

HUSTLE MAG

Hustle in Silence.

EDITION 034

VOLUME III

PREMIUM EDITION

RISK

Know your biggest risks

DEPENDENCE

Never depend on one customer



PLANNING

A plan for when things break

LEADERSHIP

Leading through a crisis

THE COVER STORY

RISK & RESILIENCE

Preparing a Business for Setbacks, Shocks and Slow Seasons

HUSTLE MAG — THE COMPLETE BUSINESS COLLECTION · EDITION 034

From the Editors

Every business will face difficult moments. A major customer leaves. A supplier fails. A key person falls ill. Systems go down. The economy slows, a season disappoints or a mistake becomes public. None of these events is unusual. What differs between businesses is how well they are prepared.

Resilience is not pessimism. It is the quiet confidence that comes from having thought about what could go wrong and done something about it in advance. Resilient businesses do not avoid every problem. They absorb shocks, adapt quickly and recover faster, often emerging stronger than competitors who were caught unprepared.

This issue builds that confidence. We begin by identifying your biggest risks and the danger of depending on a few customers or suppliers. We look at operational and digital resilience, surviving financial shocks and preparing a simple continuity plan. We finish with leading through a crisis and building a culture that handles difficulty well.

The best time to prepare for a storm is when the sky is clear. That time is now.

The Editors, Hustle Mag

EDITION 034 · RISK AND RESILIENCE

Contents

	From the Editors	2
	In This Issue	4
	RISK AND RESILIENCE	
01	Knowing Your Biggest Risks	5
	COVER STORY	
02	The Danger of Concentration	11
	DEPENDENCE	
03	Operational Resilience	18
	OPERATIONS	
04	Digital Resilience	24
	TECHNOLOGY	
05	Surviving Financial Shocks	30
	FINANCE	
06	A Continuity Plan	37
	PLANNING	
07	Leading Through a Crisis	43
	LEADERSHIP	
08	A Resilient Culture	49
	CULTURE	
	Your Action Plan	55
	THIRTY DAYS, FOUR STEPS	

Risk and Resilience

Preparing a Business for Setbacks, Shocks and Slow Seasons

Resilience is a business's ability to withstand setbacks, adapt to change and recover quickly. It is built through preparation: understanding risks, reducing dependence on single points of failure, protecting cash and planning responses before they are needed.

This issue builds resilience step by step. We start with identifying your biggest risks and reducing concentration, then strengthen operations and digital systems. We prepare for financial shocks, write a continuity plan, learn to lead through a crisis and build a culture that adapts well.

Each article ends with one step that makes your business harder to break.

The theme: Preparing a business for setbacks, shocks and slow seasons.

01

Knowing Your Biggest Risks

You cannot prepare for every possibility, but you can prepare for the risks that matter most.

FIGURE 01 · YOUR BIGGEST RISKS

A simple risk register

RISK	LIKELY	IMPACT	SCORE	ACTION
Largest client leaves	3	5	15	Diversify clients
Key person ill	3	4	12	Cross-train
Data loss	2	5	10	Test backups
Supplier delay	3	3	9	Find backup

Scores 1–5. Act on the highest first.

Every business faces risks: losing customers, supplier problems, cash shortages, technology failures, legal issues, illness, reputational damage and changes in the market. Many founders avoid thinking about risks because it feels negative or overwhelming. Yet ignoring risks does not make them disappear. It simply leaves the business unprepared.

Understanding your biggest risks allows you to focus effort where it matters most.

List possible risks

Start by brainstorming risks across different areas of the business:

- **Customers:** losing a major client, declining demand or changing preferences.
- **Suppliers:** delays, price increases or failure.

- **People:** illness, departure or skill gaps.
- **Operations:** process failures, quality problems or capacity limits.
- **Technology:** system outages, data loss or cyber attacks.
- **Finance:** cash shortages, late payments or rising costs.
- **Legal and compliance:** disputes or regulatory changes.
- **Reputation:** complaints, negative reviews or public mistakes.

Include risks specific to your industry.

Assess likelihood and impact

For each risk, estimate how likely it is to happen and how serious the impact would be. A simple scale from one to five is sufficient. Multiply the two scores to identify the most significant risks.

