SCALE COMPUTING

An Essential Guide to Backup Disaster Recovery and Preparation from an IT Perspective

Business Resilience Best Practices

White Paper

Table of Contents

Introduction

Businesses and organizations have long been aware of the need for data backup and disaster recovery planning as part of compliance with industry regulations and as best practices. As the digital age continues to evolve the way products and services are consumed, organizations must take a more comprehensive approach to ensure their business can continue during potentially disruptive events.

This paper is intended to guide organizations of all kinds and sizes on how to best prepare for business resilience from an information technology perspective. These best practices highlight current technologies that help prepare organizations to handle future threats.

Business Resilience Defined

A simple definition

A quick internet search will likely result in many definitions of business resilience. In the past, we have all thought of business resilience by other names, such as risk management, emergency management, business continuity, disaster recovery planning, and risk mitigation. Business resilience looks at a broader approach to planning, focusing on continuing organizational success when issues threaten current processes.

In this paper, we'll start with a simple definition and then expand on that definition by elaborating on different parts of it. The simple definition we'll start with is:

Business resilience is a combination of proactive and reactive planning for an organization to mitigate and adapt quickly and effectively to threats and disruptions affecting the operation and success of the organization.

Which types of organizations need business resilience?

Every organization benefits from business resilience. Despite what may be inferred from the name, business resilience is for more than just commercial businesses. Governmental organizations, from local to federal, are expected or required to have the ability to continue providing services despite disruptive events, especially when those services may be emergency-related. Even non-profit organizations such as churches and other charities offer services that are relied on in many communities, and these organizations benefit from business resilience to ensure those services continue.

Which business operations are critical to organizational success?

The answer depends entirely on the type of organization and, in some cases, the level of disruption. For a hospital, most critical operations need to continue in some capacity. For police and fire departments, the ability to respond to emergencies ensures community safety. For a small commercial business, employees must be kept safe, and internal and external communications keep employees and customers updated until business services can resume.

What are the disruptive events business resilience addresses?

Organizations risk disruption from events of all sizes, ranging from global events like large natural disasters to very localized events, like the accidental deletion of critical system files or power outages. Current events have demonstrated that many organizations must be adequately prepared for work-from-home or to handle increased cyberattacks like ransomware.

Some organizations have specific planning needs toward typical regional natural disasters such as earthquakes, floods, or hurricanes based on their office location. All organizations must generally prepare for almost any type of potential threat. Planning should consider the severity of different threat levels. For example, planning the steps needed to deal with fire in a building differs from those necessary for a ransomware attack or a server failure.

What are the elements of business resilience?

Business resilience extends well beyond the IT department to include elements such as brand protection, building evacuation plans, ensuring the organization has adequate insurance policies, setting aside cash reserves for emergency funds, and having communication plans for employees and customers to connect and get updates.

Within the IT department, there are more specific business resilience planning elements to protect the data and systems that critical business operations run on.

In this paper, we'll discuss the IT department business resilience elements/responsibilities in three categories:

Data Center Availability - Ensuring the availability of the core business services that run in the data center.
Workstation Availability - Ensuring the ability of employees to access the business systems and applications they need to do their work.
Cyber Security - Ensuring the protection, mitigation, and recovery from cyberattacks.

Business Resilience in the Data Center

The data center is the heart of IT operations. Without the data center, data and applications become disconnected between departments, teams, and individuals. The organization struggles when the data center cannot connect all the organization's parts fluidly through the flow of data. There are many aspects of data center resilience to consider.

Backup

The oldest and most prominent element of business resilience is backing up data. Data backup has been and will likely continue to be one of the most basic and necessary elements of business resilience. Next to its employees, an organization's data might be its most valuable asset. That data might include critical intellectual property or operational data that is not easily or inexpensively replaced.

However, one side of data backup that often needs more planning is properly testing those data backups. Testing allows an organization to ensure that the data backup and recovery process for that data aligns with the recovery time objectives required should recovery be necessary. Without testing data backups, organizations take a big risk when recovering from data loss.

Disaster Recovery (DR)

Beyond backups, organizations should have more comprehensive disaster recovery plans to bring critical business systems back online as quickly as possible. These plans often involve having a secondary site that can take over for the primary data center. That secondary site may be a secondary facility within the organization, a co-located site with a provider, or in the cloud.

