How to become a more resilient manufacturer

A guide to planning for and managing disruption

WIPFLI

Resilience has emerged as a key competitive differentiator

It has become shorthand for a manufacturer’s ability to manage disruption, pivot to new opportunities and scale operations to meet demand.

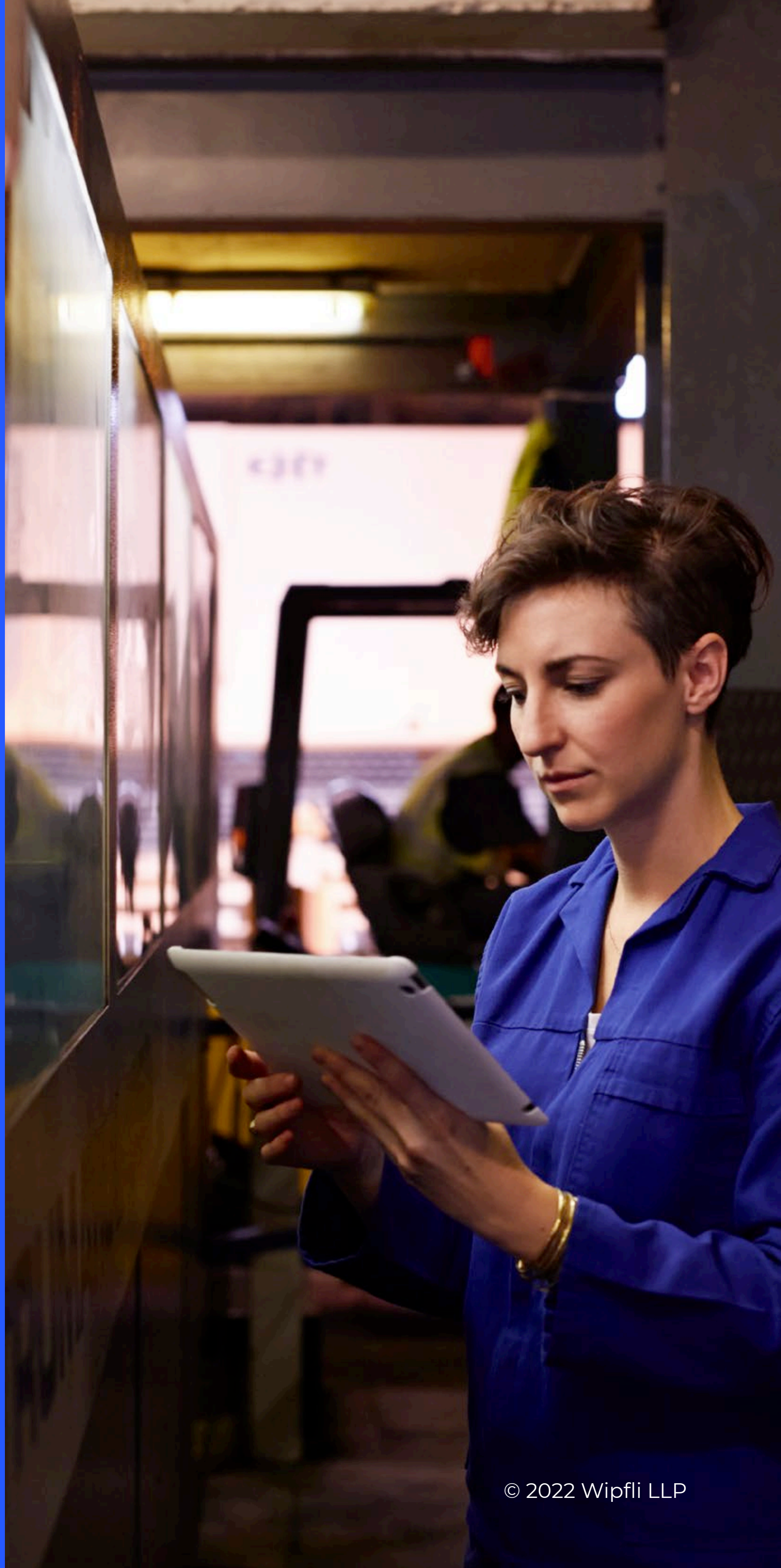
But the need for resilient manufacturing will not decline as the COVID-19 pandemic recedes. Evolving customer expectations, cyber threats, supply chain hurdles, unplanned downtime and other challenges have made disruption a mainstay of the manufacturing industry. As a result, resiliency is increasingly a factor in your ability to not just meet the challenge of the moment but also capture more revenue and new markets.

