withum

A Guide for Business Continuity and Resiliency

withum.com

Are you worried about disruption? If a disruption occurs, can your business continue to function without any impact on critical operations?

Although organizations frequently prepare for common disruptions including natural disasters, cyberattacks, supply chain issues and other business crises, many businesses do not realize the importance of preparing for disaster. Each year, various events disrupt millions of businesses, whether small or large.

Keeping your company running smoothly no matter what requires a plan. While strategies are available to help mitigate the impact of these disasters, they must be implemented now before it is too late. Companies can examine their business continuity plans and internal risk mitigation strategies to ensure they are prepared to bounce back and engage in best practices as soon as possible after a business disruption occurs.

The following guide outlines business areas and tips to consider strengthening your business continuity plan.

The strongest way to mitigate threats is to ensure that your business is equipped with a framework for business continuity. Regardless of an organization’s size, revenue, or industry, a well-developed business continuity plan should be in place and followed to minimize disruption to the health of your company's financial stability as well as reputation after a devastating event.

Prepare For The Unexpected

Create a disaster recovery plan, focusing on the safety and livelihood of your employees and addressing any property and business concerns.

Identify existing and potential disaster risks to your location.

Review insurance policies, deductibles and understand coverage limits.

> Conduct an annual insurance assessment with an insurance agent to ensure that your coverage is adequate.

Ensure the safe storage and protection of important property and governance documents.

Prepare and review financial budgets to address crisis needs and ensure funds for emergency and recovery costs.

Perform a risk assessment to determine where your business may be susceptible to loss and prevention strategies.

> Identify the nature, location, intensity and likelihood of potential risks.

> Inspect your property to determine the existence and degree of vulnerabilities and exposure to risks.

> Identify the capabilities and resources available to you and your business.

> Prioritize risks and determine countermeasures needed to address the risks.

Maintain regular communication with your team members. Every employee should know and understand the business' disaster plan and what role they play in it. Conduct periodic and regular training sessions and give team members specific assignments.

Identify an emergency management team comprised of capable and knowledgeable decision-makers. These team members will collect and analyze data to make efficient and accurate decisions in the best interests of the business and stakeholders.

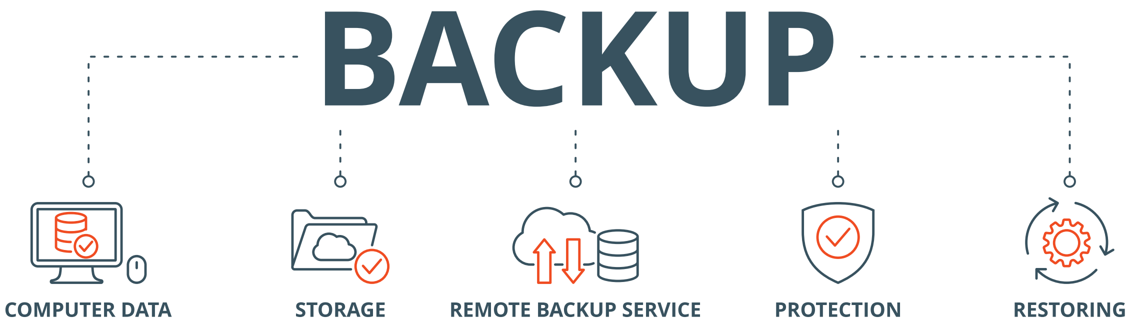
Utilize technology. Invest in updating your infrastructure to the cloud to provide your employees with secure, remote access to a Modern Digital Workplace — anytime, anywhere, and on any device.

Risk Management, Data and Cyber Security

Data loss can result from many situations — from computer viruses, ransomware, and hardware failures to file corruption, flood, fire or theft. A loss may significantly impact financial, customer and company data and your reputation. Having reliable data backup is often not enough.

Companies that only maintain a local backup of their data place themselves at considerable risk. Immutable, air-gapped backups that are stored in a secure off-site location are best. A combination of secure off-site and cloud backups provides the best protection level. There are numerous federal and state regulations that include business resiliency plans as part of those regulations. If your business is impacted by data loss, be it by malicious actor or natural disaster, the repercussions of not following state or federal regulations related to business resiliency will only compound your losses.