The key attributes of the DR site are that it is geographically distant, has sufficient computing resources to stand in for critical workloads, and can be sufficiently managed by IT staff or the hosting provider. The geographic distance is necessary to mitigate the secondary site from being caught up in the same disaster as the primary data center. This is especially important for wide-ranging regional disasters such as hurricanes, floods, and earthquakes.

The data at the DR site must be kept up to date for the DR site to stand in for the data center effectively. This is generally achieved using data replication over a WAN or other dedicated network between the sites. The most common type of replication for disaster recovery is differential snapshot-based replication of entire virtual machines that can be quickly failed over at the DR site within minutes.

After a disaster has occurred and a DR site becomes a stand-in for the data center, networking connectivity must be restored for users. This is generally accomplished with IP address redirects or gateways so that users can keep their settings to reconnect with the stand-in site applications and services. Then finally, once the primary data center has been recovered and data restored, users can be redirected back to the primary data center

.

High Availability

Disaster recovery is a reactive and important measure, especially when an organization experiences an entire site outage at the primary data center. However, failing over to a DR site is only sometimes necessary, particularly if only a single server or application fails. High availability is a preferred solution for more localized disruptions within the data center.

High availability is accomplished by having secondary, redundant systems that can quickly take over for a failed system. This is usually achieved using high availability clustering, where two or more servers are clustered together. Any server node in the cluster can take over for any other node if it fails. This failover within the cluster can happen automatically, happening so quickly that users may hardly notice the interruption. High availability clusters can almost eliminate system downtime, reducing it from hours or days to only a few minutes.

Some high-availability clusters can be geographically dispersed across sites; however, the high-speed networking requirements for such "stretch" clusters to allow operations across sites effectively can easily make them cost-prohibitive to many organizations. Failing over between sites generally falls into the definition of disaster recovery rather than true high availability

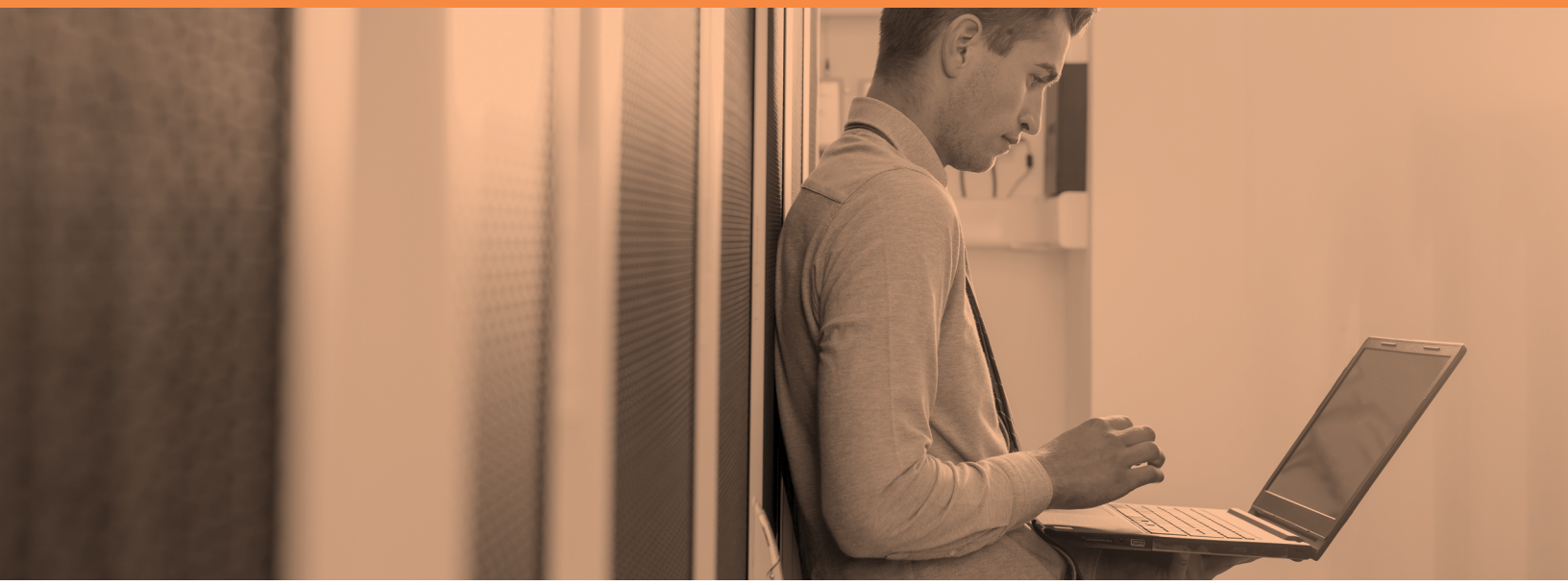
.