Resilient manufacturers have strategies in place to reduce risk and the business agility to quickly and decisively react when threats arise. But how do they do it?

Our e-book can help you better understand how to:

- Become more agile
- Increase your resilience to disruption
- Protect your operations from digital disruption
- Create a more robust business continuity program
- Use resilience as a competitive differentiator

Altogether, we’ll show you how to increase your resilience — and your competitiveness.



Becoming more agile

In a recent Wipfli survey of nearly 200 manufacturers, just 28% of respondents said they could get new products and services to customers in less than six months. Another 38% said 6-12 months. That leaves one-third of respondents late to the party when it comes to innovation and rising trends.

It's not due to a lack of desire or drive or vision. Rather, work is being left on the table because of a lack of agility — the ability to react in a proper and timely manner to both threats and opportunities. Agility is having the ability to last — to run your business in such a way that you stay in business. And that, after all, is the essence of resilience.

Manufacturing resiliency, one iteration at a time

To become more agile, manufacturers need to invest in the tools and processes that unshackle responsiveness and innovation without cutting corners.

For example, you could invest in capabilities that allow for faster prototyping, such as 3D printing or digital models. You could implement robotic process automation to make back-office functions more efficient so you have more time for managing exceptions. Or you could invest in data analytics tools to eliminate costly and time-intensive reporting activities.

Instead of waiting until month-end to review sales and production reports, you could have that information on demand at your fingertips to enable faster decision-making.

There are strategies to make improving your resilience a manageable undertaking. Rather than set out to transform your operations in one step, focus on incremental change. Target those improvements that are necessary to increase resilience. Then, break them down into smaller chunks, or versions, that can be easily managed and tracked. Finally, review, assess and adapt to improve the next iteration.

Rather than set out to transform your operations in one step, focus on incremental change.

Fine-tuning through feedback loops

The key is to tie every improvement to a feedback loop so you can adjust your course as you go. For every action you take, there are two questions that you should ask:

- Did we accomplish what we intended?
- What other insights did we gain that we didn't plan for?

In terms of the first question, it's not so much about checking tasks off a list. It's about measuring the impact on your strategic goals.

For example, perhaps you're unable to take on additional work because, like many manufacturers, you are shorthanded. You decide to automate sections of the shop where you need to increase throughput. If you accomplished what you intended, you should see more capacity for increased volume. That was an intended result. A reduction in employee burnout and absenteeism could be an unintended but beneficial insight that you gained.

The shorter the feedback loops, the more responsive you can be. Did the changes you make move the dials in the direction you wanted to go? If not, why not? What got in the way? Were incorrect assumptions made about market behavior or what customers value? Did you automate the right areas of the business? Remember, rapid assessment and response are fundamental to agility.

The good news is, most manufacturers have at least some of the tools they need for gathering feedback — think about all of the data captured by your customer relationship management platform or your enterprise resource planning system. Rather than ripping out and replacing your infrastructure with new platforms and applications, you may simply be able to build on the capabilities you already have.

By making small changes and recalibrating as you go, you will iteratively create a more resilient organization that can stay ahead of challenges and get the jump on new openings.

Increasing your resilience to disruption

One of the biggest keys to becoming a more resilient manufacturer is to understand what's within your sphere of control and your sphere of influence — and to frame your efforts accordingly.

