

Business Resiliency: 7 Steps to Successful Incident Management, Business Continuity and Disaster Recovery Planning





Content

03 Introduction

05 Plans, Plans and More Plans ... Oh My!

07 Business Resiliency Tools: Individual but Interrelated

08 Heightened Reasons for Concern

09 7 Steps to Achieve Sound Business Resiliency

20 Conclusion

21 Works Cited

Business Resiliency: 7 Steps to Successful Incident Management, Business Continuity and Disaster Recovery Planning



By Albert J. Marcella Jr., PhD, CISA, CISM
President
Business Automation Consultants, LLC

“...business resiliency is the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.”

INTRODUCTION

There are two types of organizations today: those that have experienced a disruptive event that affected ongoing business operations and those that will.

A disruptive event is a technological problem that causes your information technology (IT) capabilities to end abnormally or abruptly, without warning.

A disruptive event may result from:

- Hardware failure (e.g., hard drive malfunction, server crash)
- Software failure (e.g., system freeze, reboot or total inoperability)
- Telecommunications failure (e.g., internet, mobile communications outages)
- Human failure (e.g., poor application design, outdated updates, inadequate backup procedures, error in judgment, poor security awareness training, intentional or unintentional unauthorized acts, etc.)

INTRODUCTION

The 2021 Verizon Data Breach Investigations Report investigated 5,258 confirmed data breach cases. The median cost of an incident was \$21,659, with 95% of incidents falling between \$826 and \$653,587.²

The 2020 Legal Technology Survey Report conducted by the American Bar Association's Legal Technology Resource Center (LTRC) revealed that the number of firms experiencing a security breach (such as a lost/stolen computer or smartphone, hack, break-in or website exploit) increased over the prior year — 29% of respondents compared to 26% in 2019.³

As you are considering these numbers, note that tangible expenses may also include the cost of downtime, hardware repair/replacement, potential Digital Forensics and Incident Response (DFIR) services and increased insurance fees along with noncompliance fines and penalties. Intangible costs associated with loss of business and customer confidence may be both more difficult to calculate and to recover. See Figure 1 (page 16).

Regardless of your legal organization's size, your business is susceptible to events and incidents, some minor and some not so, that may cause disruptions to daily operations, providing client services and long-term sustainability of operations.

The ABA Profile of the Legal Profession 2020 report found that in general, the bigger the firm, the more likely they've experienced a security breach: 32% of firms with 500 lawyers or more reported in 2019 having experienced a breach sometime in the past; for solo practitioners, the number of firms impacted 14%.⁵

The implications of the American Bar Association's 2018 Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack," places an even greater responsibility on the organization to substantiate valid internal controls, implement risk management practices and bolster its ability to sustain ongoing business operations.

Opinion 483 specifically states that "lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach."⁶

A study on businesses in New Orleans recovering from Hurricane Katrina found that 12% of businesses remained closed 26 months after the storm.⁴

PLANS, PLANS AND MORE PLANS ... OH MY!

The types of plans related to business resiliency planning for organizational systems include business continuity plans (BCP), disaster recovery plans (DRP), continuity of operations plans (COOP), crisis communications plans (CMP), critical infrastructure plans (CIP), cyber incident response plans (CIRP), incident management plans (IMP) and occupant emergency plans (OEP).

