CHAPTER 1

What's Your "Why?"

Identifying and monitoring risks, and managing their impact to your organization, is a big challenge, especially given how complicated the modern threat landscape has become. Resilient organizations have measures in place to keep everyone safe and help them overcome those challenges.

Is your organization missing key technology to support resilience? If so, start by communicating this reality clearly and effectively to stakeholders within your organization, so they understand why change is necessary.

In this chapter, we'll delve into the most effective ways to establish the "Why" for your organization.

CHAPTER 1

The Evolution of Resilience

The risk landscape is evolving. Dynamic risk — where the outcomes and areas of impact are often different and more complicated than initially expected — now dominates our operating environment.

This has created a butterfly effect, in which the impacts of an event cascade throughout the organization. One risk event can affect not only your bottom line, but also your reputation, customer satisfaction, ability to attract and retain talent — the list goes on.

The major categories of critical events are all on the rise, necessitating 24/7/365 monitoring. Meanwhile, we're still feeling the effects of the pandemic.

We've adapted and will continue to do so. Remote and hybrid models have become the norm in the employment sector. Online interaction and virtual collaboration are a staple of the workday. Legal and environmental requirements have increased in response to new regulations and climate change.

The result for organizations? Many are experiencing greater ***risk fatigue***. The increase in threats is causing burnout among security and business continuity professionals, leading to an increased tolerance for risk. However, with many threats on the rise, organizations can't afford to let vigilance decline. Threats remain significant, and so must efforts to manage them.

From 2020 to 2021

Weather: Reports of blizzards and avalanches all tripled, and tsunamis more than doubled.

Fire: Arson, structure fires and fires in general all approximately doubled.

Crime and Violence: Assault, homicide and theft all more than doubled, while reports of shootings and mass shootings nearly tripled.

Transportation and Logistics: The risk involved in getting people and goods from Point A to Point B went up 146% overall.

— Data from the Global Risk Impact Report

CHAPTER 1

What Can You Do?

It's time to stop focusing on the volume of risk. Instead, focus on mitigating the impacts to your organization.

Shift to a proactive mindset: It's about having the right people, processes and technology in place before a crisis strikes.

Don't wait for the next storm or active assailant. Put those mechanisms in place now, so you can:

- ✓ **Identify** threats in advance
- ✓ **Communicate** with people in real time
- ✓ **Activate** response teams quickly
- ✓ **Protect** your people and operations, 24/7/365

Sell the Value

A Typhoon Hits a Call Center

The OnSolve® Platform alerted a customer call center in the Philippines to Typhoon Rai two days before it hit, giving them time to shift resources to a center in Manila. Not only did this keep employees safe, but it also kept operations running and made sure clients could access their funds and transactions.

LEARN MORE →

CHAPTER 1

Defining Your "Why"

Your "Why" doesn't have to be complicated. In fact, clear and simple reasons are often the most important ones.

Perhaps your goal is to:

- Keep people safe
- Ensure operational continuity
- Protect brand reputation
- Prevent lost revenue

What is a "critical event"?

Your operations can be threatened by both:

Routine Emergencies

Those your organization has previously dealt with and is prepared to handle via existing procedures, such as:

- Building damage/closures
- Production delays
- Emergency repairs
- Power outages
- System/network downtime

Crisis Emergencies

Those unanticipated by your organization, which often happen at an accelerated pace and are difficult to adapt to, such as:

- Active assailant
- Civil unrest
- Public health alerts
- Tornado warnings
- Cyberattacks

YOUR CHAPTER 1 WORKSHEET

Questions to Discover Your "Why"

DOWNLOAD
this chapter to fill out
this worksheet

These questions will help you narrow down the reasons your organization needs a change. Your answers will serve as the foundation for justifying change across the organization when you introduce your proposed solution.

1. Think back to the outcome of your last several critical events:

a) What were the negative impacts?

b) What could have been done differently?

2. Analyze the biggest changes in your industry in the past two to five years:

a) Have the threats to your organization changed?

b) What were the top five threats?

c) What events have affected similar organizations?

Questions to Discover Your "Why" (continued)

DOWNLOAD this chapter to fill out this worksheet

3. What matters most to you and your organization when disaster strikes?

4. Do you have the technology to support your resilience moving forward?

(Select all that apply. Any unchecked boxes are reasons your current solution may not support your end goals.)

Does your current technology:

a) Deliver actionable intelligence?

- □ Collaboration between AI and human analysts
- □ Structured and unstructured source data, filtered for relevance
- □ Accurate, validated information from unbiased and reliable sources
- □ Aggregated information with real-time updates

b) Ensure effective communications?

- □ Custom alerts in multiple modalities (text, voice, email, mobile app, desktop alerts)
- □ Global messaging across 190+ countries in large volumes
- □ Two-way communications with check-in and survey capabilities
- □ Detailed reporting
- □ Safety capabilities for lone workers

c) Optimize usability?

- □ Easy implementation, training and scalability
- □ Geo-intelligent targeting with ghosting options to protect privacy
- □ Threat detection with automated alerts
- □ Seamless integration with existing business systems
- □ Streamlined contact data management