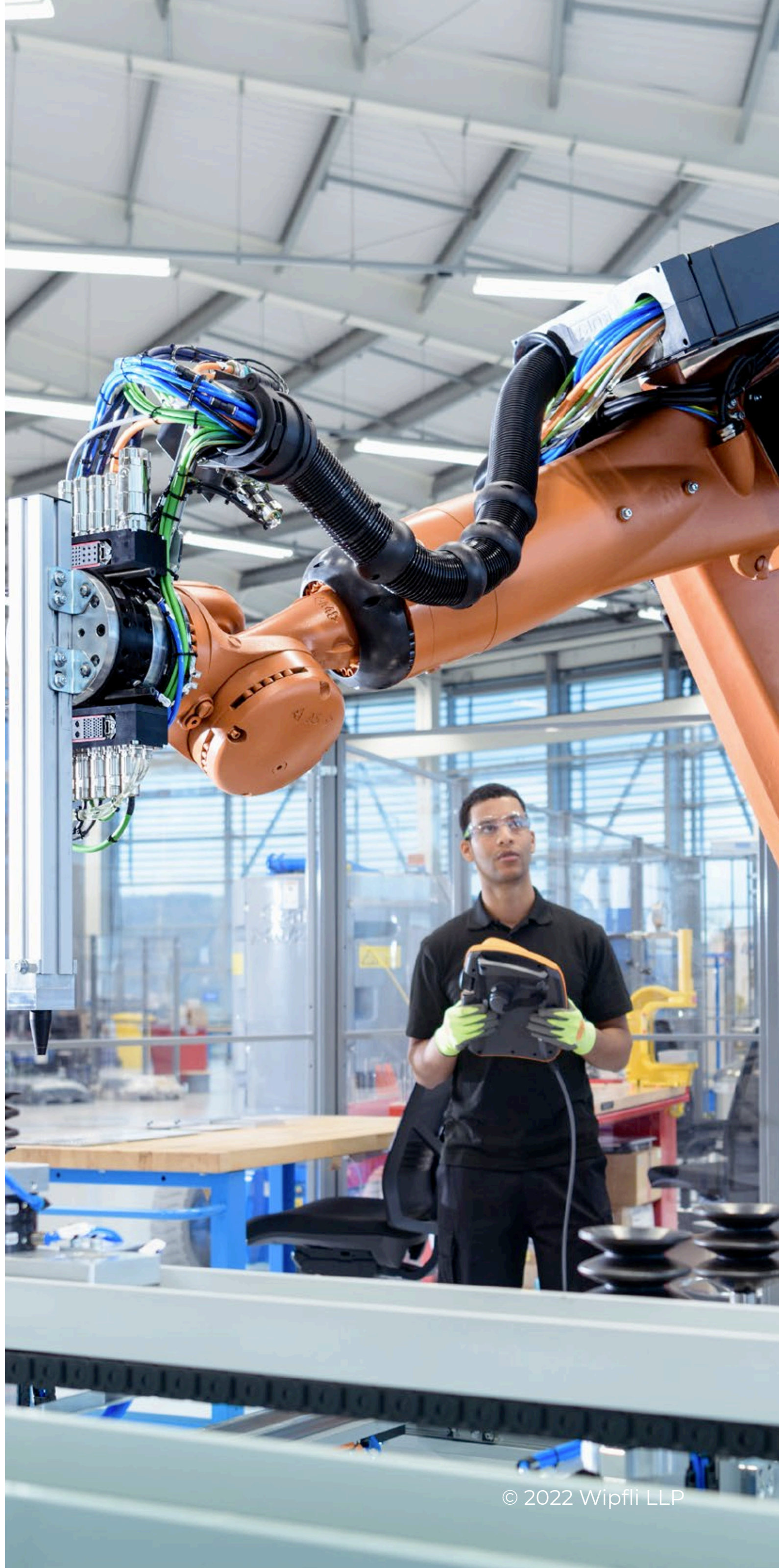
- Your sphere of control is exactly what it sounds like: the activities, processes, people, decisions and outcomes that take place within the four walls of your operation.
- Your sphere of influence refers to the outcomes that are one step removed from your four walls — in other words, your direct suppliers and direct customers.

With that in mind, here are five areas where you can shore up your operations to decrease your vulnerability to disruption:

1. IT infrastructure and technology (sphere of control)

Unplanned downtime is one of the biggest risks to any manufacturer, which is why your technology platform is a key place to fortify your operations. What functions are essential to your business, and how are you ensuring 24/7 support for them? Are you leveraging tools and strategies that decrease risk? Or are you still operating with on-premises servers and software, which experience more downtime than services in the cloud?

The best course of action is to conduct a technology audit and create a technology roadmap with the aim of building a resilient network. Don't be intimidated by the scope of work; you can prioritize initiatives based on your business imperatives, making this a much more manageable task.



2. Cybersecurity (sphere of control)

No manufacturer of any size is free from the risk of a cyberattack. As your operations increasingly go digital, you need to ensure measures are in place to protect your data from theft. A cybersecurity specialist or managed security service provider can assist with checking your digital footprint for vulnerabilities, testing your systems, building a multilayered defense and training your staff on how to prevent intrusion. Not only is it a matter of protecting your operations from disruption; it will also help keep your insurance premiums down.