Focus on the highest risks

Concentrate first on risks that are both likely and severe. These deserve immediate attention. Lower risks can be monitored and addressed later.

Decide how to respond

There are several ways to respond to risks:

- **Reduce:** take actions to lower likelihood or impact.
- **Transfer:** use insurance or contracts to share risk.

- **Avoid:** stop activities that create unacceptable risk.
- **Accept:** acknowledge minor risks and monitor them.

Choose the most appropriate response for each significant risk.

“New products, customers, people and technologies create new risks.”

Assign owners

Each major risk should have an owner responsible for monitoring it and implementing actions. In very small businesses, the founder may own most risks, but naming owners clarifies responsibility.

Review regularly

Risks change as the business grows. New products, customers, people and technologies create new risks. Review your risk list every quarter.

Look for early warning signs

Many risks show warning signs: declining orders, slower payments, increasing complaints or staff turnover. Monitoring these signals allows earlier action.

A practical tool: the risk register

Create a simple table with columns for risk, likelihood, impact, total score, owner, current controls, next action and review date. Sort by total score. Ten well-considered risks with clear actions are far more useful than a long list nobody reviews.

Questions to uncover hidden risks

Ask: What would hurt the business most if it happened tomorrow? Which person, customer, supplier or system could we not operate without? What has nearly gone wrong in the past year? What keeps me awake at night? What would a competitor do to harm us? These questions often reveal risks that never appear in routine planning.

Common mistakes

Businesses often avoid thinking about risks, create long lists without prioritising, focus only on unlikely disasters or fail to assign responsibility. Others identify risks but never take action. A short, prioritised and regularly reviewed risk register is far more effective.

An example in practice

A small catering company created its first risk register and identified three major risks: dependence on one delivery van, reliance on a single chef and a large share of revenue

from one corporate client. It arranged access to a backup van rental, trained a second cook in key dishes and began marketing to new corporate customers. When the main van broke down during a busy week, the business continued operating without disruption.

Involving the team

People closest to daily work often see risks the founder misses: an unreliable supplier, a fragile process or a customer showing signs of dissatisfaction. Ask the team each quarter what worries them about the business. Their answers make the risk register more accurate and spread responsibility for spotting problems early.

THE TAKEAWAY

Preparation begins with knowing your biggest risks. **Build a risk register with your ten most significant risks, score each for likelihood and impact, assign an owner and choose one action to reduce each of the top three.**

02

The Danger of Concentration

When too much depends on one customer, supplier, person or channel, one change can threaten everything.

FIGURE 02 · CONCENTRATION

Five dependence checks

Customers Share of revenue from the largest.	Suppliers Share of spending with the largest.	Channels Share of new customers from one source.
People Critical tasks only one person can do.	Products Share of profit from one offer.	Target Set a limit for each.

Concentration risk arises when a business depends heavily on a single source: one major customer, one supplier, one marketing channel, one employee or one product. Concentration can be efficient and profitable while things go well. When that single source changes, however, the effect can be severe.

Reducing concentration is one of the most practical ways to strengthen resilience.

Customer concentration

Many small businesses rely on one or two large customers for much of their revenue. Losing such a customer can create sudden cash shortages and force difficult decisions.

Calculate the percentage of revenue from your largest customers. If one customer represents a large share of revenue, develop a plan to diversify.

Supplier concentration

Depending on a single supplier creates risk if prices rise, quality declines or deliveries stop. Identify critical suppliers and consider backup options, even if you continue using your preferred supplier.

Channel concentration

Businesses that rely on one marketing channel, such as a single social platform, marketplace or advertising source, are vulnerable to changes outside their control. Build multiple channels, especially those you own, such as your website and email list.

People concentration

If only one person knows how to perform an important task, the business is vulnerable to illness, absence or departure. Document processes and cross-train team members.

Product concentration

A business relying on one product or service may struggle if demand changes. Consider whether complementary offers could provide additional stability.

Diversify gradually

Diversification does not mean abandoning successful relationships. It means reducing dependence gradually by developing new customers, suppliers, channels or capabilities.