Do you have complete, immutable, air-gapped backups that are regularly verified through the practice of restoring data to test their integrity?



Criminals will be 5-10 steps ahead of you on how they can exploit your environment during a business disruption.

You can certainly expect an increase in attempts at Business Email Compromise (BEC), most often through more frequent (and focused) phishing attacks as well as targeted financial/wire fraud and scam activity.

While having your data and IT infrastructure in the cloud is a good step forward in most cases, when it comes to cyber risk, care must be taken to avoid settling into a complacent security readiness posture — "we're in the cloud, it doesn't matter." This is not the case. During a cyberattack, a component of your organization's environment is impacted. Independent assessments of real business continuity assurance across the board, including the cloud, are vital in protecting your organization and your customers' data. You can never be too safe. Such assessments look at your organization from a business perspective and identify points of failure and weaknesses. These assessments also point out areas where you can scale and be resilient.

Cyber insurance policyholders should be aware of the rapidly evolving legislative and regulatory landscape, particularly regarding those applicable to their state(s) of operation.

Ransomware coverage is a pillar of most cyber insurance policies, but both the availability of ransomware coverage and the standard of proof necessary to obtain coverage (at all) are both issues changing quickly along with the post-pandemic threat landscape. In essence, ransomware claims are amongst the most frequently filed and most impactful in terms of dollar value lost. The topic of debate amongst security and legal policymakers is the validity of payouts to recover data (i.e., paying the ransom), with ransom payment opponents gaining momentum and, increasingly, legal precedent.

In 2022, North Carolina and Florida passed bans on local and state agency ransomware payments. New York, Texas, Arizona, and New Jersey also have similar bills at varied levels of consideration in mid-2022. Most of these laws currently focus on state agencies (exclusively), but New York's proposed law will extend the ransomware ban to private organizations and businesses. New York is also a bellwether for state-level tech legislation, both regionally and nationally – so other states will likely follow their lead.

INDEPTH LOOK

Cyber Insurance:
What You Should Know

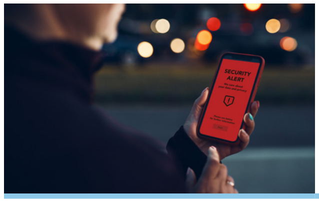
Click to Learn More.

Here are some steps to take to help protect against cyberattacks:

Consider a Virtual Chief Information Security Officer (vCISO): Every organization has limited resources no matter how big it is. A vCISO supplements leadership in technology, security and compliance which means enhanced expertise, innovation, increased efficiency and reducing overall costs to an organization.

Ensure you have sufficient data protection: Confirm reliable 24/7/365 monitoring and recovery of your critical data.

Exercise your capabilities: Test your backup/recovery and incident response processes under real-world operational conditions, with the same staff responsible as would be following an actual attack and/or breach. These "security drills" have a dual benefit of serving as user-centric training in workplace cybersecurity policies and staff roles/responsibilities. The first time you attempt to restore data should not be following a real attack, where much more depends on a positive outcome.



Configure automated incident response notifications to appropriate stakeholders from integrated, intelligent Security Information and Event Management (SEIMs) and monitoring platforms (or services). Prompt response with minimized reaction and mitigation time is the best way to avoid major business impacts and disruptions.

Data integrity and business continuity assurance policies and associated controls should be established and in-place. Speak with your cybersecurity advisors or in-house IT/Security staff on organization-specific details.

Safeguarding Against Business Interruption

According to press release #293 issued by FEMA on October 30, 2018, approximately 25 percent of businesses do not reopen after disasters. One of the primary factors behind this is the lack of sufficient insurance or the inability to prove the true value of equipment and other assets lost in the disaster. What safeguards do you have in place to prevent your company from a scenario like this? A certified appraisal can help ensure you have adequate insurance coverage to protect your business against this type of loss.

You want to ensure that all of your assets, including machinery, equipment and real estate, are insured for their current fair market or replacement cost value when purchasing business insurance. Many companies rely on their tax return depreciation schedules as the primary source for valuing the tangible assets they own; however, actual market values typically differ vastly from what is recorded on these schedules. This is because the amount of depreciation used for tax and GAAP reporting purposes is meant to recognize and write off the cost of an asset for accounting. It is not an indication of market or replacement costs to be used for insurance reporting.