Planning and Testing

For successful business resilience, planning is vital. Simply having all the components of a business resilience solution is never enough. Specific documented plans on taking the necessary steps to ensure business resilience can mean the difference between success and failure.

Not all types of emergencies or disasters warrant the same kind of response, so planning should include documenting the steps for various emergencies and disasters that may be likely or possible. These documented plans are sometimes referred to as runbooks, as they outline the steps needed to execute the plan successfully. Not only do these plans or runbooks typically involve a long list of steps, but they may involve the actions of numerous individuals. As such, all related staff should be trained adequately on these steps.

As mentioned earlier regarding data backups, testing is essential to ensuring successful business resilience. A plan is only as good as the ability of the staff to execute it. Periodically updating and testing the plans are essential to having confidence that recovery will be successful when needed. Best practices include executing real-time tests with systems or process updates, with new staffing hires, or at minimum once or twice a year.



Personnel, Training, and Expertise

When an organization faces an outage, disruption, or disaster, business resilience plan will only succeed with the assistance of the IT staff and their unique skills. Depending on the size of an organization, the IT staff may range from a single IT generalist to a large team or teams of IT specialists. An organization's size will also determine the complexity of the IT systems and business resilience plans.

The more complex the IT systems architecture, the more challenging the business resilience planning and execution will be. One of the more challenging factors in business resilience for a complex system is making sure the staff member with the required expertise to execute the plans will be available in the time of need. To accomplish this, some levels of cross-training may be required. The less expertise needed to execute the business resilience plans, the easier it will be to allow less experienced staff members to oversee plan execution.

Some organizations may outsource some or even all of their IT operations to managed service providers or other specialized consultants. These organizations must ensure that their agreements with service providers or consultants match their organizational goals for business resilience. Further, these organizations should ensure that business resilience plans can be successfully tested and executed when needed. It is also essential to determine how regional disasters may impact service levels from these service providers and consultants if they are also affected by the disaster.

.

Data Security

The physical security of systems can be essential. To comply with regulations, organizations must store and protect sensitive data and the intellectual property and trade secrets needed to be competitive. Organizations can't afford to allow employees to wander into the data center with the possibility of walking out with a stolen or copied hard drive, for example. Physically restricting access to the primary computing systems can prevent theft and vandalism of data.

Network and application security is also important. Employees and customers should only be able to access limited data sets they need to perform their work or do business. A user who accesses data outside their everyday job responsibilities may need to be made aware of the sensitive nature of the data, and they may handle it inappropriately. Users with access to data that they do not require access to may also run the risk of deleting such data. Keeping tight restrictions on data can be vital to ensure data breaches, data leaks, or data deletions do not disrupt business

.

The Cloud

Nearly all organizations have some level of cloud services in play. Some may have moved most or all of their data centers to the cloud. Some may only use select cloud-based applications such as messaging, web services, or office applications. The cloud and cloud applications are presumed to have many inherent redundancies and high availability. They should never fail, but even the most prominent cloud services fail occasionally.

Failure of cloud services and the resulting disruption can be particularly frustrating because an organization relying on those services is at the mercy of the cloud service provider to correct the issue. Part of business resilience planning should involve assessing those applications, data, and other services residing in the cloud to determine their criticality and whether the cloud platform they are running on matches the organization's business resilience goals.