3. Labor (sphere of control)

The workforce shortage is forcing many manufacturers to delay or shelve their plans for expansion. Fortunately, there are several options for extending your workforce, from expanding your talent pool to reskilling your current staff to strategically investing in automation.

Another area to consider is restructuring your benefits package to better appeal to generational differences. For example, older workers tend to want a more robust and affordable health benefits package, while younger workers tend to value higher pay and are therefore more agreeable to a larger deductible. So why not offer different benefits packages? This is an area where creative thinking and an agile response could become a differentiator in the search for talent.

4. Customer base (sphere of influence)

Customers prefer doing business with companies that make their lives easier. When you build a deeper understanding of what your customers value and prove that you can deliver better than your competitors, you can shift from being a vendor to a partner. This creates opportunities to enter into steady engagements, such as larger production runs, longer-term contracts or longer purchase events. In this way, you can take a volatile component of your business — demand — and make it more predictable.

How resilient are manufacturers?

31% of manufacturers have a dedicated resiliency strategy aligned with business strategies and goals

5% of manufacturers have standardized work and systems throughout their organizations

60% of manufacturers purchase a quarter or more of materials and components from a single supplier

45% of manufacturers have experienced three or more data breaches in the past year

Source: Resilient manufacturers study: 2022 research report

5. Supply chains (sphere of influence)

By now, you know you need to shore up your supply chain against disruption. But let's face it, your supply chain might begin in one part of the world and end in another. Your ability to manipulate logistics at that scale is extremely limited. But just as you can nurture contractual relationships with your customers, you can look for opportunities to become a preferred partner to your suppliers.

If you agree to enter into longer-term contracts or purchase larger volumes, will it provide your suppliers with greater predictability to meet demand? And if you can provide your suppliers with greater predictability, could that help them forge stronger ties with their suppliers? If so, you can straighten out some of the wrinkles that create stress in your operations.

Protecting your operations from digital disruption

There's a saying that if you don't want to get hacked, disconnect everything from the internet. But of course that's not an option in today's manufacturing industry. Digital transformation and Industry 4.0 technologies are creating efficiencies, intelligence, customer engagement opportunities and profitability that can't be replicated by analog operations.

Unfortunately, increased digitization also creates greater risk to your data and operations — and no manufacturer is too small to be safe from cybercriminals. You might think no one would hack you because your data isn't valuable to others, but hackers will disagree. They have figured out that your data is valuable to you, and that you'll likely pay to get it back. Nearly half of respondents in Wipfli's manufacturing survey had experienced three or more network breaches in the past year.

Strengthening the resilience of your manufacturing operations

It's not just a matter of protecting data. Cyberattacks can jump the border from digital to physical by locking up or seizing equipment. This is bad enough for operational uptime, but it can also pose a risk to human safety.

For example, consider a company that uses computer-controlled devices to move and store caustic chemicals. What happens if the digital devices are compromised? Could it cause a chemical spill? Or could the chemicals overheat, resulting in a fire? It might sound implausible, but as cyberattacks become more sophisticated and aggressive, it is a very real possibility.

Manufacturers can protect their operations by building resilience to cyber threats. Resilience in this case means you have the ability to resist an attack, to respond quickly and thoroughly when an attack occurs, and to efficiently recover your business if your operations are compromised. That starts by identifying weaknesses in your digital perimeter and then building a multilayered strategy to protect against and respond to an attack.

Common cybersecurity blind spots

Outdated and unsupported hardware and software on the shop floor are two of the most overlooked sources of vulnerability. Although this equipment may not be used like a traditional computer by your front-office staff, it's still connected to the network. If it isn't maintained, it's a security risk to your operations.

IT-related decisions made by non-IT departments pose another common risk. With the advancement of cloud computing and software-as-a-service models, it's easier than ever for employees to purchase new software, download applications or share files in the cloud. Systems and software that are not properly vetted or maintained could harbor security risks. In addition, they extend your attack surface without your knowledge, making it harder to protect data.

A lack of real-time monitoring is another standard blind spot in manufacturing operations. Without real-time monitoring, you have no visibility into attempts to infiltrate your network or hack your users. It's harder to resist attacks if you don't know they're occurring.