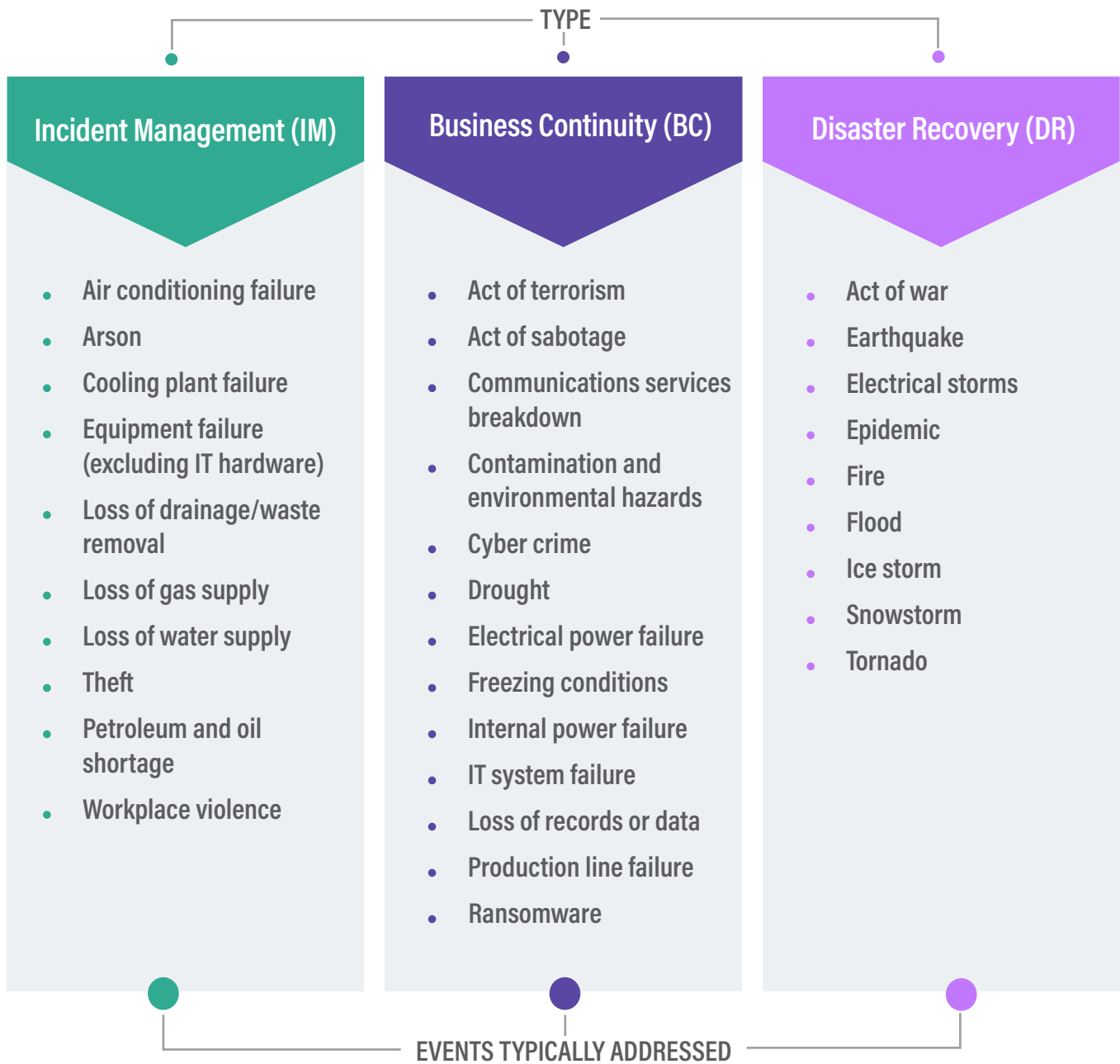
This white paper focuses on three of these plans — incident management (IM), business continuity (BC) and disaster recovery (DR). These plans form the core of an organization’s business resiliency strategy.



Incident management, business continuity and disaster recovery plans, while often discussed as a single product or response method, should not be confused as being identical in their focus, approach or objective. See Table 1 (page 6), which identifies the business resiliency plans and the type of events each plan typically addresses. The list of events identified is not exhaustive. Every business operation is unique and may face disruptive events not listed in this table.

It is also important to note that through the performance of a risk assessment and subsequent management decision, an event addressed by an IMP for organization “A” for example, could be addressed by a BCP for organization “B.”

Table 1: Business Resiliency Plans



Above all, it is important to understand that incident management, business continuity and disaster recovery represent independent yet symbiotic approaches, each aimed at achieving and sustaining business resiliency.

See the sidebar (page 7) “Business Resiliency Tools: Individual but Interrelated,” which discusses the characteristics of these tools.



Business Resiliency Tools: Individual but Interrelated

Incident management (IM) is the process of identifying, analyzing and determining an organizational response to an incident, while minimizing and controlling the damage resulting from the incident and ensuring that agreed levels of service quality are maintained. An incident is a security event that impacts in some way the confidentiality, integrity or availability of an information asset. **The Incident management plan (IMP)** provides clear and essential documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of an unplanned event. Its purpose is to return business operations back to normal as quickly as possible.

Business continuity (BC) normally applies to the business itself; it concerns the ability to continue critical functions and processes, with minimal or no downtime or service outage, during and after an emergency event. A **Business continuity plan (BCP)** includes documentation of a predetermined set of instructions or procedures that describe how an organization's business processes will be sustained during and after a significant disruption.

Disaster recovery (DR), however, refers to having the ability to restore the data and applications that run your business should your data center, servers or other infrastructure get damaged or destroyed. One important DR consideration is how quickly data and applications can be recovered and restored. To that point, a **disaster recovery plan (DRP)** refers to a written plan used to guide a business's response for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

HEIGHTENED REASONS FOR CONCERN

Data is the second most critical asset to any organization, with personnel being the first. Personnel, however, can be replaced. Can the same be said for your data?