“If only one person knows how to perform an important task, the business is vulnerable to illness, absence or departure.”

Strengthen key relationships

While diversifying, maintain strong relationships with major customers and suppliers. Regular communication, excellent service and clear agreements reduce the likelihood of sudden losses.

Monitor concentration regularly

Review concentration levels every quarter. Growth can change the balance unexpectedly, especially if one customer or channel grows faster than others.

A practical tool: the concentration check

Calculate five numbers every quarter: the share of revenue from your largest customer, from your top three customers, the share of spending with your largest supplier, the share of new customers from your main channel and the number of critical tasks only one person can do. Set a target for each and track progress.

Questions about dependence

Ask: What would happen if our largest customer left next month? If our main supplier stopped delivering? If our main platform changed its rules? If our most experienced person resigned? Each question reveals where a backup plan or diversification effort is needed most.

Common mistakes

Businesses often celebrate large customers without recognising the risk, use only one supplier, depend entirely on one marketing platform or rely on one person for critical knowledge. Others diversify too quickly and lose focus. Gradual, deliberate diversification creates stronger foundations.

An example in practice

A marketing agency earned sixty percent of its revenue from one client. When the client announced budget cuts,

the agency faced a serious challenge. Afterwards, the founder set a goal that no client would exceed twenty-five percent of revenue, increased marketing to new clients and documented processes so work could move between team members. Within two years, the agency was far more stable and less dependent on any single relationship.

Concentration and opportunity

Some concentration is unavoidable, especially in a young business. A first large client may fund the business's early growth. The aim is not to refuse large opportunities but to use them wisely: build reserves while revenue is strong and invest part of the profit in finding new customers before the relationship changes.

Concentration in skills

Beyond people, consider concentration in skills. If the business depends on a single specialist ability, such as one type of software or one technical skill held by few people, invest in training others or documenting the knowledge before it becomes a constraint.

THE TAKEAWAY

Too much dependence on one source creates fragility. Complete a concentration check for customers, suppliers, channels and people, set a target for each and take one step this month to reduce your most dangerous dependence.

03

Operational Resilience

When something breaks, resilient operations keep customers served. Build backups before you need them.

Operational resilience is the ability to keep serving customers when something goes wrong: a key person is absent, equipment fails, a supplier is late, demand surges or a process breaks. Businesses with strong operational resilience recover quickly and maintain customer trust. Those without it can grind to a halt.

Identify critical operations

Start by identifying the activities your business cannot stop without seriously affecting customers: taking orders, producing goods, delivering services, providing support or processing payments. These are your critical operations.

Find single points of failure

For each critical operation, ask what would happen if one element failed. Could the business continue if a particular person, machine, supplier or software tool became unavailable? Single points of failure are major risks.

Document critical processes

Clear documentation allows others to perform important tasks when needed. Procedures, checklists and templates reduce dependence on individual knowledge.

Cross-train team members

Ensure at least two people can perform each critical task. Cross-training improves resilience and provides flexibility during holidays, illness or busy periods.

Maintain equipment

Regular maintenance reduces the risk of unexpected equipment failure. Keep maintenance records and know how to obtain repairs or replacements quickly.

Arrange backup suppliers and partners

Identify alternative suppliers, contractors or partners who could support the business if your usual providers are unavailable. Maintain contact details and test relationships where possible.

Build flexible capacity

Consider how you would handle sudden increases in demand. Options may include trained freelancers, temporary staff, extended hours or prioritising key customers.

“Options may include trained freelancers, temporary staff, extended hours or prioritising key customers.”

Test your arrangements

Practise using backup arrangements before a crisis. For example, ask another team member to perform a critical process or test whether backup systems work.

A practical tool: the critical operations map

List each critical operation with its main person, backup person, key equipment, key supplier, backup supplier and documentation status. Mark any operation without a backup in red. The map shows immediately where a single failure could stop the business.

Questions to test resilience

Ask: If our main person for this task were unavailable for two weeks, who would do it? If this equipment failed today, how quickly could it be repaired or replaced? If this supplier stopped delivering, what would we do tomorrow? Answering honestly reveals which backups need attention first.

