Preparing for the Unexpected:

Data Protection & Your Business

NEXUSTEK WHITE PAPER

You probably know that in the event of a disaster or ransomware attack, business data is at risk of permanent loss or destruction. This "business data" includes everything you have stored in digital form, including customer data, employee data, proprietary information, legal information, and so on. Because serious consequences can occur due to loss or destruction of such data, businesses are urged to implement a business continuity and disaster recovery (BC/DR) plan to protect against data loss.

But a concerning fact is that 75% of small and medium-sized businesses (SMBs) lack a BC/DR plan[1]. If we asked SMB leaders why their business lacks a formal disaster plan, how do you suppose they would answer?

> ***"It won't happen to me."***
>
> ***"I have actual problems to deal with."***
>
> ***"We aren't in a high-risk region or industry."***
>
> ***"I can prepare after the busy season."***

These types of very common sentiments regarding disaster preparedness keep SMB leaders from taking adequate precautions today to prevent data loss at an unspecified point in the future. And although it may be perfectly natural, psychologically speaking, to prioritize objectives that are more immediately impactful, long-term risks can and do turn into today's risks—and they can make such a transformation quite suddenly, leaving your business exposed to serious damages if it is unprepared.

When Disaster Strikes: What You Stand to Lose

It is probably intuitively evident that losing critical business data could hinder business operations or even halt them entirely. Downtime can occur if you lose access to the data, software, or hardware needed to carry out various business processes. The cost of downtime alone—even if data is not ultimately lost on a permanent basis—is staggering, ranging anywhere from $137 to $427 per minute for the average SMB[2].

With the cost of downtime literally adding up by the minute, SMBs are most successful if they are able to regain normal operations as quickly as possible. This may seem like an obvious point, but the risk of not getting back up to speed swiftly is huge. To state the magnitude of this risk numerically, a FEMA study revealed that 90% of SMBs fail within 1 year if they are not able to regain operations and get back to business as usual within 5 days of a disaster[3].

Success in getting back to business as usual depends heavily upon how prepared an organization is before the incident. Strikingly, 96% of businesses with BC/DR plans can fully restore operations after data loss[4]. These two facts juxtaposed illustrate the importance of a BC/DR plan—it can literally make the difference between business success and failure after a major incident.

Understanding Your Risk: Incident Types & Your Data

The term "disaster recovery" may evoke notions of massive events that cause catastrophic, widespread destruction. Although major regional disasters are clearly important to prepare for, there are also quieter, firm-specific incidents that can be just as damaging for an individual business. To explain in more detail, the following sections review different types of incidents that can jeopardize business operations and data.

Natural Disasters: Forecast—Not Good

When you think of a natural disaster impacting an SMB's infrastructure, maybe you imagine cataclysmic tornadoes, hurricanes, or floods. These can certainly create the risk of data loss and business disruption, but other forms of disaster can as well. Earthquakes and fires can also disable a business' infrastructure and can strike without warning at any time.

Natural Disasters—The Stats

- 80% of all power outages in the U.S. are caused by weather[5].
- Over 100,000 business fires occur annually[6].
- At least one flooding event occurs in the U.S. on 8 of every 10 days[7].
- The U.S. had 6 times the number of "billion-dollar storms" during 2011-2022 than during the previous 20 years[8].

Natural Disasters—How They Impact Business Continuity & Data

When devising a solution, technological or otherwise, it is important to first understand the nature of the problem you intend to solve. So, how do natural disasters affect business infrastructure and data? Here are some key facts to understand:

- Natural disasters can result in power supply disruptions, taking local hardware offline until power is restored.
- Electrical surges resulting from damage to power infrastructure can damage IT hardware, resulting in loss of functionality.
- Floods, fires, and earthquakes can cause physical damage to hardware that may range from temporary to permanent.
- Depending on the nature of the damage to IT hardware, locally stored data may be temporarily unavailable at best, permanently corrupted or destroyed at worst.

Damage to hardware and networking after a disaster is reparable, but this takes time. Data restoration is another important step in recovering from a disaster, and although data stored within damaged hardware may be retrievable, the time involved in setting up new hardware and restoring data within the repaired infrastructure can be lengthy enough to seriously impact business longevity.

Ransomware: The Silent Disaster

Unlike weather-related natural disasters, ransomware attacks are never in the daily forecast. In fact, ransomware attacks unfold so quietly in the beginning stages that an attack may be underway while your employees go about their daily business, completely unaware. By the time employees become aware that something is amiss, the damage is already done.