Data can help your organization:

- Enhance processes
- Improve client services
- Make better decisions
- Recognize client needs
- Solve problems
- Understand organization performance

Bottom line: Our organization's resiliency is dependent upon uninterrupted access to and use of critical business data.



A 2021 global study by IBM and the Ponemon Institute found that data breaches cost surveyed companies \$4.24 million per incident on average — the highest cost in the 17-year history of the report.⁷

Your business resiliency tools should address the possible loss, damage, destruction or manipulation of data, which may result from such actions as:

- Disgruntled employees
- Human error
- Local, regionalized disaster event
- Malware
- Ransomware
- Software and/or hardware failure
- Theft

Here are seven steps specifically designed to assist you and your organization in better preparing for and sustaining business resiliency.

7 STEPS TO ACHIEVE SOUND BUSINESS RESILIENCY



STEP 1

Identify critical business activities and processes. These are functions that will need to be restored immediately in the event of an operational disruption to protect organization information assets and personnel and meet client service requirements.

Also identify the core IT infrastructure systems that support all critical organization systems (e.g., print systems, servers, virtual private networks [VPNs], email, databases, etc.).

Business resiliency questions:

1. What specific data are most critical to continued client services and business operations?
2. Is our recovery effort aimed at continuing business processes or simply recovery of operations?
3. What specific IT and non-IT resources are required to deliver the goods or services our clients require?

STEP 1a

Establish a recovery time objective (RTO) for all essential business data and information system components. RTO is the time by which business critical activities and/or their dependencies (e.g., information assets) must be recovered.

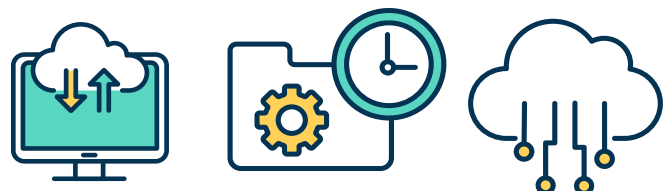
The recovery of lost or damaged information assets in many cases will not be instantaneous. Depending on the amount of critical data that will need to be recovered, where and how it is stored, the required RTO and actual download/recovery times may not be aligned, achievable or realistic. Business resiliency plans must address and account for the actual time it will take to access, download and recover business critical data, compared to the time by which those data are needed.

Several issues related to download speed, which should be considered when determining the RTO and developing your business continuity plan, include:

- Internet speeds can fluctuate even during a transfer, and the performance of your broadband will change throughout the day depending on network traffic.
- The speed can also be restricted by the connection of the server that is sending or receiving data.
- Another factor to consider is how many people will be sharing the connection because every person you add will reduce the available bandwidth. Asymmetric Digital Subscriber Line (ADSL) broadband, the basic and most common type of broadband internet connection (which has an average speed of just 10MB) can struggle to cope even with light usage if more than one person is online at the same time.
- When moving a file from one computer to another, the maximum transfer speed will depend on the slowest bandwidth that the data has to go through — which can be anywhere in the route.⁸

Business resiliency questions:

1. How fast is my organization's internet? Is it fast enough?
2. Will the current internet speed support the organization's required RTOs?
3. How do I determine if my current internet connection can provide the download speed for critical information assets that my organization requires?



STEP 2

Perform a risk assessment. This is the process of identifying, estimating and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals and other organizations. Part of this risk assessment process incorporates threat and vulnerability analyses.

Business resiliency questions:

1. What specific threats does the organization face (e.g., environmental, geographical, temporal, internal, external)?
2. What vulnerabilities exist within the organization that if compromised could lead to a disruptive incident/event?
3. What actions can the organization take to mitigate the threats identified in question No. 1?

STEP 3

Conduct a Business Impact Analysis (BIA). A BIA is an analysis of a system's (e.g., financial, marketing, client services, IT, etc.) requirements, functions and interdependencies. It is used to characterize system contingency requirements and priorities in the event of a significant disruption.⁹

Business resiliency questions:

1. If the risks identified in Step 2, question No. 2 above materialize, what will be the greatest impact to the organization (e.g., financial, legal, loss of customer confidence/trust/brand)?
2. Have the real costs (tangible and intangible) associated with the identified risks been identified and calculated?
3. Has each risk's impact been quantified as to the organization's ability to continue expected service delivery and whether/for how long can the organization continue to operate without essential systems and services?

Formulate a coordinated and controlled organization-wide

STEP 4

response to a disruptive event.