Common mistakes

Businesses often rely on one person for critical tasks, neglect equipment maintenance, lack backup suppliers or assume backup arrangements will work without testing. Others focus only on large disasters while overlooking common disruptions. Practical preparation for everyday failures creates strong operational resilience.

An example in practice

A small printing company depended on one experienced operator to run its main press. When he was unexpectedly ill for two weeks, production slowed dramatically. Afterwards, the owner trained two other team members, documented press procedures, arranged a service agreement for urgent repairs and identified a partner printer for overflow work. Future absences caused only minor delays.

Resilience in a very small business

For a solo founder or tiny team, cross-training may not be possible. Instead, build resilience through documentation, relationships with trusted freelancers who could step in, clear communication templates for customers during delays and enough buffer in delivery timelines to absorb small disruptions without breaking promises.

Prioritising during disruption

When capacity falls suddenly, decide in advance which customers and tasks come first: urgent safety issues, contractual deadlines, long-standing customers or high-value orders. A simple priority list prevents panicked decisions and helps the team act consistently while the disruption lasts.

Learning from small failures

Every small disruption, such as a late delivery, a sick day or a broken tool, is a rehearsal for larger ones. After each, ask what slowed recovery and what one change would help next time. Small improvements made regularly build resilience far more effectively than a single large plan written once and forgotten.

THE TAKEAWAY

Operational resilience keeps customers served when something breaks. **Map your critical operations, identify single points of failure, cross-train at least one person on each critical task and test one backup arrangement this quarter.**

04

Digital Resilience

When systems fail or data is lost, preparation decides whether the disruption lasts minutes or weeks.

Most modern businesses depend on digital systems: email, websites, payment platforms, accounting software, customer records, cloud storage and communication tools. When these systems fail or data is lost, operations can stop suddenly. Cyber attacks, accidental deletion, account lockouts and service outages can all disrupt a business.

Digital resilience is the ability to protect systems and recover quickly when problems occur.

Identify critical systems

List the digital systems your business cannot operate without. For each one, note what it does, who owns it, who has access and what happens if it becomes unavailable.

Back up critical data

Regular backups protect against accidental deletion, hardware failure, ransomware and account problems. Back up important files, customer data, financial records and website content. Store backups separately from the original systems.

Test restoration

Backups are only useful if they can be restored. Periodically test whether data can be recovered and how long it takes.

Secure accounts

Use strong, unique passwords and enable two-factor authentication on critical accounts. Restrict access to those who need it and remove access promptly when people leave.

Keep recovery information current

Ensure account recovery details, such as phone numbers and backup email addresses, are accurate. Store important recovery codes securely.

Plan for outages

Consider what you would do if a critical system were unavailable for a day or a week. Could you take orders manually, communicate with customers through another channel or continue operations with limited functionality?

“Ensure account recovery details, such as phone numbers and backup email addresses, are accurate.”

Use reputable providers

Choose established technology providers with clear

security practices, reliable support and data export options. Understand how they back up and protect your data.

Train your team

Teach team members to recognise phishing attempts, suspicious requests and unsafe practices. Encourage them to report concerns quickly.

A practical tool: the digital recovery sheet

For each critical system, record: what it does, who administers it, where backups are stored, how to restore them, how to recover account access, the provider's support contact and a manual workaround if the system is unavailable. Keep a copy offline. In a crisis, this sheet saves hours of panic.

Questions about each system

Ask: If this system disappeared today, what would we lose? How recent is our last backup? Have we ever tested restoring it? Who else can access the administrator account? Could we keep serving customers without it for a day? Clear answers show which systems need attention first.

Common mistakes

Businesses often assume cloud providers back up

everything automatically, never test backups, share passwords, rely on one person for administrator access or have no plan for outages. Others delay security improvements until after an incident. Proactive preparation significantly reduces disruption.

An example in practice

A small online shop lost access to its email account after a security breach. Because its website, payment notifications and supplier communications were linked to that account, operations stopped for several days. Afterwards, the owner enabled two-factor authentication, created backup administrator access, documented recovery procedures and scheduled regular backups. When another login issue occurred months later, access was restored within an hour.

