HOW TO PREPARE FOR ERP DISRUPTIONS AND DOWNTIME

March 9 2023 • Forbes • Kevin Beasley

Throw a dart at a map of the world. No matter where it lands, disruption is probably just around the corner.

For instance, the onslaught of storms in California in early 2023 left thousands of buildings damaged and without power, placing operations on pause for many businesses. Half a world away, hundreds of enterprises suspended operations in Eastern Europe due to geopolitical conflict. And everywhere in between, cyberattacks and ransomware threats are as prominent and expensive as ever.

Disruption knows no geographic or industry boundaries. In fact, over the past few years, it's been a common thread connecting organizations around the world. Yet only 55% of business leaders have implemented enterprise resource planning (ERP) software in a way that allows them to act swiftly in the face of disruption. Perhaps more importantly, as of 2021,

only 54% of organizations have a disaster recovery plan in place.

Scalable and up-to-date processes and technologies are crucial for avoiding downtime and reputational damage when disaster strikes. And that means proactivity and flexibility must remain at the core of organizations' ERP and business strategies as they plan for the challenges they face today as well as the ones they'll face in the future.

Outdated ERP Infrastructure Is Too Risky To Ignore

Too many organizations continue to rely on outdated, inflexible ERP infrastructures. In some cases, business and IT leaders relegate ERP updates to the back burner to cut costs. In other cases, comfort with existing systems restricts them from piloting a new solution.

However, neglecting technology updates creates much bigger problems in the long run. Outdated systems present a range of

issues, from security risks to data backup and integration challenges. These inefficiencies hinder day-to-day operations as well as the organization's ability to navigate disruption. Downtime is practically inevitable when disruption occurs—whether it's the result of ransomware or natural disasters. But if ERP technology isn't operating at peak performance, chaos can turn catastrophic in the blink of an eye.

Why? Because organizations rely on ERP solutions to support business processes like procurement, risk management and supply chain operations. Without proper backups and business continuity plans in place, ERP downtime means users lose access to the data and functionalities that drive these business processes. As a result, users forfeit visibility into inventory, the ability to reorder supplies and sometimes even access to all IT operations.

The inability to perform core business tasks during downtime creates a snowball effect, making it challenging to resume operations—downtime costs organizations around $300,000 per hour due to productivity losses and catch-up time. While it can't always be measured, the reputational damage following downtime can also be difficult to recover from.

It's impossible to predict the events that can disrupt your business. The good news? An agile response to disruption can go a long way toward mitigating the impact of any incident.

Three Types Of Disruption Every Business Should Prepare For

Your success as a business relies on your ability to pivot and maintain profitable operations during disruption. Now is the time to future-proof your business processes so you can maintain organizational agility and meet the evolving needs of your business.

Here's what this might look like for your organization—and how it can help you navigate whatever business disruptions come your way:

Cyberthreats

More than three-quarters of organizations experienced downtime in 2021 as a result of data loss—and of that percentage, more than a third stemmed from cyberattacks. When threat actors compromise critical data and infrastructure, you need to switch access codes, change passwords and pull impacted equipment offline.

A tight, end-to-end security posture is table stakes in mitigating the risk of cyberattacks and ensuring business continuity when an attack occurs. In addition to routine ERP security checks (which should include patch management and a review of access controls), you must implement a plan for data recovery. Cloud-based recovery with real-time backups and high availability is likely ideal so that your applications and data are readily available in the event of an attack.

Geopolitical Factors

It's easy to overlook geopolitical factors in business and cloud planning. But the relentless stream of business disruptions in recent years highlighted the impact geopolitical risks can have on an organization. For example, some countries recently passed laws that regulate data sovereignty and localization. These regulations determine how companies process and store data, which raises concerns for global enterprises collecting customer data.

Inflexible data structures make it nearly impossible to keep pace with evolving data regulations. In some cases, you have to establish separate instances for the various geographies you operate in. This requires a modern database designed for geographic dispersion—and if your database doesn't support this, it's time to replace it. Most importantly, your ERP infrastructure must have the ability to manage configurations to data structures.

Natural Disasters And Severe Weather

Earthquakes, hurricanes and even short-term weather disruptions like severe thunderstorms can wreak havoc on business operations and jeopardize physical assets (e.g., hardware infrastructure). Even if your facilities are not directly affected, severe weather can impede forms of transportation, interrupt telecom circuits and cause cell phone tower failures or power outages that result in downtime.

If you operate using only on-premise ERP, you might want to consider a cloud-based or hybrid approach. Cloud and

hybrid ERP solutions can facilitate remote operations so business operations can continue even when employees can't make it to a physical location. Additionally, cloud-based operations enable you to back up data to a remote, off-site cloud server with high availability. If your location becomes inaccessible, your data and applications remain secure and available.

Conclusion

In short, you need to consider the external forces that pose a risk to your business. Then, when it's time for periodic reviews of your processes and tech stack, you can prioritize initiatives that will set you up for business continuity through even the most serious disruptions. When the infrastructure and processes supporting your business remain flexible, downtime doesn't have to lead to your downfall.