Such a response should identify specific metrics that will enable the effective development and deployment of the organization's business resiliency tools. Such metrics would include determining:

- Recovery Point Objective (RPO): The RPO represents the point in time, prior to a disruption or system outage, to which business process data can be recovered (given the most recent backup copy of the data) after an outage.
- Maximum Tolerable Downtime (MTD): The MTD represents the total amount of time the system owner is willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with precise direction on 1) selection of an appropriate recovery method, and 2) the depth of detail that will be required when developing recovery procedures, including their scope and content.¹⁰



STEP 4a

Establish a data backup plan. The organization's retention policies (you have them, right?), along with client and compliance requirements, are a good starting point in determining 1) what data and documents are required and must be backed up; 2) what is important to daily business operations and should be backed up; and 3) what would be "nice to have backed up" but, if lost or unrecoverable, would not have a negative impact on continued business operations.

A comprehensive backup plan embodies the basic 3-2-1 rule:

3

Keep 3 copies of any important file: 1 primary and 2 backups.

2

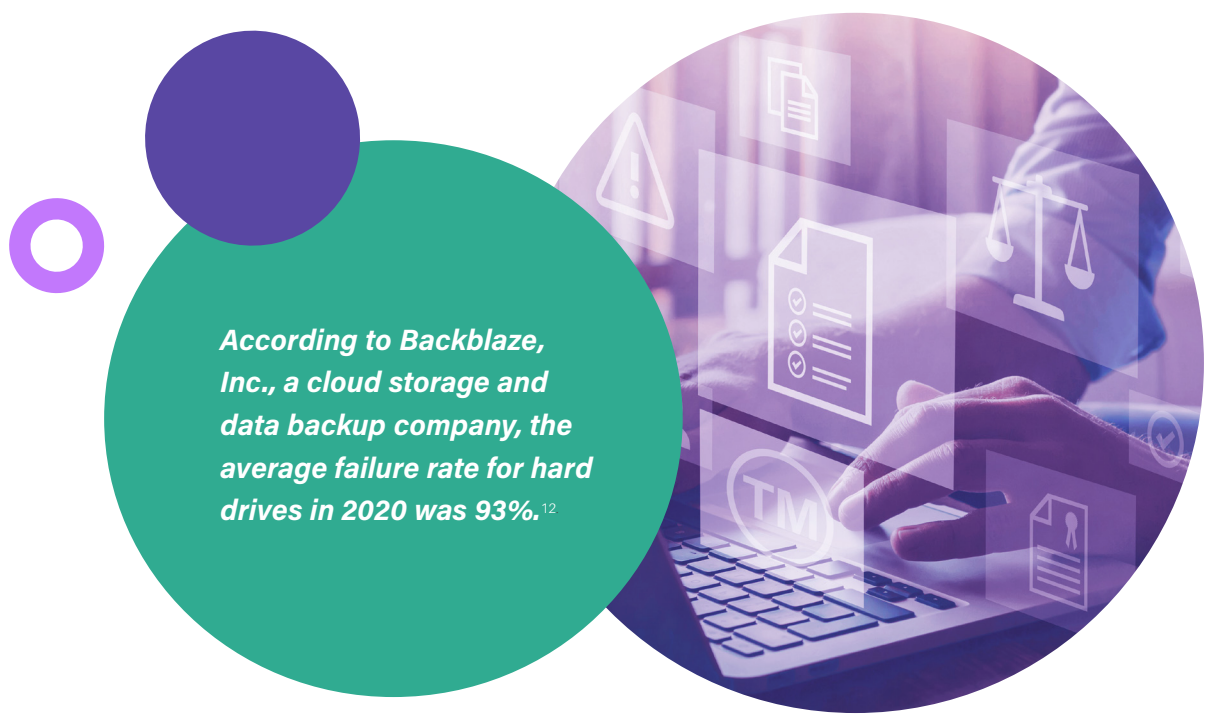
Keep the files on 2 different media types to protect against different types of hazards.

1

Store 1 copy off-site (e.g., outside your business facility, at home, at a trusted third-party site, or cloud storage).¹¹

A 3-2-1 backup strategy reduces the impact of a single point of failure, such as a disk drive error or stolen device.

The data backup plan should also identify the following data backup approaches: full, differential, incremental and mirror. See Table 2 (page 12) for a description of these basic data backup approaches.



According to Backblaze, Inc., a cloud storage and data backup company, the average failure rate for hard drives in 2020 was 93%.¹²

Table 2: Data Backup Approaches

BACKUP APPROACH	DESCRIPTION
<p>FULL BACKUP</p>	<p>A full backup is the starting point for all other types of backups and contains all the data in the folders and files that are selected to be backed up. Because full backup stores all files and folders, frequent full backups result in faster and simpler restore operations.</p>
<p>DIFFERENTIAL BACKUP</p>	<p>Differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if the differential backup is performed too many times, the size of the differential backup might grow to be larger than the baseline full backup.</p>
<p>INCREMENTAL BACKUP</p>	<p>Incremental backup stores all files that have changed since the last full, differential or incremental backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be processed, which may result in a lengthy restore job.</p>
<p>MIRROR BACKUP</p>	<p>Mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files, and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the source data.¹³</p>



Business resiliency questions:

1. Does the data backup method selected/used meet your business needs/requirements?
2. Are organization data encrypted before any off-site transfers occur?
3. Does the organization verify the integrity of the backup data on a regular basis (typically through a test restore process) to ensure they are valid?
4. What assurances (confirmation) does the organization have that validates a data backup is actually taking place? Correctly? Completely?