Planning for provider problems

Sometimes the problem is not your business but a provider's outage. Know where to check service status, how to contact support quickly and how to communicate with customers during the disruption. A short, honest message explaining the delay and when you expect to recover preserves trust far better than silence.

Ownership of digital assets

Make sure the business owns its domain name, website, social accounts and key software subscriptions, registered

to business email addresses with at least two administrators. Assets registered to former employees, freelancers or personal accounts can be lost entirely when relationships end.

THE TAKEAWAY

Digital resilience depends on backups, security and recovery planning. **List your critical systems, confirm backups exist for each, test one restoration this month, enable two-factor authentication everywhere and create a digital recovery sheet stored offline.**

05

Surviving Financial Shocks

Revenue can fall faster than costs. Preparation gives you time to respond rather than react.

FIGURE 05 · FINANCIAL SHOCKS

A three-level response plan

LEVEL 1	Tighten spending; increase sales effort.
----------------	--

Revenue -10%

LEVEL 2	Pause investments; renegotiate terms.
----------------	---------------------------------------

Revenue -20%

LEVEL 3	Deeper cuts; consult advisers.
----------------	--------------------------------

Revenue -30%

Agree triggers and actions in calm times.

Financial shocks can arrive suddenly: a major customer leaves, sales fall during an economic downturn, a supplier raises prices sharply, a large unexpected cost appears or payments are delayed. Businesses with strong cash reserves, flexible costs and clear plans can absorb these shocks. Others may face difficult decisions quickly.

This article provides general information, not financial advice. Consult a qualified adviser for your circumstances.

Maintain cash reserves

Cash reserves provide time to respond. Many businesses aim to hold several months of essential operating costs, but the right amount depends on income stability, seasonality and fixed costs.

Know your essential costs

Identify the costs required to keep the business operating: rent, salaries, key suppliers, loan repayments and essential software. Knowing these costs helps you understand how long reserves could last.

Build flexibility into costs

Businesses with flexible costs adapt more easily. Monthly contracts, freelancers, scalable tools and shared spaces can reduce risk compared with long fixed commitments.

Prepare scenario plans

Use cautious and difficult cash flow scenarios to understand how the business would respond to lower sales or delayed payments. Identify trigger points that would prompt action.

Prioritise actions in advance

Prepare a list of actions you could take if revenue fell: pausing discretionary spending, delaying non-essential investments, renegotiating supplier terms, increasing sales activity or adjusting staffing. Planning ahead makes difficult decisions faster and calmer.

Communicate early

If cash flow problems arise, communicate early with suppliers, lenders, landlords or other stakeholders. Many are more flexible when informed promptly and offered a credible plan.

“During financial pressure, maintaining service quality is essential.”

Protect customer relationships

During financial pressure, maintaining service quality is essential. Losing customers through poor service can deepen financial problems.

Review insurance and finance options

Understand what insurance policies cover and whether finance options, such as an agreed overdraft or line of credit, could provide temporary support. Arrange options before they are needed where possible.

A practical tool: the shock response plan

Write a one-page plan with three trigger levels. Level one, such as revenue ten percent below plan for two months: tighten discretionary spending and increase sales activity.

Level two, twenty percent below: pause investments and renegotiate terms. Level three, thirty percent below: activate deeper cost reductions and consult advisers. Agreed triggers turn panic into process.

Questions to test your preparation

Ask: How many months could we cover essential costs if revenue stopped? Which costs could we reduce within a week, a month and a quarter? Who would we need to talk to first? What finance could we access, and at what cost? Clear answers show how much time a shock would give you to respond.

Common mistakes

Businesses often operate with no cash reserve, rely on optimistic forecasts, carry high fixed costs, delay difficult conversations or make sudden cuts without a plan. Others assume finance will always be available when needed. Preparation and early action reduce the impact of financial shocks.

An example in practice

A small events business saw bookings fall sharply during an economic downturn. Because it had built a reserve covering four months of essential costs and prepared a response plan, it reduced discretionary spending, negotiated temporary payment arrangements with key

suppliers and focused marketing on smaller private events. The business remained stable and recovered as demand returned.