If a business undervalues tangible assets, the insurance provider may be concerned that they did not purchase enough coverage and will refuse to compensate them accurately for property claims. This is especially important to note in the current economic climate, where costs have risen sharply over the past three years. Trends provided by the Bureau of Labor and Statistics (BLS) have has estimated the cost of a commercial office building and related equipment has increased by approximately 39% and 32%, respectively, from July 2020 to June 2023. A certified appraisal will provide an accurate valuation of your business's assets and can help determine how much insurance coverage you truly need.

Navigating Business Interruption Insurance and Claims

Business interruption insurance is intended to reimburse a policy holder for sudden and unforeseen perils that are named in, or not specifically excluded from, the policy.

Many insurance policies limit the period of damages for business income to no more than 12 months, which may be less than the actual damages period. Now more than ever, this type of insurance has proven to be a critical component of every business insurance portfolio, with some businesses relying on the recovery of pending claims to ensure their survival. One should maintain the following records in case of a business interruption catastrophe:

- Insurance policy, deductible and coverage limits (inclusive of business interruption verbiage).
- Historical monthly profit and loss statements for at least a two-year period.
- Historical yearly tax returns, financial statements and general ledgers for at least three to five years.
- Forecasts and budgets prepared for the upcoming year.

A qualified vendor should have the expertise needed to quantify economic damages and assist with filing a claim with your insurance carrier should a business interruption occur. It is important to invest in a vendor who can help your business with the quantification of business interruption losses as follows:

- Review the insurance policy to assist in identifying components of business income loss and extra expenses.
- Assist in documenting the timeframe in which losses occurred.
- Assist in gathering relevant documentation needed to calculate lost business income and extra expenses.
- Quantification of business income loss based on the insurance policy components, an analysis of the company's historical operations, and assessment of industry factors affecting the company.
- Assist with reviewing the adjustor's business income loss calculations and assumptions.
- Assistance with settlement, negotiation, and litigation with the insurance company.

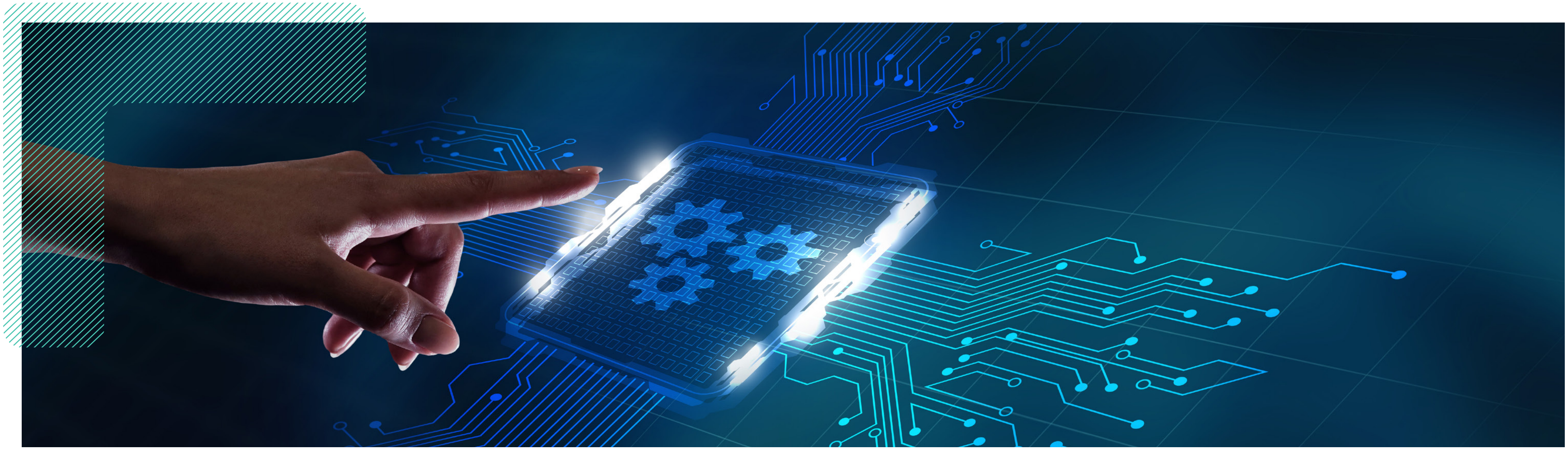
Tips on Filing a Business Interruption Claim : Click here to learn more.

