The Ultimate Guide to Organizational Resilience

7 Building Blocks of Organizational Resilience

How to Support a Hybrid Workforce
as Attack Surfaces Expand

Overview

Resilience remains a trending topic among organizations and individuals. The past 18 months have brought about an abundance of change. Organizations and individuals that can find meaningful ways to practice resilience in the face of change, from remote and hybrid working to digital acceleration, are at a significant advantage.

Remember, change for the sake of it is never a good idea. What we're discussing here is strategic and necessary to enable continued success. Think digital transformation, remote working technologies, etc. After all, being at the forefront of new technology and techniques can not only take companies forward but also give them a competitive advantage.

Resilient organizations are receptive to change rather than being rigid in their stance. They know the competition is fierce and it doesn't take much to be displaced. You can't count on last year's strategy to deliver effective results in tomorrow's ecosystem.

Resilient organizations and leaders are always looking ahead and asking questions like:

- Are we differentiating on value or price?
- What could displace us?
- How can we be more effective? How do we measure effectiveness?
- Are we measuring the right KPIs?
- What else do our customers need that we're not providing today?
- How can we help our employees better serve our customers?

Adapting to a Rapidly Changing Environment

The COVID-19 pandemic pushed organizations across the globe into a whirlwind of change. Many organizations had to learn how to work completely remotely for the first time in order to meet shifting lockdown requirements that varied by region.

One of the most interesting lessons from this period is that organizations that had already invested in technologies that enabled secure remote and hybrid work alternatives were in a far better position to transition to a remote-working model. Expanding beyond this type of technology or event allows one to keep up with technological breakthroughs that aid organizational resilience.

Why Resiliency Over Efficiency

Research firm Gartner released a study in 2020 that identified a link between efficiency and fragility.[1] It found that keenly focusing on efficiency can lead your organization down a path that favors tried-and-true methods over innovation that opens new revenue streams and supports long-term success.

As renowned leadership author and speaker Simon Sinek once said, “Innovation is not efficient.” It’s not going to happen overnight. It’s not comfortable. It’s slow. True innovation requires trial and error, refinement and dedication to experimentation. Just ask any successful entrepreneur. It’s unlikely they discovered their winning idea the first time they sat down to ideate.

Reverse engineering someone else’s idea or copying a competitor is easier. Coming up with something new and game-changing is challenging, time-consuming and costly. It is critical to understand the type of organization you currently have and, more significantly, the organization you wish to become.

How to Know if Your Organization Is Original

Go to your favorite search engine and search for your company’s category. Look for the first three to five results that aren’t yours. Are they using the same language to describe the value of their products or services that you are? If so, consider revising your messaging to home in on relevant differentiators.

The Rise of Hybrid & Remote Work

While we're not out of the woods yet, a few parts of the world are beginning to relax COVID-19 restrictions. Others remain patient, waiting for their turn to once again return to normal. The way we work, socialize and live our everyday lives has changed dramatically over the last year — and businesses are no exception.

With an increasing number of employees working remotely, executives have had to either adapt their recruiting and retention approach or lose top talent to more flexible organizations.

Smart companies have started offering "remote forever" options to reduce the risk of losing talent who might look for a remote job anywhere in the world.

In many ways, our working environments and policies have forever changed. Many think this is a good thing. But regardless of your stance on remote or hybrid work environments, it's becoming necessary for organizations of all sizes to identify long-term plans to support flexible working locations and environments.

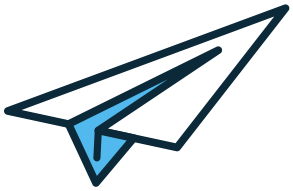
While many organizations staved off such flexibility in the past citing security risks, individuals have tasted the freedom of permanent remote work and many hope to never return to a noisy office after waiting in traffic for an hour or more.