Lessons for the good times

The best preparation for a shock happens during strong periods: building reserves from surplus months, keeping fixed costs flexible, diversifying customers and arranging finance options while the business looks healthy. Founders who use good times to prepare rarely face difficult times without options.

Protecting the owner

Financial shocks affect founders personally too. Keep personal savings separate from business funds, understand any personal guarantees you have signed and avoid moving personal money into the business without a clear plan. Protecting your personal finances preserves your ability to make calm decisions for the business.

THE TAKEAWAY

Preparation turns financial shocks into manageable challenges. **Calculate how many months your reserves would cover essential costs, write a three-level shock response plan with clear triggers and arrange any finance options before you need them.**

06

A Continuity Plan

When disruption strikes, a short written plan prevents panic and keeps the business serving customers.

FIGURE 06 · A CONTINUITY PLAN

One page per disruption

1 Who acts first A named person.	2 First three actions In order.	3 Who to contact Staff, suppliers, providers.
4 Keep running Critical activities only.	5 Tell customers A prepared message.	Store it Offline as well as online.

A continuity plan describes how the business will continue operating during and after a disruption: illness, equipment failure, system outages, supplier problems, extreme weather, building access issues or other unexpected events. Many small businesses assume such plans are only for large organisations. In reality, a simple plan can make a significant difference.

The goal is not to predict every event, but to prepare clear responses for the most likely disruptions.

Identify likely disruptions

Use your risk register to identify the disruptions most likely to affect the business. Common examples include loss of a key person, technology outages, supplier failures, premises access problems and sudden spikes or drops in demand.

Define critical activities

Determine which activities must continue during a disruption, such as serving customers, processing orders, paying staff or responding to urgent issues. Prioritise these activities.

Assign responsibilities

Decide who will lead the response, who will communicate with customers and staff, and who will handle specific tasks. Clear responsibilities prevent confusion during stressful situations.

Prepare contact information

Maintain an up-to-date list of contact details for staff, key customers, suppliers, service providers, insurers, advisers and emergency contacts. Store copies in more than one location.

Document recovery steps

For each likely disruption, outline the immediate steps to take. For example, if a key system fails: notify the provider, switch to manual processes, inform customers if necessary and restore data from backup.

Plan communication

Prepare templates for communicating with customers, staff and suppliers during disruptions. Clear, timely communication maintains trust.

“Walk through scenarios with your team and update the plan based on lessons learned.”

Keep the plan accessible

Store the plan where it can be accessed even if normal systems are unavailable. A printed copy or offline file may be useful.

Test the plan

Review the plan periodically and test key elements. Walk through scenarios with your team and update the plan based on lessons learned.

A practical tool: the one-page continuity plan

For each of your three most likely disruptions, write: the first person to act, the first three actions, who to contact,

how to keep critical activities running and how to communicate with customers. Add a contact list at the bottom. One page per disruption is enough for most small businesses.

Questions to test the plan

Ask: If the founder were unreachable for a week, who would make decisions? If the premises were inaccessible, where would we work? If our main system went down on our busiest day, what would we do in the first hour? Walking through these scenarios with the team often reveals gaps that are easy to fix.

Common mistakes

Businesses often create no plan, write lengthy documents nobody reads, store the plan only in systems that may fail or never test it. Others plan only for rare disasters while ignoring common disruptions. A short, practical and tested plan is more valuable than a detailed document that sits unused.

An example in practice

A small accountancy practice created a one-page continuity plan covering three scenarios: office inaccessibility, a system outage and the absence of the founder. When severe weather prevented staff from reaching the office, the team followed the plan, switched to remote working using

pre-arranged access and continued serving clients without interruption. Clients barely noticed the disruption.

Reviewing after real events

Whenever a disruption actually occurs, review the response afterwards: what worked, what was missing and what should change in the plan. Real events are the best test of any plan, and each review makes the business better prepared for the next disruption.

Continuity for the founder

For many small businesses, the founder is the greatest continuity risk. Record key passwords securely, document important relationships and decisions, and name a trusted person who could make essential decisions if you were unexpectedly unavailable. This preparation protects customers, staff and your own family.