Ransomware—The Stats

- 82% of ransomware attacks target SMBs[9].
- The average ransom payment is $228,125 among SMBs that fall victim to ransomware attacks[10].
- 80% of companies hit by a ransomware attack within the last year paid the ransom, but 21% of those that paid still could not recover their data[11].
- 96% of businesses with BC/DR plans survive ransomware attacks.[12]

Ransomware Attacks—How They Impact Business Continuity & Data

On the surface, ransomware attacks can have effects (i.e., data loss, downtime) that are similar to those of natural disasters. But because ransomware attacks are human engineered, they can cause hidden, diffuse damage that is more difficult to diagnose than a smashed laptop or burnt server. Consider these key facts:

- The threat actors will encrypt some—or all—of the victim's data, rendering the affected data unusable until decrypted. It will not be immediately obvious which data or devices have been impacted, making forensic investigation a necessity.
- Data backups that are accessible to the hackers at the time of attack will most likely be encrypted or destroyed as well, a strategy attackers use to make sure the victim has no other recourse but to pay the ransom.
- With data in unusable form, critical business operations will experience a slowdown or come to a stop. This paralysis may affect only some portions of the business (e.g., payment systems, phones), but can be pervasive enough to effectively stop the business from functioning in the worst of cases.
- Even after the victim pays the ransom, data may not be recoverable in full, as the decryption key provided by the threat actors may not fully restore all data that was held hostage in the attack. In some cases, the hackers will have already destroyed the victim's data and backups before delivering the decryption key.

As you might expect, recovery from ransomware attacks typically takes longer than recovery from disasters like floods or fires. This is because IT staff can more easily identify servers that have been damaged in a natural disaster. With ransomware attacks, the damage may be spread out and hard to find, prolonging the recovery period. A commonly cited Statista finding is that recovery from ransomware attacks takes an average of about 3 weeks[13]. As discussed previously, business success after the attack hinges upon swiftness of recovery of normal operations, making a prolonged investigation and restoration process potentially fatal.

Accidental Deletion: The "Oops" Factor

Far from what you might imagine when you hear the term "disaster" is accidental deletion of data. But the innocuousness of this incident type should not fool you into ignoring it. Everyone can probably recall a time when they deleted a file, or even multiple files, completely by mistake. Maybe you failed to notice which file you were deleting or thought you just didn't need the file anymore. If you were aware of your mistake, then it was probably easy enough to retrieve the file from the trash or recycle bin without issue. But sometimes such safeguards don't suffice, turning an "oops moment" into a major problem.

Accidental Deletion—The Stats

- 50% of U.S. office workers report having accidentally deleted files stored in the cloud[14].
- 20% of U.S. office workers admit to deleting data accidentally at least once each week[15].
- Accidental deletion accounts for 47% of data loss among businesses using cloud-hosted software applications[16].
- 43% of employees report that they have lied in the past to cover up accidental data deletion[17].

Accidental Deletion—How They Impact Business Continuity & Data

The mechanisms and outcomes of accidental deletion are a bit more straightforward than natural disasters or ransomware attacks. But the effects can still be detrimental, as the following illustrates:

- Following accidental deletion, if file recovery capabilities are not in place, one-of-a-kind files may be lost permanently.
- Entire groups (i.e., folders) of documents or files may be accidentally lost, misplaced, or deleted with an errant click.
- Some trash or recycle bin solutions have data retention timelines (e.g., 30 days). If the loss is not discovered within a certain timeline, it could be permanent. This is especially vexing when an employee deletes a file without being aware of having done so.
- If files are deleted and then trash or recycle bins are emptied by the employee, the loss could be permanent.
- We should note that some deletions are not accidental. A disgruntled employee may deliberately delete files without informing anyone on staff.

A point to emphasize is that, in the case of accidental deletion of files, you might not recognize that you have a problem until days, months, or even years down the road, when an employee looks for a specific file and cannot find it. This is problematic for multiple reasons. As with data loss caused by disasters and ransomware attacks, accidental deletion can remove key pieces of the business operations puzzle, causing operational dysfunction in areas ranging from bookkeeping to customer service.

In addition, compliance rules may be infringed. Personnel, legal, and medical files have recordkeeping requirements that can extend from a few years to as long as decades. Failure to maintain records can place a business out of compliance with local, state, and federal regulatory bodies, resulting in fines and more serious corrective action if the problem is severe and persistent.

BC/DR Plans: How They Prevent Business Disruptions & Data Loss

Recall the key statistic reported earlier in this discussion: 96% of businesses with BC/DR plans can fully restore operations after data loss[18]. Why is this?

BC/DR plans increase a business' resilience against downtime and data loss because:

- Business continuity assessment helps you to better understand your specific risks and identify your business-critical systems and data..
- This understanding allows you to develop a BC/DR plan that is tailored to your specific infrastructure, processes, compliance requirements, and risk factors.
- Business continuity planning results in a detailed, step-by-step plan that employees can follow to most effectively and efficiently respond to incidents that cause downtime and data loss.
- BC/DR plans empower employees to contain damage to the extent possible during and after an incident, and even more importantly, to avoid making things worse.
- Disaster-Recovery-as-a-Service (DRaaS) solutions establish redundant infrastructure that keeps your business-critical systems up and running, in the event that your primary infrastructure goes down.
- DRaaS solutions typically offer "air-gapped" data backups, meaning that they are stored separately from your primary network. This keeps your backups out of the reach of threat actors, insulates them against employee deletion, and protects them from disasters that may impact your primary infrastructure.
- When supported by a managed service provider, BC/DR plans and DRaaS solutions are tested in advance to make sure they'll work effectively when the worst happens.