Tapping Into the Global Talent Pool

Urban sprawl has taken on a whole new meaning. Teams that once sat in a single location each day are spread across the country, and in many cases, several countries — an issue that's making 2020 and 2021 tax auditing an absolute nightmare for corporations and auditors as some adventurous employees sought to ride out the pandemic in exotic locations with tax laws much different than their employer's country of origin.

Accounting and Human Resources challenges aside, remote and hybrid work seems to be here to stay, at least for the near future.

As such, organizations must pivot their technology strategies from a survival mode of "remote for now" to a longer-term strategy that supports the need for secure, compliant devices, and platforms and tools that are easy to back up and restore.



Cyber Liability Insurance Isn't a Cure-All

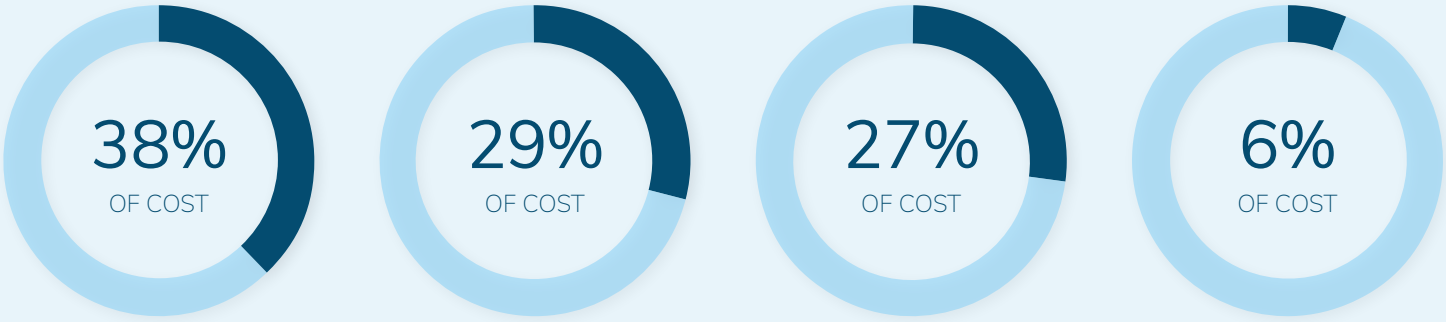
While cyber liability insurance (CLI) might cover an incident, you'll have to prove that your organization has been compliant with its policy terms in order to earn your payout. Scanning for compliance can help you avoid losing a payout in the event of an incident. However, a managed IT service provider (MSP) can help you with this. From GDPR and PHI to HIPAA considerations, an MSP can help you measure and hold accountability to compliance standards relevant to your region and industry.

Personally identifiable information, such as credit card numbers, Social Security numbers, driver's license numbers and healthcare records, as well as company information, customer lists and source code, are all common data breach targets.[3] This has the potential to destroy an organization's reputation in an instant.

Prevention Leads to Better Outcomes

The best outcome, however, when it comes to an expanding attack surface, is prevention. Customer service delays, missed opportunities and reputational damage are all consequences of downtime, even if your insurance policy covers it.

Top 4 Data Breach Costs



Lost Business

Detection & Escalation

Post-Breach Response

Notification[4]

