and associated business income loss from mechanical and machinery breakdown, based on the policy terms and conditions.



Actions to consider:

1. Establish coverage requirements by pinpointing singular points of vulnerability or specialized high-value equipment that, if compromised, could lead to significant business revenue loss.
2. Implement robust machine preventive and predictive maintenance as the first line of defense to enable continuity of operations.

Property

Property damage can significantly disrupt operations and affect profitability, especially if the property isn't adequately insured. Persisting inflation, shifts in interest rates, supply chain disruptions and labor shortages may further influence reconstruction expenses. Driven by climate change, the increasing frequency of extreme weather events in all seasons will continue to threaten global properties and supply chains.



Actions to consider:

1. Review property values and true replacement costs at least once a year to align with inflation and supply chain conditions.
2. Ensure that your resilience strategies and insurance coverages reflect current trends for natural and man-made risks.
3. Identify repair/replacement times for specialized assets (e.g. lab space, robotics, conveyor systems) critical for revenue generation. Consider equipment breakdown coverages for the most vital machinery.
4. Adjust coverages based on current and future property use. When a building is vacant due to factors such as remote work arrangements, the risk exposure for fire loss and water infiltration from internal/external sources significantly increases.



03

BUILD AND ADVANCE OPERATIONAL RESILIENCE

A resilient organization consistently demonstrates the foresight to anticipate, the initiative to proactively prepare for, and the agility to respond effectively to unexpected challenges and disruptions.

Resilience is sustained through comprehensive risk management, coupled with efficient recovery and response capability, aiming to diminish potential threats and mitigate their impact on business operations.

Enterprise Risk Management

The Risk Management function is the first line of defense in reducing the probability and impact of a disruption. It typically considers current and emerging risks, working with appropriate business functions to implement mitigation plans to avoid disruptive incidents where possible or minimize the impact on the organization. This function also monitors the organization’s incident response, crisis management and recovery capability for disruptive incidents, and often oversees risk transfer strategies (e.g., insurance, contract indemnification clauses) to minimize the financial impact.

Response Capability: An “incident” is an event that has the potential to cause an interruption, disruption, loss, emergency, disaster or catastrophe, and can escalate into a crisis. Every second matters when your organization is suddenly affected by a cyberattack, an electrical fire, or water infiltrates your critical work areas. The sooner your organization can respond to an incident, address life safety issues and fix the problem, the more control leadership can have over the impact, messages and outcomes. Many incidents, including floods, wildfires and tornadoes, typically affect a specific location and its operations.

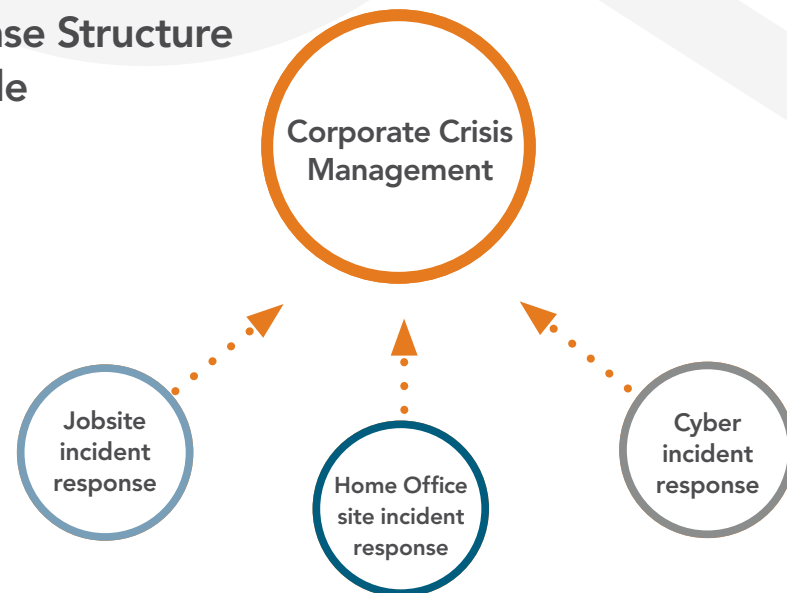
However, certain events may have a wider reach, necessitating the involvement of senior leaders to guide the response and oversee communications. Incident Response Plans define the structure, authority and team members needed to quickly respond to incidents. Multiple incident response plans may be needed to manage different locations or risks. The Corporate Crisis Management plan defines the senior leadership roles authorized to direct the company-wide response and issue all internal and external communications related to a disruptive incident. Some insurance policies include coverages to support the use of public relations firms, which can be engaged to support crisis communications at the time of disruption.