STEP 5

Plan now. When the disruptive event occurs, there will be no time!

Coordinate the communication and distribution of the plans (e.g., incident management, business continuity, disaster recovery) to recovery team personnel and any additional organization personnel who may have a “need to know” (e.g., executive management, first responders). The organization’s business resiliency plans should be considered highly confidential; therefore, their distribution, should be closely managed and distributed via methods that will assure the continued confidentiality and security of the plans and their contents.

Be prepared to communicate the status of any business disruptive event to internal personnel and external third parties. There are a variety of tools, from automated to sending basic email notification, to keep everyone informed. Determine which tool is most appropriate for

your organization’s communications response needs. Be alert! Sending confusing or incomplete information may result in further disruption, panic and misinformation as to the state of the organization’s response to evolving conditions.

Communication plans are critical in enabling incident managers and stakeholders to quickly activate, assemble and employ resources and capabilities. During an incident, the need to react appropriately is immediate, followed by the need to communicate. Lack of effective communication during a crisis can lead to inadequate resource allocation, compound risks to assets and personnel and create lingering effects on bottom-line operations.¹⁴

Prepare template voicemails, SMS messages, social media and website posts, emails, press notices, public information statements, etc., ahead of time. When a disruptive incident occurs, all you’ll need to do is to copy and paste specific details into the respective template and distribute it. Executive management should approve all external communications, especially those distributed during a business disruptive event.

Business resiliency questions:

1. Does the organization have plans that detail its response to a disruptive event/incident?
2. Will the actions the organization takes contribute to mitigating risk and address the loss and exposure of the organization’s most critical processes and their associated data?
3. Does the organization have task recovery procedures, technology recovery protocols, processes to reestablish the workplace environment and a public relations/media response plan?

STEP 5a

Once the disruptive event has been fully addressed, return to work assessments should begin and post-event notifications must be addressed and coordinated. Be prepared to notify employees how, when (and potentially, where) to return to work, vendors when they may resume providing services, and clients that you are ready to provide services. Depending on telecommunication capabilities and capacity, personnel may be allowed to work remotely.

Business resiliency questions:

1. Has the business properly communicated the plan's existence to the appropriate personnel who may be required to implement the plan?
2. Has the plan been fully integrated into the business's operating policies and business culture?
3. Does the plan communicate step-by-step recovery procedures in a clear, concise language that is easy to understand and follow, especially under conditions of stress and confusion?



STEP 5b

The organization's business continuity and disaster recovery plans should also address the question of "where" and "how" you will continue IT operations if current IT and office facilities are unavailable.

Based upon the outcome of the organization's risk assessment, the plans should identify one or multiple alternative computer processing sites (ACPS). This site is an alternate processing facility that geographically separated from the organization's primary processing site location to reduce susceptibility to the same threats. Table 3 (page 15) summarizes some ACPS options.

In addition, technologies such as redundant arrays of independent disks (RAID), automatic failover, uninterruptable power supply (UPS) and server clustering should be considered when developing the system recovery strategy piece of BC and DR plans.

Business resiliency questions:

1. Has the organization developed alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives)?
2. Has the organization identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlined explicit mitigation actions?
3. Has the organization arranged for alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats?

Table 3: ACPS Options

Cold Site	A backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment if the user must move from their main computing location to an alternate site.
Warm Site	An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
Hot Site	A fully operational off-site data processing facility equipped with hardware and software, ready to be used in the event of an information system disruption.
Mirrored Site	A fully redundant facility with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
Mobile Site	Self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. ¹⁵
Third-Party Site	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. ¹⁶

STEP 6

Any business resiliency plan is only as good as the last time it was tested. Ask yourself, “Is my organization operating and functioning today at the same levels or with the same technology as it did 12, 24 or 36 months ago?”

Business resiliency plans must adapt and change to address evolving business needs and practices. Business resiliency plans **MUST** be tested — regularly!

Be sure that any test plan also includes a hotwash. A hotwash is a debrief conducted immediately after an exercise or test with personnel involved in the test and members of the organization’s business resiliency team.