THE TAKEAWAY

A short continuity plan helps the business continue when disruption strikes. **Write a one-page continuity plan for your three most likely disruptions, assign responsibilities, prepare communication templates and store copies where they remain accessible during an outage.**

07

Leading Through a Crisis

In a crisis, people look to the leader for calm, clarity and honesty. These matter more than having every answer.

A crisis may take many forms: a major customer loss, a public complaint, a serious operational failure, a cyber incident, an economic shock or a health emergency affecting the team. In these moments, people look to the founder for direction. The way a leader responds can shape whether the business recovers quickly or suffers lasting damage.

Effective crisis leadership depends on calm thinking, clear communication and decisive action.

Stay calm

Panic spreads quickly. Take a moment to understand the situation before reacting. A calm leader helps others focus on solutions rather than fear.

Establish the facts

Gather accurate information as quickly as possible. What happened? Who is affected? What risks exist? Avoid acting on rumours or incomplete information.

Prioritise immediate safety and stability

Address urgent issues first: protecting people, securing systems, preventing further damage and maintaining essential services.

Communicate clearly and honestly

Share what you know, what you do not yet know and what actions are being taken. Honest communication builds trust, even when the news is difficult.

Communicate regularly with staff, customers, suppliers and other stakeholders as appropriate.

Assign responsibilities

Clarify who is responsible for specific actions. During a crisis, confusion about roles can slow the response.

Make decisions with available information

Waiting for perfect information can delay important actions. Make the best decisions possible with the information available, then adjust as the situation develops.

“Make the best decisions possible with the information available, then adjust as the situation develops.”

Look after people

Crises create stress. Check on team members, recognise their efforts and ensure workloads remain manageable. Supporting people helps maintain performance and loyalty.

Learn afterwards

After the immediate crisis passes, review what happened. What worked well? What could have been handled better? Update plans, systems and processes based on lessons learned.

A practical tool: the first-hour checklist

Prepare a short checklist for the first hour of any crisis: ensure people are safe, gather the facts, contain further damage, decide who leads the response, agree the first message to staff and customers, and schedule the next update. Keep it with your continuity plan. A checklist steadies thinking when stress is highest.

Questions during a crisis

Ask repeatedly: What do we know for certain? What do we not yet know? Who is affected, and what do they need from us now? What is the most important thing to do in the next hour? When will we next update everyone? Simple questions keep the response focused and prevent paralysis.

Common mistakes

Leaders often react emotionally, delay communication, speculate without facts, try to handle everything alone or forget to support their team. Others focus only on immediate fixes and neglect lessons afterwards. Calm, transparent and organised leadership helps businesses recover more effectively.

An example in practice

A small software company experienced a service outage that affected many customers during a busy period. The founder quickly assembled the team, assigned responsibilities and posted regular updates explaining the problem, progress and expected recovery time. Customers appreciated the transparency, and after service was restored, the company published a summary of improvements made to prevent future outages. Customer loyalty remained strong.

Looking after yourself in a crisis

Founders often carry the heaviest load during a crisis and neglect their own wellbeing. Take short breaks, sleep when you can and share the burden with trusted colleagues or advisers. A leader who is exhausted makes poorer decisions; looking after yourself is part of looking after the business.

Communicating with customers in a crisis

Customers usually forgive problems more readily than silence. Tell affected customers what happened, what it means for them, what you are doing and when they will hear from you next. Keep messages short, factual and human. After the crisis, explain what has changed to prevent it happening again.

THE TAKEAWAY

In a crisis, calm, clarity and honesty matter most. **Prepare a first-hour crisis checklist, decide who leads and who communicates, and commit to giving regular, honest updates to your team and customers whenever a crisis occurs.**

CULTURE · 4 MIN READ

08

A Resilient Culture

Plans and reserves help, but resilience ultimately lives in how people respond to difficulty.

Plans, reserves and backups are essential, but resilience ultimately depends on people. A resilient culture is one where team members adapt to change, solve problems, support each other and learn from setbacks. When difficulties arise, these behaviours help the business respond quickly and recover effectively.