View this 3-minute video to learn more:
[Improving Your Business Resilience Capability](#)

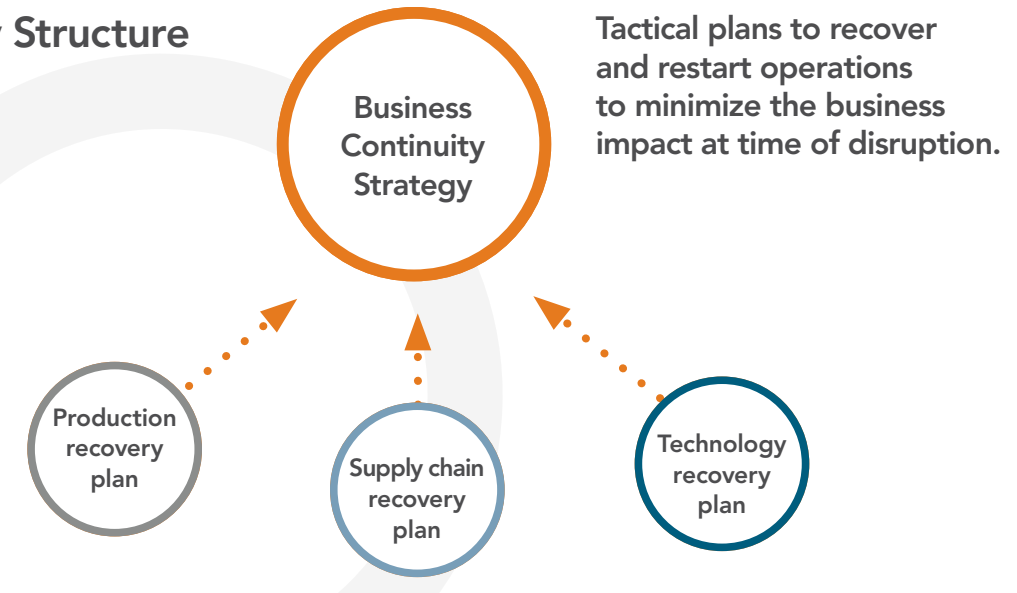


Recovery Capability: To establish a business continuity framework that can instantly initiate repairing, replacing and restarting affected operations, advanced planning is vital. The Business Continuity Management function is charged with developing strategies and plans to ensure business recovery teams have the resources needed to continue critical processes impacted by a disruption. This includes developing strategies for both internal production elements (e.g., workforce, equipment, facilities, materials and technology) and supply chain elements, which include suppliers, distributors and customers.

Response Structure Example



Recovery Structure Example



Critical Success Factors for Building Resilience

Executive sponsorship. Senior leadership needs to understand that response and recovery structures, when properly executed, can create a significant competitive advantage. This requires resources and support from all levels of the organization to support and prioritize preparedness activities.

Accountability. Although often overlooked, a business resilience steering committee and policy are important constructs to establish. A resilience steering committee is a cross-functional team that champions the development, exercises and monitoring of the organization’s resilience capability. The resilience policy should outline the purpose, scope, key definitions and roles accountable for creating and maintaining the teams and plans formed to manage the response and recovery efforts for an organization.

Continuous Improvement. Business resilience is a journey, not a destination. It is essential to review and rehearse strategies and plans using likely scenarios at least once a year in a tabletop exercise or other format. This prepares the designated leaders and team membership to immediately mobilize their response and recovery teams when a disruptive incident occurs. Activating a plan in response to a disruption replaces the need to perform an exercise. Furthermore, it is essential to conduct an After Action Review (AAR) following each activation or exercise, to refine the response plan and enhance team performance.

View this 3-minute video to learn more:
[The Value of Strategic Business Resilience.](#)



Organizational Benefits of Building Resilience

- Avoid risk impact
- Minimize loss
- Assure stakeholders
- Develop leadership
- Increase risk awareness
- Respond more effectively
- Recover more quickly

Business Resilience Program Maturity

Improving business resilience starts with an honest assessment of an organization’s current position and identifying its current level on the program maturity scale concerning the establishment of a holistic, coordinated resilience capability.

View this 3-minute video to learn more:
Assessing Your Resilience Capability.



How mature is your business resilience program?

Informal
Response and Recovery structure created at time of disruption.

Defined
Response and Recovery structures with roles and action plan in place.