Creating a multilayered security strategy

The best means to resist an attack is to establish a multilayered security strategy. At its most foundational level, the strategy should include:

- **Password protocols:** Ensure the use of good passwords.
- **Email protection:** Technologies that curtail spam and spear-phishing attempts will reduce the risk of social engineering.
- **Multi-factor authentication (MFA):** MFA requires users to take an additional step to verify their identity when logging into a system or an app. It should be implemented on all remote access points (such as email, VPN and cloud applications) as well as internal administrative accounts.
- **End-point detection and response (EDR):** EDR increases your ability to detect suspicious events by providing real-time visibility into attacks. It is not the same as antivirus software (which should also be employed in your business). Antivirus software looks for malicious programs running on your computer. EDR looks for malicious activity in the memory of your computer.
- **Regular penetration testing and vulnerability scans:** If you're not monitoring your environment, you don't know where your vulnerabilities are or how to fix them. Monthly or quarterly penetration testing of your external systems and vulnerability scans of your internal systems are essential to identify weaknesses before they become attack vectors.
- **Vulnerability management:** Cybercriminals are constantly probing for security gaps. You can make it harder for them to gain entry by applying patches and software updates, removing unnecessary software and disabling unused system processes.
- **Air-gapped backups/segmented networks:** If you can browse directly to your backup files from your primary network, they are not safe from ransomware or other cyberattacks. Cordon off your backup files on a stand-alone network that requires separate credentials.
- **Recovery testing:** Are your system backups occurring as intended? A network failure or cyberattack is the wrong time to discover your files haven't been backed up or that you don't have the means to restore them. You need to regularly test your backup processes to confirm they are working.

Employees are part of your cybersecurity strategy

The best hackers don't hack systems; they hack people. It's easier to trick someone into sharing their credentials than it is to break into a system. For that reason, you need to focus as much on your people as on your perimeter.

Your first line of defense is to put controls in place to govern how data is used, managed and stored, as well as limiting access to sensitive data to those who absolutely require it. If you don't know where your data is being kept or who has access to it, you can't be sure that it is protected.

Your second line of defense is to implement a comprehensive training program. Hackers will use a variety of social engineering techniques to steal information, including email (phishing), SMS text messages (smishing) and phone calls/voicemail (vishing). In response, you need to develop your team's ability to be professionally skeptical.

When employees know what they need to do and why, your operations will be better armed against cyber threats.

Creating a more robust business continuity program

The magnitude of the COVID-19 pandemic caused manufacturers to strengthen their business continuity plans to protect against disruption at a global scale. Other catastrophes — natural disasters, fires, cyberattacks and prolonged power outages — also pose a serious threat to manufacturing operation.

Business continuity plans provide a map for navigating your response to a business disruption and ensuring your organization is more resilient. They transform the "what ifs" — What if your shop is hit by a tornado? What if your network is compromised by ransomware? — into actionable plans to ensure continuity of key assets, technology and business processes.

Your business continuity program checklist

The process of building a business continuity program involves:

- Identifying what activities or processes are critical to your operations
- Defining and documenting procedures to respond, resume and recover the critical activities
- Testing and maintaining your plan

A strategic business continuity plan always addresses more than just IT recovery. It takes a holistic view of your entire organization and determines how you can continue business even through the disruption of technology, location or people. As the pandemic clearly illustrated, some disruptions require a much broader response than IT alone can provide.

> A strategic business continuity plan always addresses more than just IT recovery.

Here's how manufacturers can build a business continuity program that considers their full operational needs:

1. Conduct a business impact analysis

During this analysis, establish which processes are critical to your operations. To do so, identify what is impacted if you are not able to perform the process or function. Will the inability to perform the function affect your financial bottom line? Is the process or function critical to customer service?

This requires an end-to-end review of your operations, from the point that demand is triggered to the moment product goes out the door. It should also include a step-by-step review of your back-office functions; the inability to pay your employees or process invoices is also a risk to your operations.

After you identify your critical business processes and functions, determine how they are performed and what relationships exist between processes and technology.

In addition, define how long your operations can sustain a disruption. Maybe you can continue business for a short time without resources, but what about two weeks or even longer? Understanding the business impact to disruptions is key to designing your response so you can focus resources on critical operations.

2. Define and document procedures

After you complete the business impact analysis, develop contingency plans. The overall plan should include crisis or emergency plans, incident response plans, department and management continuity plans, and IT recovery plans.

