ActualTech MEDIA

TECH BRIEF

Business Continuity Is Increasingly Critical

Understanding an SMB's Business Continuity and Disaster Recovery Needs

Ed Tittel

Hewlett Packard Enterprise

IN THIS PAPER

Understanding an SMB's tolerance for downtime and data loss is critical to selecting appropriate business continuity and disaster recovery solutions. Organizations must understand the opportunity costs and financial losses that downtime imposes, and also understand how much data they can afford to lose before business operations (and income) suffers overmuch.

In particular, SMBs must understand the applications and data they depend on to conduct business, setting reasonable values for how long it takes to recover operations and the amount of valuable or irreplaceable data the SMB can stand to lose if their IT infrastructure fails.

Without access to applications and data, the ability for a small to midsize business (SMB) to operate lands somewhere between difficult and impossible. No business means no customer products or services—it also means no supplier orders or payments. This very quickly translates to zero income. No income, even for only a short period, can spell the difference between a viable, going concern and going out of business. In a nutshell, this nightmare scenario explains why business continuity and disaster recovery are, and remain vitally important to, maintaining an active, healthy, and profitable business.

> Together, business continuity and disaster recovery cover a number of tools, technologies, platforms, and practices.

The Many Faces of Business Continuity

Business continuity is a well-understood part of IT. The same is true for the related topic of disaster recovery. Together, business continuity and disaster recovery cover a number of tools, technologies, platforms, and practices. Business continuity is usually part of a bigger set of tools and responses that deals with potential business interruptions and outages, including:

- **Backup and recovery:** Typically uses special software or imaging techniques to permit file-by-file copies and/or snapshotting that can run even while applications or services are busy. This process captures volume shadow or other complete copies of systems, files, logs, and data. Please note that while backup images are usually restored as part of enacting a business continuity or disaster recovery scenario, by itself, backup/recovery is not the same thing as either business continuity or disaster recovery.
- **Archiving:** Archiving differs from backup and recovery because whereas an organization might have many backup copies, typically archives are "one of a kind," single copies of data preserved for future analysis, compliance, or disaster recovery.
- **Disaster recovery:** Requires specialized steps to bring up an organization's IT infrastructure in a different location. This might occur in the event of a failure, outage, or some natural or man-made disaster that puts the primary IT infrastructure out of action. That location may be located on-premises at a different location, in the public cloud, or at a third-party failover/recovery site.
- **Data security:** Involves a variety of mechanisms and technologies to prevent unwanted access to or disclosure of an organization's data, including breach and exfiltration of private, sensitive, or proprietary data. Data security involves a variety of tools and technologies, from encryption and access controls to monitoring and audit logs.

- **Compliance and governance:** Uses various technical and procedural means to establish, enact, and monitor policy regarding access to systems and data—especially private or confidential data related to personal identification, privacy laws and regulations, financial accounts and monies, and so forth. Organizations that fail to comply with applicable laws and regulations, or fail to meet requirements for governance, are subject to fines and penalties. The responsible officers or officials may also be personally subject to civil and criminal penalties, including jail time. Proving compliance generally involves producing audit records to demonstrate that data access and use fall within a compliance regime's guidelines.

Paths and Mechanisms for Business Recovery

When business continuity or disaster recovery is needed, such action generally involves initiation of a formal, planned (and practiced) set of activities to re-establish IT operations. In a smaller organization, that might involve having two or three designated individuals who can take charge of coordinating the business's response—almost like fire marshals. In a larger, midsize company with more resources, following an event that begins with a "disaster declaration," the first step usually involves calling in a designated disaster recovery team. Once those responsible are at work, they can enact the steps necessary to recover by following the organization's disaster recovery plan.

Business continuity is similar because it is also plan-driven and is invoked when some kind of disruption may endanger (but not actually knock out) an organization's IT infrastructure. Instead of describing how to bring up and run an alternate IT infrastructure, a business continuity plan more generally describes how to keep the business running when possible disruptions appear.

Two key metrics drive business continuity and disaster recovery. They're known as recovery time objectives (RTOs) and recovery point objectives (RPOs). RTO may be understood as determining how quickly an organization plans to return to operational capability. RPO covers the kinds of capabilities and data are available when that operational capability returns. Recovery objectives apply to the organization and its partners, customers, and other affiliates.

More formally, these two terms may be defined as follows:

- **RTO:** Refers to the length of time a system, service, or application may be unavailable or down without causing significant loss or harm to a business or an organization. RTO is not just a time interval; it accounts for the steps that IT staff must take to restore an application and its data. If an organization invests in failover capabilities for high-priority/high-value applications or services, RTO may be a matter of seconds. A four-hour RTO, on the other hand, allows enough time for on-premises recovery—starting with a bare-metal restore and ending with normal application and data access.
- **RPO:** Where RTO measures maximum sustainable downtime, RPO measures maximum sustainable data loss. Thus, RPO is often expressed as a time measurement, from the time of outage or loss to its most recent preceding backup or snapshot. If an organization backs up all its data daily, a worst-case scenario means that it would lose 24 hours' worth of data. For some applications and services, this is OK; for others, it is emphatically unacceptable. Typical intervals for an RPO in many organizations are between four and eight hours. But for applications with valuable or irreplaceable data, intervals should be shorter.