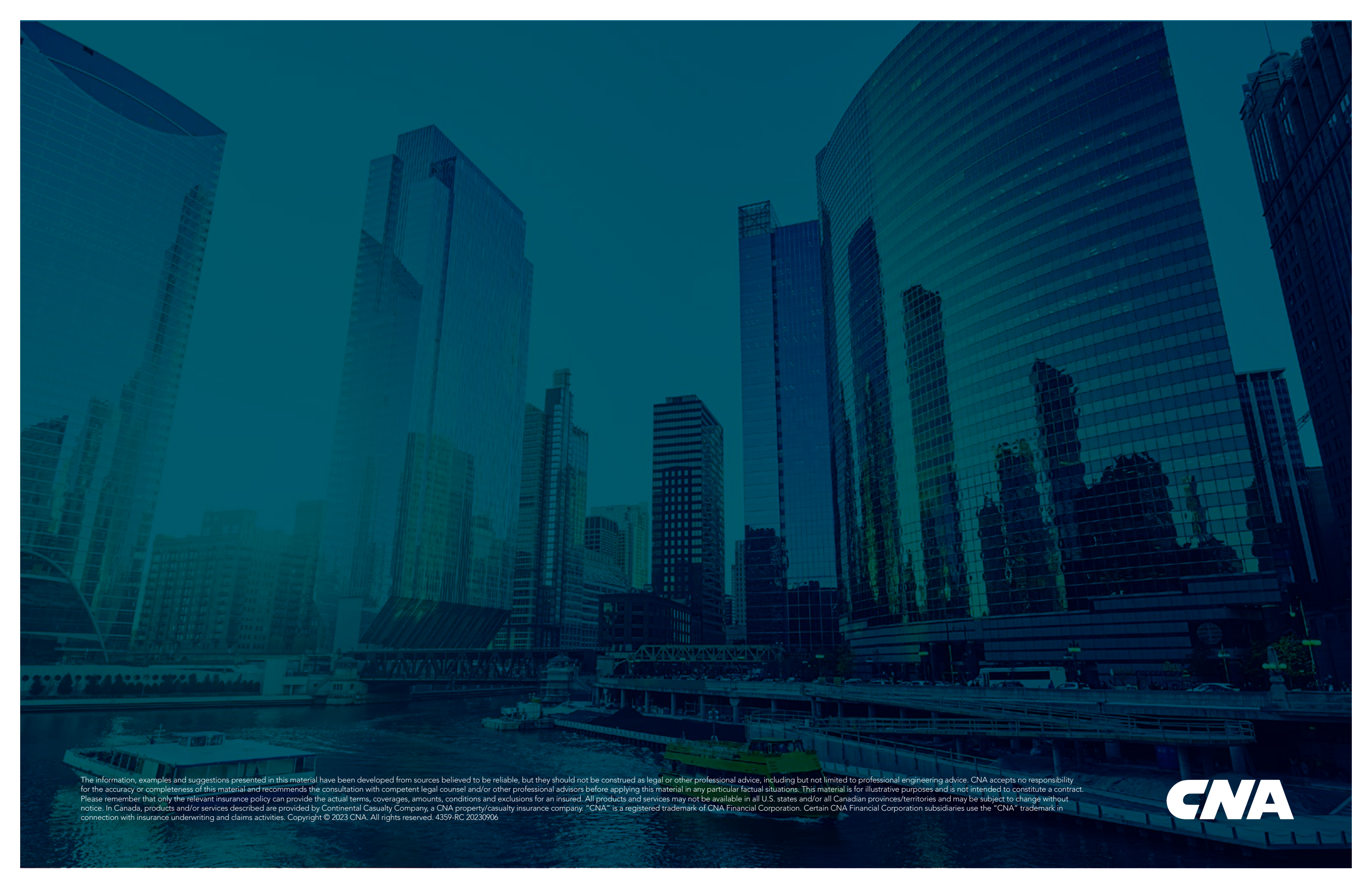
Established
Response and Recovery plans and teams in place with regular training exercises.

Managed
Response and Recovery plans and team activities traced, monitored and improved

Optimized
Resilient mindset drives business strategy and sustained response capabilities

In this complex risk environment, organizations continually face new and evolving challenges as they strive to build success. For executive leaders, integrating strategic insurance coverages that enhance response and recovery abilities is a vital part of enterprise risk management. Enhanced preparedness, facilitated by training exercises for leaders and team members combined with vigilant oversight of resilience capabilities, strengthens and elevates organizational resilience. Insurance brokers and carriers can help construct strategic risk transfer strategies that allow organizations to bolster both financial and operational resilience.

To learn more about managing your risk and increasing efficiency, visit cna.com/riskcontrol.



The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice, including but not limited to professional engineering advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all U.S. states and/or all Canadian provinces/territories and may be subject to change without notice. In Canada, products and/or services described are provided by Continental Casualty Company, a CNA property/casualty insurance company. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities. Copyright © 2023 CNA. All rights reserved. 4359-RC 20230906

CNA