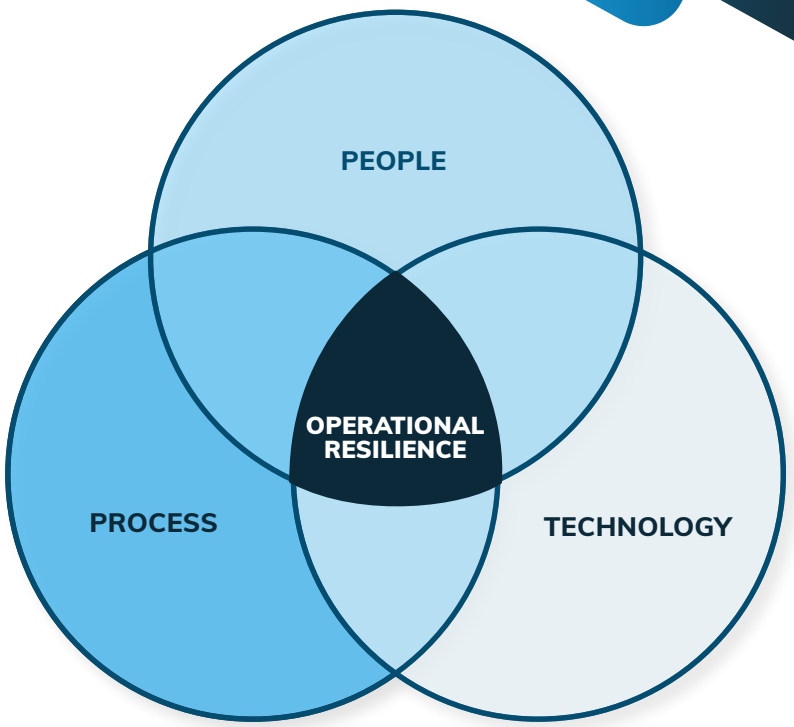
Definition:

Cyber Resilience

According to Forrester, "Cyber resiliency is the ability to predict, resist, recover from, and adapt to both adverse and changing business conditions."[5]

What's Included in Organizational Resilience

Three core elements of organizational resilience are People, Process & Technology — in that order. Ideally, processes and technology should bolster employee resilience, making it easy for them to follow effective paths and pivot as needed to ensure the organization is considering new information and market conditions.



People

Building resilience for people means investing in support systems that support mental health and equip employees with tools to avoid or minimize burnout. This is an important part of a sustainable organization. People aren't disposable. In fact, human capital is an organization's greatest asset.

When a tenured team player walks out the door, not only do you lose all the experiential knowledge they brought to the table, but you also risk losing other employees who are left to pick up the slack. Burnout has become such a global challenge for organizations that the World Health Organization (WHO) formally recognizes it as a disease.[12]

The COVID-19 global pandemic has had a significant impact on the global workforce. According to the U.S. Department of Labor, in the months of April through June of 2021 alone, 11.5 million workers quit their jobs.[13] What's been termed "The Great Resignation" doesn't apply just to the United States. Organizations across the world are facing similar challenges. From Gallup Polls to LinkedIn surveys and labor market studies, this trend shows no sign of slowing anytime soon.

Instead of "getting the most out of employees," consider the cost of burnout. According to the HBR, "burnout is an organizational problem, not an individual one."[14] To combat this issue, some U.S. companies are responding to the rapid rise of workplace burnout by providing "wellness weeks" — a week of the organization shutting down to give employees a chance to relax and recharge.[15]

A balanced approach to performance expectations and work-life balance can deliver significantly more value over time, leading to better employee and customer retention. This curbs recruitment costs and helps bolster organizational stability from a revenue standpoint.

Conduct a Technology Audit

It's really easy during times of crisis to get into "survival mode." Just keeping employees equipped and your business alive could feel like you're biting off more than you can chew. However, continuing to stay in this mode after a crisis has passed can prevent your organization from building resilience. After all, survival and resilience are very different.

As markets grow more stable and predictable, it's critical to assess toolkits, organizational structures, and internal procedures to ensure they're not only relevant, but also supporting security, compliance, and backup best practices, all of which are critical to organizational resilience.

According to TechTarget, an IT audit accomplishes these five tasks[18]:

1. **Evaluates existing systems and processes that secure company data**
2. **Determines risks to a company's information assets**
3. **Identifies methods to minimize data-security risks**
4. **Ensures information management processes are compliant with relevant laws, policies and standards**
5. **Locates inefficiencies in IT systems and system management**

"Organizational resiliency standards, such as ISO and BSI, can prepare organizations for disaster. These questions provide a starting point to validate OR readiness."[19]

– Paul Kirvan, IT Consultant, Auditor & Author, TechTarget

Pro Tip

Organizational resilience doesn't happen overnight. Much like compliance or cybersecurity mastery, it's a practice that requires ongoing evaluation and tuning. The work is never done but the result of the effort can help your organization retain top talent longer and recover from data-loss incidents and other setbacks faster.