Culture shapes how people react when things go wrong.

Encourage openness

People should feel comfortable raising concerns, reporting mistakes and sharing bad news early. Problems discovered early are usually easier to solve. Leaders can encourage openness by responding constructively rather than with blame.

Learn from mistakes

Treat mistakes as opportunities to improve processes, systems and decisions. Ask what happened, why it happened and what can be changed. A learning mindset strengthens the business over time.

Build adaptability

Encourage team members to develop a range of skills and understand different parts of the business. Cross-training and shared knowledge make teams more flexible during disruptions.

Share information

Keep team members informed about business performance, challenges and priorities. People who understand the context can make better decisions and adapt more quickly.

Support one another

Resilient teams help colleagues during busy periods, illness or unexpected challenges. Recognise and encourage collaboration.

Focus on problem-solving

When challenges arise, focus discussions on solutions rather than blame. Encourage people to suggest ideas and take initiative.

Celebrate recovery

Recognise teams that respond well to setbacks. Celebrating recovery reinforces resilience and builds confidence for future challenges.

“Resilience depends on people having the energy to cope with difficulty.”

Look after wellbeing

Resilience depends on people having the energy to cope with difficulty. Encourage reasonable workloads, rest and support during stressful periods.

A practical tool: the after-action review

After any significant problem or disruption, hold a short meeting with four questions: What happened? What went well? What could we do better? What will we change? Record the answers and actions. Regular reviews build a habit of learning that strengthens the whole team over time.

Questions to understand your culture

Ask the team: Do you feel comfortable raising problems early? What happens when someone makes a mistake? Do you know enough about the business to make good decisions under pressure? Who would you turn to for help in a crisis? Honest answers show where culture supports resilience and where it needs attention.

The founder's example

How the founder responds to setbacks sets the tone for everyone. Admitting mistakes openly, staying calm under pressure and focusing on solutions shows the team what resilience looks like in practice. Over time, the team adopts

the same habits.

Common mistakes

Businesses often blame individuals for problems, discourage people from reporting bad news, keep information within a small group or ignore stress during difficult periods. Others focus only on systems while overlooking culture. Openness, learning, adaptability and support create resilient teams.

An example in practice

A small manufacturing company experienced a production problem that delayed several customer orders. Instead of searching for someone to blame, the owner held an after-action review with the team. Together they identified a gap in quality checks and a missing supplier backup. The team implemented improvements and later handled a similar issue much more quickly. Team members said they felt trusted and more willing to raise concerns early.

Resilience in hiring and onboarding

Resilient culture begins with who joins the team and how they are welcomed. During hiring, ask candidates how they handled setbacks or mistakes. During onboarding, explain how the business responds to problems and encourage new team members to raise concerns from their first week.

Small habits that build resilience

Resilience grows through small, repeated habits: sharing a weekly update on how the business is doing, thanking someone who reports a problem early, rotating tasks occasionally so skills spread and pausing after busy periods to recover. None of these is dramatic, but together they prepare a team to handle real difficulty.

THE TAKEAWAY

A resilient culture helps people respond well when things go wrong. **Hold an after-action review after your next problem or disruption, respond to mistakes with curiosity rather than blame and share key business information with your team so they can adapt quickly.**

BEFORE YOU CLOSE THIS ISSUE

Your Action Plan

Turn what you have read into the next thirty days.

Your next 30 days

Week 1: Build a risk register. List your ten biggest risks with likelihood, impact and one action to reduce each.

Week 2: Check concentration. Calculate the share of revenue from your largest customers and spending with your largest suppliers.

Week 3: Protect operations. Document key processes, back up critical data and identify who covers each role.

Week 4: Write a continuity plan. Prepare a one-page plan for your three most likely disruptions.

Keep learning

Hustle Influence offers practical online courses and AI tools that help you turn ideas into action.

hustleinfluence.com

HUSTLE MAG

Hustle in Silence.

THE HUSTLE MAG COLLECTION · VOLUME III · EDITION 034

Continue with practical courses and AI tools at

hustleinfluence.com