Testing and confirming that your business resiliency plans can restore and sustain ongoing business operations, in line with the organization’s risk mitigation strategy, is vital.

According to the cybersecurity and data backup company Datto, depending on the size of the organization, the cost per hour of downtime is anywhere from \$10,000 to over \$5 million.

WHAT WILL DOWNTIME COST MY ORGANIZATION?

How much in employee salary would you lose if your organization was completely shut down, unable to conduct business for just one day (eight hours), because of a disruptive event?

There are many ways to calculate the cost of downtime and many factors to consider (the duration of the outage, the number of people affected, the time of day, the type of disruptive event, etc.) Not all costs are tangible.

Figure 1 provides examples of tangible and intangible costs of downtime, which should be considered in determining the overall financial impact to your organization, resulting from a disruptive event.

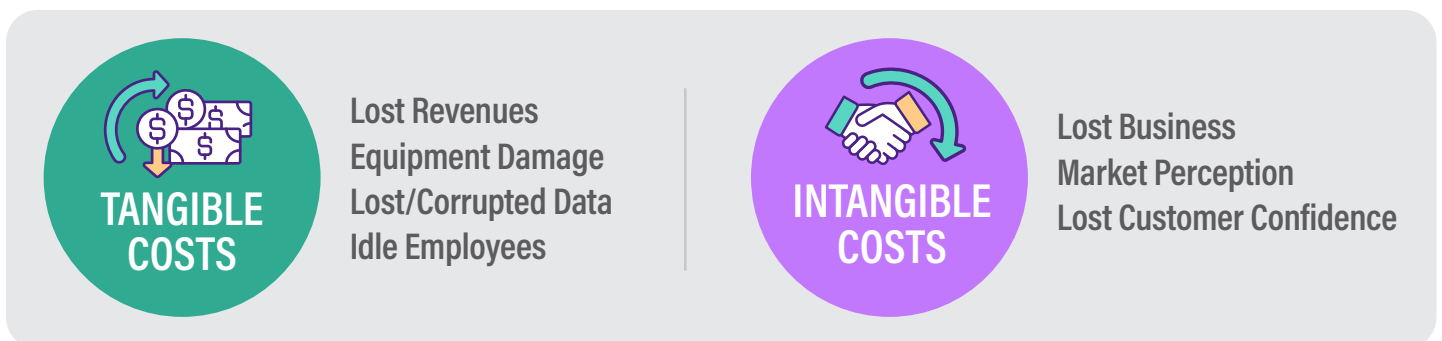


Figure 1: Tangible and Intangible Costs of Downtime

Table 4: Primary Methods for Testing Plans






<p>Comprehensive Testing</p> 	<p>For organization IT infrastructure, test all systems and components that support a recovery plan. These tests generally involve multiple components and systems and may become quite extensive in their scope.</p> <p>An example of a comprehensive test is confirming that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.</p>
<p>Functional/Full Recovery</p> 	<p>Involves a complete process of testing your backup systems and processing transactions or data. The scope of the functional recovery test can vary from parallel testing (running your live and backup systems in conjunction) to a full failover test (completely transitioning operations to your backup systems). This test should be simulated as similarly to a “real-life” disaster as possible.¹⁷</p> <p>The full plan should be tested annually. The test should be coordinated with key clients, third-party service providers, alternate (or redundant) site hosts, etc. May be coordinated with your risk assessment program (RAP).</p>
<p>Plan Review</p> 	<p>Consists of analyzing the IM, BC and DR plans and discussing potential improvements, as well as making sure contact information is up-to-date, recovery contracts are still in place and effective and applicable business continuity and disaster recovery scenarios are appropriately covered. A plan review may also include training new managers on plan details so they can pass that knowledge down to their teams.¹⁸</p>
<p>Tabletop Exercise (TTX)</p> 	<p>This activity is a discussion-based exercise where personnel with roles and responsibilities in a particular IT or business operations area meet in a classroom setting or in breakout groups to validate the content of the various business resiliency plans by discussing their roles during an emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.</p> <p>Tabletop exercises should be conducted biennially. Exercises should include executive and internal stakeholder management. Consider inviting key clients, third-party service provider representatives and emergency responders as participants.</p>
<p>Walk-Throughs</p> 	<p>The primary objective of a walk-through is to ensure that critical personnel from all areas across the organization are familiar with the business resiliency plans (e.g., IMP, BCP, DRP).</p> <p>It is characterized by:</p> <ul style="list-style-type: none"> • Discussion about the respective plans in a conference room or small group setting • Individual and team training • Clarification and highlighting of critical plan elements¹⁹

Table 4 Primary Methods for Testing Contingency Plans

CALCULATING THE COST OF DOWNTIME

The staff positions and number of personnel by job title represent a conservative view taken by the author and may not be representative of your specific organization.

