

# From crisis to recovery: A comprehensive guide to business resilience

No business is immune from crisis, so business resilience needs to be a top priority for every company. But what can organisations do to withstand a crisis, respond well, and emerge stronger on the other side?

---

In 2023, PwC found that 91% of businesses say they've recently experienced at least one disruption other than the pandemic. Unsurprisingly, the top concern aside from the pandemic was cybersecurity.

No business is immune from crisis, so business resilience needs to be a top priority for every company. But what can organisations do to withstand a crisis, respond well, and emerge stronger on the other side?

Preparing in advance is essential, and it's important to have a clear crisis plan in place. Here are some strategies your company should consider when it comes to preparing and responding to a business crisis.

## Preparing for physical crises

Physical crises can happen at any time and can be anything from a fire to a devastating weather event to burglary. How prepared is your company for these events?

Often, physical crises are some of the first that organisations consider,

especially since employee safety laws require detailed fire emergency plans and other disaster preparedness protocols. Hopefully, that means your company already has these procedures in place, and you practice them regularly.

As part of your plan, you'll want to have designated emergency preparedness storage for emergency essentials like first aid kits, bottled water, and sanitation supplies. Consider storing these items in multiple locations around the office: that ensures the supplies are nearby no matter where something happens and can help ensure emergency items are available if part of the building is damaged or unsafe.

## Protecting your business from cyber attacks

Cyberattacks are becoming more and more frequent and impact businesses of all sizes. The proliferation of consumer data collection is one reason for this. Businesses that use tools such as artificial intelligence to collect consumer data must be concerned about the ethical implications of AI-powered tools. Simply put, the more data your organisation holds, the more security and privacy issues there are.

AI is so easy to use that even small-to-medium-sized businesses are getting in on it. Just because your organisation is smaller or new doesn't mean you'll be immune to security crises. It may make you a bigger target because thieves think you aren't focused on keeping your security updated.

Cyberattacks have multiple stages where criminals scope out your company, weaponise information, and then deliver malicious files or phishing attacks and exploit your systems. Fortunately, there are a variety of steps you can take to protect your IT systems.

Keeping passwords strong and using two-factor authentication is essential, of course, as is automating as much security as possible. Human error is the source of a vast majority of cyber incidents, so the more you automate, the safer the system will be.

It's also helpful to have systems that detect problems, such as detecting a password breach. Employees and even customers can use weak passwords out of convenience or a sense that nothing bad will happen, but unfortunately, it does. Having a list of breached passwords in your identity management system can help prevent the reuse of these weak passwords, making your security stronger.

Finally, it's vital to have a full cybersecurity response plan that you can implement the moment there's a problem. The plan will help ensure your organisation loses as little data as possible and complies with all laws and regulations about letting affected customers and employees know about the attack.

## Building a resilient team that bounces back from adversity

Whether a crisis is physical, the result of a cyberattack, or comes from a completely different direction, it's important to have a resilient team that can bounce back from a crisis.

There are several ways to build a resilient team in challenging times. First, help ensure everyone on the team understands what their purpose and role in the company is. A clearly defined mission helps employees think creatively about challenges with a focus on their key goals.

Having effective communication among team members is also vital, especially in times of tension or crisis. Clear communication avoids misunderstandings and helps everyone move in the same direction with a unified message.

Finally, building strong relationships within the organisation is essential. Strong relationships help everyone feel connected and invested in the team and its results. It's also easier to check in on everyone's energy levels and mental health when strong relationships are the foundation of the team.

## Is your organisation ready for a crisis?

When it comes to a business crisis, the question isn't "if," it's "when." Preparing in advance for physical crises, cyberattacks, and other issues with written emergency procedures is the first part of being ready for these events.

The other side is creating a team that's bought into the company mission, communicates well, and has strong relationships. This kind of team will be resilient and help your organisation navigate everything from a defined crisis to a major shift in the business environment. A resilient team will be creative and find ways to overcome challenges wherever they come from.