Cloud applications and services deemed critical may require redundancies on-premises to ensure they will be available during a cloud or internet outage. Additionally, cloud applications and services should be integrated into business resilience testing because internet outages can disrupt cloud connectivity.

Business Resilience for Workstations

While the data center is the heart of the IT operations, workstations are the hands. Workstations connect users to the data and applications they need to do their work. When users cannot access the data and applications they need, the organization's business can slow dramatically or stop altogether. Business resilience for workstations can take many forms, and it is important to consider which matches an organization's needs more completely.

Workstations are any device employees use to run applications and access the needed data. These can include desktop computers, laptops, tablets, mobile phones, or other specialized digital devices.

Working Remotely

While unexpected, forces beyond control can mean pivoting quickly. Many organizations have transitioned user workstations to work from home. Traditional thinking of providing employees with a desktop computer at their office desks does not allow for a quick move to remote working. While some organizations in regions with frequent natural disasters might have already incorporated work-from-home strategies into their business resilience planning, the pandemic established that nearly all organizations need to plan for it to some extent.

One solution that enabled organizations to transition quickly to remote work was virtual desktop infrastructure (VDI). A virtual desktop is a virtual machine running on a hypervisor in the data center or on a server or appliance managed by IT that allows users to connect remotely from a workstation device. Modern VDI solutions typically support remote connections from various devices, and virtual desktop sessions can often be connected from workers' personal computers and devices.

Organizations that already had VDI solutions could adapt and allow their employees to work from home much more quickly than traditional workstations. Of course, not all employees can work remotely, but nearly all organizations have some employees who can and should be able to when the need arises with proper planning.

Device Management

How the IT team supports workstations is an important part of business resilience planning. Consider how potential threats and disruptions can disrupt the ability of the IT staff to maintain workstations. If, for example, employees with company-issued laptops must suddenly work remotely for an extended period, how quickly can IT address issues with those remote devices to maintain productivity? How fast can IT roll out necessary security patches, hotfixes, or new applications if so many employees are now remote?

Some sophisticated management tools are on the market to manage and maintain workstations; still, VDI solutions offer some unique advantages, particularly for rolling out new applications, patches, and other system updates. With VDI, IT only needs to update a single master or "golden" image to be delivered to an entire team or department automatically. If a VDI user's workstation session gets corrupted, it can be nearly instantly recovered, regardless of where the connected user resides.

Whether an organization chooses VDI or a more traditional workstation strategy, being able to continue managing workstations effectively is an important goal of business resilience. As the world becomes increasingly digital, the need for workstation connectivity will only continue to increase in importance.

Data Security

Workstation devices pose some security risks to organizations. They connect to an organization's data and applications, so a device getting into the wrong hands is of great concern for a data breach or malicious tampering of data or systems. Users may not always follow security best practices when operating these devices, making workstations a key vulnerability to cyberattacks. And, as workers work from home or other less secure networks, they extend the organization's network out to these less secure networks, increasing vulnerability.

A data breach or cyberattack infiltrating a vulnerable workstation can severely affect an organization. A ransomware attack originating from a user workstation can nearly impair an entire IT system and the business that runs on it. Addressing workstation vulnerabilities involves securing devices with strong authentication mechanisms (especially if they are used in the field) and antivirus protection, and ensuring proper best practices training to avoid data security issues.

In addition to having the right solutions and training, IT administrators should have plans and policies to update workstations with the latest security patches for operating systems and applications. Keeping workstations updated with security patches can be accomplished more efficiently in a centralized data center environment than applying them individually across each distributed user workstation.

Cyber Security

While cybersecurity measures have become more sophisticated, so have cybercriminal activities - technologically and tactically. Business resilience demands a combination of proactive and reactive measures.

Proactive Security Measures

This paper has already discussed proactive physical security measures concerning access to the data center, restrictions on data access for system users, and security of workstations. Yet additional steps can be taken to harden an organization's IT systems and to counteract security threats as they occur.

Firewalls and gateways can restrict external access and have been used for decades to harden computing networks by reducing the surface area of attack. These are still important to monitor and review for vulnerabilities. Antivirus scanners are also important to examine data, especially incoming, for various cyberattacks embedded in files. Security solutions can also scan for suspicious activity occurring on existing files and detect various types of worms or ransomware attacks that look to infect multiple files. Some security solutions detect and stop attacks and actively roll back the damage done by these attacks in real time.