Figure 2 illustrates that the total personnel cost of downtime for one week is \$105,468 or \$21,093 per day.

Calculating the Cost of Downtime		Atlanta, Georgia Firm Size Number of Attorneys: 25		
Job Title Within Organization	Total Annual Compensation (Average)	Total Weekly Compensation (Average)	Nbr. of Personnel by Job Title	Total Weekly Payroll
Executive Director/Principal Admin/COO	\$391,969	\$7,538	1	\$7,538
Benefits Coordinator/Administrator	\$89,599	\$1,723	1	\$1,723
Applications Support Analyst	\$73,237	\$1,408	1	\$1,408
Record Manager/Director	\$93,629	\$1,801	1	\$1,801
Accounting Manager/Supervisor	\$118,168	\$2,272	1	\$2,272
Paralegal/Legal Assistant	\$84,841	\$1,632	3.125	\$5,099
Legal Secretary/Administrative Assistant	\$75,183	\$1,446	6.9	\$9,976
Receptionist	\$50,251	\$966	2	\$1,933
Associate Attorney 1 or fewer years of experience	\$129,881	\$2,498	8	\$19,982
Associate Attorney 3 years of experience	\$160,515	\$3,087	14	\$43,216
Associate Attorney 7 years of experience	\$182,363	\$3,507	3	\$10,521
Total	\$1,449,636	\$27,878		\$105,468

Figure 2: The Cost of Downtime ²¹

The total cost of downtime shown in Figure 2 is for payroll only and does not include other tangible costs such as potential fines (e.g., noncompliance), penalties (e.g., privacy violations), business processes (e.g., data recovery, hardware replacement, etc.) or lost revenues that could not be billed due to the unavailability of business resources (e.g., client files, IT systems, software, telecommunications, facilities, etc.).

Additionally, the cost of downtime in this example does not account for intangible costs as previously identified in Figure 1.

If the organization in this example is lucky to suffer only a single week of downtime, the organization may be able to recover and continue as an ongoing business. If the downtime stretches beyond a week, the tangible \$105,468 payroll cost is simply multiplied by the length of the downtime. The intangible costs, however, may be much more difficult to accurately calculate and to recover.

Can your organization afford not to be prepared?

Business resiliency questions:

1. Has the organization tested the business resiliency plan's ability to respond to an event in a timely manner and to sustain operations that comply with the organization's identified RTOs and RPOs?
2. Have personnel that will be responsible for the implementation of any plan (incident management, business continuity and disaster recovery), been adequately and properly trained in their specific job duties and responsibilities associated with the implementation of these plans?
3. Do all employees have a basic understanding of their roles and responsibilities during a disruptive business event?
4. Does the organization have an accurate calculation as to the total cost of downtime per hour? Per day? Per week?

How much in employee salary would you lose if your organization was completely shut down, unable to conduct business for just one day (eight hours), because of a disruptive event?



STEP 7

Establish a maintenance and update schedule designed to keep the business resiliency plans up to date.

The primary objective of the maintenance and update process is to identify and correct any gaps in the business resiliency plans that would have an adverse impact on sustaining ongoing business operations.

Maintenance and updates to the organization's business resiliency plans should be determined based upon significant changes in business operations, technologies, client requirements, third-party service contracts, regulations, laws, compliances, etc.

Also affecting a plan's update or revision schedule are findings from the performance of a risk assessment or business impact analysis. Results from these activities that highlight changes in business operations, levels of acceptable risk or heightened exposures will warrant a review of the organization's business resiliency plans. Plans should be revised to address the identified risk(s) or exposure(s), with the objective of mitigating the risk(s)/exposure(s) to a level acceptable to management.

Organizations differ in many aspects, so no one-size maintenance and update strategy fits all. A recommended

CONCLUSION

Business resiliency is NOT a "one and done" process. Business resiliency is ongoing and evolving, which takes time, effort, money, energy, personnel and executive management commitment to succeed.

The risks of being unprepared and not having viable, implemented, functioning business resiliency plans are too high, especially when your organization's success and ongoing operations can be protected with proactive preparation and planning.

By following the steps presented in this white paper, you will better prepare your organization to sustain ongoing business operations in the face of a business disruption event.

No one wants to be a statistic harden your — business resiliency capabilities NOW!

approach is to establish a three-year review cycle. In year one, a review of all incident management plans is performed. In year two, the business continuity plan(s) are examined for any necessary revisions. Finally, in year three, a review of the disaster recovery plan is conducted. The cycle repeats and begins anew in year four.