Experts suggest that 93% of data loss incidents are preventable[19]. When you understand how different types of disasters can impact your IT infrastructure and data integrity, the preventive steps required to protect your business become clear. Whether it's natural disasters, ransomware attacks, or accidental deletion, a well-informed and thorough preparation is the best defense.

Providing managed services to small and medium-sized businesses (SMBs) for over 25 years, NexusTek offers Virtual CIO (vCIO) assessments to guide business continuity and disaster recovery planning, along with DRaaS solutions from industry-leading technology partners.

Prepare your business for success.

Schedule a consultation with a BC/DR expert today.

References

1. Bennett, S. (2023, July 11). Business continuity management statistics 2023 – Everything you need to know. WebinarCare. https://webinarcare.com/best-business-continuity-management-software/business-continuity-management-statistics/
2. Pingdom Team. (2023, January 9). Average cost of downtime per industry. Solarwinds. https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/#:~:text=Relatively%20small%20businesses’%20cost%20of,for%20just%20a%20short%20outage
3. Grainger. (2018, February 8). Coping with the aftermath: Protect your business from catastrophic loss. https://www.grainger.com/know-how/business-operations/emergency-and-disaster-preparedness/kh-coping-with-the-aftermath-protect-your-business-from-catastrophic-loss
4. Bennett, S. (2023, July 11). Business continuity management statistics 2023 – Everything you need to know. WebinarCare. https://webinarcare.com/best-business-continuity-management-software/business-continuity-management-statistics/
5. Datto. (n.d.). The business guide to power outages. https://www.datto.com/resource-downloads/PreventPowerOutageDowntime.pdf
6. EPS Security. (2019, October 10). Five essential fire statistics for business owners. https://www.epssecurity.com/news/business-security/five-essential-fire-statistics-for-business-owners/
7. Tompkins, F., & Watts, B. (2022, December 15). Flooding is nearly a daily occurrence throughout the U.S. Pew. https://www.pewtrusts.org/en/research-and-analysis/articles/2022/12/15/flooding-is-nearly-a-daily-occurrence-throughout-the-us
8. Climate Central. (2023, April 11). Severe storm, supercell, and tornado trends. https://www.climatecentral.org/climate-matters/severe-storm-supercell-and-tornado-trends-2023
9. Drapkin, A. (2022, February 7). 82% of ransomware attacks target small businesses, report reveals. Tech.co. https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals
10. Coveware. (2022, July 28). Fewer ransomware victims pay, as median ransom falls in Q2 2022. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022
11. Veeam. (2023). 2023 global report: Ransomware trends. https://www.veeam.com/ransomware-trends-report-2023
12. Bennett, S. (2023, July 11). Business continuity management statistics 2023 – Everything you need to know. WebinarCare. https://webinarcare.com/best-business-continuity-management-software/business-continuity-management-statistics/
13. Statista. (2022, July 7). Average duration of downtime after a ransomware attack from 1st quarter 2020 to 4th quarter 2021. https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/
14. VentureBeat. (2021, November 19). Report: 56% of workers admit they've accidentally deleted cloud data. https://venturebeat.com/security/report-56-of-workers-admit-theyve-accidentally-deleted-cloud-data/#:~:text=Report%3A%2056%25%20of%20workers%20admit,accidentally%20deleted%20cloud%20data%20%7C%20VentureBeat
15. VentureBeat. (2021, November 19). Report: 56% of workers admit they've accidentally deleted cloud data. https://venturebeat.com/security/report-56-of-workers-admit-theyve-accidentally-deleted-cloud-data/#:~:text=Report%3A%2056%25%20of%20workers%20admit,accidentally%20deleted%20cloud%20data%20%7C%20VentureBeat
16. Datto. (2020). The Datto advantage: Products built for the MSP. https://www.datto.com/resource-downloads/2020-Product-Brochure_ANZ.pdf
17. VentureBeat. (2021, November 19). Report: 56% of workers admit they've accidentally deleted cloud data. https://venturebeat.com/security/report-56-of-workers-admit-theyve-accidentally-deleted-cloud-data/#:~:text=Report%3A%2056%25%20of%20workers%20admit,accidentally%20deleted%20cloud%20data%20%7C%20VentureBeat
18. Bennett, S. (2023, July 11). Business continuity management statistics 2023 – Everything you need to know. WebinarCare. https://webinarcare.com/best-business-continuity-management-software/business-continuity-management-statistics/
19. SMB Group. (2020, February 10). Small business data protection. https://www.smb-gr.com/reports/small-business-data-protection/