The process involves identifying different responses related to the loss of technology, workplace and people. What happens if you lose access to your ERP for a sustained period? What if the shop gets flooded? What if another strain of COVID-19 strikes and a quarter of your workforce is out sick?

Disruptions occur, whether the resources you require to perform your functions are internal or external. Businesses can be impacted by events that are out of their control (a pandemic, as an example). The plans that you create should identify the continuity steps you would consider for each process even if you don't have access to resources.

As you develop your recovery strategies, it's essential to ensure you have the capabilities to support your plans. Don't assume anything in terms of recovery, especially when it comes to your technology. As operations increasingly become digitized, your ability to respond to disruption could be shaped in large part by your underlying IT strategy.

For example, are you operating in the cloud, or are your operations dependent on on-premises hardware? If you're dependent on on-premises technology, what happens if you lose your facility to a fire or flood? Are you backing up data every day, and are you confirming the back-up processes are working?

Or will you need to rebuild digital files if there is a disruption? Do you even know where all of your data is located?

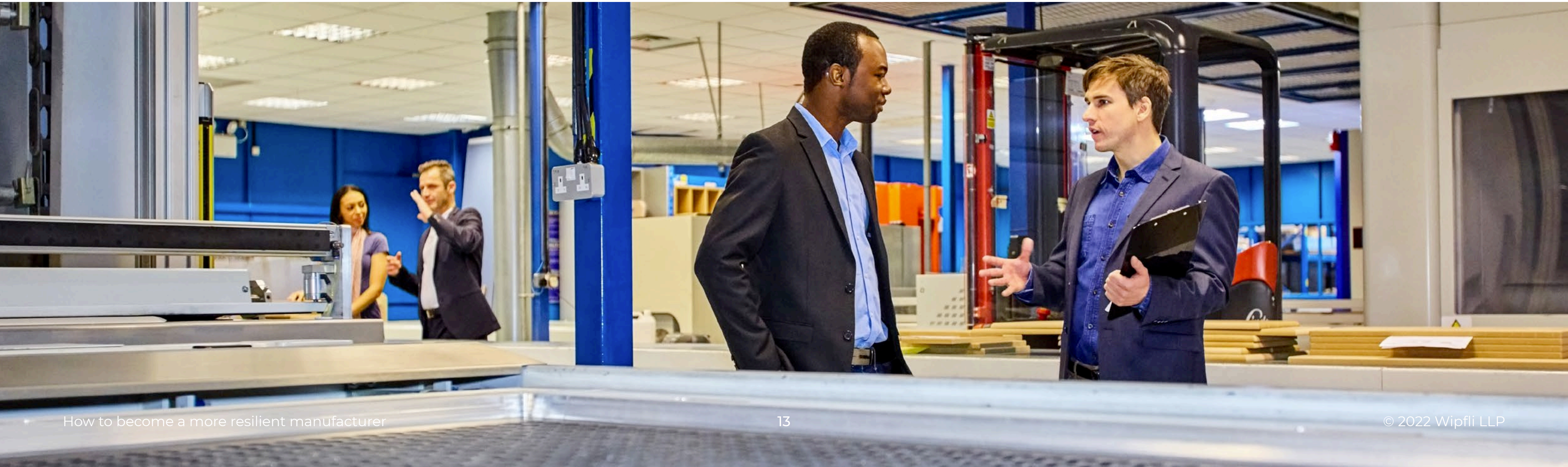
How quickly you can recover will depend on how current your backed-up data is — and how rapidly you can access and restore it.

3. Test and maintain your plans

The plan isn't complete until it has been thoroughly tested. Tabletop exercises where all relevant team members gather to talk through different scenarios are one of the most successful ways to test continuity plans. Refine the plan as needed until you are confident it addresses how to respond to varying disruptions that could affect your business.

This is not a set-it-and-forget-it process. Successful business continuity plans need to grow and adapt along with your operations. At a minimum, your plan needs to be reviewed and tested on an annual basis for several reasons:

- It presents an opportunity to incorporate any business changes that may affect the plan — such as new equipment, added production lines or new technology capabilities.
- It ensures that your recovery strategies still work as intended.
- It familiarizes your employees with the plan. Roles and responsibilities change; turnover happens. The more that people know what is expected of them during a disruption, the less likely they are to panic or make rash decisions.



Using resilience as a competitive differentiator

When you have the right programs, processes and technology in place to provide your customers with security and predictability, you create an overall better customer experience. And that matters in an industry where the ease of doing business is increasingly becoming a driver of customer decision making.