Process Automation For Business Resiliency

No matter your organization's industry, there's an opportunity to capitalize on the benefits of process automation not just for long-term resiliency but also by reducing human input error, improving product or service quality and delivery, and containing costs through the technology-enabled automation of complex business processes.

Automating your processes gives you the flexibility to be proactive and respond quickly to your employee and client demands, no matter what happens.

Business workflow automation includes modeling the steps, optimizing input, visualizing output, choosing technology and implementing. These solutions range from digitizing a paper form, applying an approval workflow, multi-step accounting workflow automation, acting on behalf of a user using Robotic Process Automation (RPA) all the way to Intelligent Process Automation (IPA) that learns and improves over time.



AUTOMATE REPEATABLE PROCESSES TO:

Reduce wasted employee time by connecting old systems

Streamline data entry tasks

Integrate with Line of Business applications

Consolidate dispersed data, both on-premises and in the cloud

EXAMPLE: AUTOMATED CONTRACT MANAGEMENT

Many organizations receive, produce and manage large volumes of contracts, which can become quite a complex and challenging business problem. The contracts are often scattered across different systems, locations, and formats, making them difficult to access, update, and analyze, especially during an unplanned business interruption. Due to the nature of these documents, they often contain sensitive and confidential information that must be safeguarded from unauthorized access and are subject to frequent changes and revisions, requiring careful tracking and verification of versions and clauses.

Traditional contract management solutions cannot be tailored easily, are expensive, often lack integration with other systems, and lack built-in intelligence. The best way to disaster-proof your contract management processes is through a robust and efficient system that stores, organizes, searches, edits, annotates, shares, and monitors these documents securely and competently.

A contract management solution powered by technologies like the Microsoft cloud and AI can allow you to:

- Streamline creation and assembly, classification and storage of contract and legal documents.
- Automatically extract key terms such as value, expiration date, customer name, etc.
- Provide content compliance and governance using Microsoft Purview, including automated OCR and content labeling.
- Allow annotation and review of documents .
- Automate e-signature and streamline review/approval of contracts.

INDEPTH LOOK

Explore Business Process Automation Solutions

Click to Learn More.

How Microsoft 365 Helps Build Resiliency and Continuity

An investment into Microsoft 365 consists of an ecosystem of technical features and business benefits providing value constantly, 99.9% guaranteed uptime, to your organization. In preparing for resiliency, Microsoft 365 propels your organization to:

BE SECURE

Provides a single cloud-based identity to access all applications at any time. Track and manage the health of physical assets. Ensure outsiders are not taking advantage of a business interruption to access your content and data.

COMMUNICATE

Provides instant access to reach team members through e-mail, chat, and meetings, or provide consistent updates to employees through news or clients through online portals – with no disruption.

COLLABORATE

Even your desktop can be hosted in the cloud, accessible anywhere, allowing work to continue. Access policies, procedures, emergency tasks, continue work as normal through video and many-to-many chat.

AUTOMATE

The more redundant work that gets removed from a team member's workload means, the more they can react to the current situation and provide high-value services internally and to clients.

EXTEND

Build on top of Microsoft 365 to support specific needs of your organization's everyday work and take the thought out of specific needs during a business interruption. Create custom forms, apps, or integrations with 3rd party tools.

MEASURE

At your fingertips, you can see your organization's security footing, how your team members are working, or you can create a custom resiliency dashboard measuring specific aspects of your business during an interruption.

Click to Learn More. **11 Benefits Of Microsoft 365 For Your Business** withum

SEE HOW WITHUM CAN HELP YOUR BUSINESS PREPARE FOR THE UNEXPECTED CHALLENGES AHEAD.

Click To Learn More
About Business Continuity.

Contact Us and
Talk To A Team Member

HLB
WE ARE AN INDEPENDENT MEMBER OF
THE GLOBAL ADVISORY
AND ACCOUNTING NETWORK