Setting RTOs and RPOs occurs on a per-application or per-service basis. It requires working with business stakeholders invested in the applications and services to help choose optimal tradeoffs. Such tradeoffs often occur between the higher costs involved in shorter intervals and the greater data losses and opportunity costs that come from longer one. HPE Pointnext Services can work with SMBs to help them make these important determinations. They can help find the best sweet spots between financial costs on the one side and data losses or opportunity costs on the other.

Eight-hour or longer RPOs will usually work within the typical time frames for restoring backups using an off-the-shelf backup solution. RPOs of four hours or less

need scheduled snapshot replication. And near-zero RPOs require special handling—namely, continuous replication. Combining near-zero RTOs and near-zero RPOs means continuous replication with failover services for maximum application and data availability.

When a disaster is declared, or business continuity must be ensured, the relevant business continuity or disaster recovery plan is called into action. Special teams get convoked to undertake the work involved in meeting RTOs and RPOs and bringing up a replacement IT infrastructure sufficient to meet those objectives. The various costs (time, money, opportunity, and so forth) and complexity of these recovery options depend on the value of the data and applications they ensure. They also encompass a variety of storage technologies; each with its own RTO/RPO capabilities.

> **Instead of describing how to bring up and run an alternate IT infrastructure, a business continuity plan more generally describes how to keep the business running when possible disruptions appear.**

Putting Business Continuity to Work

The shorter the intervals for RPO and RTO, the more an organization should expect to spend to support its disaster recovery and business continuity plans. So, for example, HPE Nimble volumes are expensive and relatively limited in capacity. Cloud storage offers minimal CapEx with OpEx costs that depend typically on storage consumption and retrieval. The more that cloud-based storage gets consumed, or the more data that is recovered on a regular basis, the higher its costs rise. Here, again, organizations must watch the tradeoffs between cost, capacity, and capability, to avoid squandering or exceeding CapEx savings on OpEx costs when business continuity or disaster recovery scenarios come into play. Tape storage offers the lowest long-term cost of any storage technology but is potentially the slowest depending on whether tapes are on-premises or off-premises when they're needed. But the offline nature of tapes stored in a vault make them the most secure form of storage to guard against the rising business continuity threat of ransomware.

Figure 1 shows how business continuity planning fits into the overall IT planning context, with special emphasis on security management and disaster recovery. Note that disaster recovery is just a part of security management, which is itself part of the overall business continuity planning process.

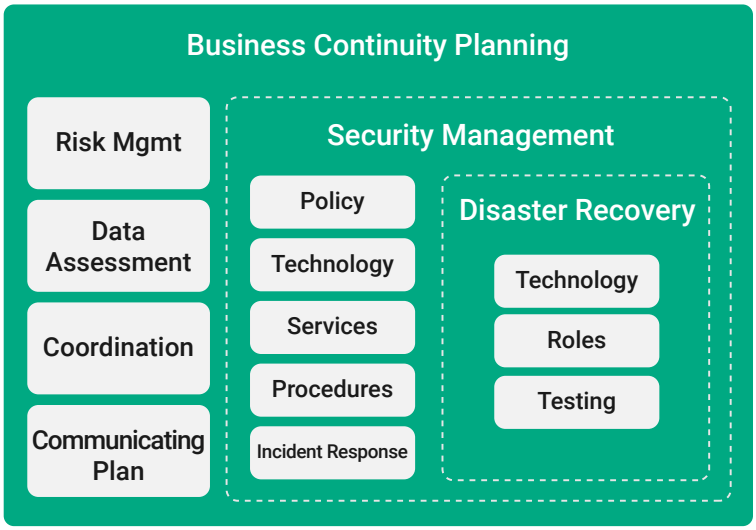

Figure 1: Disaster recovery is a subset of security management, and falls under the general heading of business continuity planning, along with risk management, data assessment, coordination, and creation/communication of the business continuity plan itself

Fortunately, SMB customers can choose among (and even combine) these options, including:

- **HPE Nimble Storage:** Flash-based, limited capacity that's extremely fast and the most expensive form of storage for data and applications
- **HPE Modular Smart Arrays (MSA):** Great SMB entry-level alternative, offers a good combination of cost, capacity, and performance
- **Deduplicated storage:** Uses HPE StoreOnce technology and may also be attractive for some SMBs, but is cost- and capacity-constrained when shorter RPO intervals are in the mix
- **Cloud storage:** Can seem compelling from a cost perspective, but comes with variable usage charges and only offers slow recovery times—may not be suitable for shorter RTO and RPO intervals
- **HPE StoreEver tape systems:** Will be attractive for their long-term, low-cost advantage and highly secure, "airgap" defenses against cyberattack and ransomware. However, tape systems will generally provide slower RTO because of the relatively long time it can take to recover data and applications from tape.
- **Hyperconverged infrastructure (HCI and dHCI) solutions:** Under certain circumstances these offer fast recovery intervals (both RPO and RTO). But they can only protect assets stored within an HCI environment (and nothing from outside it), so they may not fit specific needs or circumstances.

> **The shorter the intervals for RPO and RTO, the more an organization should expect to spend to support its disaster recovery and business continuity plans.**

> **Considering these options, it's easy to understand that most SMBs will require some combination of these solutions.**

Considering these options, it's easy to understand that most SMBs will require some combination of these solutions. Such combinations help match specific RTO/RPO requirements for specific applications and their data, with custom configured systems and solutions that meet those requirements.

So whatever an SMB's business continuity and disaster recovery needs might be, HPE has all the bases covered.

Visit HPE's Business Continuity and its Data Protection Solutions pages to see the full range of business continuity/disaster recovery and other related solutions available to SMBs.