This review cycle, as best as possible, should be coordinated with the plan testing cycle as described in Table 3 to achieve optimal efficiency and an assurance of plan readiness.

Business resiliency questions:

1. What activities associated with the organization's IT operations have changed, resulting in a direct and material impact on the ability of the business resiliency plans to meet their objectives?
2. Is analysis of the plan's ability to meet its objectives performed on a continuous and monitored basis?
3. Are organizational changes and how they may affect the organization's risk exposures and implementation of the business resiliency tools fully recognized and understood by management?

WORKS CITED

1. Locke, Gary, and Patrick Gallagher. 2011. "Managing Information Security Risk Organization, Mission, and Information System View Joint Task Force Transformation Initiative." *nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf*.
2. Review of 2021 Data Breach Investigations Report. 2021. Verizon DBIR. Verizon. *verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.246129543.2087360073.1640284828-990200011.1640284828*
3. Loughnane, J. October 19, 2020. "2020 Cybersecurity," ABA TECHREPORT 2020, American Bar Association's Legal Technology Resource Center (LTRC).
4. Lindsay, Bruce. 2019. Review of Considerations for Implementing a Small Business Disaster Grant Program. Congressional Research Service. Congressional Research Service reports. *everycrsreport.com/files/20190226_R45554_6ec44d7c951f57726fe8bc604cba06a03265eecd.pdf*.
5. Review of ABA Profile of the Legal Profession 2020. 2020. American Bar Association. American Bar Association's Legal Technology Resource Center (LTRC). *americanbar.org/content/dam/aba/administrative/news/2020/07/potlp2020.pdf, pg. 88*.
6. Review of Formal Opinion 483. 2018. American Bar Association. American Bar Association Standing Committee on Ethics and Professional Responsibility. *americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf, pg. 6*.
7. IBM. July 18, 2021. Review of Cost of a Data Breach Report 2021. Edited by Ponemon Institute. IBM and Ponemon Institute. *ibm.com/security/data-breach*.
8. Powell, M. July 29, 2021. "Broadband download speed calculator: find out your broadband download time," Broadband Genie, *broadbandgenie.co.uk/broadband/help/broadband-download-time-speed-calculator*.
9. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. 2010. Review of Contingency Planning Guide for Federal Information Systems, NIST SP 800-34 Rev. 1. National Institute of Standards and Technology. National Institute of Standards and Technology. *nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*.
10. *Ibid.*
11. Krogh, Peter. 2006. The DAM Book: Digital Asset Management for Photographers. Sebastopol, Ca: O'reilly.
12. Klein, Andy. 2021. Review of Backblaze Hard Drive Stats for 2020. Backblaze. *backblaze.com/blog/backblaze-hard-drive-stats-for-2020/*.
13. Review of FedRAMP Information System Contingency Plan (ISCP) Template. 2012. The Federal Risk and Authorization Management Program. *fedramp.gov/assets/resources/templates/SSP-A06-FedRAMP-ISCP-Template.docx*.
14. Review of ICS Cybersecurity Year in Review 2020. February 24, 2021. Dragos. *dragos.com/year-in-review, pg. 38*.
15. Swanson, Marianne, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. 2010. Review of Contingency Planning Guide for Federal Information Systems, NIST SP 800-34 Rev. 1. National Institute of Standards and Technology. National Institute of Standards and Technology. *nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*.
16. Mell, Peter. 2011. Review of The NIST Definition of Cloud Computing (NIST SP 800-145). Edited by Timothy Grace. National Institute of Standards and Technology (NIST), *csrc.nist.gov/publications/nistpubs/800-145/SP800145.pdf*.
17. Klosterman, Dan. 2019. Review of FOUR STEPS to BETTER BUSINESS CONTINUITY PLAN TESTING. *sbscyber.com/resources/four-steps-to-better-business-continuity-plan-testing*.
18. *Ibid.*
19. Board of Governors of the Federal Reserve System. 2003. Review of Federal Financial Institutions Examination Council (FFIEC) Business Continuity Planning. *fdic.gov/regulations/examinations/supervisory/insights/sisum06/bcp.pdf*.
20. Review of The Cost of Downtime. 2018. Datto. *datto.com/resource-downloads/TheCostOfDowntime_Whitepaper.pdf*.
21. Association of Legal Administrators. 2019. Review of 2019 ALA Compensation & Benefits Survey, Executive Summary. Edited by iLumen Inc. Association of Legal Administrators.
22. Lindsay, Bruce. 2019. Review of Considerations for Implementing a Small Business Disaster Grant Program. Congressional Research Service. Congressional Research Service reports. *everycrsreport.com/files/20190226_R45554_6ec44d7c951f57726fe8bc604cba06a03265eecd.pdf*.