All IT systems and security solutions will require timely updates and patching to maintain good security. Security scanners are only as good as the threats they are programmed to detect. Application vendors often respond quickly to new threats with security patches but those patches need to be applied to IT systems before the vulnerability is fixed. Having a system in place that is aware of new updates combined with the ability to roll out those updates quickly is an important part of business resilience.

Training is also a key part of proactive security measures. Users opening suspicious file attachments on emails is still a huge security concern for organizations. Proper training can significantly reduce the likelihood of phishing attacks targeting users. The more aware both users and IT staff are of the potential threats, the more likely they are to prevent them in the first place.

Reactive Recovery from Cyber Attacks

Despite its best efforts to avoid it, it's no longer a question of if a cyberattack will target an organization, but rather when. When an attack occurs, whether it is a data breach or ransomware, it is vital to have a plan to handle that occurrence. The faster an organization can respond, the less damage it may face.

Backups and system snapshots can often be used to recover from attacks. If an organization can identify when an attack occurred, they can often recover systems back to a point before the attack to restore data and functioning systems. As cyberattacks become more sophisticated, they can lie dormant for weeks or months before becoming active. In these cases, reverting back to a few hours or even days before does not fully solve the problem. This is where active security solutions that can detect attacks as they are happening and stop them become more important.

As with proactive measures, training is important for reactive measures as well. Organizations should train employees on what they should be doing in the event of different cyberattacks. Waiting to communicate these instructions until after the attack may be too late. For example, suppose files become infected, and an organization becomes aware of the attack. In that case, users should know not to continue distributing files across various systems, which can spread the infection further. While proper training, backups, and snapshots are good to have for a number of reasons, organizations must always consider security measures beyond the reactive.

Scale Computing Business Resilience Solutions

Organizations of all sizes may benefit from innovative Scale Computing solutions to address their business resilience needs.

Reliable, Self-healing, Highly Available Architecture

Scale Computing Platform was designed and built for business resilience.

With native high-availability clustering, built-in disaster recovery features, and intelligent, automated self-healing capabilities, SC//Platform is so reliable it practically eliminates downtime. It can be deployed quickly, managed easily, and scaled out seamlessly and flexibly.

With HCI, high availability and disaster recovery can be built directly into the system to keep critical production resources online without interruption. SC//HyperCore is highly available by design, and replication and disaster recovery are simple and easy-to-manage native features.

Ransomware Protection

Scale Computing has partnered with Acronis to provide active ransomware protection features and a full complement of advanced data protection, backup and recovery capabilities. Acronis actively monitors virtual machines, detects ransomware attacks as they are occurring, and automatically rolls back to safe state in real-time.

Summary

Every organization should make business resilience an essential part of their operations in an increasingly digital world with ever-present threats that can disrupt business operations. Unprepared organizations face existential threats when they are not prepared to face potential challenges that may disrupt their operations for hours, days, or even weeks or months.

Business resilience combines proactive and reactive plans that make an organization viable through a wide range of challenges, disruptions, and disasters. It can prevent small disruptions from becoming big ones and can prevent catastrophic disasters from becoming fatal to the organization.

Scale Computing experts are ready to help with business resilience solutions for organizations of all sizes, across all industries. Our customer success stories attest to how our solutions have eased the burdens of management and costs by delivering simple, reliable, flexible, and highly available solutions for modern IT infrastructure. To speak with a specialist about how we can support your business resilience needs, please email us at info@scalecomputing.com.

Additional Resources

For more information about topics related to business resilience please review these white papers:

- Disaster Recovery Strategies with Scale Computing White Paper
- BCDR Planning Guide
- Introduction to Virtual Desktop Infrastructure White Paper
- Information Security with SC//Platform
- IT Infrastructure Risk Management White Paper

For more information on Scale Computing solutions and services, visit www.scalecomputing.com/resources.

Corporate Headquarters
525 S. Meridian Street - 3E
Indianapolis, IN 46225
P. +1 317-856-9959
scalecomputing.com

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
Pays-Bas
emea@scalecomputing.com