Prioritize Technology Gaps to Bridge

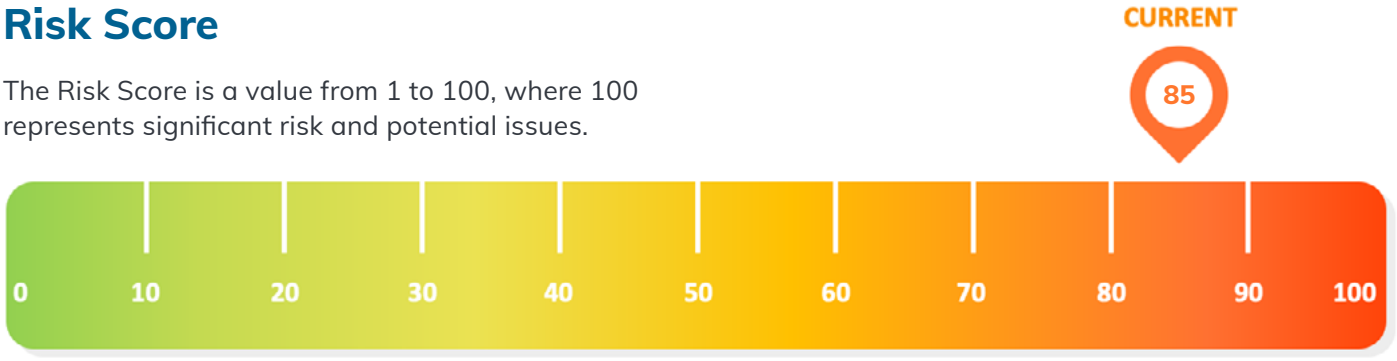
Resilience assessments can seem overwhelming if there's a lot to accomplish. Most technology environments require a fair amount of tuning, routine refreshes and ongoing support to maintain resiliency. Prioritizing tasks based on what's most important, as well as what can help your company improve productivity, customer service or another measure you care about, is a fantastic approach to keep things under control — for both budgets and teams.

Too much change all at once can create unnecessary friction points within your organization, which can result in an increase in costly mistakes, organizational stress and employee or customer churn. To get ahead of these challenges, prioritize and communicate resilience plans, timelines and goals well in advance.

Change takes time. From training people how to use the new technologies to integrating them into existing platforms and documenting new processes, new tech takes time to fully implement and adopt. However, the benefits often outweigh the initial strain.

Risk Score

The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



Pro Tip

Replacing inflexible, legacy technologies that are either no longer supported or offer poor or no integration with your technology stack is a good way to improve your cyber resilience posture.

Change Management for Resilience

Change is stressful, and ironically, adding new technologies to improve organizational outcomes will cause organizational stress. However, this is just another opportunity to put organizational resilience tenets into practice.

You've probably seen this scenario play out before. Executive management selects and implements new technology designed to improve productivity, but it's implemented at such a breakneck pace that it leads to inevitable workflow glitches and stoppages, which ultimately adds to employee stress, reduces productivity and culminates in top talent walking out the door.

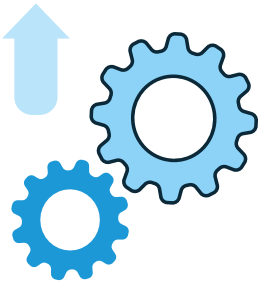
This can be completely avoidable and is an excellent example of why organizational resilience must consider people and technology — in that order.

No matter how far into the weeds we get with technology, automation and the future of work, we must always remember what we're doing is to make life a little easier for employees and customers. This must be the driving force behind technological advancements to ensure long-term success rather than merely short-term gains.