Here's how you can use resilience-building strategies to strengthen and expand your customer base and increase your business agility.

Pivot quickly to keep operations moving

When disruption happens, it doesn't just affect you. It affects your customers, too — their ability to fulfill promises, make their profitability goals and even support payroll.

Demonstrating that you have plans and processes in place to rapidly adjust to disruption offers greater peace of mind to your customers.

- **Build relationships with peers and competitors:** Cooperation between manufacturing peers was one of the most unique situations to emerge during the pandemic. Case in point: When a resin shortage buffeted the plastics industry, we saw manufacturers trading resin stocks to help each other out. Support like this has created openings for complementary and competing businesses to work together to keep orders rolling.

Demonstrating that you have plans and processes in place to rapidly adjust to disruption offers greater peace of mind to your customers.

- **Invest in inventory management technology:** Only 34% of manufacturers extensively use automation and Industry 4.0 technologies for inventory management. Yet this technology can help them stay ahead of unplanned shortages. For example, electronic replenishment technologies will automatically order new parts when supplies reach a certain level. Relatively simple solutions like these give manufacturers an advantage that they can pass on to their customers in the form of greater confidence their orders will be fulfilled as promised.

Mitigate delays with a smarter supply chain

Strategies for managing supply-chain disruptions tend to focus on protecting operations from unexpected pricing spikes or shortages. But when you have the means to predict and avoid disruption, you can also offer more certainty to your customers.

- **Digitally connect your supply chain:** Technology like digital process mining (DPM) and digital twins improve your ability to identify supply chain issues and develop a timelier workaround. DPM digitally connects supply chains and tracks actions — such as when the parts you ordered leave the shop — as they occur. Digital twins build on the data derived from DPM to forecast situations and simulate potential solutions. Both tools provide the insights to adjust your operations based on data rather than on gut feelings.
- **Diversify your supplier base:** Nearly one-quarter of manufacturers rely on a single supplier for more than 50% of their materials and components. Vetting multiple vendors for critical parts when things are going well will ensure you have alternatives lined up when your preferred supplier can't come through.
- **Audit your suppliers:** Regular audits of your suppliers' risks will help fortify your own business. How reliable are their operations? What is the status of their workforce? How vulnerable are their supply chains? You don't need to be Big Brother to your suppliers. But having greater transparency will help you understand how their risks influence your operations and your relationship with your customers.

Monitor and adjust operations with improved visibility

The ability to access and interpret real-time data is the key to speed. The greater the visibility into your operations, the better you can build on your strengths. But visibility can do more than help you navigate uncertainty. When you have the means to more quickly and confidently respond to customer questions about their orders, you create more value and a better overall experience.

- **Invest in part genealogy technology:** Components within assembled products typically come from multiple manufacturers. Parts genealogy provides the ability to trace all components to their source. If something goes wrong, you have quick access to information on how to fix it so you can keep your operations moving.
- **Employ RFID tags and geofencing:** RFID tags can be placed just about anywhere — in a bin, on a box, on a tote — to track products and parts. Geofencing identifies when something — for example, a person, a part, or an order — has entered a domain or an area. Both technologies allow you to easily track where parts or products are in your plant. In addition, geofencing can trigger workflows, such as alerting a supervisor when orders arrive in the shipping dock.
- **Implement machine monitoring:** This industrial internet of things (IIoT) technology uses sensors to monitor and track how equipment is performing. Among the many benefits of IIOT is the ability to identify and even predict suboptimal performance or unplanned downtime so you can address it before it becomes a problem.

Get started building business agility and resilience

Building a resilient shop takes time and resources, but you don't need to take on everything at once. Prioritize the areas of your operations that are most critical to your business and focus on iterative improvements.

The most productive place to start is by determining whether you have the capacity and the capability to put these plans together. Most businesses recognize they need to improve resiliency to protect their profitability and differentiate their capabilities. Finding the time and space to identify and mitigate risks in a timely fashion is more challenging.

So why not borrow a team that can do it for you? Wipfli's manufacturing and technology specialists help manufacturers reinforce their businesses against crises. We work hand in hand with your team to ask the right questions, identify vulnerabilities to your operations and develop targeted resilience strategies to keep you moving forward.

Learn more

Persepctive changes everything.

WIPFLI