As you look to tried and true frameworks, like Six Sigma, Agile Methodology and other frameworks designed to simplify project and change management, to drive these changes, also be sure to ask:

- How will this impact employees?
- How can we adjust implementation timeframes or practices to minimize stress?
- What feedback loops can we include to ensure colleagues feel heard as we make these changes?

Small perspective shifts like these can help bolster employee resilience and perseverance through meaningful and necessary technology replacements or upgrades.



Plan to Recover Sustainably, Not Just Quickly

In this digital age where everything moves at the speed of light, it can be tempting to rush through process implementations, technology upgrades and new hire training. But at what cost? Speed without accuracy can cost your organization greatly if it impacts uptime and data privacy, causes compliance issues, or unwittingly lets malicious code slip into your network.

Test, Refine, Document

Take the time to implement resilience technologies and strategies well so that they'll work toward making your organization stronger instead of opening the door to additional vulnerabilities. This means taking time to prototype and test new technologies and resilience strategies before launching them organization-wide.

Then, when your tested solutions are production-ready, ensure an adequate training program is in place for all users as well as a designated change manager who can troubleshoot issues that arise and update documentation as needed to reflect new processes.

Implement a Communications Plan

Have a communications strategy in place so that those affected (internal and external) are aware of the change that's coming and know what steps they'll need to take to be successful using new technology or following a new process.

Don't Forget About Your Supply Chain

If your supply chain becomes corrupted, it could affect your organization if you don't have modern cyber resilience technologies in place to identify, isolate and remediate threats as they arise.

From contractors, outside agencies, and third-party suppliers or fourth-party fulfillers, make sure your supply chain is secure. Before entering into partnerships, put measures in place on your side to identify, block, and/or remediate issues that could be introduced by your supply chain and also ask potential partners about the security solutions they have in place to protect your organization.

Mounting Need for Supply Chain Resilience

The need for resilience in supply chains across industries and organizations across the globe is increasing. In fact, McKinsey found that 90% of supply chain leaders recognize the need for greater resilience. [21]

Back to Basics: Agility

Agility is simply the ability to adapt quickly. When it comes to your technology stack, this might entail selecting solutions designed to work together through integration or a common platform.

Anyone who has worked for more than a few months at an organization understands the frustration of duplicating effort due to systems that should theoretically integrate but don't in practice. Building true agility for resilience means this must be rooted out. Like weeds in a garden, poor integration needs to be addressed rather than ignored until it becomes unbearable.

Commit to Tech Stack Integration

Replace legacy technology systems that simply won't integrate with alternatives. The short-term pain of switching platforms is well worth the long-term productivity as well as employee and customer satisfaction gains.

Creating a Culture of Resilience

Nurture trust. Believe it or not, there's a scientific connection between compassion and trust. Health psychologist and Stanford University lecturer Kelly McGonigal suggests that compassion is a predecessor to resilience. A highly competitive, cut-throat environment isn't likely to score high in trust or resilience. So, do the opposite. If organizational resilience is your goal, take the initiative to build your team resilience. Encourage collaboration, encourage compassion and build trusting teams that support each other during difficult times. This is the foundation of resilience.

In addition to compassion promoting human resilience, a study from Deloitte that surveyed CXOs found a strong connection between authenticity and organizational resilience.[22] This means that organizations that practice authenticity are more resilient. Therefore, encouraging compassion and authenticity within your organization can actually bolster organizational resilience.

5 Resilience Questions Deloitte Recommends Business Leaders Ponder

- Are we providing a safe environment for our workers?
- Are we instilling ethical principles in our advanced technology?
- Is our supply chain transparent?
- What cybersecurity protections do we have in place to support our customers' and employees' privacy?
- What mental health resources are we providing our employees?[23]

"Employers who support their workers — by keeping them physically safe, providing adequate mental health resources and enabling flexible work solutions — are more resilient."[24]

– Deloitte